А. В. ГЛАДКИЙ

# МАТЕМАТИЧЕСКАЯ ЛОГИКА

МОСКВА 1998

ББК 22.12
Г52

Гладкий А.В.
Г52 Математическая логика. М.: Российск. гос. гуманит. ун-т, 1998. 479 с.
ISBN 5—7281—0025—2

Книга представляет собой учебное пособие по математической логике, особенностями которого являются соединение строгости и доступности изложения, достигаемое благодаря отчетливому выделению основных идей и тщательной проработке деталей, и повышенное внимание к гуманитарным аспектам предмета — в частности, к его связям с естественным языком и лингвистикой. Излагаются семантика и синтаксис логики предложений и логики предикатов, элементы теории алгоритмов, формальная арифметика (включая теорему Гёделя о неполноте арифметики). Центральное место занимает теория доказательства, излагаемая на основе исчисления естественного вывода. Книга содержит много задач и упражнений.

Для студентов математических и физико-математических факультетов, факультетов и отделений информатики, теоретической и прикладной лингвистики, искусственного интеллекта.

Г $\frac{1602020000-008}{ОТ8(03)-98}$ 92—98

ББК 22.12

ISBN 5—7281—0025—2

© А.В. Гладкий, 1998
© Российский государственный гуманитарный университет, 1998

# ПРЕДИСЛОВИЕ

Эта книга — учебное пособие по математической логике для университетов и педагогических институтов. Она может использоваться и в других высших учебных заведениях, где изучается эта дисциплина.

Начав в 1972 г. читать математическую логику в качестве обязательного курса, я увидел, что хотя к тому времени на русском языке были уже прекрасные книги [Гильберт — Аккерман 1947][1], [Клини 1957], [Новиков 1959], [Чёрч 1960], [Гудстейн 1971], [Мендельсон 1971], ни одна из них не могла служить пособием по этому курсу, потому что в математической логике, науке сравнительно молодой, жанр учебника еще не отделился от жанра научной монографии[2]. И я решил попытаться написать более доступный учебник. Однако, начав работать над ним в 1973 г., я только к 1988 г. сумел его закончить. Как раз тогда начались времена, крайне неблагоприятные для издания научной литературы, и прошло еще восемь лет, прежде чем появилась возможность издать книгу.

Стремясь к доступности, я тем не менее не хотел достигать ее за счет упрощения и отказа от строгости, но старался все излагать ясно и разъяснять принципиальные и трудные моменты. Сейчас считается хорошим тоном избегать подробных объяснений в серьезных математических книгах, в том числе и в учебниках; распространилось мнение, что «умный и так поймет, а дураку все равно не объяснишь». Это затрудняет изучение математики многим способным людям, не имеющим специальной склонности к разгадыванию ребусов. Разумеется, вредна и другая крайность — «разжевывание» всех деталей, отучающее от самостоятельного мышления; здесь нужно уметь находить золотую середину. Но на что ни в каких случаях не следовало бы жалеть усилий, так это на разъяснение содержательного смысла

---

[1] Фамилия и год в квадратных скобках означают ссылку на помещенный в конце книги список литературы.

[2] Появившиеся позднее книги [Клини 1975], [Шенфилд 1975], [Ершов — Палюти 1979] — также не столько учебники, сколько монографии. Книга [Колмогоров — Драгалин 1982, 1984] (изданная двумя выпусками) — уже настоящий учебник, но она содержит не весь необходимый материал, и изложение в ней в ряде случаев конспективное. Еще менее полна отличающаяся оригинальностью изложения книга [Марков 1984].

формальных конструкций — а между тем он очень часто остается в тени. В математической логике такие разъяснения особенно необходимы, и я старался уделять им как можно больше внимания. Я стремился также подчеркивать общекультурный аспект математической логики — в частности, останавливаться на ее связях с естественным языком.

Мне трудно судить, в какой мере соблюдена в книге «золотая середина». Безусловно, для некоторых студентов доказательства — или часть их — окажутся чересчур детальными. Но в таких случаях читатель может провести рассуждения самостоятельно, обращаясь к тексту лишь для самоконтроля. Вообще всегда очень полезно, прочтя формулировку утверждения, отложить книгу в сторону, подумать, как можно было бы его доказать, и только потом разбирать приведенное в книге доказательство. Необходимо также решать задачи. (Содержащиеся в основном тексте желательно решать все, помещенные в конце глав — можно выборочно.) По трудности задачи весьма разнообразны — от простых упражнений до восстановления доказательств далеко не тривиальных теорем. (Трудные задачи даются только в конце глав.) Те, кому этих задач будет мало, могут обратиться к задачнику [Лавров — Максимова 1975]. Много задач по логике предложений с указаниями и решениями имеется в книге [Гиндикин 1972].

В отборе материала я в основном следовал традиции; однако ради удобства читателя добавлены некоторые простые разделы, обычно не включаемые в курс математической логики, а именно: 1) Книга начинается главой, посвященной множествам, отношениям и функциям. Это делает ее первую половину (главы 1—4) доступной для людей с математической подготовкой в объеме школьного курса. (Формально это верно и для второй половины, но фактически там требуется более высокий уровень математической культуры.) Более подготовленный читатель может пропустить или бегло просмотреть эту главу. 2) В книгу включены три приложения, посвященные отношениям эквивалентности и порядка, понятию мощности множества и математической индукции (последнее приложение содержит также элементы пеановской арифметики, знакомство с которыми необходимо для понимания главы 8). Читатель, незнакомый или плохо знакомый с этими вопросами, может обратиться к приложениям либо сразу после чтения главы 2, либо тогда, когда почувствует необходимость. Кроме того, в § 6.5 излагаются основы аристотелевской силлогистики.

В главах, посвященных логическим исчислениям, за основу взято генценовское исчисление естественного вывода, потому что оно лучше всего отражает процесс математического рассуждения. Рассматриваются и другие исчисления, но менее подробно.

Я благодарен коллегам и слушателям моих курсов, без постоянного общения с которыми книга не могла бы быть написана. Особую благодарность я хочу выразить В. А. Янкову, взявшему на себя тяжелый труд научного редактирования и сделавшему много важных замечаний.

Работая над книгой, я думал о моем учителе Петре Сергеевиче Новикове. Никто не сделал больше, чем он, для развития математической логики в нашей стране. Он был не только крупнейшим ученым, но и замечательным педагогом; все, кому посчастливилось у него учиться, испытали необыкновенное обаяние его личности. Его памяти я посвящаю эту книгу.

*А. Гладкий*
Май 1996 г.

# ВВЕДЕНИЕ

**1.** Если мы попробуем задуматься, каким образом люди получают знания о мире, нетрудно будет заметить, что для этого есть два способа: непосредственное наблюдение и получение новых знаний из уже имеющихся. В реальном процессе познания эти способы сплошь и рядом комбинируются, но по крайней мере второй из них часто используется и в чистом виде[1]. Нередко при этом новое знание возникает таким образом, что человек не может дать себе отчет, как это произошло: тогда говорят, что знание получено благодаря «догадке», или и н т у и ц и и[2]. В других случаях человек сознательно анализирует имеющиеся у него знания и делает из них выводы; это называется р а с с у ж д е н и е м. Во многих случаях (хотя и не всегда) знания, полученные рассуждением, более достоверны; поэтому рассуждения часто используются для проверки интуиции. Так, в частности, поступают обычно при решении математических задач: сначала угадывают решение — или его основную идею,— а потом пытаются обосновать догадку строгим рассуждением (или вычислением, которое есть, в сущности, «механизированное» рассуждение); при этом случается, что рассуждение не подтверждает догадку или даже опровергает ее[3]. Механизм интуиции недоступен прямому наблюдению, и изучать его можно лишь косвенными методами, разрабатываемыми психологией. Материал для изучения строения рассуждений добывается проще, так как они производятся «на свету» и выражаются с помощью слов (или заменяющих их знаков). Тем не менее исследование механизма рассуждения — чрезвычайно сложная задача, занимающая ученых уже третье тысячелетие. Наука, имеющая своим предметом изучение рассуждений и выявление закономерностей, которым они подчинены, называется л о г и к о й (греч. λογική, от λόγος — «слово, речь, суждение, довод»).

В логике принято делить рассуждения на два типа, не являющиеся, впрочем, взаимоисключающими — индуктивные и дедуктивные. И н д у к т и в н ы м и (от лат. *inducto* — «наведение»)

---

[1] Вряд ли можно сказать то же о первом: как правило, результат наблюдения становится знанием только после взаимодействия со «старыми» знаниями.

[2] От лат. *intueor* — «внимательно смотрю».

[3] В естественных науках для проверки интуиции чаще используется не рассуждение, а наблюдение или его усложненная разновидность — эксперимент.

называются рассуждения, с помощью которых из знаний об отдельных фактах получаются знания об общих закономерностях или из знаний о менее общих закономерностях — знания о более общих. Дедуктивные рассуждения (от лат. *deductio* — «выведение») — это рассуждения, состоящие в получении из имеющихся знаний нового знания по некоторым точным правилам, причем вывод является бесспорным: если исходные знания достоверны, то столь же достоверно получаемое из них новое знание. Например, если мы, зная, что два или три члена большой семьи музыкально одарены, делаем отсюда вывод, что должны быть одарены и остальные — это индуктивное рассуждение; а когда я, узнав, что какого-то человека близкие друзья называют Колей, а отца его зовут Иваном Петровичем, заключаю, что, обращаясь к нему по имени и отчеству, его нужно называть Николаем Ивановичем — я рассуждаю дедуктивно. Индуктивное рассуждение обычно не позволяет делать вывод с полной достоверностью, а только с большей или меньшей степенью правдоподобия. Однако если те единичные факты или частные случаи, из знаний о которых мы выводим общую закономерность, охватывают в совокупности все возможности (так называемая полная индукция), то вывод является абсолютно достоверным; такое рассуждение можно считать индуктивным и дедуктивным одновременно.

В науке, как и в повседневной жизни, используются рассуждения обоих типов, но сравнительная важность тех и других в разных науках различна. Науки, в которых преобладают дедуктивные рассуждения[4], принято называть точными. «Самая точная» в этом смысле наука — математика; в ней дедуктивное рассуждение — единственный способ получения знаний, за которым признается доказательная сила[5]. Закономерности дедуктивных рассуждений по самой своей природе легче поддаются систематическому описанию; поэтому те разделы логики, в которых изучаются эти рассуждения, разработаны значительно полнее и глубже, чем логика индуктивных рассуждений («индуктивная логика»).

Логика тесно связана с философией и возникла одновременно с ней в первом тысячелетии до н. э. Развитие логики на Востоке и на Западе шло разными путями. Западный путь, который привел впоследствии к возникновению математической логики, являющейся предметом этой книги, берет начало в трудах древнегре-

[4] Включая и вычисления (ср. выше).

[5] Так называемая математическая индукция (см. Приложение II) есть чисто дедуктивный способ рассуждения, лишь по форме сходный с индуктивным.

ческих мыслителей[6]. Они разработали учение о понятиях, в которых обобщаются знания об отдельных предметах и явлениях (например, понятие «лошадь» возникает в результате обобщения знаний о конкретных лошадях), суждениях, в которых выражаются знания о связи между понятиями (например, «Всякая лошадь — четвероногое» или «Некоторые параллелограммы — прямоугольники»), и умозаключениях — элементарных рассуждениях, в которых из одного или нескольких суждений, называемых посылками, получается еще одно суждение, называемое заключением, или следствием (например, из посылок «Всякий прямоугольник — параллелограмм» и «Всякий квадрат — прямоугольник» получается заключение «Всякий квадрат — параллелограмм»). Наряду с общими, методологическими вопросами теории рассуждений греческие мыслители уделяли много внимания изучению конкретных форм, в которых протекает рассуждение — тому, что впоследствии стало называться формальной логикой. Создателем формальной логики был Аристотель (Ἀριστοτέλης, 384—322 до н. э.). Он исследовал, в частности, строение простейших умозаключений — так называемых категорических силлогизмов (см. § 6.5); построенная им теория силлогизмов оказала очень большое влияние не только на развитие логики, но, в сущности, и на всю европейскую культуру — хотя бы уже потому, что в течение многих веков знание ее считалось необходимым всякому образованному человеку и было одним из основных средств дисциплинирования ума. В дальнейшем формальной логикой занимались многие ученые древности, средних веков и нового времени; но за две с лишним тысячи лет — до XIX в.— она не вышла сколько-нибудь существенно за пределы круга идей и методов, очерченного в трудах Аристотеля. Новый этап в развитии логики начался тогда, когда некоторые логики и математики стали пользоваться символическими обозначениями для простых логических операций, соответствующих союзам «и», «или», «если» и отрицанию, аналогично используемым в математике символическим обозначениям для арифметических действий. Это дало возможность изображать строение сложных суждений с помощью формул, похожих на выражения элементарной алгебры, и представлять некоторые логические закономерности в виде математических соотношений. Так возникла «алгебра логики», из которой и развилась математическая логика, своеобразная научная дисциплина, являющаяся одновременно частью логики и частью математики — частью логики потому, что изучает строение рассуж-

[6] На Востоке логика с наибольшим успехом развивалась в Индии.

дений, а частью математики потому, что пользуется типично математическими методами. («Старые» разделы логики, в которых математические методы не используются, часто называют сейчас «традиционной логикой».) Впрочем, с математикой математическую логику сближают не только ее методы, но в большой мере и ее предмет, так как она изучает не всякие рассуждения, а только дедуктивные и притом в их наиболее чистом виде, в котором они применяются по преимуществу в математике и довольно редко встречаются за ее пределами. (Иногда математическую логику так и определяют как науку о математических рассуждениях, пользующуюся математическими же методами.) Поэтому развитие математической логики стимулировалось прежде всего стремлением математиков понять природу и структуру методов своей науки. Этому развитию особенно способствовали два обстоятельства: возникновение абстрактного аксиоматического метода, окончательно оформившегося к концу XIX столетия, и открытие примерно в это же время парадоксов теории множеств.

Абстрактный аксиоматический метод отличается от конкретного, использовавшегося еще Евклидом (Εὐκλείδης, III в. до н. э.) тем, что он имеет дело с «вещами» произвольной природы. В книге Евклида «Начала», считавшейся вплоть до прошлого века образцом математической строгости, изучаются свойства поверхностей, линий и точек. Этим объектам даются «определения», которые не являются определениями в смысле современной математики, но помогают представить себе «определяемые» объекты наглядно («точка есть то, что не имеет частей» и т. п.). Основные отношения между точками, линиями и поверхностями — такие, как, например, «точка находится на линии», никак специально не описываются, их смысл считается самоочевидным. В начале книги формулируются некоторые свойства основных объектов и отношений — «аксиомы» и «постулаты»,— принимаемые без доказательства, и далее из аксиом и постулатов выводятся другие свойства этих объектов и отношений — т е о р е м ы. Но при этом фактически используются не только те свойства основных объектов и отношений, которые сформулированы в виде аксиом и постулатов, но и ряд других свойств, не сформулированных явно, но кажущихся очевидными ввиду наших наглядных представлений о точках, линиях и поверхностях. Используются эти «наглядные» свойства, разумеется, также неявно — Евклид просто не замечал, что пользуется ими. В противоположность этому, при современном абстрактном аксиоматическом изложении геометрии или любой другой математической дисциплины конкретная природа основных объектов и отношений не имеет никакого значения, лишь бы выполнялись аксиомы; поэтому исключается неявное использование

в доказательствах «наглядных» свойств объектов и отношений[7]. Тем самым математическое рассуждение приобретает полную строгость, становясь цепочкой умозаключений, в каждом из которых из точно сформулированных посылок получается столь же точно сформулированное следствие с помощью некоторого «логического правила». Однако сами логические правила не имеют еще точных формулировок и остаются интуитивными. Поэтому после появления абстрактного аксиоматического метода естественно возникло стремление дать правилам логического вывода «математически строгие» формулировки. Решение этой задачи облегчалось тем, что для суждений и логических операций уже имелись символические обозначения и существовала практика трактовки логических операций как математических, а в математике был уже накоплен опыт изучения операций самой различной природы. И действительно, в конце XIX и начале XX в. точные формулировки правил дедуктивного вывода были найдены. Системы таких правил получили название *логических исчислений*. Первые логические исчисления по своей формальной структуре были похожи на аксиоматические системы, о которых шла речь выше, отличаясь от них лишь тем, что не только аксиомы, но и правила вывода формулировались в явном виде. Такие логические системы аксиом находят широкое применение и сейчас.

Другим важным фактором, способствовавшим развитию математической логики, было, как уже говорилось, открытие парадоксов теории множеств. На этих и других логических парадоксах, т. е. рассуждениях, совершенно справедливых с интуитивной точки зрения, но приводящих тем не менее к противоречиям[8], стоит остано-

---

[7] Может возникнуть вопрос: а разве невозможно, чтобы математик, думая, что полностью отвлекся от конкретных свойств объектов и отношений, на самом деле все-таки «держал их в голове» и не замечал, как пользуется ими? В принципе это, конечно, не исключено, но весьма маловероятно из-за того, что в современных аксиоматических системах конкретные объекты и отношения, удовлетворяющие аксиомам, можно, как правило, выбирать по-разному. (Например, в системе геометрии можно понимать под точками упорядоченные тройки действительных чисел, под плоскостями — линейные уравнения с тремя неизвестными и под прямыми — системы двух таких уравнений.)

[8] Это определение логического парадокса взято из книги [Карри 1969] (с. 20). Вообще в русском языке слово «парадокс», происходящее от греческого παράδοξος — «противоречащий устоявшемуся мнению, необычный, странный» (δόξα — «мнение, представление», παρα- — приставка, имеющая, в частности, значение отступления, отклонения), означает суждение, противоречащее общепринятым мнениям. Логические парадоксы иногда называют также антиномиями (от греч. ἀντινομία — «противоречие в законе»; νόμος — «закон», ἀντι- — приставка со значением противоположности).

виться подробнее — тем более, что знакомство с ними будет нам полезно в дальнейшем. (Впрочем, читатель, которому чтение следующих абзацев покажется трудным, может отложить ознакомление с парадоксами и вернуться к ним перед чтением § 8.4.)

1) Самый старый и самый известный из логических парадоксов — *парадокс лжеца*. Полулегендарному поэту-прорицателю Эпимениду (Ἐπιμενίδης), жившему, по преданию, на Крите в VI в. до н. э., приписывается изречение «Все критяне лжецы». Такое высказывание в устах критянина звучит странно, потому что он обвиняет во лжи также и самого себя. Правда, здесь нет еще настоящего противоречия: даже если считать, что лжец никогда не говорит правду, мы можем, услышав от критянина, что все критяне лжецы, заключить отсюда только, что это высказывание ложно — поскольку, если бы оно было истинным, это означало бы, что всякое высказывание всякого критянина ложно, в том числе и оно само. Но можно видоизменить эту ситуацию так, чтобы получился настоящий парадокс: как заметил еще в IV в. до н. э. Эвбулид (Εὐβουλίδης), если кто-либо говорит: «Предложение, которое я сейчас произношу, ложно», то из истинности этого предложения следует, что оно ложно, а из ложности — что оно не ложно, т. е. истинно. Это и есть парадокс лжеца.

Для дальнейшего полезно заметить, что парадокс лжеца можно получить, не пользуясь сложным по смысловому строению словом «сейчас»[9]. Пусть выбраны моменты времени $t_1$, $t_2$, $t$, такие, что $t_1 < t < t_2$, и пусть в момент $t$ некий человек — которого мы будем называть по-прежнему «критянином» — говорит: «Всякое предложение, которое я произношу между моментами $t_1$ и $t_2$, ложно», и больше он между $t_1$ и $t_2$ не говорит ничего. (Для простоты мы считаем произнесение предложения «моментальным» актом.) Это предложение не может быть ни истинным, ни ложным: из его истинности по самому его смыслу следовала бы его ложность, а если бы оно было ложно, т. е. не всякое предложение, произнесенное критянином между $t_1$ и $t_2$, было бы ложным, то, поскольку это самое предложение — единственное, которое он произнес в данный промежуток времени, оно было бы истинно.

[9] Сложность его состоит в том, что оно обозначает не какой-то определенный момент времени, а тот, в который произносится содержащая его фраза — подобно тому, как слова «я» и «ты» обозначают говорящего и того, к кому он обращается. Чтобы убедиться, что такие слова сложнее по смыслу, чем слова, обозначающие конкретные моменты времени или конкретных людей, достаточно вспомнить, что детям, как правило, бывает много труднее научиться употреблять местоимения, чем существительные.

2) *Парадокс Кантора.* Пусть $M$ — множество всех множеств и $M'$ — множество всех подмножеств $M$. Из теории множеств известно, что мощность множества всех подмножеств произвольного множества больше мощности самого этого миожества[10]. Поэтому мощность $M'$ больше мощности $M$. Но всякое подмножество $M$ также есть множество, так что $M' \subset M$ и, следовательно, мощиость $M'$ не превосходит мощности $M$.

3) *Парадокс Рассела.* Назовем множество самосодержащим, если оно является своим собственным элементом (пример — множество всех множеств). Пусть $R$ — множество всех несамосодержащих множеств. Тогда, если $R$ — самосодержащее множество, это значит, что $R \in R$, а так как $R$ по определению состоит из несамосодержащих множеств, то и $R$ — несамосодержащее; если же $R$ — несамосодержащее множество, это значит, что $R \notin R$, а так как $R$ по определению содержит в с е несамосодержащие множества, то $R$ — самосодержащее.

Заметим, что парадокс Рассела можно сформулировать, пользуясь вместо понятия множества понятием свойства. Именно: некоторые свойства справедливы в применении к самим себе (иначе: «обладают сами собой»); например, свойство «быть абстрактным» само абстрактно. Назвав такие свойства «самообладающими», мы можем, рассуждая точно так же, как выше (читателю рекомендуется провести это рассуждение), установить, что свойство «быть несамообладающим» не может быть ни самообладающим, ни несамообладающим.

4) *Парадокс Берри* (G.G. Berry). Некоторые словосочетания русского языка служат названиями конкретных натуральных чисел. (Например, число 23 можно назвать с помощью словосочетаний «число, на единицу меньшее числа, вдвое большего двенадцати», «наименьшее простое число, большее двадцати» и т. д.) Очевидно, число натуральных чисел, которые можно назвать с помощью словосочетаний, содержащих менее 60 слогов, конечно. Поэтому словосочетание «наименьшее натуральное число, которое нельзя назвать с помощью словосочетания русского языка, содержащего менее шестидесяти слогов» называет некоторое натуральное число. Но само это словосочетание содержит всего пятьдесят один слог!

5) *Парадокс Ришара* (Jules Richard, 1862—1956). Некоторые словосочетания русского языка служат определениями функций нату-

[10] См. теорему 18 в Приложении II к этой книге.

рального аргумента, принимающих натуральные значения. (Например, «сумма делителей данного числа», «число, на единицу большее числа, вдвое большего, чем данное число» и т. п.) Все такие словосочетания можно занумеровать натуральными числами, расположив их так, как располагают слова в словарях, и приписав тому словосочетанию, которое окажется первым, номер 1, тому, которое окажется вторым, номер 2 и т. д. Функцию, определяемую словосочетанием, имеющим номер $n$, будем обозначать $f_n$. Рассмотрим теперь словосочетание «число, на единицу большее значения функции, определяемой словосочетанием, номером которого служит данное число, при значении аргумента, равном данному числу». Это словосочетание определяет некоторую функцию натурального аргумента с натуральными значениями и, следовательно, должно получить некоторый номер $n_0$. По определению функции $f_{n_0}$ имеем $f_{n_0}(n) = f_n(n) + 1$ для любого $n$. Но отсюда следует, в частности, что $f_{n_0}(n_0) = f_{n_0}(n_0) + 1$.

Когда обнаружилось, что математические рассуждения, вполне согласующиеся, по-видимому, с общепринятыми нормами, могут приводить к противоречиям, это было воспринято многими математиками как кризис, ставящий под сомнение надежность методов математики, всегда считавшейся достовернейшей из наук. Правда, все парадоксы связаны с «экзотическими» объектами, определения которых содержат явное или неявное упоминание о них самих: содержанием предложения, приводящего к парадоксу лжеца, является утверждение о его собственной ложности; множество всех множеств состоит из элементов, среди которых имеется, в частности, оно само, и так же обстоит дело с любым самосодержащим множеством; в словосочетании, которое служит именем числа, дающего парадокс Берри, фактически идет речь о множестве, содержащем это число в качестве элемента; функция, фигурирующая в парадоксе Ришара, определяется через множество всех функций натурального аргумента с натуральными значениями, одним из элементов которого опять-таки является сама эта функция. В конкретных математических дисциплинах, таких, как арифметика, элементарная геометрия, дифференциальное исчисление и т. п., подобные объекты не встречались, и можно было надеяться, что эти дисциплины не окажутся под угрозой. Но чтобы иметь в этом уверенность, нужен был тщательный анализ способов образования математических понятий и способов математических рассуждений, который позволил бы отличать «законные» способы от «незаконных». Возникла новая область научных исследований «на стыке» математики и философии — о с н о в а н и я м а т е м а т и к и; ее главным инструментом стала матема-

тическая логика, развитие которой сделалось, таким образом, насущной задачей. В изучение оснований математики внесли свой вклад многие ученые, в том числе весьма выдающиеся — Г. Фреге, Б. Рассел, Д. Гильберт, Л. Брауэр, Г. Вейль и др. Как всегда бывает в философии и смежных с ней областях, мнения ученых о природе кризиса и путях его преодоления были различны. В философии математики появились разные направления. В частности, л о г и ц и с т ы считали математику частью логики и видели пути преодоления кризиса в уточнении используемых в логике способов образования понятий. Ф о р м а л и с т ы придерживались мнения, что в математике первостепенную важность имеет не содержание, а форма ее конструкций; поэтому они выдвинули программу построения здания математики в виде формальной дедуктивной системы, которая имела бы дело только с конечными (или, как иначе говорят, ф и н и т н ы м и) объектами — например, конечными последовательностями записанных на бумаге значков,— и все действия с этими объектами производились бы чисто механически. При этом они надеялись строго доказать, что в такой системе невозможны противоречия. (О том, к чему привели попытки осуществить эту программу, мы расскажем в гл. 8.) Полностью противоположных взглядов придерживались и н т у и ц и о н и с т ы; они считали, что математика может опираться только на непосредственную интуицию, и поэтому лишь те математические понятия имеют право на существование, которые этой интуиции отвечают. С таких позиций интуиционисты подвергли критике абстракцию актуальной бесконечности, позволяющую обращаться с бесконечными множествами так, как если бы все их элементы были нам в самом деле «даны» и мы могли бы сразу со всеми этими элементами производить какие-то действия. Эта абстракция, на которой основана «классическая» канторова теория множеств (см. гл. 1 и приложение II), представлялась им противоречащей интуиции. Не отвечающими интуиции представлялись им также «чистые» доказательства существования: с их точки зрения существование некоторого объекта можно считать доказанным лишь при условии, что указан способ его построить. (О дальнейших выводах, к которым приводит такая позиция, будет сказано в § 5.2.) Позднее, в середине XX в., выступили к о н с т р у к т и в и с т ы. По их мнению, математика должна заниматься только к о н с т р у к т и в н ы м и объектами, т. е. такими, которые можно строить из некоторых однотипных простых частей по простым правилам (как, например, слова в конечном алфавите). С этих позиций конструктивисты присоединяются к интуиционистской критике абстракции актуальной бесконечности и «чистых» доказательств существования (хотя и расходятся с интуиционистами в ряде принципиальных вопросов). Подробнее останавливаться на различных направлениях в

основаниях математики мы не можем"[11]. Но следует сказать, что все они так или иначе способствовали развитию математической логики и углублению знаний математиков о природе понятий и методов своей науки. Был получен ряд результатов, по большей части неожиданных, которые, хотя и не привели к общему согласию в главных вопросах оснований математики (в том числе в вопросе о происхождении и значении парадоксов), но позволили гораздо лучше, чем раньше, представить себе, что можно и чего нельзя сделать с помощью формальных математических методов. (С наиболее важными из этих результатов мы познакомимся в гл. 8.) Кроме того, сами логические исчисления (см. выше), особенно так называемые исчисления естественного вывода (о них мы расскажем в гл. 5 и 6), дали возможность лучше понять, как устроены математические доказательства. Был подвергнут анализу и другой вид деятельности, составляющий не менее важную часть работы математика, чем доказательство теорем: вычисления и всевозможные формальные выкладки. В результате этого анализа возникла теория алгоритмов, также ставшая составной частью математической логики. Элементам теории алгоритмов будет посвящена гл. 7.

Современная математическая логика включает в себя еще и другие разделы, не получившие отражения в нашей книге. Сюда относится, например, аксиоматическая теория множеств, возникшая в начале XX в. в связи со стремлением уточнить методы теории множеств таким образом, чтобы избежать парадоксов. В аксиоматических системах теории множеств на способы образования множеств накладываются ограничения, делающие невозможными конструкции того типа, которые приводят к парадоксам Кантора и Рассела. Впоследствии с помощью аксиоматических методов удалось получить фундаментальные результаты, относящиеся к решению ряда трудных проблем, возникших в теории множеств в конце прошлого и начале нынешнего столетия, в том числе проблемы континуума (см. конец Приложения II). Еще один обширный раздел математической логики, оставшийся за рамками книги — теория моделей, в которой логические понятия исследуются с помощью методов классической теории множеств и алгебры. (Впрочем, главное в этом разделе понятие модели будет рассмотрено в гл. 6 и 8.) Мы не будем также касаться логических систем,

[11] Довольно подробное изложение различных точек зрения на проблемы основания математики имеется в книге [Френкель — Бар-Хиллел 1966]. Там же есть обширная библиография по этому вопросу. С позицией интуиционизма можно познакомиться по книге [Гейтинг 1965], конструктивизма — по статье [Марков 1962] или дополнениям А.А. Маркова к книге [Гейтинг 1965]. См. также введение к книге [Карри 1969] и посвященную формализации интуиционистской математики книгу [Клини — Весли 1978].

в которых наряду с истинными и ложными суждениями имеются неопределенные (многозначная логика) или возможные и необходимые (модальная логика), или такие, истинность которых зависит от времени (временна́я логика), а также некоторых других разделов математической логики. Все эти разделы нужно изучать по специальным руководствам (например, [Куратовский — Мостовский 1970], [Френкель — Бар-Хиллел 1966], [Манин 1979] — по аксиоматической теории множеств, [Робинсон 1967] — по теории моделей, [Bolc — Borowik 1992] — по многозначной логике, [Фейс 1974], [McArthur 1976] — по модальной логике, [Chellas 1993] — по временной логике). Многие новые понятия и результаты из разных областей математической логики изложены в коллективной монографии [Справочная книга 1982—1983][12].

Говоря о современной математической логике, нельзя не сказать еще о том, что, начиная с конца 30-х годов, идеи и методы математической логики используются и за пределами логики и математики. Имеются две области такого их использования. Во-первых, это конструирование и эксплуатация различных автоматических устройств, в том числе вычислительных машин. В ряде случаев здесь используется технический аппарат математической логики (пример такого использования мы рассмотрим в § 3.5); сверх того, что особенно важно, идеи математической логики — в первую очередь теории алгоритмов, но также и всей науки в целом — и свойственный ей стиль мышления оказали и продолжают оказывать очень большое влияние на те своеобразные области деятельности, содержанием которых является автоматическая переработка информации (информатика) и автоматизация процессов управления (кибернетика)[13]. Можно сказать, что математическая логика — один из главных источников идеологии информатики и кибернетики.

Другой областью использования идей и методов математической логики стала лингвистика (языковедение). В этой науке в первой половине XX в. произошли революционные изменения, связанные

[12] Это именно монография, а не справочник, вопреки ее названию.

[13] Термин «информатика», приблизительно соответствующий английскому Computer Science, стал употребляться у нас сравнительно недавно для обозначения всего, что связано с разработкой принципиальных схем вычислительных машин и их использованием; сюда, в частности, относится так называемое математическое обеспечение ЭВМ — программирование, разработка трансляторов и т. д. Мы назвали информатику и кибернетику «областями деятельности», потому что для них трудно подобрать более узкое родовое понятие; обычно их относят к наукам, но в действительности они представляют собой прежде всего области практической деятельности; если бы слово «ремесло» не получило (к сожалению) несколько пренебрежительного оттенка значения, следовало бы сказать, что это своеобразные ремесла.

с осознанием того факта, что в языке существенна не материальная природа его элементов, а только отношения между ними (по словам крупнейшего лингвиста конца XIX и начала XX в. Фердинанда де Соссюра, «язык есть система чистых отношений»), и эти отношения подчиняются строгим закономерностям, напоминающим математические. Стала очевидной желательность разработки математических методов исследования строения языка. При этом своеобразие языковых явлений делало невозможным, за небольшими исключениями, использование готового математического аппарата, предназначенного для других целей; математический аппарат для лингвистики предстояло создать заново. Это было сделано в 50—60-е годы, когда появилась новая математическая дисциплина — математическая лингвистика, занимающаяся разработкой и изучением математического аппарата для описания естественного языка. Главными источниками идей и методов этой новой науки были математическая логика и абстрактная алгебра. Центральное место в математической лингвистике занимает теория формальных грамматик, родственная теории алгоритмов и имеющая с ней много точек соприкосновения (см. § 7.9, пункт 7). Впрочем, математическая логика влияет на современное языковедение не только через математическую лингвистику, но и непосредственно: основные понятия математической логики — предикаты, кванторы, пропозициональные связки (см. гл. 2) вошли в «повседневный обиход» лингвистов; «математико-логический дух» все больше проникает в лингвистические теории и исследования[14]. Все это, разумеется, не случайно: столь важное значение математической логики для лингвистики обусловлено тем, что язык математики, изучением которого занимается математическая логика, представляет собой фрагмент естественного языка, обработанный и развитый специальным образом с целью обеспечить максимальную точность, но все же сохранивший некоторые очень существенные черты естественного языка. Поэтому, когда лингвистике потребовались точные методы, аппарат математической логики мог служить образцом для их создания.

Следует сказать, что упомянутые области приложения идей и методов математической логики имеют много точек соприкосновения: с одной стороны, формальные грамматики, созданные для исследования строения естественных языков, оказались также и удобным средством анализа языков программирования и дру-

[14] Что касается непосредственного использования для исследования естественного языка сложного математико-логического аппарата, то здесь, кажется, единственным примером остаются появившиеся в 60-х годах так называемые грамматики Монтегю (см. [Монтегю 1985], [Циткин 1985])

гих формальных языков: с другой — в информатике большое место занимают задачи, связанные с переработкой информации, выраженной на естественном языке, и требующие применения точных методов лингвистики.

Представляется вероятным, что со временем сфера внематематических приложений математической логики будет расширяться. (Уже сейчас можно говорить, например, о важности ее идей для некоторых разделов психологии.)

Все сказанное, надо надеяться, в достаточной мере объясняет, почему математическая логика, еще 40—50 лет назад преподававшаяся у нас лишь в немногих учебных заведениях в качестве спецкурса, к настоящему времени стала неотъемлемой составной частью математического образования. Ей должен уделить известные усилия всякий, кто всерьез изучает математику. И эти усилия более чем окупятся, если он почувствует ее красоту и испытает ее дисциплинирующее влияние.

ГЛАВА

1

# МНОЖЕСТВА, ОТНОШЕНИЯ И ФУНКЦИИ

## § 1.1. МНОЖЕСТВА

1. В разных науках и в повседневной жизни постоянно встречаются совокупности тех или иных «предметов». Например, физики имеют дело с большими и малыми совокупностями элементарных частиц, атомов, молекул и т. д., астрономы — с галактиками, состоящими из звезд, биологи — с совокупностями клеток и организмов. В математике также рассматриваются совокупности, состоящие, однако, не из материальных предметов, а из придуманных людьми абстрактных «конструктов»[1] — например, чисел в арифметике, точек, прямых и плоскостей в геометрии. Совокупности различных предметов обладают, само собой, различными свойствами; но есть и такие свойства совокупностей — наиболее общие и универсальные,— которые не зависят от природы составляющих эти совокупности «вещей». Изучением таких свойств занимается особая математическая дисциплина — теория множеств; ввиду своей универсальности она образует базу всей математики, и ее понятия могут считаться самыми важными «словами» математического языка.

2. Основные понятия теории множеств — *множество, элемент* и *принадлежность*.

*Множеством* в математике называют любую совокупность любых «предметов» — или, если угодно, «вещей» или «объектов»,— конкретная природа и свойства которых могут быть какими угодно. Можно говорить, например, о множестве всех коров в некотором стаде; о множестве всех целых положительных чисел; о множестве всех букв русского алфавита; о множестве рек, впадающих в

[1] От лат. *constructum* — «построение».

Волгу ниже Твери и выше Оки; о множества, состоящем из числа 8, Александра Македонского, Луны и слова «множество». «Предметы», из которых состоит множество, называются *его элементами*; о них говорят, что они *принадлежат* данному множеству (или *входят в* него). Если множество и его элементы обозначены какими-либо символами — например, буквами,— то вместо слова «принадлежит» на письме часто используется значок $\in$; таким образом, $a \in A$ означает то же, что «$a$ принадлежит $A$». Вместо «$a$ принадлежит $A$» говорят также «$A$ *содержит* $a$». Итак: предложения «$a$ есть элемент $A$», «$a$ принадлежит $A$» и «$A$ содержит $a$» означают одно и то же (в лингвистике такие предложения называются синонимичными); то же самое означает и символическая запись $a \in A$.

Таким образом, мы познакомились с пятью словами математического языка: «множество», «элемент», «принадлежит», «входит в», «содержит». Слова «принадлежит» и «входит в» означают в точности одно и то же — это синонимы. (Что касается значка $\in$, то это не особое слово, а сокращенная запись слова «принадлежит»,— так же, как «и т. д.» есть сокращенная запись для «и так далее».) «Множество» и «принадлежит»— первоначальные неопределяемые понятия, они лежат в основе всей теории множеств (и всей математики вообще); мы не определяем их через другие математические понятия, а только поясняем их смысл примерами и «приблизительным переводом» на естественный язык. (Такой «приблизительный перевод» мы делаем, говоря, что множество — это «совокупность», «собрание», «коллекция» каких-то «вещей».) Понятия «элемент» и «содержит» уже определяются через «множество» и «принадлежит»: их определения состоят в указании, что предложения «$a$ есть элемент $A$» и «$A$ содержит $a$» означают то же, что «$a$ принадлежит $A$»[2].

Вместо слов «не принадлежит» часто пользуются значком $\notin$ (или $\overline{\in}$). Если, напрнмер, $M$ означает множество всех четных чисел, то $2 \in M$, $-5 \notin M$, $0 \in M$ и т. д.

3. Если каждый элемент множества $A$ является также и элементом множества $B$, то говорят, что множество $A$ есть *подмножество*, или *часть*, множества $B$, или, иначе — что $A$ *содержится в* $B$, или, наконец, что $B$ *содержит* $A$ (все эти предложения, таким образом, синонимичны), а для краткости часто пишут $A \subset B$. Следует обратить внимание, что слово «содержит» может употребляться в двух различных значениях: «содержит в качестве элемента» и «содержит в качестве подмножества». На самом деле то и другое «содержит» —

[2] Точно так же можно было бы иностранцу, знающему, что значит по-русски «купить», но не знающему, что значит «продать», объяснить смысл этого последнего слова, сказав, что «Иван продал корову Петру» означает то же, что «Петр купил корову у Ивана».

разные слова, совпадающие по произношению и написанию, но различающиеся по смыслу так же, как «лук» в смысле «оружие» и в смысле «овощ»; такие слова называются, как известно, о м о н и м а м и.

Если, например, $A_1$ означает множество всех целых чисел, а $A_2$, $A_3$ и т. д.— соответственно множество всех целых чисел, делящихся на 2, на 3 и т. д., то $A_1 \subset A_1$, $A_2 \subset A_1$, $A_3 \subset A_1$, $A_2 \subset A_2$, $A_4 \subset A_2$, $A_6 \subset A_2$ и т. д.; в то же время, например, $A_1 \subset A_2$ неверно.

Важно заметить, что по точному смыслу определения каждое множество является частью (подмножеством) самого себя: ведь утверждение «каждый элемент множества $A$ есть элемент множества $A$» справедливо для любого $A$.

Говорят, что множество $A$ *равно* множеству $B$, или что множества $A$ и $B$ *равны*, если $A$ и $B$ состоят из одних и тех же элементов — иначе говоря, если все элементы $A$ являются элементами $B$ и все элементы $B$ — элементами $A$, т. е. если справедливо $A \subset B$ и $B \subset A$. Поскольку множество, кроме своих элементов, никакой другой «сущности» не имеет, мы можем, установив, что два множества равны, считать, что это на самом деле не два разных множества, а одно и то же. Вместо «$A$ равно $B$» пишут для краткости $A = B$, вместо «$A$ не равно $B$» — $A \neq B$. Ясно, что для любых множеств $A$, $B$, $C$: а) $A = A$; б) если $A = B$, то $B = A$; в) если $A = B$ и $B = C$, то $A = C$.

Если $A \subset B$ и $A \neq B$, говорят, что множество $A$ есть *истинное (или собственное) подмножество* множества $B$ — иначе, *истинная* (или *собственная*) *часть* множества $B$. Так, в приведенном выше примере $A_4$ и $A_6$ — истинные части множества $A_2$.

4. Множества можно задавать различными способами. Самый простой из них — перечислить все элементы множества, т. е. назвать их один за другим («множество, состоящее из чисел $7, -3, 5, 18, \frac{3}{4}$», «множество, состоящее из города Торжка и планет Марса и Юпитера» и т. п.). Это далеко не всегда можно сделать; бывает, однако, что хотя в буквальном смысле перечислить в с е элементы множества нельзя, их можно называть один за другим так, что л ю б о й элемент был бы когда-нибудь назван, если бы мы располагали неограниченным временем. Например: «множество, состоящее из чисел 0, 2, 4, 6 и т. д.» (начиная с нуля, каждый раз прибавляем к очередному числу двойку), «множество, состоящее из чисел 1, 4, 9, 16, 25 и т. д.» (начиная с единицы, каждый раз берем квадрат следующего по порядку натурального числа). В этом случае мы также будем говорить, что множество задано *перечислением* элементов.

Для обозначения множества, заданного «настоящим» перечислением его элементов, пользуются фигурными скобками, внутри которых пишутся обозначения всех элементов множества, разделенные

запятыми: например, $\left\{2, 7, -2, \frac{1}{2}\right\}$ означает множество, состоящее из чисел 2, 7, $-2$ и $\frac{1}{2}$ (это множество можно обозначить также $\left\{7, -2, 2, \frac{1}{2}\right\}$, $\left\{\frac{1}{2}, -2, 2, 7\right\}$ и т. д.). Если выписывать обозначения всех элементов утомительно и в то же время интуитивно ясно, как их перечислить, то такое обозначение обычно сокращают, заменяя знаки некоторых элементов многоточием — например, {1, 2, 3, ..., 100} означает множество всех целых чисел от 1 до 100 включительно. Подобными обозначениями пользуются и для множеств, заданных «бесконечным перечислением»: {0, 2, 4, 6,...}, {1, 4, 9, 16, 25,...} и т. п.

Другой обычный способ задать множество — указать какое-либо *характеристическое свойство* его элементов, т. е. свойство, которым обладают все элементы данного множества и только они («множество всех четных чисел», «множество всех целых положительных чисел, меньших семи», «множество королей Франции, вступивших на престол после 1600 г.»). Для множеств, заданных таким способом, также имеется удобный способ обозначения, сущность которого будет ясна из следующих примеров: $\{2k \mid k = 0, \pm 1, \pm 2, \ldots\}$ означает множество всех четных чисел; $\{3k + 1 \mid k = 0, 1, 2, \ldots\}$ — множество всех целых положительных чисел, дающих при делении на 3 в остатке 1; $\{x \mid x$ — целое, $x < 10\}$ — множество всех целых чисел, меньших 10.

Вместо прямой черты часто пользуются двоеточием, например: $\{2k + 1 : k = 0, \pm 1, \pm 2, \ldots\}$.

Можно задавать множества и другими способами, но рассмотренные нами — наиболее важные.

**Задачи.** 1) Для каждых двух из следующих множеств определить, равны ли они и содержится ли какое-либо из них в другом: множество квадратов целых неотрицательных чисел; {1, 4, 9, 16,...}; $\{(-n)^2 \mid n$ — целое$\}$; множество квадратов всех целых положительных чисел, кроме 1, 2, 3 и 9; $\{k^2 \mid k$ — целое, $k > 20\}$; множество квадратов всех целых чисел, кроме 1, 2, 3 и 9.

2) Тот же вопрос для множеств: $\{n \mid n$ — целое, $-25 < n < 25\}$; {0, 1, 2,..., 25}; {0, 1, 2,..., 24}; $\{0, \pm 1, \pm 2, \ldots \pm 24\}$.

5. Читателю должно быть уже ясно, что во множестве не обязательно должно быть «много» элементов[3] — так же, как чернила не всегда черные. Множество $\{n \mid n$ — целое, $1 < n < 4\} = \{2, 3\}$ состоит всего из двух элементов, множество $\{n \mid n$ — целое, $0 < n < 2\} = \{1\}$ —

[3] Кстати, слово «много» не обозначает никакого конкретного количества, в разных случаях «много» может иметь разный смысл.

из одного. Более того, можно говорить о множестве, не содержащем ни одного элемента; только такой смысл может иметь, например, обозначение $\{n \mid n$ — целое, $0 < n < 1\}$, ничем существенным не отличающееся от только что приводившихся. Множество, не содержащее ни одного элемента, называется *пустым* и обозначается символом $\varnothing$. По точному смыслу определения равенства множеств все пустые множества равны между собой (действительно, все они «состоят из одних и тех же элементов», а именно, «не состоят ни из каких»), или, лучше сказать, существует только одно пустое множество. Таким образом, $\{n \mid n$ — целое, $0 < n < 1\}$ — то же самое, что множество королей Франции, вступивших на престол после 1900 г.

По определению считается, что пустое множество — часть любого множества, т. е. для любого множества $A$ имеет место[4] $\varnothing \subset A$. (Это не противоречит данному выше определению части: утверждение $A \subset B$ может быть опровергнуто только указанием элемента $A$, не являющегося элементом $B$, но при $A = \varnothing$ такого элемента заведомо нет.)

Заметим еще, что множества могут быть, в свою очередь, элементами множеств. Например, $\{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2.3\}, \{1,3\}, \{1,2,3\}\}$ — множество всех подмножеств трехэлементного множества $\{1,2,3\}$; $\{\varnothing\}$ — множество, единственным элементом которого является пустое множество[5]; $\{1, 2, \{1,2\}\}$ — множество, состоящее из чисел 1, 2 и множества $\{1, 2\}$.

Задача. Какие из следующих множеств пусты: множество положительных корней уравнения $x^2 - 5x + 6 = 0$; множество отрицательных корней того же уравнения; множество корней уравнения $\sin x + \cos x = 1$?

6. Если даны два произвольных множества $A$ и $B$, то по ним можно образовать три новых множества, называемых их *объединением*, *пересечением* и *разностью*, следующим образом:

*Объединением* множеств $A$ и $B$ (или: множества $A$ с множеством $B$) называется множество, состоящее из всех элементов $A$ и всех элементов $B$. Объединение $A$ и $B$ обозначается $A \cup B$.

*Пересечением* множеств $A$ и $B$ (или множества $A$ с множеством $B$) называется множество, состоящее из тех элементов $A$, которые являются также и элементами $B$. (Иногда вместо «пересечение» говорят *«общая часть»*.) Пересечение $A$ и $B$ обозначается $A \cap B$.

*Разностью* между множеством $A$ и множеством $B$ называется множество, состоящее из тех элементов $A$, которые не являются элементами $B$. Разность между $A$ и $B$ обозначается $A \setminus B$.

---

[4] «Имеет место» означает то же, что «верно».

[5] Само это множество, очевидно, не пусто!

На рис. 1 множества $A$ и $B$ условно изображены в виде кругов, по-разному заштрихованных. Множество $A \cup B$ будет при этом изображаться всей так или иначе заштрихованной областью, $A \cap B$ — дважды заштрихованной областью, $A \setminus B$ и $B \setminus A$ — областями, несущими штриховку только одного вида.

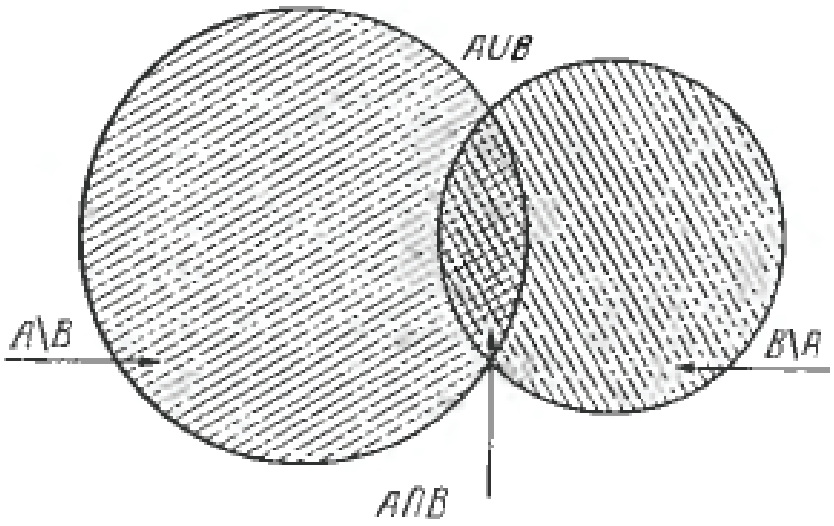



Рис. 1

**Примеры.** 1) Пусть $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 5\}$. Тогда $A \cup B = \{1, 2, 3, 4, 5\}$, $A \cap B = \{2, 3\}$, $A \setminus B = \{1, 4\}$, $B \setminus A = \{5\}$.

2) Пусть $X = \{1, 3, 5, \ldots\}$, $Y = \{2, 4, 6, \ldots\}$. Тогда $X \cup Y = \{1, 2, 3, \ldots\}$, $X \cap Y = \varnothing$, $X \setminus Y = X$, $Y \setminus X = Y$.

Из определения ясно, что если $A \subset B$, то $A \cup B = B$, $A \cap B = A$, $A \setminus B = \varnothing$. Если $A \cap B = \varnothing$, говорят, что $A$ и $B$ не пересекаются. В этом случае, очевидно, $A \setminus B = A$, $B \setminus A = B$.

Ясно также, что для любого множества $A$ имеет место $A \cup \varnothing = A$, $A \cap \varnothing = \varnothing$, $A \setminus \varnothing = A$.

**Задача.** Пусть $A = \{1, 2, 3, \ldots\}$, $B = \{n \mid n$ — целое, $n < 6\}$. Найти $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$.

7. Понятия объединения и пересечения можно обобщить[6] следующим образом. Пусть $P$ — какое-либо множество, элементы которого мы будем называть индексами[7], и пусть каждому индексу $\alpha \in P$ поставлено в соответствие некоторое множество $A_\alpha$. Тогда мно-

[6] О б о б щ и т ь понятие означает ввести новое понятие, более общее, чем данное,— иначе говоря, такое, для которого данное есть частный случай. Понятие, возникающее в результате обобщения, также называют обобщением (ср. сказанное ниже, в п. 8, о словах «объединение» и «пересечение»). Например, понятие «населенный пункт» — обобщение понятия «город», а также понятий «деревня», «поселок» и т. п.: каждое из этих понятий — частный случай понятия «населенный пункт».

[7] От лат. *index* — «указатель».

жество, состоящее из всех тех элементов, которые принадлежат хотя бы одному $A_\alpha$, называется *объединением множеств $A_\alpha$ по $P$* и обозначается $\bigcup\limits_{\alpha\in P} A_\alpha$; множество, состоящее из всех тех элементов, которые принадлежат всем $A_\alpha$ одновременно, называется *пересечением множеств $A_\alpha$ по $P$* и обозначается $\bigcap\limits_{\alpha\in P} A_\alpha$. Например, если $P = \{1, 2, 3, \ldots\}$ и $A_n = \{0, 1, \ldots n\}$ для каждого $n\in P$, то $\bigcup\limits_{\alpha\in P} A_\alpha = \{0, 1, 2, \ldots\}$, $\bigcap\limits_{\alpha\in P} A_\alpha = \{0, 1\}$. Если все $A_n$ равны одному и тому же множеству $A$, то $\bigcup\limits_{\alpha\in P} A_\alpha = \bigcap\limits_{\alpha\in P} A_\alpha = A$. При $P = \{1, 2\}$ получается частный случай, рассмотренный выше.

Вместо $\bigcup\limits_{i\in\{1,2,\ldots n\}} A_i$ пишут $\bigcup\limits_{i=1}^{n} A_i$, вместо $\bigcup\limits_{i\in\{2,\ldots n\}} A_i$ — $\bigcup\limits_{i=2}^{n} A_i$, вместо $\bigcup\limits_{i\in\{1,2,\ldots\}} A_i$ — $\bigcup\limits_{i=1}^{\infty} A_i$ и т. п. Аналогичный смысл имеют обозначения $\bigcap\limits_{i=1}^{n} A_i$, $\bigcap\limits_{i=2}^{n} A_i$, $\bigcap\limits_{i=1}^{\infty} A_i$ и т. п.

Задача. Введем следующие обозначения, общепринятые в теории числовых множеств: $\{x \mid a < x < b\} = (a, b)$; $\{x \mid a \le x \le b\} = [a, b]$; $\{x \mid a < x \le = b\} = (a. b]$; $\{x \mid a \le x < b\} = [a, b)$; здесь всюду $x$ — действительное число, $a$ и $b$ — заданные постоянные действительные числа. (Множество вида $(a, b)$ называется *интервалом*, вида $[a, b]$ — *сегментом*, или *отрезком*, вида $(a, b]$ или $[a, b)$ — *полуинтервалом*, иначе *полусегментом*.) Пусть теперь $\mathbf{R}_+$ — множество всех положительных действительных чисел. Найти $\bigcup\limits_{\alpha\in\mathbf{R}_+} (0, a)$; $\bigcap\limits_{\alpha\in\mathbf{R}_+} (0, a)$; $\bigcup\limits_{\alpha\in\mathbf{R}_+} [0. a]$; $\bigcap\limits_{\alpha\in\mathbf{R}_+} [0. a]$; $\bigcup\limits_{\alpha\in\mathbf{R}_+} (0. a]$; $\bigcap\limits_{\alpha\in\mathbf{R}_+} (0, a]$; $\bigcup\limits_{\alpha\in\mathbf{R}_+} [0, a)$; $\bigcap\limits_{\alpha\in\mathbf{R}_+} [0, a)$.

8. Подобно тому, как в арифметике изучаются действия над числами — сложение, состоящее в образовании по двум числам их суммы, умножение, состоящее в образовании по двум числам их произведения, и др.,— в теории множеств рассматриваются действия, или операции[8], над множествами, из которых важнейшими являются следующие три:

1) Операция, состоящая в образовании по двум множествам $A$ и $B$ их объединения $A\cup B$. Сама эта операция также называется *объединением*.

2) Операция, состоящая в образовании по двум множествам $A$ и $B$ их пересечения $A\cap B$. Сама эта операция также называется *пересечением*.

3) Операция, состоящая в образовании по двум множествам $A$ и $B$ их разности $A\setminus B$. Эта операция называется *вычитанием* ($B$ из $A$).

[8] От лат. *operatio* — «действие».

Таким образом, каждое из слов «объединение» и «пересечение» означает и операцию, и ее результат. Среди названий арифметических действий нет таких, которые совпадали бы с названиями их результатов: результат сложения называется суммой, и т. п. Однако в обычном русском языке немало слов, которые могут обозначать, с одной стороны, некоторое действие, а с другой — его результат: «работа» (ср. «Я наблюдаю за его работой» и «Эта вещь — работа мастера»), «решение» (ср. «Решение задачи заняло три дня» и «Решение оказалось простым»), «сочинение», «постройка» и т. п.

9. Введенные только что операции над множествами обладают некоторыми важными свойствами, во многом похожими на хорошо известные читателю свойства арифметических действий.

Вот эти свойства:

I. $A \cup (B \cup C) = (A \cup B) \cup C$ (*ассоциативность*[9] *объединения*).

Доказательство этого свойства несложно, но мы проведем его подробно, поскольку это первый пример доказательства равенства множеств, заданных по-разному. Для доказательства таких равенств обычно пользуются тем, что два множества равны тогда и только тогда, когда каждое из них содержится в другом (см. выше, п. 3). Так мы поступим и сейчас — докажем, что:

а) $A \cup (B \cup C) \subset (A \cup B) \cup C$; б) $(A \cup B) \cup C \subset A \cup (B \cup C)$.

Доказательство включения[10] а) По определению $X \subset Y$ означает, что каждый элемент $X$ есть элемент $Y$. Но если $x \in A \cup (B \cup C)$, то — по определению объединения — либо $x \in A$, либо $x \in B \cup C$.

Случай 1. $x \in A$. В этом случае, по определению объединения, $x \in A \cup B$, а отсюда — по тому же определению — $x \in (A \cup B) \cup C$.

Случай 2. $x \in B \cup C$. Тогда либо $x \in B$, либо $x \in C$; из первой возможности — $x \in B$ — следует $x \in A \cup B$, а отсюда — $x \in (A \cup B) \cup C$; из второй возможности — $x \in C$ — сразу следует $x \in (A \cup B) \cup C$. Итак, во всех возможных случаях имеем $x \in (A \cup B) \cup C$.

Доказательство включения б) аналогично, поэтому изложим его короче. Пусть $x \in (A \cup B) \cup C$. Тогда либо $x \in A \cup B$, либо $x \in C$.

Случай 1. $x \in A \cup B$. Тогда либо $x \in A$, либо $x \in B$. Из $x \in A$ следует $x \in A \cup (B \cup C)$; из $x \in B$ следует $x \in B \cup C$, а отсюда $x \in A \cup (B \cup C)$.

Случай 2. $x \in C$. Тогда $x \in B \cup C$, а отсюда $x \in A \cup (B \cup C)$.

II. $A \cup B = B \cup A$ (*коммутативность*[11] *объединения*). Это свойство очевидным образом следует из определения объединения.

---

[9] От лат. *iungo* — «соединяю».

[10] Включением называется всякое соотношение вида $P \subset Q$ (подобно тому, как соотношение вида $P = Q$ называется равенством).

[11] От лат. *commuto* — «изменяю», «обмениваю».

III. $A\cap(B\cap C) = (A\cap B)\cap C$ (*ассоциативность пересечения*).

**Доказательство.** а) Докажем, что $A\cap(B\cap C) \subset (A\cap B)\cap C$. Пусть $x\in A\cap(B\cap C)$. Тогда $x\in A$ и $x\in B\cap C$, откуда следует, что $x\in B$ и $x\in C$. Но из $x\in A$ и $x\in B$ следует, что $x\in A\cap B$, а отсюда и из $x\in C$ — что $x\in(A\cap B)\cap C$.

б) Доказательство включения $(A\cap B)\cap C \subset A\cap(B\cap C)$ предоставляется читателю.

IV. $A\cap B = B\cap A$ (*коммутативность пересечения*).

Очевидным образом следует из определения пересечения.

Благодаря коммутативности объединения и пересечения мы можем переставлять члены в выражениях вроде $A\cup B$, $A\cap B$, а благодаря ассоциативности — писать, например, вместо $A\cup(B\cup C)$ или $(A\cup B)\cup C$ просто $A\cup B\cup C$. Заметим, что $A_1\cup A_2\cup\cdots\cup A_n = \bigcup_{i=1}^{n} A_i$, $A_1\cap A_2\cap\cdots\cap A_n = \bigcap_{i=1}^{n} A_i$.

V. $A\cap(B\cup C) = (A\cap B)\cup(A\cap C)$ (*дистрибутивность*[12] *пересечения по отношению к объединению*).

**Доказательство.** Обозначим для краткости левую часть доказываемого равенства через $M$, правую — через $N$.

а) Докажем, что $M\subset N$. Пусть $x\in M$; тогда $x\in A$ и $x\in B\cup C$; последнее соотношение означает, что либо $x\in B$, либо $x\in C$. Если $x\in B$, то, поскольку $x\in A$, имеем $x\in A\cap B$, откуда $x\in(A\cap B)\cup(A\cap C) = N$. Если же $x\in C$, точно так же получаем $x\in A\cap C$, откуда $x\in N$.

б) Докажем, что $N\subset M$. Пусть $x\in N$; тогда либо $x\in A\cap B$, либо $x\in A\cap C$. В первом случае $x\in A$ и $x\in B$; из $x\in B$ следует $x\in B\cup C$, что вместе с $x\in A$ дает $x\in A\cap(B\cup C) = M$. Во втором случае рассуждаем аналогично.

Заметим, что доказанные свойства объединения и пересечения совершенно аналогичны известным свойствам сложения и умножения чисел, причем объединение соответствует сложению, а пересечение — умножению[13].

Однако следующее свойство уже не имеет аналога в арифметике:

VI. $A\cup(B\cap C) = (A\cup B)\cap(A\cup C)$ (*дистрибутивность объединения по отношению к пересечению*).

Доказательство. Обозначим левую часть через $M$, правую — через $N$.

а) Докажем, что $M\subset N$. Пусть $x\in M$; тогда либо $x\in A$, либо

[12] От лат. *distribuo* — «распределяю».

[13] Иногда объединение так и называют «сложением множеств», а пересечение — «умножением множеств».

$x \in B \cap C$. В первом случае сразу имеем $x \in A \cup B$ и $x \in A \cup C$, откуда $x \in N$. Во втором случае имеем $x \in B$, откуда $x \in A \cup B$, и $x \in C$, откуда $x \in A \cup C$: но $x \in A \cup B$ и $x \in A \cup C$ дает $x \in N$.

б) Доказательство включения $N \subset M$ предоставляется читателю.

VII. $A = (A \setminus B) \cap (A \cap B)$.

**Доказательство.** Обозначим правую часть через $P$. Пусть $x \in A$; тогда, если $x \in B$, имеем $x \in A \cap B$, откуда $x \in P$, а если $x \notin B$, то $x \in A \setminus B$, откуда также $x \in P$. Итак, $A \subset P$. Пусть теперь $x \in P$; тогда либо $x \in A \setminus B$, откуда $x \in A$, либо $x \in A \cap B$, откуда также $x \in A$. Итак, $P \subset A$.

Отметим еще два очевидных равенства: $A \cup A = A$, $A \cap A = A$.

**Задача.** Доказать, что:

(1) $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$;

(2) $(A \setminus B) \cap C = (A \cap C) \setminus B$.

**10.** Очень часто бывает, что рассматриваются всевозможные множества, являющиеся частями одного и того же множества $U$, и никакие другие множества не рассматриваются. Множество $U$ называют в этом случае *универсальным* и для произвольного множества $A$, содержащегося в $U$, разность $U \setminus A$ обозначают через $CA$ и называют *дополнением $A$ до $U$*; если $U$ все время одно и то же (как бывает чаще всего), слова «до $U$» опускают. Рассматривается также операция, состоящая в образовании по множеству $A$, содержащемуся в $U$, его дополнения (до $U$); эта операция тоже называется *дополнением (до $U$)*.

Основные свойства дополнения (в предположении, что все рассматриваемые множества содержатся в $U$):

I. $CCA = A$.

**Доказательство.** а) Пусть $x \in CCA$. Это значит, что $x \in U$ и $x \notin CA$; но $CA$ — это множество элементов $U$, не принадлежащих $A$; поэтому $x \in U$ и $x \notin CA$ дает $x \in A$.

б) Если $x \in A$, то $x \notin CA$, но отсюда, поскольку $x \in U$, следует $x \in U \setminus CA = CCA$.

II. $C(A \cup B) = CA \cap CB$.

**Доказательство.** а) Пусть $x \in C(A \cup B)$. Тогда $x \notin A \cup B$, а это значит, что $x$ не принадлежит ни $A$, ни $B$. Из $x \notin A$ — ввиду $x \in U$ — следует $x \in CA$, а из $x \notin B$ — $x \in CB$. Итак, $x \in CA \cap CB$.

б) Пусть $x \in CA \cap CB$. Тогда $x \in CA$ и $x \in CB$. Из $x \in CA$ следует $x \notin A$, из $x \in CB$ — $x \notin B$. Поэтому $x \notin A \cup B$, откуда $x \in C(A \cup B)$.

III. $C(A \cap B) = CA \cup CB$.

Доказательство предоставляется читателю.

Понятие дополнения и его свойства легко проиллюстрировать на рис. 1, если считать универсальным множество всех точек плоскости рисунка. Тогда $CA$ и $CB$ будут представлять собой множества точек,

лежащих вне соответствующих кругов, $C(A \cup B) = CA \cap CB$ — множество точек, свободных от всякой штриховки, $C(A \cap B) = CA \cup CB$ — множество точек, заштрихованных только одной штриховкой или вовсе не заштрихованных.

Задача. Доказать, что $C(A \setminus B) = CA \cup B$.

11. В математике (и не только в ней) часто приходится иметь дело с *упорядоченными парами* элементов того или иного множества, т. е. с парами, в которых один элемент считается *первым*, а другой *вторым*. (В частном случае первый и второй элементы могут совпадать.) Например, координаты точки на плоскости — это упорядоченная пара действительных чисел, в которой первым элементом считается абсцисса, вторым — ордината. Упорядоченную пару с первым элементом $a_1$ и вторым элементом $a_2$ принято обозначать $(a_1, a_2)$. Например, $(3, -1)$ — упорядоченная пара, первый элемент которой — число 3, второй — число $-1$; $(2.2)$ — упорядоченная пара, первый и второй элементы которой равны 2, и т. п.

Наряду с упорядоченными парами рассматриваются *упорядоченные тройки*, *четверки* и т. д. Обозначаются они аналогично: упорядоченная $n$-ка (подробнее — *упорядоченная система n элементов*[14]) с первым элементом $a_1$, вторым элементом $a_2$, ..., $n$-м элементом $a_n$ записывается в виде $(a_1, a_2, ..., a_n)$. Например, $(2, 7, 6)$ — упорядоченная тройка с первым элементом 2, вторым элементом 7 и третьим элементом 6.

В повседневной жизни упорядоченные системы используются, когда нужно дать «имена» большому количеству однородных предметов, причем разные предметы должны иметь разные «имена». Так, номер телефона представляет собой упорядоченную $n$-ку элементов множества $\{0, 1, ..., 9\}$ (число $n$ в разных городах разное); используемые в России почтовые индексы суть упорядоченные шестерки элементов того же множества[15].

Нередко приходится иметь дело и с такими упорядоченными парами, тройками и т. д., в которых первые элементы берутся из одного множества, вторые — из другого, третьи — из третьего и т. д. Например, полное имя человека в России есть упорядоченная тройка, первый элемент которой принадлежит множеству личных имен, второй — множеству отчеств и третий — множеству фамилий.

Примечание. Внимательный читатель, вероятно, заметил, что мы не дали строгого определения упорядоченной $n$-ки (и даже упорядоченной пары), т. е. фактически ввели еще одно неопределяемое понятие.

---

[14] Упорядоченные системы часто называют также *кортежами*.

[15] То, что номера телефонов и почтовые индексы пишутся без запятых и без скобок, очевидно, несущественно.

**12.** Пусть заданы $n$ произвольных множеств: $A_1, A_2, \ldots, A_n (n \geq 2)$. Множество всевозможных упорядоченных $n$-ок вида $(a_1, \ldots, a_n)$, таких, что $a_1 \in A_1, \ldots, a_n \in A_n$, называется *декартовым произведением*[16] множеств $A_1, \ldots, A_n$ и обозначается $A_1 \times \cdots \times A_n$ или $\prod_{i=1}^{n} A_i$. (В частном случае, когда $n = 2$, говорят: «*декартово произведение $A_1$ на $A_2$*».) Например, если $A = \{a, b, c, d, e, f, g, h\}$ и $B = \{1, \ldots, 8\}$, то $A \times B$ — множество, состоящее из 64 упорядоченных пар: $\{(a, 1), (a, 2), \ldots, (h, 8)\}$. (Если писать эти пары без скобок и без запятых, получим общепринятые обозначения полей шахматной доски.)

Декартово произведение $\underbrace{A \times \cdots \times A}_{n \text{ раз}}$ называется $n$-ой *декартовой степенью* множества $A$ и обозначается $A^n$; в частности, $A \times A = A^2$ называется *декартовым квадратом* $A$. Например, если R — множество действительных чисел[17], то $\mathrm{R}^2$ — множество упорядоченных пар действительных чисел.

Операция, состоящая в образовании по множествам $A_1, \ldots, A_n$ их декартова произведения $A_1 \times \cdots \times A_n$, называется *декартовым умножением*.

Важно заметить, что декартово умножение не коммутативно, т. е. в декартовом произведении нельзя, вообще говоря[18], переставлять сомножители. Например, если $A = \{0,1\}$, $B = \{1,2\}$, то $A \times B = \{(0,1), (0,2), (1,1), (1,2)\}$, $B \times A = \{(1,0), (1,1), (2,0), (2,1)\}$.

**Задачи.** (1) Выписать все элементы множества

$\{a, б, в\} \times \{а, в\} \times \{б, в\}$.

(2) Пусть множество $A$ состоит из $m$ элементов и множество $B$ из $n$ элементов. Из какого числа элементов состоит множество $A \times B$?

(3) Найти (и изобразить на чертеже) множество точек плоскости, координаты которых принадлежат множеству $[1,4] \times [2,3]$. (Здесь использовано введенное в задаче на с. 27 обозначение отрезка.)

(4) Совпадает ли множество возможных в России полных имен людей с множеством И × О × Ф, где И, О, Ф — множества возможных в России имен, отчеств и фамилий соответственно?

---

[16] В честь великого французского ученого Рене Декарта (René Descartes, 1596—1650), который впервые ввел в обиход математики упорядоченные системы.

[17] Выражения вида «множество действительных чисел», «множество точек плоскости» и т. п. означают «множество всех действительных чисел», «множество всех точек плоскости» и т. п., если только впереди не стоит слово типа «некоторое», «какое-либо», «любое», «всякое», «произвольное».

[18] Выражения «вообще говоря, нельзя», «вообще говоря, не является» и т. п. означают «не всегда можно» (т. е. есть случаи, когда нельзя, и, может быть, есть и такие, когда можно), «не всегда является» и т. п.

## § 1.2 ОТНОШЕНИЯ И ФУНКЦИИ

1. Теперь мы должны познакомиться еще с одним важнейшим математическим понятием — понятием *отношения*[19]. Мы введем это понятие как неопределяемое и поясним его на примерах из естественного языка и элементарной математики.

В естественном языке много слов, обозначающих различные отношения между двумя лицами, между лицом и предметом, между двумя предметами и т. п. Например, в каждой из следующих фраз выделенное слово обозначает некоторое отношение: Миша старше Вани; Это дерево выше, чем то; Мать любит сына; Ученик уважает учителя; Анна — жена Ивана; Петров — подчиненный Сидорова; Пушкин — автор «Евгения Онегина»; Книга принадлежит библиотеке; Деревня расположена на берегу. Некоторые из этих слов выражают отношения между объектами одной природы (например, «подчиненный»: вопрос «Является ли $X$ подчиненным $Y$-а?» имеет смысл только тогда, когда $X$ и $Y$ — люди), другие — отношения между разнородными объектами (например, «автор»).

В математике также приходится иметь дело с отношениями между элементами одного и того же или различных множеств. Например, «лежит на» во фразе «точка $A$ лежит на прямой $l$» выражает некоторое отношение между элементом множества точек пространства и элементом множества прямых в пространстве; «параллельна» во фразе «прямая $l$ параллельна прямой $m$» выражает отношение между двумя элементами множества прямых в пространстве. Если прямая $l$ параллельна прямой $m$, можно сказать, что $l$ и $m$ «связаны» отношением параллельности, или «находятся» в этом отношении. Для произвольного отношения $R$ также говорят: «$x$ и $y$ *связаны* отношением $R$», или «$x$ и $y$ *находятся* в отношении $R$»; короче это записывают так: $xRy$. Здесь $R$ может представлять собой либо словесное обозначение отношения — «$x$ параллельна $y$», «$x$ меньше $y$» и т. п., либо символическое — $x < y$, $x = y$ и т. п. Множество, из которого берется первый из связанных отношением $R$ элементов — тот, обозначение которого пишется слева от $R$ — мы будем называть *областью первых элементов* или *областью отправления* отношения $R$, а множество, из которого берется второй элемент — *областью вторых элементов* или *областью прибытия* $R$. Если $P$ и $Q$ — соответственно области отправления и прибытия отношения $R$ и при этом

[19] Иногда вместо «отношение» говорят «соотношение».

$x \in P$ и $y \in Q$, то $x$ и $y$ могут находиться или не находиться в отношении $R$, но, во всяком случае, вопрос «находятся ли $x$ и $y$ в отношении $R$?» должен иметь смысл. Например, для рассмотренного выше отношения «лежит на» областью отправления служит множество точек, а областью прибытия — множество прямых; для отношения «быть автором» область отправления — множество людей, область прибытия — множество произведений человеческого ума и рук.

Если область отправления и область прибытия отношения совпадают, т. е. равны одному и тому же множеству $M$, мы говорим, что отношение *задано на множестве* $M$. Примерами могут служить отношение параллельности, заданное на множестве прямых, отношение $<$ («меньше»), заданное на множестве действительных чисел, отношение $=$ («равно»), также заданное на множестве действительных чисел.

Если $R$ — отношение с областью отправления $P$ и областью прибытия $Q$, то множество $\{(x, y) \mid x \in P, y \in Q, xRy\}$ (содержащееся, очевидно, в $P \times Q$) называется *графиком* отношения $R$. Так, для отношений $<$ и $=$, заданных на множестве действительных чисел, графиками будут множества $\{(x, y) \mid x < y\}$ и $\{(x, y) \mid x = y\}$ соответственно. Пара (Пушкин, «Евгений Онегин») принадлежит графику отношения «быть автором», а пара (Пушкин, «Ревизор») не принадлежит.

Если отношение $R$ задано на множестве действительных чисел, то множество точек плоскости, координаты которых принадлежат графику отношения $R$ (т. е. точек с координатами $x$, $y$, где $xRy$), обычно тоже называют *графиком* отношения $R$. Таким образом, можно сказать, что графиками отношений $=$ и $<$ служат соответственно биссектриса первого и третьего координатных углов и полуплоскость, расположенная выше этой биссектрисы (см. рис. 2).

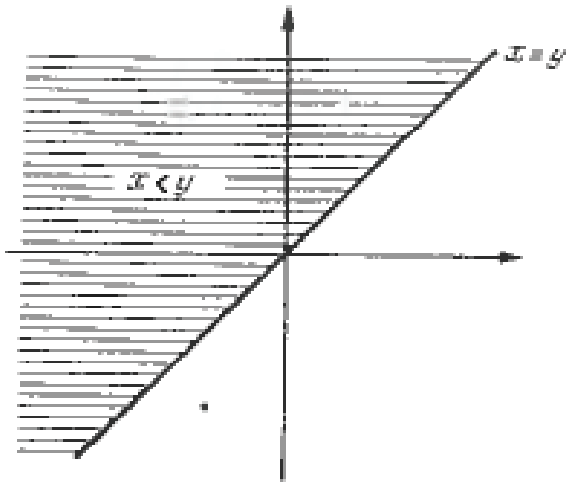



Рис. 2

Если $R$ — отношение с областью отправления $P$ и областью прибытия $Q$, то множество тех элементов $P$, которые связаны отношением $R$ с какими-либо элементами $Q$, называется *областью определения* отношения $R$, а множество тех элементов $Q$, которые связаны отношением $R$ с какими-либо элементами $P$,— *множеством значений* отношения $R$. Иногда область определения совпадает с

областью отправления и множество значений — с областью прибытия; так обстоит дело для рассмотренных выше отношений «лежит на», $=$, $<$. Но это не всегда так. Пусть, например, $T_0$ — следующее отношение, область отправления которого есть множество $Г$ городов мира и область прибытия — множество $Б$ русских букв: $xT_0y$ тогда и только тогда, когда русское название города $x$ начинается и оканчивается буквой $y$. Ясно, что область определения $Г_1$ отношения $T_0$ есть соб-ственная часть $Г$, а его множество значений $Б_1$ — собственная часть $Б$; читатель сам укажет примеры городов, не принадлежащих $Г_1$, и букв, не принадлежащих $Б_1$. Другой пример: пусть $K$ — следующее отношение, заданное на множестве действительных чисел: $xKy$ тогда и только тогда, когда $x^2 + y^2 = 1$. Легко убедиться, что область определения и множество значений отношения $K$ совпадают с сегментом $[-1, 1]$. (Заметим, что графиком этого отношения служит — в силу теоремы Пифагора — окружность радиуса 1 с центром в начале координат.)

Отношение $T$ называют *обратным* для отношения $R$, если $xTy$ тогда и только тогда, когда $yRx$. Отношение, обратное для $R$, обозначают обычно $R^{-1}$. Очевидно, область отправления (область определения) отношения $R$ является областью прибытия, соответственно множеством значений $R^{-1}$, а область прибытия (множество значений) $R$ — областью отправления, соответственно областью определения $R^{-1}$[20]; в частности, если $R$ задано на множестве $M$, то и $R^{-1}$ задано на том же множестве. Ясно, что отношение $R$ является, в свою очередь, обратным для $R^{-1}$; поэтому говорят, что $R$ и $R^{-1}$ *взаимно обратны*.

Примеры: для отношения $<$ обратное отношение есть $>$, для «лежать на» — «проходить через» («прямая $l$ проходит через точку $A$» означает то же, что «точка $A$ лежит на прямой $b$»), для «быть женой» — «быть мужем». (Имеются и такие отношения, которые сами себе обратны — например, равенство, параллельность, приведенное выше отношение $K$.)

Задачи. (1) Пусть $S$ — отношение с областью отправления $\{0, 1, \ldots, 9\}$ и областью прибытия $\{а, б, \ldots, и\}$, определяемое так: $xSy$ означает, что русское название цифры $x$ начинается с буквы $y$. Выписать все элементы графика $S$ и все элементы множества значений $S$.

(2) Пусть $R_1$ и $R_2$ — отношения, заданные на множестве действительных чисел и такие, что $xR_1y$ означает $x = y^2$, $xR_2y$ означает

[20] Выражение вида «$A(B)$ есть $A_1$, соответственно $B_1$» означает «$A$ есть $A_1$, а $B$ есть $B_1$».

$|x| = |y|$. Найти и изобразить на чертеже графики этих отношений; найти их области определения и множества значений.

(3) Найти графики отношений, обратных отношениям задач (1) и (2). Изобразить графики отношений $R_1^{-1}$ и $R_2^{-1}$ на чертеже.

2. Сделаем теперь следующее отступление. Одной из характерных особенностей математического языка является широкое употребление буквенных обозначений, т. е. использование букв[21] для именования различных объектов. Иногда буквы служат «собственными именами» — например, буква $\pi$ обозначает одно вполне определенное число, подобно тому, как слово «Торжок» обозначает один вполне определенный город. Но такое употребление букв является исключением; в роли «собственных имен» в языке математики чаще выступают другие символы: цифры и последовательности цифр, специальные значки вроде $+$, $-$, $\sqrt{\ }$, стандартные буквосочетания — log, sin и т. п. Буква же обычно служит *переменной*, т. е. обозначает произвольный объект того или иного типа — число, точку, прямую, множество и т. п. (Иначе говоря, объект, обозначаемый данной буквой, может изменяться; отсюда и термин «переменная».) При этом каждый раз специально указывается, какого рода объекты имеются в виду; как правило, переменная обозначает произвольный элемент некоторого множества, которое называют в этом случае *областью изменения* данной переменной и говорят, что переменная *изменяется* в этом множестве, или *принимает значения* в нем, или *пробегает* его. Элементы области изменения переменной называют *значениями* этой переменной. Однако указание о том, что означает данная переменная, т. е. какова ее область изменения, всегда является «временным»: оно имеет силу только в пределах некоторого отрезка математического текста, чаще всего — одного рассуждения или одной формулировки. За пределами этого отрезка та же буква может уже означать что-либо другое — что именно, должно быть снова указано в тексте. Нередко в том или ином месте рассуждения произвольно выбранное значение какой-либо переменной *фиксируется*, т. е. объявляется до окончания какого-то этапа рассуждения неизменным; часто бывает также, что выбор значения одной переменной зависит от выбора значения другой (подробнее об этом см. в следующем пункте). Но и в этих случаях сохраняется главная особенность употребления переменных: у них нет своих собственных, раз навсегда связанных с ними значений (в отличие от таких символов, как 1, +, sin и т. п.); что означает та или иная

[21] Иногда с индексами — дополнительными значками, цифровыми или тоже буквенными (помещаемыми чаще всего справа внизу): $x_1$, $a_2$, $b_n$ и т. п., а также с дополнительными значками иного вида: $x'$, $a^*$, $\overline{y}$, $\widetilde{\alpha}$ и т. п.

переменная, можно узнать только из контекста. Это сближает переменные с местоимениями естественного языка: «он», «этот», «такой» и т. п., которые представляют собой слова-заместители, также не имеющие «своих собственных» значений и могущие обозначать «что угодно» в зависимости от контекста.

3. Мы подошли теперь ко второму по важности (после множества) математическому понятию — функции. Мы введем его на базе понятия отношения.

Отношение называется *функциональным*, если каждый элемент его области определения связан этим отношением не более чем с одним элементом области прибытия — или, что то же самое, если каждый элемент его области определения связан данным отношением ровно с одним элементом множества значений.

Функциональное отношение обычно называют просто *функцией*[22].

Функцию (функциональное отношение) $F$ естественно представлять себе как некоторый «закон соответствия», по которому каждому элементу $a$ области определения отношения $F$ «сопоставляется» (или «ставится в соответствие») строго определенный элемент множества значений — а именно тот единственный элемент $b$, который связан с $a$ отношением $F$, т. е. тот, для которого справедливо $aFb$. Этот элемент $b$ обозначается $F(a)$ (читается: «$F$ от $a$») и называется *образом* элемента $a$; этот последний, в свою очередь, называется *прообразом* элемента $b$. Прообраз, в отличие от образа, не обязан быть единственным. Множество всех прообразов элемента $b$ называют *полным прообразом* этого элемента. Вместо $b = F(a)$ пишут также $a \overset{F}{\mapsto} b$, а если функция предполагается известной — просто $a \mapsto b$. Если $x$ и $y$ — переменные, пробегающие соответственно область определения и множество значений $F$, то $x$ называют *независимой переменной*, или *аргументом*[23], а $y$ — *зависимой переменной*. Если $a$ — произвольное значение независимой переменной, т. е. произвольный элемент области определения функции $F$, то естественно сказать, что соответствующее значение $b = F(a)$ зависимой переменной *зависит* от $a$ (подробнее — «зависит по закону $F$»); этим и объясняются названия «независимая переменная» и «зависимая переменная». Вместо «функция $F$» часто говорят и пишут «функ-

[22] От лат. *fungor* — «выполняю, совершаю» (некоторое действие, работу). Выбор термина обусловлен тем, что с понятием функции первоначально связывалось представление о некотором действии, превращающем значение аргумента в значение зависимой переменной.

[23] От лат. *argumentum* — «то, о чем идет речь» (от *arguo* «утверждаю»), собственно «содержание, предмет, сюжет литературного произведения». Другое значение слова *argumentum* — «довод, доказательство»; отсюда русское «аргумент» — «довод».)

ция $F(x)$» (читается: «$F$ от $x$») или «функция $y = F(x)$», причем подразумевается, что $x$ — независимая, а $y$ — зависимая переменная[24]. (Разумеется, вместо $x$ и $y$ можно использовать любые другие буквы!) Если $x_0$ — какое-либо значение независимой переменной, то значение $y_0 = F(x_0)$ зависимой переменной (т. е. образ $x_0$) называют *значением функции $F$, соответствующим $x_0$* (иначе — значением функции при значении аргумента, равном $x_0$).

**Примеры функций.** (1) Пусть $xMy$ означает «$y$ — мать $x$-а». Областью отправления отношения $M$ можно считать множество людей, областью прибытия — множество женщин. Очевидно, отношение $M$ есть функция (поскольку у каждого человека только одна мать).

(2) Рассмотренное на с. 35 отношение $T_0$ есть функция.

(3) Отношение $=$, заданное на множестве действительных чисел $\mathbf{R}$, также есть функция.

(4) Отношение $f_1$, заданное на том же множестве $\mathbf{R}$ и такое, что $xf_1y$ означает $y = x + 1$, является функцией: очевидно, для каждого действительного числа $x$ имеется только одно число $y$, равное $x + 1$.

(5) То же верно для заданного на $\mathbf{R}$ отношения $f_2$, где $xf_2y$ означает $y = \frac{1}{x}$: для каждого действительного $x$ имеется не более одного $y$, равного $\frac{1}{x}$ (хотя не для всякого $x$ такое $y$ существует!).

(6, 7) То же верно для заданных на $\mathbf{R}$ отношений $f_3$ и $f_4$, где $xf_3y$ означает $y = x^2$ и $xf_4y$ тогда и только тогда, когда либо $x < 0$ и $y = x + 1$, либо $x > 1$ и $y = x^2 + 1$. (Обратить внимание, что область определения $f_4$ не совпадает с $\mathbf{R}$, как и выше для $f_2$!)

(8) *Целой частью* действительного числа $x$ называется наибольшее целое число, не превосходящее $x$. Целая часть $x$ обозначается $[x]$. (Например: $[0] = \left[\frac{1}{3}\right] = 0$; $[3] = [3{,}5] = 3$; $[-1{,}6] = [-2] = -2$.) Если $xf_5y$ означает $y = [x]$, то отношение $f_5$ является, очевидно, функцией.

(9) Пусть $xf_6y$ ($x$ и $y$ — действительные числа) означает $y = 1$. Очевидно, $f_6$ есть функция.

---

[24] В обозначениях некоторых часто встречающихся в математике функций скобки принято опускать (пример — тригонометрические функции: $\sin x$ вместо $\sin(x)$, $\cos x$ и т. п.).

Замечание. Для конкретных функций наряду с обозначениями стандартного вида $F(x)$ или $Fx$ (см. сноску на с. 38) часто пользуются обозначениями, устроенными иначе. Все эти обозначения имеют вид $...x...$ или $y = ...x...$, где $...x...$ — символическое выражение, содержащее независимую переменную $x$, а $y$ — зависимая переменная. При этом выражение $...x_0...$, получаемое из $...x...$ подстановкой вместо переменной $x$ некоторого ее значения $x_0$, служит обозначением соответствующего значения функции. Например, рассмотренная только что функция $f_1$ обычно обозначается просто $x + 1$ или $y = x + 1$, функция $f_2$ обозначается $\frac{1}{x}$ или $y = \frac{1}{x}$, функция $f_3$ — $x^2$ или $y = x^2$, функция $f_5$ — $[x]$ или $y = [x]$, функция $f_6$ — $y = 1$ (так что выражение в правой части равенства может даже не содержать $x$; это возможно лишь тогда, когда все значения функции одинаковы). Функция $=$ обозначается $y = x$. Другие примеры подобных обозначений: $\sqrt{x}$, $a^x$, $x^2 + x + 1$.

В большинстве случаев при задании функции не указывают ее область отправления, ограничиваясь указанием области определения и области прибытия[25]. Таким образом, чтобы задать функцию, достаточно задать ее область определения и область прибытия и для каждого элемента области определения указать соответствующий ему элемент области прибытия. Если $F$ — функция с областью определения $A$ и областью прибытия $B$, говорят, что *$F$ отображает множество* во $A$ множество $B$[26]; если при этом множество $A$ значений $F$ совпадает с $B$, говорят, что *$F$ отображает $A$ на $B$*. Вместо «функция, отображающая множество $A$ в (на) множество $B$» говорят также «*отображение* множества $A$ *в*, соответственно *на*, множество $B$». (Обратите внимание, что «отображение на» — частный случай «отображения в»). Отображение, множество значений которого совпадает с областью прибытия, часто называют *сюръективным*; вместо «сюръективное отображение» говоря также «*сюръекция*».

(Таким образом, фраза типа «данное отображение $A$ в $B$ сюръективно» означает «данное отображение $A$ в $B$ есть отображение $A$ на $B$.)

Вместо «$F$ есть функция, отображающая $A$ в (на) $B$» (или: $F$ есть отображение $A$ в (на) $B$) нередко пишут символически $F : A \to B$.

---

[25] Что касается множества значений, то его нет надобности задавать особо — оно полностью определяется заданием области определения и самой функции («закона соответствия»).

[26] Иногда говорят еще и так: «$F$ осуществляет отображение $A$ в $B$». Это — обычное в естественном языке так называемое синонимическое преобразование: по-русски «отображать» = «осуществлять отображение», так же, как «ремонтировать» = «производить ремонт», «путешествовать» = «совершать путешествие», «уважать» = «испытывать уважение».

соответственно $F : A \overset{\text{на}}{\to} B$ (Обратить внимание на различие между стрелками здесь и на с. 37!)

Если областью определения функции $F$ является множество $A$, говорят, что *$F$ определена на $A$*.

Примеры. Пользуясь обозначениями вышеприведенных примеров (1) — (8), мы можем записать: $M : H \to F$, где $H$ — множество всех людей и $F$ — множество всех женщин; $T_0 : Г \to Б$ (см. пункт 1); $f_1 : \mathbf{R} \overset{\text{на}}{\to} \mathbf{R}$ (здесь и далее $\mathbf{R}$ означает множество действительных чисел); $f_2 : \mathbf{R}\setminus\{0\} \overset{\text{на}}{\to} \mathbf{R}\setminus\{0\}$; $f_3 : \mathbf{R} \to \mathbf{R}$; $f_4 : \mathbf{R}\setminus[0, 1] \to \mathbf{R}$; $f_5 : \mathbf{R} \overset{\text{на}}{\to} \mathbf{Z}$, где $\mathbf{Z}$ — множество целых чисел; $f_6 : \mathbf{R} \to \mathbf{R}$. Заметим, что для функций $M$, $T_0$, $f_3$, $f_4$, $f_6$ нельзя заменить $\to$ на $\overset{\text{на}}{\to}$; читателю предоставляется найти множества значений функций $f_3$, $f_4$ и $f_6$.

*График функции $F$* — это, в соответствии с общим определением графика отношения (пункт 1), множество всех тех упорядоченных пар $(x, y)$, для которых $y = F(x)$. Если $D$ — область определения функции, то для каждого $x \in D$ график функции содержит, очевидно, только одну пару с первым элементом $x$.

В частности, пусть область определения и множество значений функции $F$ состоят из действительных чисел, так что $F$ можно рассматривать как отношение, заданное на множестве $\mathbf{R}$; для таких отношений в пункте 1 было указано геометрическое представление графика. Тогда приведенное только что свойство графика функции можно сформулировать так: всякая прямая, параллельная оси ординат, пересекает график функции не более чем в одной точке.

Если $F$ — произвольная функция, т. е. функциональное отношение, то обратное ему отношение $F^{-1}$ может, вообще говоря, не быть функциональным. Если же оно является функциональным, его естественно назвать *функцией, обратной* для $F$. Так, для функции $f_1$ (см. выше) обратное отношение функционально — иначе говоря, существует обратная функция $F^{-1}$ (а именно, $y = f_1^{-1}(x) = x - 1$[27]), а для функции $f_3$ обратное отношение не функционально, т. е. обратной функции не существует (доказать это!). Читателю предоставляется для каждой из остальных вышеприведенных функций найти обратную или доказать, что ее не существует.

Если $F$ — функция с областью определения $A$ и множеством значений $B$, то для произвольного $C \subset A$ множество образов всех его

[27] С таким же успехом можно было бы написать $x = f^{-1}(y) = y - 1$ или, скажем, $z = f^{-1}(t) = t - 1$.

элементов называется *образом множества* $C$, а для произвольного $D \subset B$ множество всех прообразов всех его элементов называется *прообразом множества* $D$.

**Примеры.** Для функции $y = x + 1$ с областью определения $\mathbf{R}$ образом отрезка $[0, 1]$ является отрезок $[1, 2]$, прообразом — отрезок $[-1, 0]$. Для функции $y = x^2$ с областью определения $\mathbf{R}$ полным прообразом всякого числа $a > 0$ является двухэлементное множество $\{-\sqrt{a}, \sqrt{a}\}$ образом отрезка $\left[-1, -\frac{1}{2}\right]$ — отрезок $\left[\frac{1}{4}, 1\right]$, прообразом отрезка $\left[\frac{1}{4}, 1\right]$ — множество $\left[-1, -\frac{1}{2}\right] \cup \left[\frac{1}{2}, 1\right]$. Для функции $y = \sin x$ с областью определения $\mathbf{R}$ полным прообразом числа 1 является множество $\left\{\frac{\pi}{2} + 2\pi n \mid n = 0, \pm 1, \pm 2, \cdots\right\}$, образом отрезка $\left[0, \frac{\pi}{2}\right]$ — отрезок $[0, 1]$, прообразом отрезка $[0, 1]$ — объединение всевозможных отрезков вида $[2\pi n, \pi(2n + 1)]$, где $n = 0, \pm 1, \pm 2, \ldots$.

**Задача.** Пусть $F$ — функция с областью определения $A$ и множеством значений $B$ и пусть: $C_1, C_2 \subset A$; $D_1, D_2 \subset B$. Доказать, что: а) образ объединения $C_1$ и $C_2$ равен объединению образов $C_1$ и $C_2$; б) образ пересечения $C_1$ и $C_2$ содержится в пересечении образов $C_1$ и $C_2$; в) прообраз объединения $D_1$ и $D_2$ равен объединению прообразов $D_1$ и $D_2$; г) прообраз пересечения $D_1$ и $D_2$ равен пересечению прообразов $D_1$ и $D_2$.

Введем еще несколько важных понятий, относящихся к функциям. Пусть $F: D \to R$, т. е. $F$ есть функция, отображающая множество $D$ в множество $R$ — или, иначе, отображение $D$ в $R$. Говорят, что функция $F$ *отображает* $D$ в $R$ *взаимно однозначно*, или что *отображение* $F$ *является взаимно однозначным*, если прообразы различных элементов $R$ различны (т. е. каждый элемент $R$ имеет не более одного прообраза) — или, что то же самое, если существует функция, обратная для $F$ (можно сказать также «отображение, обратное для $F$»). Синонимы слова «взаимно однозначный»: *«одно-однозначный»*; *«инъективный»*. Вместо «взаимно однозначное» (или «инъективное») отображение говорят также *«инъекция»*.

Отображение, являющееся одновременно инъективным и сюръективным, называется *биективным* (так что фраза «отображение $F$ множества $A$ во множество $B$ биективно» означает то же, что «$F$ есть взаимно однозначное отображение $A$ на $B$» или «$F : A \xrightarrow{\text{на}} B$ и $F$ взаимно однозначно»). Вместо «биективное отображение» нередко говорят

*«биекция»*[28]. Употребляется также термин *«взаимно однозначное (или одно-однозначное) соответствие* между $A$ и $B$», означающий то же, что «взаимно однозначное отображение $A$ на $B$».

Пусть, далее, $F$ — отображение множества $A$ во множество $B$ и $G$ — отображение множества $B$ во множество $C$. Тогда каждому $x \in A$ отвечает единственное $y = F(x) \in B$, а этому $y$, в свою очередь — единственное $z = G(y) = G(F(x)) \in C$. Определим теперь новое отображение $H: A \to C$, положив для каждого $x \in A$ соответствующий образ $H(x)$ равным $G(F(x))$. Это отображение называется *композицией*[29] *отображений $F$ и $G$ или произведением отображения $F$ на отображение $G$* и обозначается $F \circ G$. Таким образом, $F \circ G(x) = G(F(x))$. Если $F : A \overset{\text{на}}{\to} B$ и $G : B \overset{\text{на}}{\to} C$, то очевидно, $F \circ G : A \overset{\text{на}}{\to} C$.

Отображение $E$ множества $A$ на себя называется *тождественным*, если $E(x) = x$ для каждого $x \in A$. Если $F : A \overset{\text{на}}{\to} B$ и $E(E')$ есть тождественное отображение $A$, соответственно $B$ на себя, то, очевидно, $E \circ F = F \circ E' = F$. Очень важно также заметить, что если $F : A \overset{\text{на}}{\to} A$ и $F$ взаимно однозначно, то $F \circ F^{-1} = F^{-1} \circ F = E$, где $E$ — тождественное отображение $A$ на себя.

Пример: подстановки.

Отображения множества $\{1, 2, \ldots, n\}$ ($n = 1, 2, \ldots$) на себя называются *подстановками степени $n$*. Если $F$ — подстановка и $F(i) = j$, говорят, что $F$ *переводит $i$ в $j$*; если при этом $i = j$ — т. е. $F$ переводит $i$ в себя,— говорят, что $F$ *оставляет $i$ на месте*. Для подстановок принят следующий весьма наглядный способ записи: числа $1, 2, \ldots, n$ выписываются в строку без повторений в каком угодно порядке и под каждым числом пишется его образ. Полученную таблицу обычно заключают в круглые скобки. Например $\begin{pmatrix} 12345 \\ 24315 \end{pmatrix} = \begin{pmatrix} 25431 \\ 45132 \end{pmatrix}$ есть подстановка пятой степени, переводящая 1 в 2, 2 в 4, 4 в 1 и оставляющая на месте 3 и 5. Такую запись подстановки мы назовем *стандартной*. Число различных стандартных записей одной подстановки степени $n$ равно числу различных строк без повторений — т. е. перестановок — из чисел $1, 2, \ldots, n$.

Всякая подстановка есть взаимно однозначное отображение. Действительно, поскольку подстановка отображает множество

---

[28] Термины «сюръекция», «инъекция», «биекция» образованы от основы пассивного причастия латинского глагола *jacio* — «бросаю» с приставками *sur-* (от французского *sur* — «на», «над»), *in-* («международная» приставка латинского происхождения, приблизительно соответствующая русской «в-»; ср. термин «инъекция» в медицине), *bi-* («международная» приставка латинского происхождения, означающая «дву-»; ср. «бицепс»). От той же основы: «объект», «субъект», «проект», «проекция».)

[29] От лат. *compositio* — «составление», «соединение».

$\{1, 2, \ldots, n\}$ на себя, в нижней строке стандартной записи присутствуют все элементы этого множества; следовательно, в ней нет повторений[30], т. е. образы различных чисел различны. Этот факт можно иначе выразить так: для всякой подстановки степени $n$ существует обратная ей подстановка степени $n$. (Заметим, что если в стандартной записи подстановки $F$ переставить строки, то получится стандартная запись подстановки $F^{-1}$.)

Задачи. (1) Выписать все подстановки 1-й, 2-й, 3-й, 4-й степени (каждую в какой-либо одной стандартной записи).

(2) Как из стандартных записей подстановок $F$ и $G$ получить стандартную запись подстановки $F \circ G$? Найти всевозможные попарные произведения подстановок 3-й степени.

(3) Принятый для подстановок способ записи можно использовать для произвольных отображений, у которых области определения и области прибытия заданы перечислением элементов. Например, отображение $F:\{1, 2, 3\} \to \{а, б, в\}$, такое, что $F(1) = F(3) = б$, $F(2) = а$, можно записать в виде $\begin{pmatrix} 123 \\ баб \end{pmatrix}$. Пользуясь этой записью: а) выписать все отображения множества $\{1, 2, 3\}$ в себя; б) выписать все отображения $\{а, б, в\}$ в $\{0, 1\}$. Какие из отображений а) и б) сюръективны?

4. Выше, в пункте 1, говоря об отношениях, мы для простоты ограничивались теми из них, в которых участвуют только два объекта. Однако в естественном языке есть и такие слова, которые выражают отношения между тремя объектами — например, д а л (кто — что — кому: Иван дал книгу Петру), н а у ч и л (кто — кого — чему: Отец научил сына грамоте), р а с с к а з а л (кто — кому — о чем: Ваня рассказал Мише о своей работе), между четырьмя — к у п и л (кто — у кого — что — почем: Иван купил у Петра корову за сто рублей), и даже между пятью — а р е н д о в а л[31] (кто — у кого — что — на какой срок — за какую плату: Смит арендовал у Джонса пять акров земли на два года за двести фунтов).

В математике также встречаются отношения между тремя, четырьмя и более объектами. Например, если $A$, $B$, $C$ — точки, лежащие на одной прямой, то фраза «$C$ лежит между $A$ и $B$» выражает определенное отношение между этими тремя точками; фраза «прямые $k$ и $l$ пересекаются в точке $A$» выражает отношение между тремя объектами, два из которых — прямые, а третий — точка; если $a$, $b$, $c$ — числа, то выражение $a + b = c$ представляет собой утверждение о том, что между данными числами имеется определенное отноше-

[30] В самом деле, если бы какое-нибудь число повторялось дважды, то для какого-то другого не хватило бы места.

[31] Пример Ю. Л. Ершова.

ние: сумма первых двух равна третьему; аналогично для выражений $a - b = c$, $a \cdot b = c$ и т. п. Отношение пропорциональности: $\frac{a}{b} = \frac{c}{d}$ — связывает уже четыре объекта.

В дальнейшем, говоря об *отношениях*, мы будем подразумевать отношения между любым числом объектов. Отношения между двумя объектами называются *бинарными*[32], или *двуместными*, между тремя объектами — *тернарными*[33], или *трехместными*; отношения, в которых участвует точно $n$ объектов, $n = 2, 3, \ldots$ называются $n$-арными или $n$-местными.

Многие понятия, введенные выше в связи с бинарными отношениями, можно непосредственно обобщить на случай произвольных отношений. Именно: для произвольного $n$-арного отношения $R$ говорят: «$x_1, x_2, \ldots, x_n$ *связаны* отношением» или «$x_1, x_2, \ldots, x_n$ *находятся* в отношении $R$»; множество, из которого берется первый (второй, третий и т. д.) из связанных отношением элементов, мы будем называть *областью первых* — соответственно *вторых*, *третьих* и т. д. — *элементов* отношения $R$; если для $n$-арного отношения $R$ области первых, вторых, ..., $n$-х элементов совпадают с одним и тем же множеством $M$, мы говорим, что $R$ *задано на множестве* $M$. *Графиком* $n$-арного отношения $R$ называется подмножество декартова произведения $M_1 \times \ldots \times M_n$, где $M_i$ $(i = 1, \ldots, n)$ — область $i$-х элементов $R$, состоящее из всех тех упорядоченных $n$-ок $(x_1, \ldots, x_n)$, для которых $x_1, \ldots, x_n$ связаны отношением $R$.

**Примеры.** 1) Для тернарного отношения «$x$ и $y$ — отец и мать $z$-а соответственно» область первых элементов есть множество мужчин, область вторых элементов — множество женщин, область третьих — множество людей.

2) Графику отношения «наибольший общий делитель чисел $x$ и $y$ равен $z$», заданного на множестве целых чисел, принадлежат, например, упорядоченные тройки (42, 60, 6), (−15, 10, 5), (3, 18, 3) и не принадлежат тройки (10, 6, 3), (−2, 4, 4).

3) График заданного на множестве действительных чисел отношения $x + y + z = u$ содержит, например, упорядоченные четверки (2, 1, 5, 8), $(\sqrt{3}, -\sqrt{3}, 0, 0)$ и не содержит четверок (2, 1, 5, 6), $\left(\frac{1}{2}, \frac{1}{2}, -1, \sqrt{2}\right)$.

Теперь мы можем обобщить также и понятие функционального отношения (функции).

$(n + 1)$-местное отношение $(n = 2, 3, \ldots)$ называется *функцио-*

[32] От лат. *bini* — «по два».

[33] От лат. *terni* — «по три».

нальным, если ни для какой упорядоченной $n$-ки $(x_1, \ldots, x_n)$ не может существовать более одного $y$, такого, что $x_1, \ldots, x_n, y$ связаны данным отношением.

Если в этом определении допустить также значение $n$, равное единице, и при $n = 1$ вместо упорядоченной $n$-ки брать просто $x_1$, то введенное в пункте 3 понятие функционального бинарного отношения окажется частным случаем введенного только что общего понятия функционального отношения. $(n + 1)$-местное функциональное отношение обычно называют *функцией* $n$ переменных[34]. В частности, функции одной переменной — это то же самое, что «просто» функции, рассматривавшиеся в пункте 3.

Иногда мы будем называть функцию $n$ переменных также $n$-местной функцией и будем говорить, что ее *вместимость* равна $n$. (Таким образом, «функция» и «функциональное отношение» — не полные синонимы: «двуместная функция» — то же, что «трехместное функциональное отношение».

Многие из введенных в пункте 3 понятий и обозначений можно теперь распространить на случай любого числа переменных. Прежде всего, *областью определения* и *множеством значений* функции (функционального отношения) $F$ называются соответственно множество тех упорядоченных $n$-ок $(x_1, \ldots, x_n)$, для которых существуют $y$, такие, что $x_1, \ldots, x_n, y$ связаны отношением $F$, и множество тех $y$, для которых существуют $x_1, \ldots, x_n$, такие, что $x_1, \ldots, x_n, y$ связаны отношением $F$. Если $n$-ка $(a_1, \ldots, a_n)$ принадлежит области определения функции $F$, то тот единственный элемент $b$ множества значений $F$, который связан с $a_1, \ldots a_n$ отношением $F$, обозначается $F(a_1, \ldots, a_n)$; саму функцию обозначают $F(x_1, \ldots, x_n)$ (читается: «$F$ от $x_1, \ldots, x_n$») или $y = F(x_1, \ldots, x_n)$, где $x_1, \ldots, x_n$ — переменные, такие, что $n$-ка $(x_1, \ldots, x_n)$ пробегает область определения $F$, и $y$ — переменная, пробегающая множество значений $F$. Переменные $x_1, \ldots, x_n$ называют здесь *независимыми переменными*, или *аргументами*, а $y$ — *зависимой переменной*. Если $x_1^0, \ldots, x_n^0$ — какие-либо значения независимых переменных $x_1, \ldots, x_n$ соответственно, то значение $y^0 = F(x_1^0, \ldots, x_n^0)$ зависимой переменной называют *значением функции* $F$, *соответствующим* значениям $x_1^0, \ldots, x_n^0$ независимых переменных.

Область $i$-х элементов $(i = 1, \ldots, n)$ функции (функционального отношения) $F(x_1, \ldots, x_n)$ иногда называют *областью изменения*

[34] Иногда говорят «функция от $n$ переменных».

*переменной* $x_i$. Чтобы задать функцию $n$ переменных, достаточно задать ее область определения и для каждой упорядоченной $n$-ки значений независимой переменной указать соответствующее значение функции.

*График* функции $y = F(x_1, \ldots x_n)$ есть, в соответствии с общим определением графика отношения (см. выше), множество тех упорядоченных систем $(a_1, \ldots, a_n, b)$, для которых справедливо равенство $b = F(a_1, \ldots, a_n)$.

Примеры. 1) Пусть $d(x, y)$ означает наибольший общий делитель целых положительных чисел $x$ и $y$. Область определения этой функции есть $\mathbf{Z}_+^2$, где $\mathbf{Z}_+$ — множество целых положительных чисел; множество ее значений есть $\mathbf{Z}_+$. Имеем, например, $d(42, 60) = 6$; $d(2, 10) = 2$; $d(5, 8) = 1$.

2) Площадь прямоугольника есть функция длин его сторон $x$ и $y$; обозначая эту функцию через $S(x, y)$, имеем: $S(x, y) = xy$. Область определения функции $S(x, y)$ есть $\mathbf{R}_+^2$, где $\mathbf{R}_+$ — множество положительных действительных чисел; ее множество значений есть $\mathbf{R}_+$.

3) Окончание русского прилагательного (точнее, полного прилагательного в положительной степени) зависит от его основы (например, основа прилагательного *белый* есть *бел-*, основа прилагательного *настольный* — *настольн-*) и четырех грамматических характеристик, по которым прилагательное согласуется с существительным: рода, одушевленности/неодушевленности, числа и падежа. Иначе говоря, окончание русского прилагательного есть функция пяти переменных $x, y, z, u, v$, где переменная $x$ пробегает множество всевозможных основ русских прилагательных (довольно обширное, но конечное и вполне обозримое), переменная $y$ пробегает множество {*муж*, *жен*, *ср*}, переменная $z$ — множество {*одуш*, *неодуш*}, переменная $u$ — множество {*ед*, *мн*} и переменная $v$ — множество {*им*, *род*, *дат*, *вин*, *тв*, *предл*}. Смысл обозначений здесь ясен. Обозначив эту функцию $Fl(x, y, z, u, v)$, мы будем иметь, например:

$Fl$(*больш-*, *муж*, *одуш*, *ед*, *вин*) = *-ого*;

$Fl$(*больш-*, *жен*, $z$, *ед*, *вин*) = *-ую* при любом значении $z$;

$Fl$(*маленьк-*, $y$, $z$, *мн*, *тв*) = *-ими* при любых значениях $y$ и $z$.

4) Если $u = f(x, y, z) = x + y + z$ — функция с областью определения $\mathbf{R}^3$, где $\mathbf{R}$ — множество действительных чисел, то $f(1, 1, 2) = 4$, $f\left(-1, \frac{1}{2}, 3\right) = \frac{5}{2}$ и т. п.

Обычно говорят просто «функция $u = x + y + z$», «функция $z = xy$» и т. п.

Заметим, наконец, что при $n > 1$ функция $n$ переменных превращается в функцию $n - 1$ переменных, если значение одной из пере-

менных фиксировано. Например, из функции трех переменных $u = x + y + z$ получаем, полагая $y = 2$, функцию двух переменных $u = x + z + 2$, а из этой последней, полагая $z = 1$, — функцию одной переменной $u = x + 3$.

**Задача.** Найти множества значений следующих функций с областью определения $\mathbb{Z}^2$, где $\mathbb{Z}$ — множество целых чисел:

(а) $z = 3(x + y)$;

(б) $z = r_3(x, y)$, где $r_3(x, y)$ — остаток от деления суммы $x + y$ на 3.

## Задачи и упражнения

1) Для каждого из следующих множеств выписать все его элементы:

(а) $\{m \mid m$ — целое, $-5 < m < 5\}$;

(б) $\{p \cdot q \mid p, q$ — простые числа, $p < 6$, $q < 10\}$;

(в) $\{x \mid x \cdot (x^2 + 2x - 8) = 0\}$;

(г) $\{k + l \mid k, l$ — положительные делители числа $12\}$.

2) По образцу равенства $\{1, 3, 5, \ldots\} = \{2n - 1 \mid n = 1, 2, \ldots\}$ найти другие способы задания для следующих множеств:

(а) $\left\{\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \ldots\right\}$;

(б) $\{0, 3, 8, 15, 24, \ldots\}$;

(в) $\{2^k + 3 \mid k = 0, 1, 2, \ldots\}$.

3) Для каждого из следующих множеств выписать все его элементы:

(а) $\{X \mid \{a, b\} \subset X \subset \{a, b, c, d\}\}$;

(б) $\{A \mid A \subset \{a, b, c, z, d\}, a \notin A, b \in A\}$;

(в) $\{A \mid A \subset \{a, b, c, z, d\}, \{a, b\} \not\subset A\}$[18].

4) (а) Каким условиям должны удовлетворять числа $a$, $b$, $c$, $d$, чтобы было $[a, b] \subset [c, d]$?

(б) Тот же вопрос для включения $(a, b) \subset (c, d)$.

(в) То же для включения $(a, b) \subset [c, d)$.

(г) То же для включения $[a, b] \subset (c, d)$.

5) Найти:

(а) $[1, 3] \cap [2, 6]$;

(б) $[1, 3] \cup [2, 6]$;

(в) $[1, 3] \setminus [2, 6]$;

(г) $[2, 6] \setminus [1, 3]$.

6) Доказать, что:

а) $[-1, 5] \setminus (0, 1] = [-1, 0] \cup (1, 5]$;

б) $([0, 2] \cup [4, 6]) \cap [1, 7) = [1, 6] \setminus (2, 4)$.

В задачах 7) — 15) требуется доказать справедливость выписанных равенств для произвольных множеств.

7) $X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$.

[18] $\not\subset$ означает «не содержится в».

8) $X\setminus(Y\cap Z) = (X\setminus Y)\cup(X\setminus Z)$.

9) $(X\setminus Z)\cap(Y\setminus Z) = (X\cap Y)\setminus Z$.

10) $X\setminus(Y\setminus Z) = (X\setminus Y)\cup(X\cap Z)$.

11) $X\cup Y = X\cup(Y\setminus X)$.

12) $X\cap Y = X\setminus(X\setminus Y)$.

13) $X\setminus(Y\setminus X) = X$.

14) $CX\cup Y = CX\cup(X\cap Y) = C(X\setminus Y)$.

15) $CX\cap Y = CX\setminus CY$.

16) Доказать, что:

а) Тогда и только тогда $X\subset Z$ и $Y\subset Z$, когда $X\cup Y\subset Z$;

б) Тогда и только тогда $X\subset Y$ и $X\subset Z$, когда $X\subset Y\cap Z$.

17) Доказать, что равенство $Y = (X\cap CY)\cup(Y\cap CX)$ равносильно $X = \varnothing$.

18) Всегда ли справедливо $(X\setminus Y)\cup Z = (X\cup Z)\setminus(Y\cup Z)$?

19) Показать на примерах, что:

а) не всегда $(X\cup Y)\cap Z = (X\cup Z)\cap Y$,

б) не всегда $(X\cap CY)\cup(Y\cap CX)\subset Y$;

в) при $X\cap Y\neq\varnothing$, $Y\cap Z\neq\varnothing$, $X\cap Z\neq\varnothing$ возможно $X\cap Y\cap Z = \varnothing$.

20) Для конечного множества $X$ будем обозначать число его элементов через $N(X)$. Доказать, что $N(X\cup Y) = N(X) + N(Y) - N(X\cap Y)$.

21) Доказать, что:

(а) $A\cap\bigcup\limits_{i=1}^{n}B_i = \bigcup\limits_{i=1}^{n}(A\cap B_i)$;

(б) $A\cup\bigcap\limits_{i=1}^{n}B_i = \bigcap\limits_{i=1}^{n}(A\cup B_i)$.

22) Доказать, что если $A_1\subset A_2\subset\ldots\subset A_n$, то $\bigcap\limits_{i=1}^{n}A_i = A_1$, $\bigcup\limits_{i=1}^{n}A_i = A_n$.

23) Пусть $N_i = \{i, i+1, i+2, \ldots\}$. Доказать, что $\bigcap\limits_{i=1}^{\infty}N_i = \varnothing$.

24) Пусть $N = \{1, 2, \ldots\}$ и для каждого $n = 0, 1, \ldots$ $N_n$ есть множество тех целых положительных чисел, которые делятся на $2^n$, но не делятся на $2^{n+1}$. Доказать, что

(а) $\bigcup\limits_{n=0}^{\infty}N_n = N$;

(б) $\bigcap\limits_{n=0}^{\infty}N_n = \varnothing$.

25) Найти и изобразить на чертеже множества точек плоскости, координаты которых принадлежат множествам:

(а) $\{-1, 0, 1, 2\}^2$;

(б) $[0, 1]\times\{0, 1\}$.

26) Доказать, что:

(а) при непустых $A_1, \ldots, A_n$ тогда и только тогда $A_1\times\ldots\times A_n\subset B_1\times\ldots\times B_n$, когда $A_1\subset B_1, \ldots, A_n\subset B_n$;

(б) при непустых $A$ и $B$ тогда и только тогда $A \times B = B \times A$, когда $A = B$.

27) Выписать все элементы областей определения, множеств значений и графиков следующих бинарных отношений:

(а) Отношения $R_1$, заданного на множестве $\mathbf{Б}$ русских букв: $xR_1y$ означает, что в слове «парапсихологический» имеется буквосочетание $xy$.

(б) Отношения $R_2$, заданного на множестве $\mathbf{Z}$ целых чисел: $xR_2y$ означает, что $x + y = x \cdot y$.

(в) Отношения $R_3$ с областью отправления $\mathbf{Б}$ и областью прибытия $\mathbf{Z}$: $xR_3y$ означает, что порядковый номер буквы $x$ в русском алфавите равен $y$ и $y$ — четное число.

28) Выписать все элементы графиков отношений, обратных отношениям предыдущей задачи.

29) Найти области определения, множества значений и графики следующих бинарных отношений, заданных на множестве действительных чисел (графики изобразить на чертеже):

(а) $S_1$: $xS_1y$ означает $x^2 < y^2$;

(б) $S_2$: $xS_2y$ означает $2x + y > 0$;

(в) $S_3$: $xS_3y$ означает, что $x < 0$ и $y < 0$;

(г) $S_4$: $xS_4y$ означает $|x| = |y|$;

(д) $S_5$: $xS_5y$ означает $x - [x] = y - [y]$.

30) Найти и изобразить на чертеже графики отношений, обратных отношениям предыдущей задачи.

31) Пусть $Q$ — бинарное отношение, заданное на множестве $\mathbf{Б}$ русских букв: $xQy$ означает, что $x$ предшествует $y$ в обычном алфавитном порядке (например, $aQб$, $aQг$). Найти число пар, принадлежащих графику $Q$.

32) Доказать, что графики взаимно обратных бинарных отношений, заданных на множестве действительных чисел, симметричны друг другу относительно прямой $x = y$.

33) Если $x$ — слово естественного языка, выражающее бинарное отношение, то слово, выражающее обратное отношение (если такое слово существует), называется *конверсивом*[16] слова $x$. Найти конверсивы слов: севернее, потомок, начальник, ученик, автор, спрашить, нравиться, радовать, дружить.

34) Какие из отношений задачи 27 функциональны?

35) Выписать все элементы графика функции, определенной на множестве порядковых номеров слов в тексте настоящей задачи, считая с начала, и такой, что для каждого слова значение функции от его номера равно числу букв в этом слове.

---

[16] От лат. *conversio* — «обращение».

36) Изобразить на чертеже графики следующих функций, определенных на множестве действительных чисел $\mathbf{R}$:

(а) $y = |x|$;

(б) $y = \begin{cases} 2x, & \text{если } x < 0 \\ x, & \text{если } x \geq 0; \end{cases}$

(в) $y = \begin{cases} x-1, & \text{если } x < 0 \\ x+1, & \text{если } x \geq 0; \end{cases}$

(г) $y = \begin{cases} -\sqrt{-x}, & \text{если } x \leq 0 \\ \sqrt{x}, & \text{если } x > 0; \end{cases}$

(д) $y = 1$.

Какие их этих функций осуществляют взаимно однозначные отображения? Какие из них отображают $\mathbf{R}$ на себя?

37) Сколько существует отображений множества {1, 2, 3, 4} в себя? Сколько существует функций, отображающих это множество в себя и не принимающих значений 1?

38) Доказать, что умножение отображений ассоциативно.

39) Пользуясь «подстановочными» обозначениями (ср. задачу (3) на с. 43) положим

$$F = \begin{pmatrix} а & б & в \\ г & д & е \end{pmatrix}, \quad G = \begin{pmatrix} а & б & в \\ б & д & а \end{pmatrix}, \quad H = \begin{pmatrix} г & д & е \\ д & е & г \end{pmatrix}.$$

Записать в тех же обозначениях: $F \circ H$; $G^2$; $H^2$; $F \circ H^2$; $G \circ F \circ H$; $F^{-1}$; $H^{-1}$; $H \circ F^{-1} \circ G$; $F \circ H \circ F^{-1}$.

40) В лингвистике принято обозначать через *Magn*[37] функцию, определенную на некотором подмножестве множества слов заданного естественного языка (например, русского), и такую, что *Magn*(*x*) есть слово, обозначающее «высокую степень» от *x*; например, *Magn*(аплодисменты) = бурные, *Magn*(плакать) = горько, *Magn*(опечаленный) = глубоко. Найти значения *Magn* от слов: уважение, свет, тьма, ненависть, храбрость, грех, спать, дурак, дождь, победа, поражение, здоровье, болезнь.

41) Выписать все элементы графиков следующих тернарных отношений, заданных на множестве целых чисел:

(а) $x + y + z = x \cdot y \cdot z$, $x \cdot y \cdot z \neq 0$;

(б) $x \cdot y \cdot z = -x \cdot y \cdot z$, $0 < |x \cdot y \cdot z| \leq 5$;

(в) $x^2 + y^2 + z^2 < 10$.

42) Сколько существует функций трех переменных:

а) с областью определения {1, 2, 3} и множеством значений {0, 1}?

(б) с областью определения {1, 2} и множеством значений {0, 1}?

---

[37] От лат. *magnus* — «большой».

ГЛАВА

2

# СИМВОЛИЧЕСКИЙ ЯЗЫК

## § 2.1. ПРЕДЛОЖЕНИЯ

1. Сейчас мы познакомимся с принятым в математической логике символическим способом записи предложений. Этот способ пригоден лишь для некоторых предложений, особенно простых в смысловом отношении. Именно: в математической логике рассматриваются только предложения, имеющие характер четко сформулированных утверждений о каких-то фактах — так что для каждого такого утверждения можно спросить, истинно оно или ложно, и на этот вопрос имеется недвусмысленный ответ «Да» или «Нет». Всякое математическое рассуждение может быть изложено так, чтобы оно состояло только из таких предложений[1]; поэтому при анализе строения математических рассуждений — что и является главной задачей математической логики — другими предложениями можно не интересоваться.

2. Теперь мы введем в рассмотрение множество, состоящее из двух элементов — русских слов «истина» и «ложь», которые будут называться *истинностными значениями* и записываться всегда сокращенно: *И*, *Л*. О каждом предложении интересующего нас типа мы будем говорить, что ему *присвоено* одно и только одно из истинностных значений: *И*, если утверждение, выражаемое данным предложением, истинно, и *Л*, если это утверждение ложно (обычно говорят просто: «предложение истинно», «предложение ложно»). Вместо «предложению присвоено истинностное значение $z$» говорят также: «Предложение имеет истинностное значение $z$» или «Истинностное значение предложения есть $z$».

[1] Хотя в действительности далеко не всегда математические рассуждения излагают таким образом.

Например, предложениям «Кит — млекопитающее», «6 — четное число», «Волга впадает в Каспийское море», «2 < 5», «2 + 2 = 4», «Россия продала Аляску Соединенным Штатам за 7,2 млн. долларов», «Каждое кубическое уравнение с действительными коэффициентами имеет действительные корни» присваивается значение *И*, а предложениям «Кит — рыба», «5 — четное число», «Днепр впадает в Балтийское море», «5 < 2», «2 + 2 = 5», «Каждое квадратное уравнение с действительными коэффициентами имеет действительные корни» — значение *Л*. Для предложения «Вчера здесь шел снег» истинностное значение зависит от того, когда и где это сказано, для предложения «Прямые $l_1$ и $l_2$ параллельны» — от того, какие прямые обозначены через $l_1$ и $l_2$; однако если известны время и место в первом случае и прямые $l_1$ и $l_2$ во втором, то истинностные значения присваиваются однозначно.

Примеры предложений, которым не имеет смысла присваивать истинностные значения: «Докажем, что прямые $l_1$ и $l_2$ параллельны», «Докажите это самостоятельно», «Кажется, вчера здесь шел снег», «Вот это удача!», «Можно войти?».

Если предложению $A$ присвоено истинностное значение $z$, мы будем писать $A \equiv z$ ($A$ может быть здесь как словесной записью предложения, так и символической.)

Например: Волга впадает в Каспийское море $\equiv$ *И*;

Кит — рыба $\equiv$ *Л*;

$2 + 2 = 4 \equiv$ *И*;

$2 + 2 = 5 \equiv$ *Л*.

В дальнейшем, говоря о предложениях, мы всегда будем подразумевать предложения, которым присвоены истинностные значения.

Замечания. 1) Говоря о наличии недвусмысленного ответа на вопрос, истинно или ложно некоторое предложение, мы имеем в виду принципиальную возможность дать такой ответ, а не фактическое его наличие при нынешнем состоянии знаний. Так, до сих пор неизвестно, истинно ли предложение: «Существует бесконечно много пар простых чисел $p_1$, $p_2$, таких, что $p_1 - p_2 = 2$» («проблема близнецов»), но ясно, что оно либо истинно, либо ложно.

2) Иногда вместо *И* пишут 1 и вместо *Л* — 0. В отдельных случаях это удобнее, но обозначения *И*, *Л* хороши тем, что напоминают о содержательном смысле истинностных значений.

3) Для обозначения предложений, которым присвоены истинностные значения, часто пользуются специальным термином — «высказывания». Однако без такого термина вполне можно обойтись.

3. В науке о языке — лингвистике, или языковедении — предложение рассматривается как частный случай языкового

знака[2]. Языковой знак есть двуплановая единица: он имеет две стороны, внутреннюю и внешнюю. Внутренняя сторона знака — это его смысл, внешняя — его материальная (т. е. звуковая или графическая[3]) форма. Смысл языкового знака соотносится с его формой по определенным законам, изучение которых составляет главную задачу лингвистики. Математическая логика тоже, в сущности, занимается изучением соотношения между смыслом и формой языковых знаков определенного вида — предложений; однако в отличие от лингвистики, стремящейся к полному и всестороннему охвату смысла, она сознательно ограничивается рассмотрением одной «составной части» смысла предложения — его истинностного значения. Такое сужение рамок исследования может показаться на первый взгляд недостатком, но на деле оно оборачивается преимуществом — благодаря упрощению задачи удается добиться исключительной ясности и точности описания[4].

Отмеченная аналогия между математической логикой и лингвистикой позволяет уяснить следующее: подобно тому, как для лингвиста предложение — это не просто последовательность звуков, а единство формы и смысла, так и для нас предложение будет представлять собой единство формы (т. е. символической записи) и истинностного значения; присвоенное предложению истинностное значение есть не что-то отдельное от него, а одна из его «сторон» — его «часть», если угодно.

Замечание. Есть и такие разделы математической логики, в которых наряду с истинностными значениями рассматриваются некоторые другие аспекты смысла предложения. Сюда относится, например, модальная логика, имеющая дело с понятиями «необходимость» и «возможность». Этих разделов мы не будем касаться.

4. Подход математической логики к изучению предложений отличается от подхода лингвистики еще в одном отношении: предложения, имеющие с лингвистической точки зрения один и тот же смысл (такие предложения называются *синонимичными*), в математиче-

---

[2] Языковыми знаками являются также словосочетания, слова, морфемы (морфемами называются минимальные значащие языковые единицы — корни, суффиксы и т. п.).

[3] Для естественных языков графическая форма вторична по отношению к звуковой.

[4] Надо сказать, что и лингвисты добились определенных успехов в анализе соотношения между смыслом и формой предложения лишь после того, как научились в какой-то степени «схематизировать» смысл. При этом известную роль сыграло использование опыта, накопленного математической логикой (см. следующий пункт). Это вполне естественно, так как схематизация и рассмотрение явлений по отдельным аспектам вообще характерны для науки (в отличие, например, от искусства, берущего явления «целиком»).

ской логике, как правило, не различаются и символически записываются одинаково[5]. Например, предложения «15 делится на 3», «Число 15 делится на число 3», «Тройка есть делитель пятнадцати», «Тройка является делителем пятнадцати», «Число 15 кратно трем» с точки зрения математической логики представляют собой одно и то же предложение.

Одной из главных задач современной лингвистики является формализация понятия смысла предложения. Наиболее естественным путем решения этой задачи представляется в настоящее время разработка универсального способа «смысловой записи» предложений, при котором синонимичные предложения либо записывались бы одинаково, либо их записи получались бы друг из друга с помощью некоторых строго определенных формальных преобразований. Излагаемый ниже символический язык, выработанный математической логикой для записи «самых простых» предложений, может рассматриваться как первое приближение — правда, еще очень не близкое — к такому универсальному способу «смысловой записи». В течение последних десятилетий лингвистами предложен ряд других приближений, идущих значительно дальше[6]. В некоторых из них непосредственно используется аппарат и символика математической логики, в других применяется иной аппарат — однако для всех этих работ символический язык математической логики прямо или косвенно служил базой, наличие которой сделало исследование возможным. В то же время лингвистика и математическая логика интересуются при изучении предложений разными вещами: лингвиста интересует, как соотносится смысл предложения с его звуковой формой, а специалиста по математической логике — как с этим же смыслом, который для него уже является формой (вспомним, что форма предложений в математической логике — это его символическая запись, а символические записи предложений с одинаковым смыслом совпадают), соотносится истинностное значение.

## § 2.2. ПРЕДИКАТЫ И КВАНТОРЫ

1. При построении символического языка для записи предложений — к чему мы сейчас и приступаем — естественно начать с предложений, устроенных наиболее просто.

[5] Имеются в виду абсолютно синонимичные предложения, полностью совпадающие по смыслу. Ниже, в начале гл. 3, мы столкнемся с более слабой «логической синонимией».

[6] См., например, [Мельчук 1974], [Падучева 1974].

Самые простые (по смысловой структуре) предложения представляют собой утверждения о том, что тот или иной «предмет» обладает каким-то свойством. В наиболее типичном случае имя «предмета» является в предложении подлежащим или группой подлежащего, а имя свойства — сказуемым или группой сказуемого. Например: «7 — простое число», «7 — составное число», «Треугольник $ABC$ — равнобедренный»; первое из этих утверждений истинно, второе ложно, третье может оказаться истинным или ложным смотря по тому, какой треугольник обозначен через $ABC$.

Рассмотрим серию предложений, утверждающих, что различные индивидуальные предметы обладают некоторым свойством, все время одним и тем же. Например:

1) 6 — четное число;
2) − 2 — четное число;
3) 5 — четное число;
4) 0 — четное число;
5) − 3 — четное число и т. п.

Предложения 1), 2), 4) истинны, 3) и 5) ложны, но устроены все эти предложения одинаково: сказуемое в них одно и то же, а подлежащим каждый раз служит обозначение некоторого конкретного целого числа. Введя переменную $x$, пробегающую множество целых чисел $\mathbf{Z}$, мы можем записать «общую схему» предложений этой серии:

(*) $x$ — четное число.

При каждом значении переменной $x$ эта схема превращается в конкретное предложение — иногда истинное и иногда ложное. Можно сказать, что схема (*) определяет функцию — мы будем обозначать ее $G$, — отображающую множество $\mathbf{Z}$ в множество предложений; для каждого целого числа $x_0$ соответствующим значением этой функции будет по определению предложение «$x_0$ — четное число». Таким образом, предложения 1), 2) и т. д. запишутся теперь как $G(6)$, $G(-2)$ и т. д. При этом имеем, пользуясь введенным на с. 52 способом записи:

$$G(6) \equiv И,\ G(-2) \equiv И,\ G(5) \equiv Л \text{ и т. п.}$$

Важно заметить, что в соответствии со сказанным в конце предыдущего параграфа мы должны отождествить схему (*) со схемами «Число $x$ — четное», «$x$ является четным числом», «$x$ есть четное число» и т. п., так что, например, «6 — четное число», «Число 6 — четное», «6 является четным числом», «6 есть четное число» — это не разные предложения, а варианты[7] одного и того же предложения, записываемого символически в виде $G(6)$.

[7] «Свободные варианты», как сказал бы лингвист.

Функцию $G$ мы определили с помощью схемы (*), которая, в свою очередь, отвечает некоторому свойству целых чисел — именно, свойству «быть четным». Аналогичным образом можно любому свойству целых чисел сопоставить функцию, отображающую $\mathbf{Z}$ в множество предложений. Например, свойству «быть нечетным» отвечает функция $U$, такая, что для любого целого $x_0$ ее значением служит предложение «$x_0$ — нечетное число» (так что $U(1) \equiv И$, $U(2) \equiv Л$ и т. п.); свойству «делиться на 5» отвечает функция $D_5$, сопоставляющая каждому целому $x_0$ предложение «$x_0$ делится на 5» (так что $D_5(5) \equiv И$, $D_5(6) \equiv Л$, $D_5(-20) \equiv И$ и т. п.).

Итак, свойство определяет серию предложений с постоянным сказуемым и переменным подлежащим, а эта серия в свою очередь определяет функцию, отображающую множество, пробегаемое «переменным подлежащим» (в наших примерах этим множеством было $\mathbf{Z}$, но ясно, что вместо него можно было бы взять любое множество), в множество предложений. Такие функции называют *предикатами*, от латинского грамматического термина *praedicatum* — сказуемое, так как именно сказуемое служит, как правило, именем свойства, определяющего эту функцию[8]. Точнее, эти функции принято называть *одноместными предикатами* — в отличие от многоместных предикатов, которые будут введены в следующем пункте. Подытоживая сказанное, получаем следующее определение:

Функция (одной переменной), отображающая произвольное непустое множество $M$ в множество предложений, называется *одноместным предикатом*, определенным на $M$.

2. Второй по сложности тип предложений (с точки зрения смысловой структуры) — это утверждения о том, что те или иные «предметы» находятся в некотором отношении. В типичном случае имя отношения является сказуемым, а имена «предметов» — подлежащим и дополнением (или дополнениями). В «математических» предложениях такой способ выражения типичен для бинарных отношений («прямая $l$ пересекает плоскость $P$», «6 делится на 3»), но есть и другие способы, в частности — с использованием однородных членов предложения («прямые $l$ и $m$ параллельны»); для тернарных отношений этот последний способ преобладает («5 и 3 дают в сумме 8», «наибольший общий делитель чисел 9 и 12 равен 3»). Широко используются также символические обозначения («$3 < 5$», «$a \in M$», «$5 + 3 = 8$», «$6 \cdot 4 = 8 \cdot 3$»); более чем трехместные отношения почти всегда записываются символически.

[8] Кроме того, сказуемое можно рассматривать как оператор, который, действуя на имя предмета, превращает его в предложение. Об истории термина «предикат» см. в § 6 гл. 6.

Рассмотрим теперь серию предложений, утверждающих, что различные индивидуальные предметы находятся в некотором отношении, все время одном и том же (для простоты — бинарном). Например:

6 делится на 3;
— 49 делится на 5;
12 делится на 7;
28 делится на 4;
— 28 делится на — 9
и т. п.

Все эти предложения устроены одинаково, хотя некоторые из них истинны, а другие ложны. Введя переменные $x$ и $y$, пробегающие множество целых чисел $\mathbf{Z}$, мы можем записать «общую схему» этой серии предложений:

(**) $x$ делится на $y$.

(Эту схему можно записать также в виде «Число $x$ делится на число $y$», или «$y$ есть делитель $x$-а», или «$y$ является делителем $x$-а», или «Число $x$ кратно числу $y$» и т. п.— ср. выше, стр. 55).

Со схемой (**) мы свяжем, по аналогии с предыдущим пунктом, функцию двух переменных $d(x, y)$ с областью определения $\mathbf{Z}^2$, значением которой для каждой пары целых чисел $x_0$, $y_0$ будет предложение «$x_0$ делится на $y_0$» (так что предложения нашей серии запишутся так $d(6, 3)$, $d(-49, 5)$ и т. д.; при этом $d(6, 3) \equiv И$, $d(-49, 5) \equiv Л$ и т. п.

Такую функцию можно ввести, очевидно, для любого отношения. Например, отношению «быть медианой» отвечает «схема предложений» «Отрезок $x$ есть медиана треугольника $y$», а с этой схемой естественно связывается функция $M(x, y)$ с областью определения $A_0 \times A_\Delta$, где $A_0$ есть множество отрезков и $A_\Delta$ — множество треугольников, такая, что ее значением для каждого отрезка $x_0$ и каждого треугольника $y_0$ служит предложение «Отрезок $x_0$ есть медиана треугольника $y_0$». Заданному на множестве натуральных чисел N отношению «быть наибольшим общим делителем (н. о. д.)» отвечает схема «число $z$ есть н. о. д. чисел $x$ и $y$»; с этой схемой связывается функция $D(x, y, z)$ с областью определения $\mathbf{N}^3$, значением которой для каждой тройки натуральных чисел $(x_0, y_0, z_0)$ является предложение «Число $z_0$ есть н. о. д. чисел $x_0$ и $y_0$» (так что $D(16, 8, 4) \equiv И$, $D(6,8, 4) \equiv Л$ и т. п.). Такие функции естественно назвать, как и рассмотренные в предыдущем пункте, *предикатами*, поскольку при словесном выражении именем отношения обычно бывает сказуемое. В отличие от одноместных предикатов предыдущего пункта эти пре-

дикаты называют *многоместными*, коикретнее — *двуместными*,[9] *трехместными* и т. п.

Итак:

Фуикция $n$ переменных ($n = 1, 2, \ldots$) с непустой областью определения, зиачениями которой служит предложения. называется *$n$-местным предикатом*.

Мы иамеренно допустили здесь и случай $n = 1$: благодаря этому определение предыдушего пункта оказывается частным случаем только что сформулированного.

Об $n$-местиом предикате мы будем говорить, что его *вместимость* равна $n$.

Если область определеиия $n$-местного предиката имеет вид $M^n$ — иначе говоря, если все независимые переменные пробегают одно и то же миожество $M$ — мы говорим, что предикат *определен на множестве $M$* (не на $M^n$!). Например, $G(x)$, $U(x)$, $D_k(x)$ (см. пункт 1), $d(x, y)$ — предикаты, определенные на $\mathbf{Z}$.

Может оказаться, что все значения предиката — истинные предложения; такой предикат называется *тождественно истинным*. Примерами могут служить определеиные иа $\mathbf{Z}$ предикаты, отвечающие свойству «делиться иа 1» и отиошению «число $x$ либо меньше, либо больше, либо равно числу $y$»; если обозиачить эти предикаты через $D_1(x)$ и $A(x, y)$ соответствеиио, получим $D_1(x_0) \equiv И$ при любом $x_0$ и $A(x_0, y_0) \equiv И$ при любых $x_0$, $y_0$. Аналогично, предикат иазывается *тождественно ложным*, если все его значения — ложиые предложения. Таковы, например, определеиные на $\mathbf{Z}$ предикаты, отвечающие свойству «делиться на 0. не будучи равным нулю» и отношеиию «число $x$ одновремеино больше и меньше числа $y$».

Если $F(x_1, \ldots, x_n)$ — предикат и $x_1^0, \ldots, x_n^0$ — какой-либо набор значений его аргументов, то истинностное значение предложения $F(x_1^0, \ldots, x_n^0)$ мы будем называть *истинностным значением предиката $F(x_1, \ldots, x_n)$*, соответствующим данному набору значений аргумеитов. (Таким образом, значения предиката следует отличать от его истинностиых зиачений; истиниостное значеиие предиката — это истинностиое значение его зиачения.) Например, для рассмотренного на с. 57 предиката $D(x.y.z)$, означающего «число $z$ есть н. о. д. чисел $x$ и $y$», значением, соответствующим тройке чисел 10, 25, 5, будет предложение «Число 5 есть н. о. д. чисел 10 и 25», а истинностным значением для той же тройки чисел — буква $И$.

Предикаты $F(x_1, \cdots, x_n)$ и $G(x_1, \ldots, x_n)$ с одной и той же областью

[9] Встречающийся иногда вариант «двухместный предикат» представляется нам неправильным. Двухместными могут быть экипажи, палатки, номера в гостиницах и т. п., но не предикаты.

определения мы будем называть *равносильными*, если для любого набора значений аргументов $x_1, \ldots, x_n$ истинностные значения $F$ и $G$ совпадают. Равносильны, например, одноместные предикаты «$x$ — неотрицательное число» и «$x$ есть квадрат некоторого действительного числа», определенные на множестве действительных чисел; то же верно для двуместных предикатов «$x$ и $y$ дают при делении на 5 одинаковые остатки» и «разность $x - y$ делится на 5», определенных на множестве целых чисел.

Равносильность предикатов $F(x_1, \ldots, x_n)$ и $G(x_1, \ldots, x_n)$ будет обозначаться так: $F(x_1, \ldots, x_n) \equiv G(x_1, \ldots, x_n)$.

**Замечания.** 1) Если в многоместном предикате фиксировать значения некоторых, но не всех, независимых переменных, получается новый предикат меньшей вместимости. Например, из предиката $d(x, y)$ — «$x$ делится на $y$»,— получаем, положив $y = 2$, одноместный предикат $d(x, 2)$, означающий «$x$ есть четное число»; из предиката $S(x, y, z)$, определенного на множестве действительных чисел и означающего $x + y = z$, получаем, полагая $z = 0$, двуместный предикат $S(x,y,0)$, означающий «$x$ и $y$ взаимно противоположны», а полагая $y = 1$ — предикат $S(x, 1, z)$ — «$z$ на единицу больше, чем $x$»; из предиката $D(x, y, z)$ — «н. о. д. чисел $x$ и $y$ равен $z$» — получаем, полагая $u = 2$ и $z = 1$, одноместный предикат $D(x, 2, 1)$, фактически означающий «$x$ есть нечетное число».

2) Мы можем теперь в математическом языке выделить некоторые аналоги частей речи. Именно: слова, словосочетания и символы, обозначающие отношения и свойства,— аналоги глаголов: «делится», «пересекает», «параллельны», «больше», «является четным», $=$, $<$, $\in$; слова, словосочетания и символы, обозначающие объекты и классы объектов,— аналоги существительных: «целое число», «прямая», «множество», 0, 1, $\pi$; аналогами местоимений служат переменные. Из примеров видно, что, скажем, «глагол» математического языка может не быть глаголом в языке естественном.

3. Следующими по сложности смысловой структуры можно считать предложения, являющиеся утверждениями о том, что все элементы заданного множества обладают заданным свойством: «всякий равносторонний треугольник является равноугольным», «всякая точка биссектрисы угла одинаково удалена от его сторон», «квадраты всех действительных чисел неотрицательны» (иначе: «всякое действительное число имеет неотрицательный квадрат») — и о том, что в заданном множестве существует элемент, обладающий заданным свойством: «существуют правильные двенадцатигранники» (иначе: «существуют двенадцатигранники, являющиеся правильными»), «существует действительное число, равное своему квадрату», «существуют действительные числа, не являющиеся корнями алгебраических уравнений с целыми коэффициентами». Для таких предложе-

ний принят следующий символический способ записи. Если $F$ — свойство элементов множества $M$ и $F(x)$ — соответствующий этому свойству предикат[10] (определенный на $M$), то предложение «все элементы множества $M$ обладают свойством $F$» — или, что то же самое, «каждый (или «любой», или «всякий») элемент множества $M$ обладает свойством $F$» — записывается в виде $\forall x\, F(x)$, а предложение «во множестве $M$ существует (или «есть», или «имеется», или «найдется») элемент, обладающий свойством $F$» — в виде $\exists x\, F(x)$. Читаются эти выражения обычно так: «Для всякого (или «для всех») $x$ $F(x)$», «Существует $x$ такое, что $F(x)$»[11]. Выражения $\forall x$ и $\exists x$ называются *квантором общности* (или *всеобщности*) и *квантором существования* соответственно. При этом обычно говорят «квантор *по* переменной $x$».

Предложение $\forall x\, F(x)$ очевидно, истинно, если $F(x)$ — тождественно истинный предикат, и ложно в противном случае, предложение $\exists x\, F(x)$ ложно, если предикат $F(x)$ тождественно ложен, в противном случае оно истинно.

Подчеркнем, что поскольку выражения $\forall x\, F(x)$ и $\exists x\, F(x)$ — не предикаты, а предложения, они в действительности не зависят от переменной $x$ (точно так же, как не зависит от $x$ выражение $\int_a^b f(x)dx$, являющееся постоянным числом; ср. также $\sum_{i=1}^{n} a_i$, $\prod_{i=1}^{n} a_i$ — эти выражения не зависят от $i$). Переменная $x$ является здесь, как говорят, *связанной*. Переменную, пробегающую множество, на котором задан предикат, можно, очевидно, обозначить и любой другой буквой; поэтому вместо $\forall x\, F(x)$ можно писать $\forall y\, F(y)$, $\forall z\, F(z)$ и т. п. (потому что предложения $\forall y\, F(y)$, $\forall z\, F(z)$ и т. п. истинны тогда и только тогда, когда истинно $\forall x\, F(x)$; ср. равенства $\int_a^b f(x)dx = \int_a^b f(y)dy = \int_a^b f(z)dz$); аналогично для квантора существования: вместо $\exists x\, F(x)$ можно писать $\exists y\, F(y)$, $\exists z\, F(z)$ и т. п.

Постановку квантора общности и квантора существования можно, очевидно, рассматривать как особые операции, каждая из которых состоит в образовании по одноместному предикату некоторого предложения.

---

[10] Обозначая свойство и предикат одной и той же буквой, мы хотим подчеркнуть, что предикат — это, в сущности, «и есть» свойство: задать свойство — значит задать предикат.

[11] Таким образом, множество $M$ явно не упоминается: это вполне естественно, так как, поскольку предикат $F$ задан, тем самым задано и множество, на котором он определен.

Пусть, например, $F_1(x)$, $F_2(x)$, $F_3(x)$, $F_4(x)$, $F_5(x)$ — предикаты, определенные на множестве многоугольников и означающие: $F_1(x)$ — «$x$ имеет столько же вершин, сколько сторон», $F_2(x)$ — «$x$ имеет диагонали», $F_3(x)$ — «$x$ не имеет диагоналей», $F_4(x)$ — «$x$ имеет больше вершин, чем сторон», $F_5(x)$ — «$x$ имеет меньше вершин, чем сторон». Тогда предложение $\forall x\, F_1(x)$ истинно, и тем более истинно $\exists x\, F_1(x)$ [12]; $\forall x\, F_2(x)$ и $\forall x\, F_3(x)$ — ложные предложения, но $\exists x\, F_2(x)$ и $\exists x\, F_3(x)$ — истинные; предложения $\exists x\, F_4(x)$ и $\exists x\, F_5(x)$ ложны, и тем более ложны $\forall x\, F_4(x)$ и $\forall x\, F_5(x)$.

Операции постановки кванторов нетрудно обобщить на случай произвольных предикатов; однако в применении к многоместному предикату результаты операций будут не предложениями, а тоже предикатами, но на единицу меньшей вместимости. Именно: для $(n+1)$-местного предиката $F(x_1, \ldots, x_n, x_{n+1})$ $(n = 1, 2, \ldots)$ выражения $\forall x_{n+1} F(x_1, \ldots, x_n, x_{n+1})$ и $\exists x_{n+1} F(x_1, \ldots, x_n, x_{n+1})$ означают соответственно следующие $n$-местные предикаты от переменных $x_1, \ldots, x_n$: «Для всякого элемента $x^0_{n+1}$ области изменения переменной $x_{n+1}$ выполняется $F(x_1, \ldots, x_n, x^0_{n+1})$; «Существует такой элемент $x^0_{n+1}$ области изменения переменной $x_{n+1}$, что выполняется $F(x_1, \ldots, x_n, x^0_{n+1})$».

То, что мы выделили именно последнюю переменную, не имеет, разумеется, никакого значения — точно так же можно определить выражения $\forall x_i F(x_1, \ldots, x_i, \ldots, x_{n+1})$, $\exists x_i F(x_1, \ldots, x_i, \ldots, x_{n+1})$ $(i = 1, \ldots, n+1)$, являющиеся $n$-местными предикатами от переменных $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$.

Примеры. 1) Пусть предикат $Q(x, y)$ определен на множестве действительных чисел и означает $x^2 = y$. Тогда $\exists x Q(x, y)$ есть предикат от переменной $y$, значения которого являются истинными предложениями для неотрицательных значений $y$ и ложными для отрицательных значений $y$. Например. $\exists x Q(x, 1) \equiv И$, $\exists x Q(x, -2) \equiv Л$.

2) Пусть $d(x, y)$ — предикат, определенный на множестве целых чисел и означающий «$x$ делится на $y$». Тогда: $\forall y\, d(x, y)$ есть предикат от $x$, значение которого при $x = 0$ есть истинное предложение, а все остальные значения — ложные предложения; значения предиката $\forall x\, d(x, y)$ — истинные предложения при $y = \pm 1$ и ложные при всех остальных $y$; предикаты $\exists x\, d(x, y)$ и $\exists y\, d(x, y)$ тождественно истинны.

3) Пусть $S_1(x, y, z)$ — предикат, определенный на множестве неотрицательных целых чисел и означающий $x + y = z$. Значения пре-

[12] Вообще из истинности предложения $\forall x\, F(x)$ вытекает истинность предложения $\exists x\, F(x)$ (поскольку область определения предиката всегда непуста).

диката $\exists y S_1(x, y, z)$ — истинные предложения при $x \le z$ и ложные при $x > z$.

К многоместному предикату операции постановки кванторов можно применять несколько раз. Их $l$-кратное применение к $n$-местному предикату даст $(n - l)$-местный предикат при $l < n$ и предложение при $l = n$: более чем $n$-кратное применение, очевидно, смысла не имеет.

Если, например, $M_1(x, y, z)$ — предикат, определенный на множестве целых чисел и означающий $xy = z$, то $\exists y M_1(x, y, z)$ — двуместный предикат, означающий «$z$ делится на $x$» (в обозначениях только что рассматривавшегося примера 2) этот предикат записывается как $d(z, x)$; предикат $\forall z \exists y M_1(x, y, z)$ становится (как уже отмечалось) истинным предложением при $x = \pm 1$ и ложным при всех остальных $x$; предложение $\exists x \forall z \exists y M_1(x, y, z)$ истинно; предложение $\forall x \forall z \exists y M_1(x, y, z)$ ложно.

Если в многоместном предикате значения некоторых переменных фиксировать, а остальные переменные, как обычно говорят, *связать* кванторами, то также, разумеется, получится предложение. Так, если $M_1$ означает то же, что в только что рассмотренном примере, то $\forall z \exists y M_1(1, y, z)$ — истинное предложение, $\forall z \exists y M_1(2, y, z)$ — ложное предложение.

**Задача.** Пусть предикаты $Q_1(x, y)$ и $Q_2(x, y)$ определены на множестве действительных чисел и означают $y < x^2$ и $x^2 + y^2 = 1$ соответственно.

а) Для каких $y$ значения предиката $\forall x Q_1(x, y)$ — истинные предложения? Истинны ли предложения: $\exists y \forall x Q_1(x, y)$? $\forall y \forall x Q_1(x, y)$?

б) Те же вопросы для предиката $\exists x Q_2(x, y)$ и предложений $\exists y \exists x Q_2(x, y)$ и $\forall y \exists x Q_2(x, y)$.

Заметим, что кванторы общности и существования не перестановочны: предложения $\forall x \exists y F(x, y)$ и $\exists y \forall x F(x, y)$ могут иметь разные истинностные значения. Например, если $M(x, y)$ — предикат, определенный на множестве действительных чисел и означающий $x < y$, то предложение $\forall x \exists y M(x, y)$ истинно (для всякого действительного числа найдется большее), но предложение $\exists y \forall x M(x, y)$ ложно (нет такого действительного числа, которое было бы больше всех действительных чисел).

**Задача.** Если $A$ — произвольное подмножество декартова произведения $M_1 \times \cdots \times M_n$, то для каждого $i = 1, \ldots, n$ множество

$$\{x_i \mid \exists x_1 \cdots \exists x_{i-1} \exists x_{i+1} \cdots \exists x_n (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) \in A\}$$

называется *i-ой проекцией* множества $A$. (Попросту говоря, $i$-я про-

екция множества $A$ — это множество $i$-ых элементов всех $n$-ок, входящих в $A$. В частности, если $n = 2$ и $M_1 = M_2 = \mathbf{R}$, где $\mathbf{R}$ — множество действительных чисел, то $A$ можно считать множеством точек плоскости; в этом случае первая и вторая проекции — это проекции на оси абсцисс и ординат соответственно в обычном геометрическом смысле.)

Найти:

а) обе проекции множества $M \subset Б^2$, где $Б$ — множество букв русского алфавита и $M$ состоит из пар $(x, y)$, таких, что в слове «соответствию» буква $x$ где-нибудь непосредственно предшествует букве $y$;

б) проекции на оси абсцисс и ординат множеств $\{(x, y) | \ x^2 + y^2 = 1\}$ и $\{(x, y) | x = y\}$ (в обоих случаях $x$ и $y$ — действительные числа).

## § 2.3. ПРОПОЗИЦИОНАЛЬНЫЕ СВЯЗКИ

1. В предыдущем параграфе мы ввели символическую запись для «простых» предложений, т. е. для тех, которые получаются из предикатов фиксированием значений переменных и связыванием переменных кванторами. Теперь мы сделаем то же самое для «сложных» предложений, образованных с помощью союзов. При этом из большого числа имеющихся в естественном языке союзов нас будут интересовать только три: «и», «или», «если»[13]; их мы «переведем» на символический язык. Перевод будет несколько схематичным, но для наших целей вполне удовлетворительным.

Начнем с союза «и». В русском языке сложное предложение, образованное с его помощью — или с помощью близкого по значению союза «а»,— истинно в том и только в том случае, когда истинны оба составляющих его простых предложения. Например, предложение «Лиса — хищное животное, и медведь больше лисы» истинно, а каждое из предложений «Лиса — хищное животное, и медведь меньше лисы», «Лиса — травоядное животное, и медведь больше лисы», «Лиса — травоядное животное, и медведь меньше лисы» ложно. предложение «Столица Англии — Лондон, а столица Франции — Париж» истинно, а каждое из предложений «Столица Англии — Стокгольм, а столица Франции — Париж», «Столица Англии —

[13] Вместо русских союзов можно было бы с таким же успехом отправляться, скажем, от немецких «und», «oder», «wenn», английских «and», «or», «if» или французских «et», «ou», «si».

Лондон, а столица Франции — Осло», столица Англии — Стокгольм, а столица Франции — Осло» ложно.

В математической логике принято для произвольных предложений «$A$» и «$B$» записывать предложение «$A$ и $B$» символически в виде $A\&B$. Это предложение называется *конъюнкцией*[14] предложений «$A$» и «$B$»; оно истинно, если оба предложения $A$, $B$ истинны, в противном случае оно ложно.

Замечание. Вместо знака & иногда используется знак $\wedge$.

Правило присвоения конъюнкции истинностного значения можно записать в виде таблицы:

| $A$ | $B$ | $A\&B$ |
|---|---|---|
| *И* | *И* | *И* |
| *И* | *Л* | *Л* |
| *Л* | *И* | *Л* |
| *Л* | *Л* | *Л* |

Здесь в каждой строке слева от вертикальной черты записана одна из четырех возможных комбинаций истинностных значений предложений $A$ и $B$, а справа — соответствующее истинностное значение предложения $A\&B$. Подобными *истинностными таблицами* мы будем широко пользоваться и впредь.

Пример. Пусть $P$ означает «дважды два — четыре», $Q$ — «снег бел», $P'$ — «дважды два — пять», $Q'$ — «снег черен». Тогда предложение $P\&Q$ истинно, а $P\&Q'$, $P'\&Q$, $P'\&Q'$ ложны.

Конечно, в реальной речи весьма маловероятно встретить предложения вроде «Дважды два — четыре, и снег бел», но объясняется это не свойствами языка, а тем, что снег и таблица умножения обычно в одном рассуждении не встречаются. Можно, впрочем, представить себе ситуацию, в которой такая фраза естественна. Вообразим, например, что некий шутник, желая разыграть своего приятеля, яростного спорщика и любителя объяснять общеизвестные истины, стал уверять его, что дважды два — пять и что снег черен. Если приятель примет это всерьез, он вполне может воскликнуть: «Да ист же, дважды два — четыре, и снег бел!».

2. Обратимся теперь к союзу «или». В русском языке этот союз имеет несколько различных значений. Из них нас будет интересовать только одно, наиболее употребительное — то, которое выступает в таких, например, предложениях: 1) «Здесь близко река или озеро» (иначе: «Здесь близко река или здесь близко озеро»); 2) «Это

[14] От латинского *conjunctio* — «соединение, связь». Символ & — стилизованное написание латинского *et* — «и».

яблоко сорвано с той или с соседней яблони» (иначе: «Это яблоко сорвано с той яблони или это яблоко сорвано с соседней яблони»); 3) «Завтра мне придется побывать в школе или в библиотеке» (иначе: «Завтра мне придется побывать в школе или завтра мне придется побывать в библиотеке»); 4) «Завтра в 10 часов вечера я буду уже в Москве или в Петербурге» (иначе: «Завтра в 10 часов вечера я буду уже в Москве или завтра в 10 часов вечера я буду уже в Петербурге»[15]. Все приведенные предложения отличаются следующей особенностью: каждое из них состоит из двух предложений — скажем, $A$ и $B$ — причем ни об $A$, ни о $B$ в отдельности говорящий не знает, истинно оно или ложно, однако он утверждает, что хотя бы одно из них истинно — а может быть, и оба. Например, предложение 1) будет признано истинным, если в действительности поблизости есть река, но нет озера, или реки нет, но есть озеро, или есть и река, и озеро; если же поблизости ни реки, ни озера нет, это предложение будет признано ложным. (Конечно, в случаях 2) и 4) $A$ и $B$ не могут быть истинны одновременно, но не потому, что «или» употреблено в них в ином значении, чем в 1) и 3), а потому, что в этих случаях несовместимы факты, выражаемые соединяемыми предложениями[16].

В математической логике предложение «$A$ или $B$», где «или» понимается в разъясненном только что смысле, записывается символически в виде $A \vee B$. Это предложение называется *дизъюнкцией*[17] предложений «$A$» и «$B$»; оно истинно, если хотя бы одно из предложений $A$, $B$ истинно, в противном случае (т. е. если $A$ и $B$ оба ложны) оно ложно.

Правило присвоения дизъюнкции истинностного значения можно записать в вид следующей истинностной таблицы:

| $A$ | $B$ | $A \vee B$ |
|---|---|---|
| И | И | И |
| И | Л | И |
| Л | И | И |
| Л | Л | Л |

[15] Из других значений союза «или» можно указать, в частности, пояснительное («Самолет, или аэроплан, есть летательный аппарат тяжелее воздуха»). Однако в этом значении «или» употребляется не для соединения предложений.

[16] Следующий пример позволяет особенно наглядно убедиться, что значение союза «или» — одно и то же в предложениях типа 1), 3) и типа 2), 4): фраза «Завтра его можно будет увидеть во Владивостоке или в Москве», если бы она была произнесена до появления реактивных самолетов, должна бы была быть причислена к типу 2), 4), но сейчас ее можно отнести к типу 1), 3).

[17] От лат. *disjunctio* — «разъединение, разобщение».

Пример. Если $P$, $Q$, $P'$, $Q'$ означают то же, что в примере после определения конъюнкции, то предложения $P \vee Q$, $P \vee Q'$, $P' \vee Q$ истинны, а $P' \vee Q'$ ложно.

Конечно, надеяться встретить в реальной речи[18] предложение «Дважды два — четыре или снег бел» еще труднее, чем «Дважды два — четыре и снег бел», и понятно, почему: как уже было сказано, союз «или» в интересующем нас значении употребляется в реальной речи для соединения предложений[19] в тех случаях, когда ни об одном из этих предложений в отдельности говорящий не знает, истинно ли оно; так что если бы мы захотели придумать ситуацию, в которой предложение «Дважды два — четыре или снег бел» могло бы быть произнесено, нам пришлось бы вообразить себе человека, не знающего, сколько будет дважды два и какого цвета снег, но берущегося рассуждать об этом.

3. Займемся теперь переводом союза «если». В русском языке он имеет два основных значения: условное и противопоставительное. Нас будет интересовать только первое — выступающее, например, в таких предложениях: 1) «Если эта книга поступила в магазин, то она поступила и в библиотеку»; 2) «Если завтра будет хорошая погода, то мы пойдем в лес»; 3) «Если он вчера не был в городе, то новость еще не дошла до него»: 4) «Если интересующий нас треугольник — прямоугольный, то мы можем воспользоваться теоремой Пифагора»; 5) «Если меня не обманывает зрение, то это Иван Иванович»[20]. В каждом из этих предложений утверждается, что некоторое предложение — скажем, $B$ — истинно при условии, что истинно некоторое другое предложение — скажем, $A$. При этом говорящий не знает, является ли $A$ в действительности истинным, или по крайней мере сомневается — или делает вид, что сомневается — в его истинности (как в 5))[21]. Как зависит здесь истинностное значение сложного предложения от истинностных значений $A$ и $B$, мы постараемся уяснить себе на примере предложения 1). Пусть некто — скажем, Иван — произнес это предложение; чтобы узнать, правду ли он ска-

[18] Не в качестве логического примера.

[19] Точнее — для соединения предложений, выражающих единичные факты. Возможно еще использование его для соединения «предложений с переменными», т. е. предикатов (об этом будет речь в следующем параграфе).

[20] Что касается противопоставительного «если», то оно означает приблизительно конъюнкцию с дополнительным значением «противопоставления», например: «Если на севере промышляли больше охотой, то на юге основу хозяйства составляло земледелие».

[21] Возможен еще случай, когда истинность $A$ — предмет спора: «Если его, как ты думаешь, не было дома, то почему же в окне горел свет?». Однако в таких случаях предложение $B$ не относится к интересующему нас типу предложений, которым имеет смысл присваивать истинностные значения.

зал, нужно выяснить, поступила ли книга в магазин и в библиотеку. При этом возможны четыре случая: а) Книга поступила и в магазин и в библиотеку; в этом случае естественно считать, что Иван сказал правду. б) Книга не поступила ни в магазин, ни в библиотеку. И в этом случае нельзя считать, что Иван сказал неправду[22]. в) Книга не поступила в магазин, но поступила в библиотеку. В этом случае также нет оснований уличить Ивана во лжи. г) Книга поступила в магазин, но в библиотеку не поступила. В этом случае Иван сказал неправду.

Таким образом, поскольку предложению «Если $A$, то $B$» должно быть присвоено истинностное значение при любом распределении значений предложений $A$ и $B$, это предложение должно получить значение $Л$ в случае, когда $A$ истинно и $B$ ложно, и значение $И$ во всех остальных случаях.

Предложение «Если $A$, то $B$» в математической логике записывается символически в виде $A \supset B$ и называется *импликацией*[23] предложений «$A$» и «$B$»; оно ложно, если $A$ истинно и $B$ ложно, а в противном случае (т. е. если либо $A$ ложно, либо $B$ истинно) оно истинно.

Предложения $A$ и $B$ часто называют соответственно *посылкой* и *заключением* импликации $A \supset B$.

Замечание. Вместо знака $\supset$ иногда используется знак $\rightarrow$.

Истинностная таблица, выражающая правило присвоения импликации истинностного значения, имеет вид:

| $A$ | $B$ | $A \supset B$ |
|---|---|---|
| $И$ | $И$ | $И$ |
| $И$ | $Л$ | $Л$ |
| $Л$ | $И$ | $И$ |
| $Л$ | $Л$ | $И$ |

Пример. Если $P$, $Q$, $P'$, $Q'$ означают то же, что в двух предыдущих примерах, то предложения $P \supset Q$, $P' \supset Q$ и $P' \supset Q'$ истинны, а $P \supset Q'$ ложно.

---

[22] Нет также оснований откладывать решение до тех пор, пока книга поступит в библиотеку — ведь в предложении 1) идет речь только о том, что было до его произнесения.

[23] От лат. *implico* — «вплетаю», «впутываю», «тесно связываю». Такой выбор названия можно объяснить тем, что здесь $A$, так сказать, «влечет за собой» $B$ («раз $A$ истинно, то и $B$ тоже») — как если бы $B$ было «привязано» к $A$. Отсюда и термин «влечет», иногда используемый для словесного выражения импликации (см. ниже, с. 72).

Разумеется, в реальной речи предложение «Если дважды два — четыре, то снег бел» не встретится — по той причине, что произносящий это должен не знать, сколько будет дважды два, да к тому же еще считать, что от результата умножения двух на два зависит цвет снега. Предложения «Если число 18 делится на 6, то оно четно», «Если число 17 делится на 6, то оно четно», «Если число 17 делится на 6, то оно нечетно» (все они истинны!) также кажутся достаточно странными — потому что всякий, кто знает, что из делимости на 6 следует четность, должен знать и о том, что 18 делится на 6, а 17 не делится. (В то же время фраза «Если число делится на 6, то оно четно» вполне естественна, так как здесь говорящему неизвестно, о каком конкретном числе идет речь, и, стало быть, неизвестно истинностное значение посылки импликации.) Однако необходимость считать такие странные предложения истинными не означает, что само понятие импликации — «странное», «неестественное» или, как иногда говорят, «парадоксальное»[24]. Ведь эти «необычные» предложения — не более чем примеры, приводимые ради лучшего уяснения «внутреннего устройства» понятия импликации; приводя такие примеры, мы как бы разглядываем понятие через увеличительное стекло — а разве не странно выглядит под увеличительным стеклом обыкновенная муха? С таким же успехом можно было бы из примитивности и искусственности текстов на первых страницах учебника иностранного языка сделать вывод, что сам этот язык примитивен и неестественен.

4. Наряду с рассмотренными тремя союзами, весьма распространенными и в обиходной речи, при изложении математических рассуждений используется «специфически математический» союз «если и только если» (иначе — «тогда и только тогда, когда». Предложение «$A$ если и только если $B$» означает, что предложения «$A$» и «$B$» эквивалентны[25], т. е. что из истинности одного из них следует истинность другого (например: «Число делится на 10, если и только если оно делится на 2 и на 5).

В математической логике предложение «$A$ если и только если $B$» записывают символически в виде $A \leftrightarrow B$ и называют *эквиваленцией* предложений «$A$» и «$B$»; оно истинно, если $A$ и $B$ оба истинны или оба ложны, и ложно в противном случае (т. е. если одно из предложений $A$, $B$ истинно, а другое ложно).

**Пример.** Если $P$, $Q$, $P'$, $Q'$ означают то же, что в предыдущих

---

[24] О конъюнкции и дизъюнкции можно сказать то же самое, но импликация вызывает обычно наибольшие затруднения.

[25] Слово «эквивалентный» (от лат. *aequus* — «равный», *valens* — «сильный») означает в обычном русском языке «вполне равноценный в каком-либо отношении», «равносильный».

примерах, то предложения $P \leftrightarrow Q$ и $P' \leftrightarrow Q'$ истинны, а $P \leftrightarrow Q'$ и $P' \leftrightarrow Q$ ложны.

В реальной речи предложение «Дважды два — четыре, если и только если снег бел», конечно, не встретится; причина этого аналогична приведенной выше для импликации.

5. Нам остается перевести на символический язык еще одно слово, дающее в естественном языке исключительно важное средство образования одних предложений из других — отрицательную частицу «не». Именно, нас будет интересовать тот случай ее употребления, когда она ставится перед сказуемым и в полученном таким образом новом предложении отрицается то, что утверждалось в старом. Например: «Он не ездил вчера в город», «Искомое число — не целое». Если исходное предложение есть $A$, то новое предложение означает «Неверно, что $A$». Это предложение в математической логике записывается символически в виде $\neg A$ и называется *отрицанием* предложения $A$.

Замечание. Вместо $\neg A$ иногда пишут $\overline{A}$; встречается также обозначение $\sim A$.

Истинностная таблица, представляющая правило присвоения отрицанию истинностного значения, имеет вид:

| $A$ | $\neg A$ |
|---|---|
| *И* | *Л* |
| *Л* | *И* |

Пример. Если $P$, $Q$, $P'$, $Q'$ означают то же, что в предыдущих примерах, то предложения $\neg P$ и $\neg Q$ ложны, а $\neg P'$ и $\neg Q'$ истинны.

Символы $\&$, $\vee$, $\supset$, $\leftrightarrow$, и $\neg$ называются *пропозициональными связками*[26].

Замечание. Значения слов естественного языка, которые мы «перевели» на наш символический язык с помощью пропозициональных связок, на самом деле гораздо богаче и сложнее значений этих последних, и «переводы» далеко не точны (кроме случая дизъюнкции, довольно точно передающей смысл русского слова «или»). Подробный анализ значений соответствующих русских слов можно найти в работах [Гладкий 1979], [Гладкий 1982], [Гладкий — Дрейзин 1983]. Однако для целей математической логики и такой схематический и неточный перевод оказывается вполне удовлетворительным.

Задача. Пусть $X$, $X'$, $Y$, $Y'$ означают соответственно: «7 — простое число», «7 — составное число», «8 — простое число», «8 — составное число».

---

[26] Т. е. «связками, связывающими предложениями» (от латинского *propositio* — «предложение»).

а) Какие из предложений $X\&Y$, $X\&Y'$, $X'\&Y$, $X'\&Y'$ истинны и какие ложны?

б), в), г) То же с заменой & на $\vee$, на $\supset$ и на $\leftrightarrow$.

д) То же для предложений $\neg X$, $\neg Y$, $\neg X'$, $\neg Y'$.

**6.** Каждой пропозициональной связке естественным образом сопоставляется некоторая операция над предложениями. Например, конъюнкции отвечает бинарная[27] операция, состоящая в образовании по двум предложениям их конъюнкции; аналогично определяются операции, отвечающие дизъюнкции, импликации и эквиваленции. Отрицанию отвечает унарная[28] операция, состоящая в образовании по предложению его отрицания. Всего мы получаем пять операций — четыре бинарных и одну унарную. Эти операции также называются *конъюнкцией, дизъюнкцией, импликацией, эквиваленцией и отрицанием.* (Таким образом, каждое из этих слов означает и операцию, и ее результат, подобно терминам «объединение» и «пересечение» в теории множеств — см. выше, с. 27-28.)

## § 2.4. ФОРМУЛЫ

1. Пусть у нас имеется произвольный набор предложений $X_1, \ldots, X_n$; мы будем называть их *элементарными предложениями* и их «внутренним устройством» пока интересоваться не будем. Будем применять к этим предложениям операции конъюнкции, дизъюнкции, импликации, эквиваленции и отрицания: к полученным предложениям будем снова применять эти операции, и т. д. В результате мы будем получать «сложные предложения», например, $X_1 \supset (\neg X_1)$, $X_1 \& (X_2 \vee X_3)$, $((\neg X) \supset (X_2 \supset X_2)) \& X_3$, $\neg(\neg X_4) \supset (\neg(X_2 \supset (X_1 \& (\neg(X_4 \supset (\neg(\neg(\neg X_3)))))))))$ и т. п. Такие выражения — составленные из элементарных предложений с помощью пропозициональных связок — называются *формулами логики предложений* (иначе — *логики суждений* или *логики высказываний*). Сами элементарные предложения также считаются формулами логики предложений.

Для упрощения записи формул логики предложений вводится соглашение о порядке действий, аналогичное принятому в арифметике. Именно, считается, что дизъюнкция связывает теснее, чем

[27] Операцию называют *бинарной* (ср. термин «бинарное отношение»), если она производится над двумя объектами.

[28] Операцию называют *унарной* (от лат. *unus* — «один») если она производится над одним объектом.

импликация и эквиваленция, конъюнкция — теснее, чем дизъюнкция, импликация и эквиваленция, а отрицание — теснее всех остальных операций. Например: $\neg X\&Y$ означает $(\neg X)\&Y$ (а не $\neg(X\&Y)$); $X\vee Y\&Z$ означает $X\vee(Y\&Z)$ (а не $(X\vee Y)\&Z$)[29] $X\vee Y\supset Z$ означает $(X\vee Y)\supset Z$ (а не $X\vee(Y\supset Z)$); $\neg X\supset\neg Y\&Z\vee X\&Y$ означает $(\neg X)\supset(((\neg Y)\&Z)\vee(X\&Y))$; $\neg(X\supset Y\&Z)\vee(X\&\neg Y\vee Z)$ означает $(\neg(X\supset(Y\&Z)))\vee((X\&(\neg Y))\vee Z)$.

**Задача.** Пусть $X$ означает «В огороде бузина», $Y$ — «В Киеве дядька».

а) Записать с помощью формул логики предложений: а1) В огороде бузина, а в Киеве дядька; а2) Если неверно, что в огороде нет бузины, то или в Киеве дядька, или в огороде бузина; а3) Неверно, что если в Киеве нет дядьки и в огороде нет бузины, то или в огороде бузина, или неверно, что в Киеве нет дядьки; а4) Если неверно, что если неверно, что если неверно, что в Киеве дядька, то в огороде бузина, то в огороде бузина, то в огороде бузина.

б) Записать по-русски: б1) $\neg X\supset\neg Y$; б2) $\neg(X\supset Y)\supset X\&\neg X$; б3) $(Y\vee X)\&\neg Y\supset X$; б4) $\neg(\neg(\neg X\supset Y)\supset Y)\supset Y$.

2. В отличие от естественных языков, для которых основной формой[30] является устная (звуковая), для символического языка математической логики основная форма — письменная (графическая). Однако существует и «устная форма» этого языка: его выражения иногда приходится читать вслух. Поэтому мы остановимся на правилах чтения формул логики предложений. Правила эти зависят от естественного языка, которым пользуется читающий, и строятся они таким образом, чтобы получаемые при чтении выражения как можно лучше гармонировали со строем этого языка.

Для русского языка можно предложить следующие правила.

**Основные правила.** 1) Для формулы[31] вида $X$, $Y$, $X_1$ и т.п. единственное допустимое прочтение — «икс», «игрек», «икс-один» и т.п. соответственно.

2) Формулу $\underbrace{\neg\neg\ldots\neg X}_{n\text{ раз},\ n\geq 1}$ можно читать $\underbrace{\text{не}-\text{не}-\ldots\text{не икс}}_{n\text{ раз}}$ (аналогично для $\neg\neg\ldots\neg Y$, $\neg\neg\ldots\neg X_1$ и т. п.).

3) Если $A$ — какое-либо допустимое прочтение формулы $\mathfrak{A}$, то формулу $\neg\mathfrak{A}$ можно читать «неверно, что $A$».

4) Если $\mathfrak{A}$, $\mathfrak{B}$ — любые формулы и $A$, $B$ — какие-либо их допустимые прочтения, то формулу $\mathfrak{A}\&\mathfrak{B}$ можно читать «$A$ и $B$», формулу $\mathfrak{A}\vee\mathfrak{B}$ — «$A$ или $B$», формулу $\mathfrak{A}\supset\mathfrak{B}$ — «если $A$, то $B$», формулу $\mathfrak{A}\leftrightarrow\mathfrak{B}$ — «$A$, если и только если $B$».

---

[29] Аналогично тому, как в арифметике $a+b\cdot c$ означает $a+(b\cdot c)$, а не $(a+b)\cdot c$.

[30] Для многих из них — единственной.

[31] В этом и следующем пунктах слово «формула» всегда будет означать формулу логики предложений.

Дополнительные правила. 1) Формулу $\mathfrak{A} \supset \mathfrak{B}$ можно читать также «Из того, что $A$, следует, что $B$», или «Из $A'$ следует, что $B$», или «Из того, что $A$, следует $B'$», или «Из $A'$ следует $B$» или «то, что $A$, влечет $B'$», или «$A'$ влечет $B'$», где $A$, $B$ — любые прочтения формул $\mathfrak{A}$, $\mathfrak{B}$, а $A'$, $B'$ — «номинализованные формы»[32] этих формул, определяемые следующим образом:

а) Если формула $\mathfrak{A}$ прочтена по основным правилам без использования слов «неверно» и «если», такое прочтение является номинализованной формой формулы $\mathfrak{A}$.

б) Если формула $\mathfrak{C}$ имеет вид $\mathfrak{A}\&\mathfrak{B}$, соответственно $\mathfrak{A} \vee \mathfrak{B}$, $\mathfrak{A} \supset \mathfrak{B}$, $\mathfrak{A} \leftrightarrow \mathfrak{B}$ и $C$ — любое прочтение формулы $\mathfrak{C}$, то выражение «конъюнкция $C$», соответственно «дизъюнкция $C$», «импликация $C$», «эквиваленция $C$» является номинализованной формой формулы $\mathfrak{C}$.

Например, выражение «импликация "если игрек, то неверно, что не зет или икс" — номинализованная форма формулы $Y \supset \neg(\neg Z \vee X)$.

в) Если $\mathfrak{A}$, $\mathfrak{B}$ — любые формулы и $A'$, $B'$ — их номинализованные формы, то выражения «конъюнкция $A'$ и $B'$», «дизъюнкция $A'$ и $B'$», «импликация $A'$ и $B'$», «эквиваленция $A'$ и $B'$», «отрицание $A'$» являются номинализованными формами формул $\mathfrak{A}\&\mathfrak{B}$, $\mathfrak{A} \vee \mathfrak{B}$, $\mathfrak{A} \supset \mathfrak{B}$, $\mathfrak{A} \leftrightarrow \mathfrak{B}$ и $\neg\mathfrak{A}$ соответственно. При этом, если выражение $A'(B')$ склоняется, оно должно стоять в родительном падеже.

Например, выражение «дизъюнкция не икс и импликации игрека и зета» есть номинализованная форма формулы $\neg X \vee (Y \supset Z)$. (Названия букв $X$, $Y$, $Z$ склонять не обязательно.)

Не рекомендуется, однако, читать «из того, что $A$», «то, что $A$», «что $B$» в случае, когда $A$, соответственно $B$, является одновременно номинализованной формой формулы $\mathfrak{A}$ ($\mathfrak{B}$). Например, формулу $X \vee Y \supset \neg(Z\&X)$ можно прочесть «Из икс или не игрек следует, что неверно, что зет и икс», но не рекомендуется читать «Из того, что икс или не игрек...»

2) Формулу $\mathfrak{A} \leftrightarrow \mathfrak{B}$ можно читать также «то, что $A$, эквивалентно тому, что $B$», или «$A'$ эквивалентно тому, что $B$», или «то, что $A$, эквивалентно $B'$», или «$A'$ эквивалентно $B'$», где $A$, $B$, $A'$, $B'$ означают то же, что в (дополнительном) правиле 1), с теми же ограничениями на чтение «то, что $A$» и «тому, что $B$».

3) В основном правиле 1) и в дополнительных правилах 1) и 2) одно из выражений $A$, $B$ или оба можно заменять выражением «имеет место (или «выполняется», или «справедливо») $A'$ (соответственно $B'$)», где $A'(B')$ — номинализованная форма формулы $\mathfrak{A}$ (соответственно $\mathfrak{B}$). Формулу $\neg\mathfrak{A}$ можно читать также «не имеет места (или «не выполняется») $A'$», где $A'$ имеет тот же смысл.

Например, формулу $\neg\neg(X \vee Y) \supset Z$ можно прочесть «Если неверно, что не выполняется дизъюнкция икса и игрека, то зет».

Любую формулу можно прочесть, пользуясь только основными правилами, но использование дополнительных правил часто позволяет получать более понятные и естественное звучание выражения — прежде всего за счет разнообразия в чтении одних и тех же связок. Например, формула

[32] От латинского nomen — «имя».

$((X \supset Y) \supset Z) \supset (\neg(X \vee \neg Y) \supset \neg Z)$ допускает чтение «Если если если $X$, то $Y$, то $Z$, то если неверно, что $X$ или не $Y$, то не $Z$», но гораздо лучше сказать «Если из того, что $X$ влечет $Y$, следует $Z$, то из отрицания дизъюнкции "$X$ или не $Y$" следует не $Z$». (Ср. также задачу на стр. 71; как записать более понятно предложение а4) из этой задачи?) Впрочем, очень громоздкие формулы обычно не читают словами.

3. Каждая формула логики предложений представляет собой предложение, истинностное значение которого зависит от истинностных значений входящих в формулу элементарных предложений. Эта зависимость для каждой формулы может быть представлена с помощью *истинностной таблицы*, аналогичной приведенным в § 3 таблицам для пропозициональных связок. Например, для формулы $\neg(X_1 \supset \neg X_2)$ истинностная таблица имеет следующий вид:

| $X_1$ | $X_2$ | $\neg(X_1 \supset \neg X_2)$ |
|---|---|---|
| *И* | *И* | *И* |
| *И* | *Л* | *Л* |
| *Л* | *И* | *Л* |
| *Л* | *Л* | *Л* |

Действительно: а) Если $X_1$ и $X_2$ истинны, то $\neg X_2$ ложно, поэтому $X_1 \supset \neg X_2$ ложно и, значит, $\neg(X_1 \supset \neg X_2)$ истинно; б) если $X_1$ истинно, а $X_2$ ложно, то $\neg X_2$ истинно, $X_1 \supset \neg X_2$ истинно и $\neg(X_1 \supset \neg X_2)$ ложно; в) если $X_1$ ложно, то $X_1 \supset \neg X_2$ истинно при любом $X_2$, и $\neg(X_1 \supset \neg X_2)$ ложно.

Другой пример: истинностная таблица для формулы $(X_1 \supset X_2) \& \neg(X_2 \vee X_1)$ имеет вид:

| $X_1$ | $X_2$ | $(X_1 \supset X_2) \& \neg(X_2 \vee X_1)$ |
|---|---|---|
| *И* | *И* | *Л* |
| *И* | *Л* | *Л* |
| *Л* | *И* | *Л* |
| *Л* | *Л* | *И* |

Легко убедиться, что таблица записана верно, непосредственно «вычислив» значение формулы для каждого из четырех наборов значений $X_1$ и $X_2$ — *ИИ*, *ИЛ*, *ЛИ*, *ЛЛ*. Например, для набора *ИИ* дизъюнкция $X_2 \vee X_1$ принимает значение *И*, а ее отрицание $\neg(X_2 \vee X_1)$ — значение *Л*, поэтому конъюнкция $(X_1 \supset X_2) \& \neg(X_2 \vee X_1)$ ложна (так что значение импликации $X_1 \supset X_2$ вычислять не нужно).

Приведем пример построения истинностной таблицы для формулы, содержащей три элементарных предложения $X_1$, $X_2$, $X_3$. В этом случае таблица имеет 8 строк: всевозможных наборов истинностных значений предложений $X_1$, $X_2$ имеется 4, и каждый из них может сочетаться с двумя значениями предложения $X_3$. (Читателю предоставляется доказать, пользуясь методом математической индукции, что для произвольного $n = 1, 2, \ldots$ число всевозможных наборов истинностных значений предложений $X_1$, $X_n$ равно $2^n$.) При составлении истинностных таблиц удобно располагать наборы значений элементарных предложений («слова» из букв *И*, *Л*) в лексикографическом порядке, т. е. так, как располагают слова в обычных словарях[33] (так мы поступали и при $n = 2$). При этом расположении строк для формулы $\neg(X_2 \vee \neg X_1) \supset X_1 \& X_3$ получаем следующую таблицу:

| $X_1$ | $X_2$ | $X_3$ | $\neg(X_2 \vee \neg X_1) \supset X_1 \& X_3$ |
|---|---|---|---|
| *И* | *И* | *И* | *И* |
| *И* | *И* | *Л* | *И* |
| *И* | *Л* | *И* | *И* |
| *И* | *Л* | *Л* | *Л* |
| *Л* | *И* | *И* | *И* |
| *Л* | *И* | *Л* | *И* |
| *Л* | *Л* | *И* | *И* |
| *Л* | *Л* | *Л* | *И* |

Последний столбец может быть заполнен путем непосредственного «вычисления» для каждой строки. Можно, однако, значительно упростить эту процедуру, заметив, что, во-первых, если предложения $X_1$ и $X_3$ оба истинны, то импликация имеет истинное заключение и поэтому истинна, и, во-вторых, если $X_2$ истинно или $X_1$ ложно, то импликация также истинна, так как имеет ложную посылку. Остается произвести непосредственное «вычисление» для одной строки — той, где $X_1$ истинно, $X_2$ ложно и $X_3$ ложно.

Вот еще один пример того, как можно упростить составление истинностной таблицы: для формулы $X_1 \& (X_2 \supset X_3) \supset (X_1 \supset X_3)$ можно заметить, что если $X_1$ ложно или $X_3$ истинно, то импликация $X_1 \supset X_3$ истинна и, значит, истинна вся формула, если же $X_1$ истинно, а $X_3$ ложно, то импликация $X_1 \supset X_3$ ложна, а импликация $X_2 \supset X_3$ и вместе

[33] Вообще в русском языке слово «лексикографический» (от греческого λεξικον — «словарь») означает «относящийся к составлению словарей».

с ней конъюнкция $X_1\&(X_2\supset X_3)$ — а значит и вся формула — истинна при ложном $X_2$ и ложна при истинном $X_2$.

Задача. Составить истинностные таблицы для формул:

а) $\neg(\neg X_1\vee\neg X_2)$;

б) $(X_1\&X_2)\vee X_3$;

в) $(X_1\supset\neg X_2)\supset\neg(X_1\vee X_2)\&\neg X_3$;

г) $(X_1\supset X_2)\&(\neg X_3\supset\neg X_3)$.

**4.** Пропозициональные связки, введенные в § 2.3 для связывания предложений, можно использовать и для связывания предикатов. Именно, пусть $F(x_1, ..., x_n)$ и $G(x_1, ..., x_n)$ $(n = 1, 2, ...)$ — произвольные предикаты с областью определения $M_1\times\cdots\times M_n$. Для каждой упорядоченной $n$-ки значений переменных $(x_1^0, ..., x_n^0)\in M_1\times\cdots\times M_n$ предикат $F(x_1, ..., x_n)$ при подстановке на место каждого $x_i$ соответствующего $x_i^0$ превращается в предложение $F(x_1^0, ..., x_n^0)$; то же имеет место для предиката $G(x_1^0, ..., x_n^0)$. Естественно назвать *конъюнкцией предикатов* $F(x_1, ..., x_n)$ и $G(x_1, ..., x_n)$ и обозначить $F(x_1, ..., x_n)\&\ \&G(x_1, ..., x_n)$ предикат, значением которого для каждой $n$-ки $(x_1^0, ..., x_n^0)\in M_1\times\cdots\times M_n$ служит предложение $F(x_1^0, ..., x_n^0)\&\ \&G(x_1^0, ..., x_n^0)$. То же самое слово в слово можно повторить для дизъюнкции, импликации, эквиваленции и отрицания.

Пример 1. Пусть $D_n(x)$ $(n = 1, 2, 3, ...)$ — предикат, определенный на множестве целых чисел и означающий «$x$ делится на $n$». Тогда: $D_2(x)\&D_3(x)$ — предикат, означающий «$x$ делится на 2 и на 3» (дающий истинные предложения для тех и только для тех $x$, для которых $D_6(x)\equiv И$); $D_2(x)\vee D_3(x)$ — предикат, означающий «$x$ делится на 2 или на 3» (значения которого являются истинными предло-жениями, например, для $x = 2, 3, 4, 6, 8$ и ложными для $x = 1, 5, 7, 11, 35$); $D_2(x)\supset D_3(x)$ — предикат, означающий «если $x$ делится на 2, то $x$ делится на 3» (дающий истинные предложения, например, для $x = 1, 3, 5, 6, 7, 9, 11, 12$ и ложные для $n = 2, 4, 8, 10, 14$); $D_6(x)\supset D_3(x)$ — предикат, означающий «если $x$ делится на 6, то $x$ делится на 3» (тождественно истинный); $\neg D_2(x)$ — предикат, означающий «$x$ не делится на 2».

Предикаты можно соединять пропозиционными связками и тогда, когда они зависят не от одних и тех же переменных (так что от некоторых переменных зависит только первый предикат, от некоторых — только второй и от некоторых — оба; общих переменных может и не быть). При этом получается предикат, зависящий от всех

тех переменных, от которых зависит хотя бы один из соединяемых предикатов.

**Пример 2.** Пусть $M(x, y)$ — предикат, определенный на множестве действительных чисел $\mathbf{R}$ и означающий $x < y$. Тогда: $M(x, y)\&M(y, z)$ есть предикат, означающий $x < y < z$; $(M(x, y)\&M(y, z)) \vee (M(z, y)\&M(y, x))$ — предикат, означающий «$y$ расположено между $x$ и $z$».

**Пример 3.** Пусть $Pl(x)$ и $Mi(x)$ — предикаты, определенные на $\mathbf{R}$ и означающие $x > 0$ и $x < 0$ соответственно. Тогда $(Pl(x)\&Pl(y)) \vee (Mi(x)\&Mi(y))$ — предикат, означающий «$x$ и $y$ имеют одинаковые знаки»; $\neg(Pl(x) \vee Mi(x)) \vee \neg(Pl(y)) \vee Mi(y))$ — предикат, означающий «хотя бы одно из чисел $x$, $y$ равно нулю».

**Пример 4.** Если $D_2(x)$ означает то же, что в примере 1, то $(D_2(x)\&D_2(y)) \vee (\neg D_2(x)\&\neg D_2(y))$ означает «$x$ и $y$ имеют одинаковую четность».

Итак, мы имеем теперь семь операций, с помощью которых можно образовывать из предикатов новые предикаты и предложения: пять операций, соответствующих пропозициональным связкам, и две операции постановки кванторов. Выражения, образованные с помощью этих операций из предикатов, «внутренним строением» которых мы не интересуемся (эти предикаты мы будем называть элементарными) называются *формулами логики предикатов* (далее мы называем их просто *формулами*). Например, если $F_1(x, y, z)$, $F_2(x, y, z)$, $G(x, y)$, $H(x, y)$, $P(x)$, $Q(x)$ — элементарные предикаты, то следующие выражения являются формулами:

а) $F_1(x_1, x_2, x_3) \supset P(x_4)$;

б) $\forall x \exists z F_2(x, y, z) \vee \neg H(u, v)$;

в) $\exists y \neg \exists z F_1(z, y, y) \supset \neg \forall z(\neg P(z)\&\exists x G(x, z))$;

г) $\exists v(F_1(u, v, t)\&Q(v) \supset \forall x \neg P(x))$;

д) $\exists x(G(x, y) \leftrightarrow \forall y(F_1(x, y, z) \vee F_2(u, v, y)))$;

е) $\neg \forall x \neg \forall y(F_1(x, y, z) \vee \neg F_1(z, y, x)\&F_1(t, t, t))$.

Здесь и далее при записи формул мы пользуемся сформулированным на стр. 71 соглашением о порядке действий, к которому теперь добавляется еще один пункт: кванторы связывают теснее, чем конъюнкция, дизъюнкция, импликация и эквиваленция.

Для каждого входящего в формулу квантора тот предикат (иначе — та часть формулы), к которому этот квантор относится, называется его *областью действия*. Например, в формуле в) область дей-

ствия первого квантора есть $\neg\exists z F_1(z, y, y)$, второго — $F_1(z, y, y)$, третьего — $\neg P(z)\&\exists x G(x, z)$, четвертого — $G(x, z)$.

О вхождениях переменной, по которой берется квантор, в его область действия говорят, что они *связаны* этим квантором. Например, в формуле в) первый квантор связывает два вхождения $y$, второй — одно вхождение $z$, третий — два вхождения $z$ и четвертый — одно вхождение $x$. Те вхождения переменных, которые связаны кванторами, а также вхождения переменных в сами кванторы называются *связанными* вхождениями переменных в данную формулу; остальные вхождения переменных в формулу называются *свободными*. Например, формула д) содержит три связанных и одно свободное вхождение $y$, три связанных вхождения $x$ и по одному свободному вхождению $z$, $u$ и $v$; в формуле а) все вхождения переменных — свободные, в в) — все связанные.

Говорят, что переменная является в некоторой формуле *свободной*, соответственно *связанной*, если в данной формуле имеются свободные, соответственно связанные вхождения этой переменной. Например, в формуле г) переменные $u$ и $t$ — свободные, $v$ и $x$ — связанные; в формуле д) переменная $y$ является и свободной, и связанной.

Формула, не содержащая свободных переменных, называется *замкнутой*.

Поскольку при связывании переменной в предикате квантором предикат перестает зависеть от этой переменной (см. с. 60), каждая замкнутая формула представляет собой предложение, а незамкнутая — предикат, зависящий от ее свободных переменных (и только от них!). Например, формула а) выражает четырехместный предикат (от переменных $x_1$, $x_2$, $x_3$, $x_4$), формула с) — двуместный (от $z$ и $t$), формула в) — предложение.

В дальнейшем нам будет иногда полезно следующее обозначение: для произвольной формулы $\mathfrak{A}$ мы будем обозначать через $\mathfrak{A}|_y^x$ формулу, полученную из $\mathfrak{A}$ заменой всех свободных вхождений переменной $x$ вхождениями переменной $y$ (если $\mathfrak{A}$ не содержит свободных вхождений $x$, то $\mathfrak{A}|_y^x = \mathfrak{A}$).

**5.** Чтобы сформулировать правила чтения формул логики предикатов, введем сначала следующие термины.

Формулу вида $F_n(x_1, \ldots, x_n)$, где $F$ — элементарный предикат и $x_1, \ldots, x_n$ — переменные ($n = 1, 2, \ldots$), назовем атомной.

Будем говорить, что формула *начинается с квантора*, если она имеет вид $\forall x\mathfrak{A}$ или $\exists x\mathfrak{A}$ ($x$ — переменная), причем областью действия квантора является «вся остальная часть» формулы (например, формула $\forall x(F(x)\&G(x))$ начинается с квантора, а $\forall x F(x)\&G(x)$ — нет). Аналогич-

ным образом будет употребляться выражение *«формула начинается с отрицания»*.

Теперь можно сформулировать правила чтения следующим образом.

Основные правила. 1′) Атомные формулы читаются в соответствии с общим правилом чтения обозначений функций (см. с. 37 и 45).

Например, $F(x, y)$ читается «эф от икс, игрек».

2′) Если $A$ какое-либо допустимое прочтение формулы $\mathfrak{A}$, то формулу $\forall x\mathfrak{A}$ можно читать «для всякого (или «для каждого», «для любого», «для всех») $xA$», формулу $\exists x\mathfrak{A}$ — «существует (или «найдется») $x$ такое, что $A$''»

3′) Если $A$ — какое-либо допустимое прочтение формулы $\mathfrak{A}$, то формулу $\neg\mathfrak{A}$ можно читать «неверно, что $A$», а если $\mathfrak{A}$ атомная или начинается с квантора или отрицания — также «не $A$» (причем, если $\mathfrak{A}$ начинается с квантора существования, нужно читать: «не существует $x$ такого, что ...»).

4′ Это правило дословно совпадает с правилом 4) на с. 71.

Дополнительные правила получаются из дополнительных правил на с. 72, если пункт а) определения номинализованной формы заменить следующим:

а′) Если формула образована из атомных с помощью операций конъюнкции, дизъюнкции и отрицания и прочтена по основным правилам без использования слова «неверно», такое прочтение является ее номинализованной формой.

Пример. Формулу в) на с. 76 можно прочесть: «Если существует $y$ такое, что не существует $z$ такого, что $F_1(z, y, y)$, то не для всякого $z$ имеет место конъюнкция "не $P(z)$ и существует $x$ такое, что $G(x, z)$"».

**Замечания.** 1) Если несколько одноименных кванторов стоят подряд, допустимо сокращенное чтение: например, $\exists x\exists y\exists z$ читается «Существуют $x$, существует $y$ и существует $z$, такие, что» или «Существуют $x$, $y$ и $z$ такие, что»; $\forall x\forall y\forall z$ читается «для любых $x$, $y$ и $z$».

2) В формулах логики предикатов для эквиваленции допустимо и даже предпочтительно чтение «тогда и только тогда, когда» (в формулах логики предложений такое чтение не рекомендуется, так как слова «тогда» и «когда» подразумевают наличие более чем одной возможности).

3) Если в качестве элементарных выступают широко употребительные предикаты, имеющие стандартные обозначения (такие, как $x = y$, $x < y$ и т.п.), эти обозначения обычно сохраняются и в формулах логики предикатов (например, вместо $\exists z M(z, y)$, где $M(z, y)$ означает $z < y$, пишут просто $\exists z(x < y)$; дальнейшие примеры см. в следующем пункте). Тогда формулы становятся, в сущности, сокращенными записями обычных математических формулировок, и при чтении их должны получаться правильные русские предложения. Чтение по нашим правилам дает именно такой результат, если добавить к ним следующую оговорку: формула, в которой для элементарных предикатов используются «обычные», не функциональные обозначения, никогда не совпадает со своей номинализованной формой.

4) В повествовательной речи в предложениях с союзом «если» посылка нередко стоит после заключения («Мы пойдем в лес, если будет хорошая

погода»). Однако при чтении логических формул такой порядок не допускается. Более того, он за редкими исключениями невозможен и в обычных формулировках математических утверждений.

Дело в том, что в русском предложении на первом месте обычно стоит так называемая т е м а, т. е. «отправная точка» для развертывания сообщения. (То, что об этой «отправной точке» сообщается, составляет вторую часть предложения — р е м у: тема — это, грубо говоря, «старое, известное», р е м а — «новое».) Однако в импликативных формулировках математических утверждений темой практически всегда служит посылка (анализ причин этого явления увел бы нас далеко за пределы математики).

Тем не менее «словесные импликации» с заключением впереди посылки нередки в математических текстах: так очень часто формулируют **определения**, строение которых мы сейчас вкратце охарактеризуем.

В отличие от математических утверждений, в которых, как показывает само их название, что-то у т в е р ж д а е т с я о некоторых объектах, считающихся заранее заданными, в определениях в в о д я т с я н о в ы е о б ъ е к т ы, представляющие собой конструкты, образованные из старых (или определенные частные случаи старых), и этим новым объектам д а ю т с я и м е н а. Стандартная форма определения имеет приблизительно следующий вид:

«Если $X$ образован ("получается") таким-то способом из $A$, $B$, $C$, ...,
или
«Если $X$ обладает такими-то свойствами,
или
«Если $X$ находится в таких-то отношениях к $A$, $B$, $C$, ...,

то $X$ называется $N$»
или
то $X$ есть по определению $N$»

Здесь $A$, $B$, $C$ — старые объекты, $X$ — переменная, обозначающая новый объект, $N$ — имя нового объекта.

Например:

«Если число $x$ получается из числа $a$ умножением его на себя, то $x$ называется квадратом числа $a$»;

«Если натуральное число отлично от единицы и делится только на единицу и на себя, оно называется простым»;

«Если возведение числа в степень $n$ дает $a$, то это число называется корнем степени $n$ из $a$».

(Роль переменной $X$ во втором примере играет словосочетание «натуральное число», в третьем — слово «число».)

Таким образом, математическое определение представляет собой импликацию, условие которой есть обычное математическое утверждение о каких-то объектах, в то время как заключение математическим утверждением не является: в нем только сообщается имя некоторого объекта,

описанного в условии[34]. Но когда определение входит в состав связного математического текста, та его часть, где сообщается имя, нередко оказывается темой и ставится поэтому на первое место, например: «Одним из важнейших понятий теории чисел является понятие простого числа. Натуральное число называется простым, если оно отлично от единицы и делится только на единицу и на себя», или: «Корни. Число $x$ называется корнем степени $n$ из $a$, если $x^n = a$». Вместо «называется» часто говорят «есть по определению», причем слова «по определению» большей частью для краткости опускаются, а иногда исчезает и «есть», заменяясь на тире. Так возникают формулировки вроде «Натуральное число — простое, если оно отлично от единицы и делится только на единицу и на себя», «Число $x$ есть корень степени $n$ из $a$, если $x^n = a$» и т. п.[35]

6. Теперь мы можем подвести итог всему сделанному. Мы построили символический язык, в котором предложения имеют вид математических формул. Этот язык хорошо приспособлен для записи математических предложений (а также любых других, содержание которых достаточно просто и может быть выражено в точных терминах). Особенно удобно пользоваться символическим языком для записи сложных формулировок — таких, например, как определения важнейших понятий математического анализа: предела функции, непрерывности и т.п. (см. ниже пример 4) — поскольку в этих случаях символическая запись позволяет лучше понять структуру формулировок. Для сплошной записи математических текстов символическим языком не пользуются, так как это сделало бы их чересчур громоздкими и неудобочитаемыми. Главное же достоинство символического языка состоит в том, что он позволяет логические связи между предложениями представлять в виде математических соотношений, а вывод одних предложений из других — т. е. рассуждение — в виде последовательности математических выкладок.

Сейчас мы проиллюстрируем на примерах представление предикатов с помощью формул и запись предложений на символическом языке (точнее, на языке логики предикатов). При этом для некоторых широко употребительных предикатов мы будем пользоваться не функциональными обозначениями, а обычной записью, принятой в математике. Кроме того, иногда мы будем подставлять в предикаты

[34] Таким образом, истинностное значение заключения — а тем самым и всей импликации — зависит здесь не от объективных свойств «вещи», как в случае математического утверждения, а от соглашения о том, как назвать эту «вещь».

[35] Заметим еще, что в формулировках определений на вновь вводимый термин падает так называемое логическое ударение, выражаемое в произношении особой интонацией, а на письме очень часто подчеркиванием, жирным шрифтом, разрядкой и т. п. В кратких формулировках типа «Натуральное число — простое, если ...» логическое ударение особенно сильное.

вместо переменных выражения вида $x + y$, $x + y + z$, $xy$, $(xy)z$ и т. п., образованные из переменных с помощью символов функций. Без этого можно было бы обойтись, но тогда пришлось бы вводить дополнительные предикаты, что сильно усложнило бы формулы.

**Пример 1.** Возьмем в качестве элементарного единственный предикат $x = y$, определенный на множестве натуральных чисел.

Выразим через этот предикат равенства некоторые арифметические предикаты, используя при этом также функцию $xy$ (произведение $x$ на $y$).

а) Предикат $d(x, y)$ — «$x$ делится на $y$» представляется формулой $\exists z(yz = x)$ (Вместо $\exists z(yz = x)$ можно бы написать, скажем, $\exists u(yu = x)$ или $\exists t(yt = x)$ — ср. с. 60; это следует иметь в виду и далее).

б) Предикат «$z$ является общим делителем для $x$ и $y$» — будем обозначать его $D_0(x, y, z)$ — представляется выражением $d(x, z)\& \& d(y, z)$; устраняя сокращение $d$, получаем $\exists u(zu = x)\&\exists v(zv = y)$.

в) Предикат $D(x, y, z)$ — «$z$ является наибольшим общим делителем (н. о. д.) для $x$ и $y$» — представляет несколько бо́льшую трудность. Чтобы выразить его требуемым образом, мы несколько изменим обычную формулировку определения н.о.д. — «н. о. д. чисел $x$ и $y$ есть такой общий делитель $x$ и $y$, который делится на любой их общий делитель» — и скажем так: «н. о. д. чисел $x$ и $y$ есть такое число $z$, что: 1) $z$ есть общий делитель $x$ и $y$; 2) если какое-либо число $t$ является общим делителем $x$ и $y$, то $z$ делится на $t$». Это уже нетрудно перевести на символический язык:

$$D_0(x, y, z)\&\forall t(D_0(x, y, t)\supset d(z, t)).$$

Устраняя сокращения, получаем:

$$\exists u(zu = x)\&\exists v(zv = y)\&\forall t(\exists r(tr = x)\&\exists s(ts = y)\supset\exists w(tw = z)).$$

г) Аналогичным приемом мы воспользуемся, чтобы записать предикат $P(x)$ — «$x$ есть простое число». Именно, предложение «$x$ есть простое число», т. е. «$x \neq 1$ и $x$ делится только на 1 и на себя», мы представим в виде «$x \neq 1$ и если $x$ делится на какое-либо число $z$, то $z = 1$ или $z = x$». Получаем для $P(x)$ такое выражение:

$$\neg(x = 1)\&\forall z(\exists u(zu = x)\supset(z = 1)\vee(z = x)).$$

д) Запишем теперь на символическом языке какое-либо арифметическое предложение, например: «Если $x$ делится на $y$ и $y$ делится на $z$, то $x$ делится на $z$». Оно представится так:

$$\forall x\forall y\forall z(d(x, y))\&d(y, z)\supset d(x, z)).$$

е) Предложение: «Если произведение двух чисел делится на про-

стое число, то на него делится хотя бы один из сомножителей» выражается формулой:

$$\forall x \forall y \forall z \forall u (xy = u \& d(u, z) \& P(z) \supset d(x, z) \vee d(y, z)).$$

Сокращения в д) и е) читатель устранит сам.

ж) Ассоциативность умножения:

$$\forall x \forall y \forall z [(xy)z = x(yz)].$$

**Пример 2.** Возьмем в качестве элементарных четыре предиката, определенных на множестве точек и прямых, лежащих в одной плоскости: $T(x)$ — «$x$ есть точка», $Пр(x)$ — «$x$ есть прямая», $i(x, y)$ — «$x$ есть точка, лежащая на прямой $y$», $x = y$ — «$x$ совпадает с $y$».

а) Предикаты $Пер(x, y)$ и $Пар(x, y)$ — «$x$ и $y$ — пересекающиеся прямые» и «$x$ и $y$ — параллельные прямые» — записываются символически в виде

$$Пр(x) \& Пр(y) \& \exists z (i(z, x) \& i(z, y)) \& \neg (x = y)$$

и

$$Пр(x) \& Пр(y) \& \neg \exists z (i(z, x) \& i(z, y)).$$

б) Предикат $\Delta(x, y, z)$ — «$x$, $y$, $z$ — вершины некоторого треугольника» (т. е. «точки $x$, $y$ и $z$ не лежат на одной прямой») — записывается так:

$$T(x) \& T(y) \& T(z) \& \neg \exists t (i(x, t) \& i(y, t) \& i(z, t))^{36}.$$

в) Предложение «Через любые две различные точки проходит прямая и притом только одна» выглядит так:

$$\forall x \forall y [T(x) \& T(y) \& \neg (x = y) \supset \exists z (i(x, z) \& i(y, z) \& \forall u (i(x, u) \&$$

$$\& i(y, u) \supset z = u))].$$

г) Предложение «Две различные прямые не могут иметь больше одной общей точки»:

$$\forall x \forall y \forall u \forall v [\neg (x = y) \& i(u, x) \& i(u, y) \& i(v, x) \& i(v, y) \supset u = v].$$

**Пример 3.** Возьмем в качестве элементарных следующие предикаты, заданные на множестве людей: $P(x, y, z)$ — «$x$ и $y$ — отец и мать $z$-а соответственно», $M(x)$ — «$x$ — лицо мужского пола», $x = y$ — «$x$ и $y$ — один и тот же человек». Через эти три предиката

[36] Мы пользуемся здесь конъюнкцией трех предложений, которая, собственно, не была определена, но смысл ее очевиден: это предложение, истинное тогда и только тогда, когда истинны все три составляющих ее предложения.

можно выразить все термины кровного родства[37]. Например:

а) Предикаты «$x$ — отец $y$-а» и «$x$ — мать $y$-а» записываются соответственно как $\exists z P(x, z, y)$ и $\exists z P(z, x, y)$.

б) «$x$ — сын $y$-а»: $(\exists z P(y, z, x) \vee \exists z P(z, y, x)) \& M(x)$.

в) «$x$ — бабушка $y$-а»: $\exists u \exists v | P(u, x, v) \& (\exists z P(v, z, y) \vee \vee \exists z P(z, v, y)) |$.

г) «$x$ и $y$ — сестры (не сводные, т. е. и по отцу и по матери)»: $\exists z \exists t (P(z, t, x) \& P(z, t, y)) \& \neg M(x) \& \neg M(y) \& \neg(x = y)$.

Пример 4. а) Пусть $f$ — функция, определенная на некотором подмножестве $M$ миожества действительных чисел R и принимающая значения в R. Взяв в качестве элементарных определенные на R предикаты $x<y$ и $x \in M$ и используя, кроме функционального символа $f$, символы еще двух функций: разности и абсолютной величины (модуля), — мы можем следующим образом записать определения предела и непрерывности функции в точке:

Число $b$ есть предел функции $f$ в точке $a$, если

$$\forall \varepsilon | \varepsilon > 0 \supset \exists \delta (\delta > 0 \& \forall x (x \in M \supset (0 < |x - a| < \delta \supset |f(x) - b| < \varepsilon))) |.$$

(«Двойное неравенство» $0< |x - a| <\delta$ следует понимать как сокращенную запись конъюнкции $0<|x - a| \ \& \ |x - a|<\delta$.)

Функция $f$ непрерывна в точке $a$, если

$$\forall \varepsilon | \varepsilon > 0 \supset \exists \delta (\delta > 0 \& \forall x (x \in M \supset (|x - a| < \delta \supset |f(x) - f(a)| < \varepsilon))) |.$$

В приложениях математической логики иногда используются так называемые *ограниченные кванторы*: вместо $\forall x (P(x) \supset F(x))$ пишут $\underset{P(x)}{\forall x} F(x)$ (читается: «Для всякого $x$, обладающего свойством $P$, ...») и вместо $\exists x (P(x) \& F(x))$ — $\underset{P(x)}{\exists x} F(x)$ (читается: «Существует $x$, обладающее свойством $P$, такое, что...»). Предикат $P(x)$ называется здесь *ограничением*. С помощью ограниченных кванторов наши определения можно переписать в более обозримом виде:

Число $b$ есть предел функции $f$ в точке $a$, если

$$\underset{\varepsilon>0}{\forall \varepsilon} \ \underset{\delta>0}{\exists \delta} \ \underset{x \in M}{\forall x} (0 < |x - a| < \delta \supset |f(x) - b| < \varepsilon).$$

Функция $f$ непрерывна в точке $a$, если

$$\underset{\varepsilon > 0 \delta > 0}{\forall \varepsilon} \ \underset{x \in M}{\exists \delta \ \forall x} (|x - a| < \delta \supset |f(x) - f(a)| < \varepsilon).$$

[37] Точнее, все термины кровного родства, имеющиеся в русском языке. В некоторых других языках (например, в тюркских, в венгерском) термины родства связаны также со старшинством

б) Пусть $a_0, a_1, \ldots$ — числовая последовательность. Взяв в качестве элементарных определенные на R предикаты $x<y$ и $x\in\mathbf{N}$, где N — множество натуральных чисел, и используя те же две функции, что и выше, мы можем записать определение предела последовательности так:

Число $a$ есть предел последовательности $a_n$, если

$$\underset{\varepsilon>0}{\forall\varepsilon}\ \underset{N>0}{\exists N}\ \underset{n\in\mathbf{N}}{\forall n}(n > N \supset |a-a_n| < \varepsilon).$$

Такая «кванторная запись» определений в последнее время получила в преподавании математического анализа довольно широкое распространение. При этом ограниченные кванторы чаще пишутся не так, как у нас (и как вообще принято в математической логике), а в виде $(\forall\varepsilon > 0)$, $(\exists\delta > 0)$, $(\forall x\in M)$. Для данных конкретных ограничений — $x>0$, $x\in M$ — такие обозначения ничем не хуже, но их нельзя распространить на ограничения более общего вида; поэтому лучше пользоваться для ограниченных кванторов обозначениями, принятыми в математической логике.

Замечание. Из примеров видно, что употребление пропозициональных связок для соединения предикатов приводит к совершению «естественным» предложениям — в отличие от употребления их для соединения предложений о единичных фактах. Это вполне понятно, так как использование союзов «или» и «если» в «предложениях с переменными», т. е. в предложениях, в которых речь идет о неопределенных объектах, очень близко к употреблению этих союзов в обычной речи (см. § 2.3).

Задачи. (1) (а) Записать с помощью предиката равенства (определенного на множестве натуральных чисел), используя функцию $xy$:

(а1) $z$ есть общее кратное для $x$ и $y$;

(а2) $z$ есть наименьшее общее кратное для $x$ и $y$;

(а3) $x$ и $y$ взаимно просты;

(а4) Если один из двух сомножителей делится на некоторое число, то на него делится и произведение;

(а5) Если произведение $xy$ делится на простое число $z$ и $x$ не делится на $z$, то $y$ делится на $z$;

(а6) Произведение любого числа $x$ на единицу равно $x$;

(а7) Коммутативность умножения.

б) Перевести на русский язык:

(б1) $\exists z(2z = x)$;

(б2) $\neg\exists z(3z = x)$;

(б3) $\exists y(yy = x)$;

(б4) $\exists y \exists z(yy = z) \,\&\, (zy = x)$;

(б5) $\exists y \exists z(yy = z) \,\&\, (zz = x)$;

(б6) $\forall x \forall y(\exists u(yu = x) \,\&\, \exists v(xv = y) \supset (x = y))$;

(б7) $\forall x \forall y \forall z \forall t((yz = t) \,\&\, \exists u(tu = x) \supset \exists v(yv = x) \,\&\, \exists w(zw = x))$.

(2) (а) Записать с помощью элементарных предикатов примера 2:

(а1) Прямая, проходящая через точки $x$ и $y$, параллельна прямой, проходящей через точки $z$ и $u$. [Указание. Воспользоваться тем, что этот предикат можно представить так: «Всякая прямая, проходящая ... параллельна всякой прямой ...» — поскольку на самом деле прямая, проходящая через две точки, единственна];

(а2) $x$ есть точка пересечения прямых $y$ и $z$;

(а3) Прямые $x$, $y$, $z$ не проходят через одну точку;

(а4) Через всякую точку, не лежащую на прямой, можно провести прямую, параллельную данной;

(а5) Через всякую точку, не лежащую на прямой, можно провести не более одной прямой, параллельной данной.

б) Перевести на русский язык (смысл обозначений тот же, что в примере 2):

(б1) $\exists x \exists y \exists z \neg \exists t(i(x, t) \,\&\, i(y, t) \,\&\, i(z, t))$;

(б2) $\forall x \forall y \forall z(Пр(x) \,\&\, Пр(y) \,\&\, Пр(z) \,\&\, \neg(x = z) \,\&\, \neg \exists u(i(u, x) \,\&$

$\&\, i(u, y)) \,\&\, \neg \exists v(i(v, y) \,\&\, i(v, z)) \supset \neg \exists w(i(w, x) \,\&\, i(w, z)))$;

(б3) $\forall x \forall y \forall z(Пр(x) \,\&\, Пр(y) \,\&\, Пр(z) \,\&\, \neg \exists u(i(u, x) \,\&\, i(u, y)) \,\&$

$\&\, \exists v(i(v, x) \,\&\, i(v, z)) \,\&\, \neg(x = z) \supset \exists w(i(w, y) \,\&\, i(w, z) \,\&\, \neg(y = z))$.

(3) (а) Записать с помощью элементарных предикатов примера 3:

(а1) $x$ — внук $y$-$a$;

(а2) $x$ — дядя $y$-$a$ по отцу (древнерусск. *стрый*, польск. *stryj*);

(а3) $x$ — дядя $y$-$a$;

(а4) $x$ — племянница $y$-$a$;

(а5) $x$ и $y$ — двоюродные братья;

(а6) $x$ — двоюродный брат $y$-$a$;

(а7) $x$ — правнук $y$-$a$.

(б) Перевести на русский язык (смысл обозначений тот же, что в примере 3):

(б1) $\exists u \exists v[P(x, u, v) \,\&\, (\exists z P(v, z, y) \vee \exists z P(z, v, y))]$;

(б2) $\exists z \exists u \exists v[(P(y, z, u) \vee P(z, y, u)) \,\&\, (P(u, v, x) \vee$

$\vee P(v, u, x))] \,\&\, \neg M(x)$;

(б3) $\exists z \exists t(P(z, t, x) \,\&\, P(z, t, y)) \,\&\, \neg M(y) \,\&\, \neg(x = y)$.

4) (а) С помощью элементарных предикатов примера 4 и функций $x - y$ и $|x|$ записать следующие определения:

(а1) ограниченной последовательности;

(а2) предела всюду определенной фукиции при $x \to +\infty$;

(а3) то же при $x \to -\infty$;

(а4) равномерной непрерывности функции на множестве.

б) Указать, каким понятиям анализа отвечают формулы:

(б1) $\forall S \exists N \forall n (n > N \supset a_n > S)$:

(б2) $\forall \varepsilon \underset{\varepsilon > 0}{} \exists \delta \underset{\delta > 0}{} \forall x \underset{x \in M}{} (0 < x - a < \delta \supset |f(x) - b| < \varepsilon)$;

(б3) $\forall S \exists \delta \underset{\delta > 0}{} \forall x \underset{x \in M}{} (0 < a - x < \delta \supset f(x) < S)$.

### Задачи и упражнения

1) Найти значения и истинностные значения предиката $F(n)$, определенного на множестве целых положительных чисел и означающего «русское название числа $n$ состоит из четного числа букв», для следующих значений аргумента: 2, 5, 15, 42, 223.

2) Найти значения и истинностные значения предиката $B(x, y)$, определенного на множестве рек земного шара и означающего «$x$ впадает в $y$», для следующих пар значений аргументов: (Обь, Иртыш), (Иртыш, Обь), (Клязьма, Ориноко), (Ориноко, Ориноко).

3) Пусть $M(x, y)$ — предикат, определенный на множестве целых положительных чисел и означающий $x < y$.

а) Для каждого из предикатов $\forall x M(x, y)$, $\exists x M(x, y)$, $\forall y M(x, y)$, $\exists y M(x, y)$ указать, для каких значений аргумента он дает истинные предложения и для каких — ложные. Являются ли какие-либо из этих предикатов тождественно истинными? Тождественно ложными?

(б) Связывая кванторами обе переменные, можно получить из предиката $M(x, y)$ 8 различных предложений. Выписать эти предложения и найти их истинностные значения.

(в) Выполнить предыдущие два задания для предиката $B(x, y)$ из предыдущей задачи.

4) Пусть $S_1(x, y, z)$ — предикат примера 3 на стр. 61. Ответить на вопросы задачи 3а для следующих предикатов:

$\exists y \exists z S_1(x, y, z)$; $\exists x \exists y S_1(x, y, z)$; $\forall x \forall y S_1(x, y, z)$; $\exists z \exists x S_1(x, y, z)$.

5) Пусть $m(x, y, z)$ — предикат, определенный на множестве $\{-1, 0, 1\}$ и означающий $xy = z$.

а) Сколько двуместных предикатов можно получить из $m(x, y, z)$, фиксируя значения переменных или связывая их кванторами?

б) Сколько одноместных предикатов можно получить из $m(x, y, z)$ тем же способом?

в) Сколько предложений можно получить этим способом из $m(x, y, z)$?

г) Имеются ли среди предикатов пункта а) тождественно истинные? тождественно ложные?

д) Тот же вопрос для предикатов пункта б).

е) Среди предложений пункта в) указать примеры истинных и ложных.

6) Кроме фиксирования переменных и связывания их кванторами, имеется еще один способ получать из многоместных предикатов предикаты меньшей вместимости — *отождествление переменных*. Например, из двуместных предикатов $E(x, y)$, $M(x, y)$ и $Q(x, y)$, определенных на множестве действительных чисел и означающих $x = y$, $x < y$ и $x^2 = y$ соответственно, отождествлением переменных получаем одноместные предикаты $E(x, x)$, $M(x, x)$ и $Q(x, x)$ (первый из них тождественно истинен, второй тождественно ложен, третий истинен при $x = 0$ и $x = 1$ и ложен при всех остальных значениях $x$).

а) Пусть $A(x, y)$, $B(x, y)$ и $C(x, y)$ — предикаты, определенные на множестве действительных чисел и означающие $x<y^2$, $x<[y]$ и $x>[y]$ соответственно. ($[y]$ — целая часть $y$, см. с. 38.) При каких значениях $x$ истинны предикаты $A(x, x)$, $B(x, x)$, $C(x, x)$?

(б) Аналогичный вопрос для предикатов $S_1(x, x, y)$, $S_1(x, y, x)$, $S_1(x, x, x)$, $m(x, x, y)$, $m(x, x, x)$, где $S_1(x, y, z)$, $m(x, y, z)$ — предикаты из задач 4 и 5.

7) По аналогии с определениями конъюнкции, дизъюнкции, импликации и эквиваленции определить пропозициональную связку, которая служила бы «переводом» на символический язык выражения «То, что ... противоречит тому, что ...» (например: «то, что число делится на 4, противоречит его нечетности», иначе «то, что число делится на 4, противоречит тому, что оно нечетно»).

8) По аналогии с примером, приведенным в сноске 16, подобрать другие примеры, иллюстрирующие, что совместимость или несовместимость предложений, соединяемых союзом «или», может зависеть от обстоятельств.

9) Русские союзы «а» и «но» выражают, очевидно, конъюнкцию с дополнительным значением «противопоставления». Указать другие примеры русских союзов, выражающих конъюнкцию с теми или иными дополнительными значениями.

10) Пусть $A$ означает «Андрей выдержал экзамен», $Б$ — «Борис выдержал экзамен», $B$ — «Виктор выдержал экзамен».

(а) Записать с помощью формул логики предложений:

(а1) Неверно, что ни Андрей, ни Борис не выдержали экзамена;

(а2) Из того, что Андрей и Борис выдержали экзамен, не следует, что его выдержал Виктор;

(а3) Если Борис или Виктор выдержал экзамен, то и Андрей его выдержал.

(б) Записать по-русски:

(б1) $7(7B\&7A\supset 7Б)$;

(б2) $77((A\vee Б)\ \&\ 7B)$.

11) Для каждой из формул предыдущей задачи составить истинност-

ную таблицу и с помощью этой таблицы перечислить все случаи, когда соответствующее данной формуле утверждение оказывается опровергнутым. [Образец: утверждение (а3) будет опровергнуто в трех случаях: если Андрей не выдержал экзамена, а Борис и Виктор выдержали; если Андрей и Виктор не выдержали экзамена, а Борис выдержал; если Андрей и Борис не выдержали экзамена, а Виктор выдержал.]

12) Составить истинностные таблицы для следующих формул логики предложений:

(а) $\neg(X \vee \neg Y \supset (X \& \neg Y \vee \neg X \supset Y))$;

(б) $X \& \neg Y \supset (Y \vee \neg X \supset \neg Z)$;

(в) $\neg[(X \supset \neg(Y \leftrightarrow \neg Z \vee X)) \& (Y \supset X \& Z)]$;

(г) $\neg X_1 \vee X_2 \supset X_4 \& \neg X_3$;

(д) $(\neg X \vee Z) \& (Y \supset (U \supset X))$;

(е) $(X_1 \supset (X_2 \supset \ldots \supset (X_{n-1} \supset X_n)\ldots))$;

(ж) $X_1 \vee X_2 \vee \ldots \vee X_n \supset Y_1 \& Y_2 \& \ldots \& Y_m$;

(з) $\underset{\substack{i,j=1,\ldots,n \\ i \neq j}}{\&} \neg(X_i \leftrightarrow X_j)$.

13) Пусть $B(x, y)$ — предикат задачи 2. Указать примеры рек и пар рек, для которых являются истинными предложениями значения следующих предикатов:

$\neg\exists y B(x, y)$; $\exists z(B(x, z) \& B(z, y))$; $\exists z(B(z, x) \& B(y, z))$.

14) С помощью единственного элементарного предиката $x < y$, определенного на множестве действительных чисел, записать:

(а) $x$ — положительное число;

(б) Числа $x$ и $y$ имеют разные знаки.

15) (а) Присоединив к предикату предыдущей задачи предикат $x = y$, записать:

(а1) предикат $x \leq y$,

(а2) предикат (зависящий от $x$, $a$ и $b$) $x \in [a, b]$;

(а3) предложение «Для любых двух различных чисел найдется число, расположенное между ними».

(б1) Записать в обычных обозначениях: $(a < x) \& ((x < b) \vee (x = b))$.

(б2) Перевести на русский язык:

$\forall x \forall y((x < 0) \& \neg(x < y) \supset (y < 0))$.

16) Пусть $\Gamma(x)$ и $C(x)$ — предикаты, определенные на множестве $Б$ русских букв и означающие «$x$ — гласная» и «$x$ — согласная» соответственно. Пусть кроме того, $A(x, y, z)$ — предикат с областью определения $Б^* \times Б \times Б$, где $Б^*$ — множество всевозможных «слов», т. е. конечных последовательностей из русских букв (не обязательно являющихся в самом деле русскими словами), означающий «в слове $x$ встречается двубуквенное "подслово" $yz$» (например, если $x_0 = барокко$, то предложения $A(x_0, б, а)$, $A(x_0, о, к)$, $A(x_0, к, о)$, $A(x_0, к, к)$ истинны, $A(x_0, а, б)$, $A(x_0, б, р)$, $A(x_0, э, я)$ ложны).

(а) Пользуясь предикатами $\Gamma$, $C$ и $A$ как элементарными, записать следующие предикаты:

(а1) В слове $x$ никакие две гласные не стоят рядом;

(а2) Слово $x$ состоит не менее чем из двух букв.

(б) Перевести на русский язык (смысл обозначений тот же);

(б1) $\exists y\exists z(A(x, y, z) \& C(y) \& \Gamma(z)) \& \neg\exists u\exists v(A(x, u, v) \& \Gamma(u)) \&$

$\& \neg\exists u\exists v(A(x, u, v) \& C(v))$;

(б2) $\neg\exists z A(x, z, z)$.

17) (а) С помощью определенного на множестве целых положительных чисел предиката $x = y$ и функций $x + y$ и $xy$ записать:

(а1) Если числа $x$ и $y$ делятся на $z$, то их сумма также делится на $z$;

(а2) Если два числа $x$ и $y$ делятся на $z$, то их разность, если она существует, также делится на $z$;

(а3) Сумма двух чисел, имеющих различную четность, нечетна;

(а4) $x < y$;

(а5) Остаток от деления $x$ на 5 равен двум.

(б) Перевести на русский язык (смысл обозначений тот же):

(б1) $\exists u(zu = x + y) \& \neg\exists v(zv = x) \supset \neg\exists w(zw = y)$;

(б2) $(\exists z(2z = x) \& \exists u(2u = y)) \vee (\neg\exists z(2z = x) \&$

$\& \neg\exists u(2u = y)) \supset \exists v(2v = x + y)$;

(б3) $\forall x[\exists u\exists v\exists w\exists t(x = uu + vv + ww + tt) \vee$

$\vee \exists u\exists v\exists w(x = uu + vv + ww) \vee$

$\vee \exists u\exists v(x = uu + vv) \vee \exists u(x = uu)]$.

18) С помощью элементарных предикатов примера 2 на с. 82 записать предикат «$x$, $y$, $z$, $u$ — вершины некоторого параллелограмма».

19) Присоединив к элементарным предикатам примера 2 на с. 82 предикаты $K(x, y, z, u)$ — «$x$, $y$, $z$, $u$ — точки, и отрезок $xy$ равен отрезку $zu$» и $K_1(x, y, z, u, v, w)$ — «$x$, $y$, $z$, $u$, $v$, $w$ — точки, и $\angle xyz = \angle uvw$» (имеются в виду углы, отсчитываемые против часовой стрелки), записать:

(а) Точка $z$ — середина отрезка $xy$.

(б) Точка $z$ делит отрезок $xy$ в отношении 1 : 2;

(в) Отрезок $xu$ лежит на биссектрисе угла $\angle yxz$;

(г) Отрезок $xu$ делит угол $\angle yxz$ в отношении 1 : 2;

(д) Отрезок $xu$ — медиана треугольника $xyz$;

(е, ж) То же с заменой медианы на высоту и биссектрису;

(з, и, к) Медианы (высоты, биссектрисы) треугольника пересекаются в одной точке;

(л, м, н) Признаки равенства треугольников.

20) Присоединив к элементарным предикатам примера 3 на с. 82 предикат $C(x, y)$ — «$x$ и $y$ — супруги» — выразить следующие термины родства через брак: тесть, теща, свекор, свекровь, зять, сноха, шурин, деверь, золовка, свояченица, свояк. (Имеется в виду запись предикатов «$x$ — тесть $y$-а» и т. п.)

21) Способом, аналогичным использованному в примере 4 на с. 83, записать следующие определения:

(а) Сходимости числового ряда;

(б) Сходимости функционального ряда в точке;

(в) Равномерной сходимости фуикционального ряда на множестве.

ГЛАВА

3

# СЕМАНТИКА ЛОГИКИ ПРЕДЛОЖЕНИЙ

## § 3.1. БУЛЕВЫ ФУНКЦИИ. РАВНОСИЛЬНОСТЬ ФОРМУЛ

1. Логикой предложений (иначе — логикой высказываний) называется раздел математической логики, в котором изучаются свойства операций над предложениями (пропозициональных связок) или, что то же самое, свойства выражений, образованных с помощью этих операций, т. е. формул логики предложений. Сейчас мы займемся изучением соотношения между формой этих выражений и их смыслом, т. е. их истинностными значениями. Строение связей между формой и смыслом выражений того или иного языка, естественного или искусственного, принято называть семантикой[1] этого языка. Таким образом, нас будет интересовать семантика языка логики предложений; впрочем, слово «языка» здесь обычно опускают.

Приступая к занятиям семантикой логики предложений, следует прежде всего заметить, что две разные формулы[2] могут иметь одинаковый смысл, т. е. быть синонимичными. Возьмем, например, предложения $A$ = «Неверно, что Иванов и Петров — оба студенты» и $B$ = «По крайней мере один из двоих — Иванов или Петров — не студент». Ясно, что эти предложения означают одно и то же. Введя элементарные предложения $X$ = «Иванов студент» и $Y$ = «Петров студент», мы можем записать $A$ и $B$ в виде $\neg(X \,\&\, Y)$ и $\neg X \vee \neg Y$ соответ-

[1] От греческого σημαντικός — «обозначенный» (σῆμα — «знак», σημαίνω — «обозначаю»). Семантикой — точнее, лингвистической семантикой — называется также раздел языковедения, в котором изучаются связи между формой и смыслом языковых единиц.

[2] Всюду в этой главе слово «формула» будет означать «формула логики предложений».

ственно. Теперь легко понять, почему $A$ и $B$ синонимичны — составив истинностные таблицы для соответствующих формул, мы видим, что эти таблицы совпадают:

| $X$ | $Y$ | $\neg(X \,\&\, Y)$ | $\neg X \vee \neg Y$ |
|---|---|---|---|
| *И* | *И* | *Л* | *Л* |
| *И* | *Л* | *И* | *И* |
| *Л* | *И* | *И* | *И* |
| *Л* | *Л* | *И* | *И* |

(Здесь две таблицы самоочевидным образом сведены в одну.)

Ясно, что предложения, выражаемые этими формулами, останутся синонимичными, если взять в качестве $X$ и $Y$ любые другие предложения; таким образом, мы имеем здесь дело, в сущности, с синонимией не предложений, а формул; эта синонимия имеет логическую природу — она обусловлена свойствами логических операций (в данном случае конъюнкции, дизъюнкции и отрицания).

Замечание. Рассматривая предложения $A$ и $B$ как «совпадающие по смыслу», мы, строго говоря, допустили неточность. Эти предложения вполне равнозначны лишь с точки зрения истинности/ложности, смыслы же их совпадают не до конца: тот, кто произносит предложение $A$, предполагает, что у его собеседника возникло или может возникнуть мнение, что Иванов и Петров — оба студенты, и он делает акцент на опровержении этого мнения, тогда как в предложении $B$ этот смысловой оттенок отсутствует. (Еще нагляднее это различие видно на примере более простых предложений «Иванов студент» и «Неверно, что Иванов не студент».) Такие предложения — равнозначные с точки зрения истинностных значений — можно было бы назвать *логически синонимичными*, в отличие от «полностью синонимичных» — абсолютно тождественных по смыслу[1]. (Впрочем, в некоторых случаях логическая синонимия предложений, обусловленная синонимией формул, может приводить к настоящей синонимии. Например, формулы $X \,\&\, Y$ и $Y \,\&\, X$ синонимичны (обе они принимают значение *И* тогда и только тогда, когда как $X$, так и $Y$ истинны), и поэтому предложения «Париж — столица Франции, и Лондон — столица Англии» и «Лондон — столица Англии, и Париж — столица Франции» логически синонимичны; но эти предложения синонимичны и «на самом деле». В то же время предложения «Он поднял руку, и стало тихо» и «Стало тихо, и он поднял

[1] Надо сказать, что и в лингвистике термин «синонимы» означает не абсолютное тождество смыслов, а лишь совпадение основных значений. Например, слова «горе» и «беда» считаются синонимами, хотя в значении второго из них есть дополнительный смысл «неожиданности», которого нет в первом.

руку» имеют, очевидно, совсем разный смысл!) Так что нам не случайно пришлось на с. 53—54, говоря об отождествлении синонимичных предложений в математической логике, сказать, что они отождествляются лишь к а к п р а в и л о, а не всегда. Теперь мы можем уточнить это так: в математической логике синонимичные предложения отождествляются, если их синонимия вызвана не синонимией выражающих их формул логики предложений или логики предикатов, а какими-либо другими причинами (как в примерах на с. 54)[4].

Мы могли бы теперь сказать, что синонимия формул — это совпадение истинностных таблиц. Такое определение было бы, однако, недостаточно общим: совпадение истинностных таблиц предполагает, что обе формулы содержат в точности одни и те же элементарные предложения, но интуитивно очевидная синонимия возможна не только в этом случае. Например, формулы

$$(X\&Y\supset Z)\ \&\ (X\&\neg Y)\supset Z \text{ и } X\supset Z$$

естественно считать имеющими один и тот же смысл, потому что первая из них, как легко проверить, истинна в точности для тех же пар значений $X$ и $Z$, для которых истинна вторая, независимо от значения $Y$[5]. Чтобы дать общее определение синонимии формул или, как принято говорить, их равносильности, мы введем некоторые новые понятия, имеющие и самостоятельное значение.

2. Пусть $\mathfrak{A}$ — произвольная формула, содержащая элементарные предложения $X_1, \ldots, X_n$ (и только эти). Рассматривая их как переменные, пробегающие двухэлементное множество $\{И, Л\}$, мы можем сказать, что формула $\mathfrak{A}$ задает некоторую функцию от этих переменных, значение которой для каждой упорядоченной $n$-ки значений переменных $X_1, \ldots, X_n$ равно соответствующему истинностному значению формулы $\mathfrak{A}$. Например, формула $X_1\&X_2$ задает функцию $\varphi(X_1, X_2)$, такую, что $\varphi(И, И) = И$, $\varphi(И, Л) = \varphi(Л, И) = \varphi(Л, Л) = Л$. Подобные функции называют булевыми»[6]. Именно: *булева функция* есть функция $n$ переменных ($n = 1, 2, \ldots$) с областью определения $\{И, Л\}^n$ и множеством значений, содержащимся в $\{И, Л\}$.

---

[4] Понятие синонимии формул логики предложений будет сейчас еще расширено. О синонимии формул логики предикатов см. следующую главу.

[5] В математических рассуждениях нередко оказывается удобно вместо доказательства импликации $X\supset Z$ доказывать две импликации $X\&Y\supset Z$ и $X\&\neg Y\supset Z$, или, что то же самое, их конъюнкцию. Например, доказывая какое-либо общее свойство целых чисел, иногда доказывают его отдельно для неотрицательных и для отрицательных чисел. (Здесь роль $X$ играет предложение «Данное число — целое», роль $Z$ — «Данное число обладает нужным свойством», роль $Y$ — «Данное число — неотрицательное».) Это не что иное, как доказательство разбором случаев (взаимоисключающих). Таких случаев может быть и больше двух (см. задачу 4е в конце главы).

[6] В честь одного из создателей математической логики Джорджа Буля (см. § 6.6).

Любую булеву функцию можно, очевидно, задать истинностной таблицей точно такого же вида, как те истинностные таблицы, которые сопоставляются формулам. Если истинностная таблица, задающая булеву функцию $F$, совпадает с истинностной таблицей некоторой формулы $\mathfrak{A}$, говорят, что формула $\mathfrak{A}$ *представляет* (или *задает*, или *реализует*) функцию $F$.

Естественно возникает вопрос: всякая ли булева функция может быть представлена формулой? Ниже мы докажем, что ответ на этот вопрос — положительный.

Пусть $F(X_1, \ldots, X_n)$ — произвольная булева функция. Будем говорить, что переменная $X_i$ $(i = 1, \ldots, n)$ является для этой функции *несущественной*, если значения $F$ не зависят от значений $X_i$ — иначе говоря, если для любого набора[7] $X_1^0 \ldots, X_{i-1}^0, X_{i+1}^0 \ldots, X_n^0$ значений остальных переменных $F(X_1^0 \ldots, X_{i-1}^0, И, X_{i+1}^0 \ldots, X_n^0) = F(X_1^0 \ldots, X_{i-1}^0, Л, X_{i+1}^0 \ldots, X_n^0)$.

В противном случае мы будем называть переменную $X_i$ *существенной для* $F$. Булеву функцию, для которой все ее переменные существенны, назовем *приведенной*.

Пример. Рассмотрим функцию $\varphi(X_1, X_2, X_3)$, заданную следующей истинностной таблицей:

| $X_1$ | $X_2$ | $X_3$ | $\varphi(X_1, X_2, X_3)$ |
|---|---|---|---|
| *И* | *И* | *И* | *И* |
| *И* | *И* | *Л* | *Л* |
| *И* | *Л* | *И* | *И* |
| *И* | *Л* | *Л* | *Л* |
| *Л* | *И* | *И* | *Л* |
| *Л* | *И* | *Л* | *Л* |
| *Л* | *Л* | *И* | *Л* |
| *Л* | *Л* | *Л* | *Л* |

Легко проверить, что для этой функции переменные $X_1$ и $X_3$ существенны, а $X_2$ несущественна.

Если из истинностной таблицы функции $F$ вычеркнуть столбцы, отвечающие несущественным переменным, получится таблица, в которой каждая строка будет повторяться несколько раз[8]. Вычерк-

[7] Слово «набор» здесь и далее означает то же, что «упорядоченная система» (ср. выше, с. 73—74, где мы уже пользовались этим словом).

[8] Два раза, если вычеркнут один столбец, четыре раза, если вычеркнуты два столбца, $2^k$ раз, если вычеркнуто $k$ столбцов.

нув затем «лишние» строки, мы получим новую истинностную таблицу, которая будет определять некоторую булеву функцию $G(X_{i_1}, ..., X_{i_s})$, где $X_{i_1}, ..., X_{i_s}$ — все существенные независимые переменные функции $F$. Для любого набора $X_1^0, ..., X_n^0$ значений переменных $X_1, ..., X_n$ имеем, очевидно, $F(X_1^0, ..., X_n^0) = G(X_{i_1}^0, ..., X_{i_s}^0)$. Эту функцию $G$ — очевидно, приведениую — мы иазовем *основой* фуикции $F$.

Например, из рассмотреиной только что таблицы после вычеркивания столбца, отвечающего $X_2$, с последующим вычеркиванием «лишних» строк получится следующая таблица, определяющая функцию $\psi(X_1, X_3)$ — основу функции $\varphi(X_1, X_2, X_3)$:

| $X_1$ | $X_3$ | $\psi\ (X_1, X_3)$ |
|---|---|---|
| *И* | *И* | *И* |
| *И* | *Л* | *Л* |
| *Л* | *И* | *Л* |
| *Л* | *Л* | *Л* |

Замечание. Вычеркивая все совпадающие строки, кроме одной, мы можем, разумеется, оставить любую. Но если мы хотим, чтобы в новой таблице наборы значений независимых переменных были упорядочены лексикографически (при условии, что так было в старой), то годятся уже не все варианты вычеркивания. Самый простой способ сохранить лексикографический порядок — оставлять каждый раз первую из совпадающих строк. Доказать пригодность этого способа предоставляется читателю.

В частном случае, когда функция $F$ сама приведенная, ее основа по определению будет совпадать с ней самой.

Возможен и «противоположный» случай, когда все независимые переменные иесущественны. Это будет, очевидно, тогда и только тогда, когда функция для всех наборов зиачений независимых переменных принимаст одно и то же значение *И* или *Л*. В первом случае такую функцию называют *тождественно истинной*, во втором — *тождественно ложной*. Основами тождественно истиных и тождественно ложных булевых функций мы будем считать констаиты *И* и *Л* соответственно. Иногда мы ради общности будем называть эти константы *булевыми функциями от* 0 *переменных*.

Теперь мы можем, наконец, сформулировать определение равиосильности формул. Именно, мы будем называть две формулы *равносильными* (друг другу), если представляемые ими булевы функции имеют одну и ту же основу.

Для частного случая, когда множества входящих в формулы пропозициональных переменных совпадают, определение равносильности можно сразу же упростить: такие формулы равносильны тогда и только тогда, когда они представляют одну и ту же булеву функцию — поскольку две различные булевы функции от одного и того же множества переменных не могут иметь одну и ту же основу. (В самом деле, если функции $F_1(Y_1, \ldots, Y_n)$ и $F_2(Y_1, \ldots, Y_n)$ имеют общую основу $G(Y_{i_1}, \ldots, Y_{i_k})$, то для любого набора $Y_1^0, \ldots, Y_n^0$ значений переменных будет $F_1(Y_1^0, \ldots, Y_n^0) = G(Y_{i_1}^0, \ldots, Y_{i_k}^0) = F_2(Y_1^0, \ldots, Y_n^0)$.) Иначе говоря, равносильность формул от одного и того же множества переменных означает совпадение их истинностных таблиц. В общем случае, если формула $\mathfrak{A}$ содержит переменные $Y_1, \ldots, Y_n, Z_1, \ldots, Z_m$, а формула $\mathfrak{B}$ — переменные $Y_1, \ldots, Y_n, U_1, \ldots, U_p$, также не обязательно для проверки на равносильность находить основы представляемых формулами функций $F_1(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m)$ и $F_2(Y_1, \ldots, Y_n, U_1, \ldots, U_p)$; вместо этого можно сравнить истинностные таблицы функции $G_1(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m, U_1, \ldots, U_p)$, полученной из $F_1$ добавлением несущественных переменных $U_1, \ldots, U_p$ (т. е. такой, что для каждого набора $Y_1^0, \ldots, Y_n^0, Z_1^0, \ldots, Z_m^0, U_1^0, \ldots, U_p^0$ значений всех переменных $G_1(Y_1^0, \ldots, Z_m^0, U_1^0, \ldots, U_p^0) = F_1(Y_1^0, \ldots, Z_m^0))$ и фуикции $G_2(Y_1, \ldots, Y_n, Z_1, \ldots, Z_m, U_1, \ldots, U_p)$, полученной аналогичным образом из $F_2$: формулы равносильны тогда и только тогда, когда эти истинностные таблицы совпадают. Действительно, $G_1$ имеет, очевидно, ту же основу, что и $F_1$, а $G_2$ — ту же, что и $F_2$, и по предыдущему основы функций $G_1$ и $G_2$ совпадают тогда и только тогда, когда совпадают их истинностные таблицы.

Примеры. 1) Пара таблиц на с. 92 доказывает равносильность формул $\neg(X \& Y)$ и $\neg X \vee \neg Y$.

2) Следующая пара таблиц (также сведенных в одну) доказывает равносильность формул $(\neg X_1 \& X_2) \vee (\neg X_1 \& \neg X_2)$ и $(X_3 \supset \neg X_1) \& (\neg X_3 \supset \neg X_1)$:

| $X_1$ | $X_2$ | $X_3$ | $(\neg X_1 \& X_2) \vee (\neg X_1 \& \neg X_2)$ | $(X_3 \supset \neg X_1) \& (\neg X_3 \supset \neg X_1)$ |
|---|---|---|---|---|
| *И* | *И* | *И* | *Л* | *Л* |
| *И* | *И* | *Л* | *Л* | *Л* |
| *И* | *Л* | *И* | *Л* | *Л* |

Окончание табл. см. на стр. 97

| $X_1$ | $X_2$ | $X_3$ | $(\neg X_1 \& X_2) \vee (\neg X_1 \& \neg X_2)$ | $(X_3 \supset \neg X_1) \& (\neg X_3 \supset \neg X_1)$ |
|---|---|---|---|---|
| *И* | *Л* | *Л* | *Л* | *Л* |
| *Л* | *И* | *И* | *И* | *И* |
| *Л* | *И* | *Л* | *И* | *И* |
| *Л* | *Л* | *И* | *И* | *И* |
| *Л* | *Л* | *Л* | *И* | *И* |

Для упражнения полезно найти общую основу этих формул.

Вместо «формулы $\mathfrak{A}$ и $\mathfrak{B}$ равносильны» мы часто будем писать $\mathfrak{A} \equiv \mathfrak{B}$.

Читатель без труда докажет, что отношение равносильности формул является отношением эквивалентности, т. е. что оно рефлексивно, симметрично и транзитивно (см. Приложение I).

Задача. Доказать, что

(а) $X \supset \neg Y \equiv Y \supset \neg X$;

(б) $X \supset (Y \supset Z) \equiv X \& Y \supset Z$;

(в) $X \equiv (X \& Y \& Z) \vee (X \& Y \& \neg Z) \vee (X \& \neg Y \& Z) \vee (X \& \neg Y \& \neg Z)$.

**3.** Пользуясь понятием равносильности формул, можно установить ряд простых соотношений, которые мы сейчас выпишем; читатель без труда докажет их самостоятельно. Ради удобства запоминания мы разобьем эти соотношения (иногда называемые *основными равносильностями логики предложений*) на три группы.

В группу I войдут восемь соотношений, в которых участвуют только конъюнкция и дизъюнкция:

I 1. $X \vee (Y \vee Z) \equiv (X \vee Y) \vee Z$ (ассоциативность дизъюнкции).

I 2. $X \vee Y \equiv Y \vee X$ (коммутативность дизъюнкции).

I 3. $X \& (Y \& Z) \equiv (X \& Y) \& Z$ (ассоциативность конъюнкции).

I 4. $X \& Y \equiv Y \& X$ (коммутативность конъюнкции).

I 5. $X \& (Y \vee Z) \equiv X \& Y \vee X \& Z$ (дистрибутивность конъюнкции по отношению к дизъюнкции).

I 6. $X \vee (Y \& Z) \equiv (X \vee Y) \& (X \vee Z)$ (дистрибутивность дизъюнкции по отношению к конъюнкции).

I 7. $X \vee X \equiv X$ (идемпотентность[8a] дизъюнкции).

---

[8a] От лат. *idem* — «то же самое» и *potentia* — «степень» (смысл этого термина в том, что если понимать операцию — в данном случае дизъюнкцию — как «умножение», то $a^n = a$ для любого $n$.

I 8. $X\&X \equiv X$ (идемпотентность конъюнкции).

Группу II составляют три соотношения, в которых, кроме конъюнкции и дизъюнкции, участвует также отрицание:

II 1. $\neg\neg X \equiv X$ («правило снятия двойного отрицания»).

II 2. $\neg(X \vee Y) \equiv \neg X \& \neg Y$
II 3. $\neg(X \& Y) \equiv \neg X \vee \neg Y$ } («законы Де Моргана»[9]).

Читатель, видимо, заметил, что соотношения групп I и II похожи на выведенные в гл. I свойства операций над множествами. Именно, если заменить равносильность равенством, дизъюнкцию — объединением, конъюнкцию — пересечением и отрицание — дополнением, то равносильности I 1—I 6 превратятся в равенства I—VI из пункта 9 § 1.1, I 7,8 — в равенства $A \cup A = A$ и $A \cap A = A$ (с. 30) и II 1—II 3 — в равенства I—III из пункта 10 § 1.1. Это сходство не случайно. Чтобы объяснить его, рассмотрим произвольное множество $U$, которое будем считать универсальным, и каждому множеству $A \subset U$ сопоставим определенный на $U$ предикат $F_A(x)$, такой, что $F_A(x) \equiv И$ при $x \in A$ и $F_A(x) \equiv Л$ при $x \notin A$ (так называемый *характеристический предикат* множества $A$). Очевидно, два подмножества $U$ тогда и только тогда равны, когда их характеристические предикаты равносильны[10]. Если $A$ и $B$ — произвольные подмножества $U$, то предикат $F_{A \cup B}(x)$ будет принимать значение $И$ для тех и только для тех $x \in U$, которые принадлежат хотя бы одному из множеств $A$ и $B$ — иначе говоря, для тех $x \in U$, для которых хотя бы один из предикатов $F_A(x)$ и $F_B(x)$ принимает значение $И$, т. е. для тех, для которых принимает значение $И$ предикат $F_A(x) \vee F_B(x)$. Итак, предикат $F_{A \cup B}(x)$ равносилен $F_A(x) \vee F_B(x)$. Точно так же можно показать — читатель сделает это самостоятельно,— что предикат $F_{A \cap B}(x)$ равносилен $F_A(x)$ & $F_B(x)$, а $F_{\bar{A}}(x)$ равносилен предикату $\neg F_A(x)$. Теперь мы можем из любой равносильности между формулами, содержащими только знаки конъюнкции, дизъюнкции и отрицания, вывести соответствующее теоретико-множественное равенство. Для примера докажем таким образом дистрибутивность пересечения относительно объединения. Обозначим множество $A \cap (B \cup C)$ через $M$ и $(A \cap B) \cup (A \cap C)$ — через $N$. Предикат $F_N(x)$ равносилен, по доказанному, предикату $F_{A \cap B}(x) \vee F_{A \cap C}(x)$, а этот последний — $F_A(x)$ & $F_B(x) \vee F_A(x)$ & $F_C(x)$. Точно так же видим, что $F_M(x)$ равно-

[9] О Де Моргане см. в § 6.6.

[10] Определение равносильности предикатов см. на с. 59.

силен $F_A(x)\ \&\ (F_B(x) \vee F_C(x))$. Но при любом $x_0 \in U$ предложения $F_A(x_0)\ \&\ F_B(x_0) \vee F_A(x_0)\ \&\ F_C(x_0)$ и $F_A(x_0)\ \&\ (F_B(x_0) \vee F_C(x_0))$ принимают одинаковые истинностные значения (соотношение I 5); поэтому предикаты $F_A(x)\ \&\ (F_B(x) \vee F_C(x)) \equiv F_M(x)$ и $F_A(x)\ \&\ F_B(x) \vee \vee F_A(x)\ \&\ F_C(x) \equiv F_N(x)$ равносильны и, следовательно, $M = N$.

Задача. Вывести соответствующие теоретико-множественные равенства из остальных соотношений групп I и II.

Последнюю группу соотношений составляют три равносильности, в которых участвует импликация, и еще одна, содержащая также эквиваленцию:

III 1. $X \supset Y \equiv \neg X \vee Y$;

III 2. $X \supset Y \equiv \neg(X \& \neg Y)$;

III 3. $X \supset Y \equiv \neg Y \supset \neg X$ («закон контрапозиции»[1]).

III 4. $X \leftrightarrow Y \equiv (X \supset Y)\ \&\ (Y \supset X)$.

Для лучшего усвоения этих соотношений полезно иметь в виду их очень простой содержательный смысл: предложение «Из $X$ следует $Y$» означает то же, что каждое из двух предложений: «Либо $Y$ верно, либо $X$ неверно» (III 1) и «Невозможно, чтобы $X$ было верно, а $Y$ неверно» (III 2); если из верности $X$ следует верность $Y$, то из неверности $Y$ следует неверность $X$, и если из неверности $Y$ следует неверность $X$, то из верности $X$ следует верность $Y$ (III 3); $X$ эквивалентно $Y$ тогда и только тогда, когда из $X$ следует $Y$ и из $Y$ следует $X$ (III 4).

Замечание. Если в формулу, представляющую булеву функцию $F(X_1, \ldots, X_n)$, вместо каждой переменной $X_i$ подставить некоторую формулу $\mathfrak{B}_i$, представляющую булеву функцию $G_i(Y_{k_{i1}}, \ldots, Y_{k_{is_i}})$, то полученная формула будет, очевидно, представлять функцию

$$F(G_1(Y_{k_{11}}, \ldots, Y_{k_{1s_1}}), \ldots, G_n(Y_{k_{n1}}, \ldots, Y_{k_{ns_n}})).$$

Но если в две булевы функции $F$ и $G$, имеющие общую основу $H(Z_1, \ldots, Z_l)$, подставить вместо всех переменных какие-либо булевы функции, то полученные при такой подстановке функции также будут иметь общую основу — совпадающую с основой функции $H(L_1(U_{m_{11}}, \ldots, U_{m_{1r_1}}), \ldots, L_l(U_{m_{l1}}, \ldots, U_{m_{lr_l}}))$, где $L_j(U_{m_{j1}}, \ldots, U_{m_{jr_j}})$,— та функция, которая подставлена вместо $Z_j$. Поэтому любые две равносильные формулы остаются равносильными, если заменить в них все переменные произвольными формулами (причем, разумеется, все вхождения одной и той же переменной должны заменяться одной и

[1] От лат. *contrapositio* — «противоположение».

той же формулой). В частности, все основные равносильности остаются справедливыми при замене переменных $X$, $Y$, $Z$ любыми формулами.

## § 3.2. ТОЖДЕСТВЕННЫЕ ПРЕОБРАЗОВАНИЯ. НОРМАЛЬНЫЕ ФОРМЫ. ТОЖДЕСТВЕННО ИСТИННЫЕ И ТОЖДЕСТВЕННО ЛОЖНЫЕ ФОРМУЛЫ

1. Основные равносильности логики предложений позволяют производить *тождественные преобразования* формул, т. е. переходить от одних формул к другим, равносильным, аналогично тому, как производятся тождественные преобразования в элементарной алгебре. В частности, благодаря соотношениям I 1,3 можно опускать скобки в выражениях вида $X \vee (Y \vee Z)$, $(X \& Y) \& Z$ и т. п.[12]; соотношения I 2,4 дают возможность переставлять члены в дизъюнкциях и конъюнкциях, соотношение I 5 — раскрывать скобки. Здесь, однако, есть одна тонкость, которую с первого взгляда можно и не заметить. Именно: мы можем, конечно, быть уверены — учитывая замечание в конце предыдущего параграфа — что, скажем, формула $(\mathfrak{A} \vee \mathfrak{B}) \& \mathfrak{C}$ (где $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ — произвольные формулы) равносильна формуле $\mathfrak{A} \& \mathfrak{C} \vee \mathfrak{B} \& \mathfrak{C}$; но следует ли отсюда, что $(\mathfrak{A} \vee \mathfrak{B}) \& \mathfrak{C}$ можно заменять на $\mathfrak{A} \& \mathfrak{C} \vee \mathfrak{B} \& \mathfrak{C}$ внутри более сложных формул? Будет ли, например, формула $\neg(\mathfrak{D} \supset (\mathfrak{A} \vee \mathfrak{B}) \& \mathfrak{C})$ равносильна $\neg(\mathfrak{D} \supset \mathfrak{A} \& \& \mathfrak{C} \vee \mathfrak{B} \& \mathfrak{C})$? Ответ, как мы сейчас увидим, положительный — но это, разумеется, нужно доказать; необходимо сначала достаточно четко сформулировать вопрос в общем виде.

С этой целью мы введем в рассмотрение понятие подформулы. Именно, мы будем называть *подформулой формулы* $\mathfrak{A}$ всякую формулу $\mathfrak{B}$, «входящую в состав» $\mathfrak{A}$, т. е. такую, что формулу $\mathfrak{A}$ можно получить из некоторой формулы $\mathfrak{C}$ заменой некоторого вхождения некоторой переменной на вхождение формулы $\mathfrak{B}$. Например, формула $\mathfrak{A}_0 = \neg X \supset \neg X \& Y$ — в более педантичной записи $\mathfrak{A}_0 = (\neg(X)) \supset \supset ((\neg(X)) \& (Y))$[13] — может быть получена из формулы $(\neg(X)) \supset (Z)$

[12] Выражение $X_1 \& \ldots \& X_n$ можно было бы определить и независимо как предложение, истинное тогда и только тогда, когда истинны все предложения $X_1 \& \ldots \& X_n$; аналогично можно определить $X_1 \vee \ldots \vee X_n$. Ср. сноску 36 к гл. 2

[13] Здесь нам удобно заключать в скобки даже элементарные предложения (ср. строгое определение формулы в § 5.2).

заменой (единственного в ней) вхождения переменной $Z$ вхождением формулы $(\neg(X)) \,\&\, (Y)$, так что эта последняя есть подформула формулы $\mathfrak{A}_0$. Подформулами $\mathfrak{A}_0$ являются также $X$, $Y$, $\neg(X)$ и сама $\mathfrak{A}_0$. При этом подформула $\neg(X)$ входит в $\mathfrak{A}_0$ дважды — иначе говоря, $\mathfrak{A}_0$ содержит два вхождения этой подформулы; то же верно для подформулы $X$.

Далее, мы будем называть формулу $\mathfrak{B}$ *непосредственной составляющей* формулы $\mathfrak{A}$, если $\mathfrak{A}$ имеет либо вид $\neg(\mathfrak{B})$, либо $(\mathfrak{B})\ \alpha\ (\mathfrak{C})$, либо $(\mathfrak{C})\ \alpha\ (\mathfrak{B})$, где $\mathfrak{C}$ — какая-то формула и $\alpha$ — один из знаков $\&$, $\vee$, $\supset$, $\sim$. (Например, $\neg(X)$ и $(\neg(X))\&(Y)$ — непосредственные составляющие формулы $\mathfrak{A}_0$ предыдущего абзаца.) Для каждого вхождения подформулы $\mathfrak{B}$ в формулу $\mathfrak{A}$ существует, очевидно, единственная последовательность вхождений подформул $\mathfrak{C}_0, \mathfrak{C}_1, \ldots, \mathfrak{C}_p$ в формулу $\mathfrak{A}$, такая, что: ($\alpha$) данное вхождение $\mathfrak{B}$ в $\mathfrak{A}$ является одновременно вхождением в каждую подформулу $\mathfrak{C}_i$; ($\beta$) $\mathfrak{C}_0 = \mathfrak{A}$; ($\gamma$) $\mathfrak{C}_p = \mathfrak{B}$; ($\delta$) для каждого $i = 1, \ldots p$ формула $\mathfrak{C}_i$ есть непосредственная составляющая формулы $\mathfrak{C}_{i-1}$[14]. (Например, для второго — считая слева направо — вхождения $X$ в $\mathfrak{A}_0$ эта последовательность имеет вид: $\mathfrak{A}_0$, $(\neg(X)) \,\&\, (Y)$, $\neg(X)$, $X$. Число $p$, т. е. уменьшенное на 1 число членов этой последовательности, мы назовем *глубиной* данного вхождения $\mathfrak{B}$ в $\mathfrak{A}$. (Например, глубины первого и второго вхождений $X$ в $\mathfrak{A}_0$ равны 2 и 3 соответственно, глубина вхождения $(\neg(X)) \,\&\, (Y)$ равна 1, глубина вхождения $\mathfrak{A}_0$ равна 0.)

Теперь точную формулировку нашего вопроса и одновременно ответ на него даст нам

**Теорема о замене равносильных формул (логики предложений).** Если в формуле $\mathfrak{A}$ заменить вхождение подформулы $\mathfrak{B}$ вхождением формулы $\mathfrak{B}'$, равносильной $\mathfrak{B}$, то полученная формула $\mathfrak{A}'$ будет равносильна $\mathfrak{A}$.

Доказательство мы проведем индукцией по глубине заменяемого вхождения подформулы $\mathfrak{B}$. (О доказательстве по индукции см. Приложение III.)

Базис. Пусть глубина заменяемого вхождения $\mathfrak{B}$ в $\mathfrak{A}$ равна нулю. Тогда $\mathfrak{B} = \mathfrak{A}$, $\mathfrak{B}' = \mathfrak{A}'$, и доказываемая равносильность совпадает с данной.

Индукционный шаг. Допустим, что наше утверждение доказано для вхождений глубины $p-1$ (где $p$ — произвольное целое положи-

[14] Понятие вхождения подформулы в формулу (или, более общо, одного слова в другое), интуитивно довольно ясное, мы оставили пока без строгого определения. Дать такое определение нетрудно, но наши формулировки стали бы тогда громоздкими и менее прозрачными. Впрочем, потом нам все же придется это сделать (см. с. 382).

тельное число), и докажем его для случая, когда глубина заменяемого вхождения $\mathfrak{B}$ в $\mathfrak{A}$ равна $p$. Рассмотрим последовательность, фигурирующую в определении глубины: $\mathfrak{A} = \mathfrak{C}_0, \mathfrak{C}_1, \ldots, \mathfrak{C}_p = \mathfrak{B}$. Интересующее нас вхождение $\mathfrak{B}$ в $\mathfrak{A}$ является также вхождением $\mathfrak{B}$ в $\mathfrak{C}_1$, причем глубина его здесь равна $p-1$; поэтому, если $\mathfrak{C}_1'$ — формула, получаемая из $\mathfrak{C}_1$ заменой этого вхождения $\mathfrak{B}$ вхождением $\mathfrak{B}_1'$, то по предположению индукции $\mathfrak{C}_1' \equiv \mathfrak{C}_1$. Поскольку $\mathfrak{C}_1$ есть непосредственная составляющая формулы $\mathfrak{A}$, возможны три случая: (а) $\mathfrak{A} = (\mathfrak{C}_1)\alpha(\mathfrak{D})$; (б) $\mathfrak{A} = (\mathfrak{D})\alpha(\mathfrak{C}_1)$; (в) $\mathfrak{A} = 7(\mathfrak{C}_1)$ (в случаях (а) и (б) $\alpha = \&, \vee, \supset, \leftrightarrow$). В случае (а), обозначая через $F(X, Y)$, $G$, $G'$ и $H$ булевы функции, представляемые формулами $(X)\alpha(Y)$, $\mathfrak{C}_1$, $\mathfrak{C}_1'$ и $\mathfrak{D}$ соответственно, видим, что формула $\mathfrak{A}$ представляется функцией $F(G, H)$, а формула $\mathfrak{A}'$ — функцией $F(G', H)$; но $G$ и $G'$ имеют общую основу, и поэтому то же верно для $F(G, H)$ и $F(G', H)$ (совпадающую с основой функции $F(L, H)$, где $L$ — общая основа $G$ и $G'$), т. е. $\mathfrak{A} \equiv \mathfrak{A}'$. В случаях (б) и (в) рассуждения совершенно аналогичны.

2. Теперь мы действительно имеем право производить с помощью основных равносильностей тождественные преобразования так же, как это делается в элементарной алгебре. Производя эти преобразования в определенном порядке, можно привести произвольную формулу к некоторому особенно простому виду. Прежде всего, пользуясь соотношением II 1, мы можем устранить двойные отрицания, т. е. заменить каждую часть формулы, имеющую вид $\underbrace{7 7 \cdots 7}_{n \text{ раз}}\mathfrak{A}$ (здесь $\mathfrak{A}$ означает произвольную формулу), на $\mathfrak{A}$, если $n$ четно, и на $7\mathfrak{A}$, если $n$ нечетно. Далее, пользуясь III 4, можно устранить все знаки эквиваленции, а затем, пользуясь соотношениями III 1 и III 2 (где как удобнее) — также и все знаки импликации; если при этом возникнут двойные отрицания, устраняем их, как указано выше. После этого, пользуясь законами Де Моргана, «загоняем внутрь» знаки отрицания, т. е. заменяем части формулы, имеющие вид $7(\mathfrak{A} \vee \mathfrak{B})$ или $7(\mathfrak{A} \& \mathfrak{B})$, на $7\mathfrak{A} \& 7\mathfrak{B}$ или на $7\mathfrak{A} \vee 7\mathfrak{B}$ соответственно; при этом каждый раз, если возникнет необходимость, устраняем двойные отрицания. Проделав такие преобразования нужное число раз, мы в конце концов получим формулу, в которой знаки отрицания стоят разве лишь перед элементарными предложениями — иначе говоря, выражение, составленное из элементарных предложений и их отрицаний с помощью знаков дизъюнкции и конъюнкции. Если в этом выражении раскрыть все скобки по соотношению I 5, получится формула, представляющая собой дизъюнкцию конъюнкций, состоящих из элементарных предложений и их отрицаний (точно так же, как в элементарной алгебре многочлен, т. е. выражение, составленное из букв и чисел с помощью знаков сложения и умножения, после раскрытия

скобок становится суммой одночленов — произведений букв и чиссл).

Замечание. Собственно гововоря, некоторые члены дизъюнкции могут оказаться не конъюнкциями, а просто элементарными предложениями или отрицаниями элементарных предложений: но для единообразия мы будем называть такие выражения «конъюнкциями из одного члена». Кроме того, вместо дизъюнкции конъюнкций может получиться одна конъюнкция: в этом случае мы также будем говорить о «дизъюнкции из одного члена».

Примеры. 1) $\neg(((X\supset\neg\neg Y)\supset\neg\neg(Y\supset Z\vee\neg X))\vee Z)\equiv$

$\equiv\neg(((X\supset Y)\supset\neg(Y\supset Z\vee\neg X))\vee Z)\equiv\neg((\neg(X\supset Y)\vee$

$\vee\neg(Y\supset Z\vee\neg X))\vee Z)\equiv\neg((\neg\neg(X\&\neg Y)\vee\neg\neg(Y\&\neg(Z\vee\neg X)))\vee Z)\equiv$

$\equiv\neg(((X\&\neg Y)\vee(Y\&\neg(Z\vee\neg X)))\vee Z)$[15] $\equiv$

$\equiv\neg((X\&\neg Y)\vee(Y\&\neg(Z\vee\neg X)))\&\neg Z\equiv(\neg(X\&\neg Y)\&$

$\&\neg(Y\&\neg(Z\vee\neg X)))\&\neg Z$[16] $\equiv(\neg X\vee\neg\neg Y)\&((\neg Y)\vee\neg\neg(Z\vee\neg X))\&\neg Z\equiv$

$\equiv(\neg X\vee Y)\&(\neg Y\vee Z\vee\neg X)\&\neg Z\equiv(\neg\bar{X}\&\neg\bar{Y}\&\neg\bar{Z})\vee$

$\vee(\neg\bar{X}\&Z\&\neg\bar{Z})\vee(\neg\bar{X}\&\neg\bar{X}\&\neg\bar{Z})\vee(Y\&\neg\bar{Y}\&\neg\bar{Z})\vee$

$\vee(Y\&Z\&\neg\bar{Z})\vee(Y\&\neg X\&\neg\bar{Z})$.

2) $((X_1\vee X_2)\&(X_1\vee X_3))\vee\neg X_2\equiv(X_1\&X_1)\vee$

$\vee(X_1\&X_3)\vee(X_2\&X_1)\vee(X_2\&X_3)\vee\neg X_2$.

Мы будем теперь называть *элементарной конъюнкцией* всякую формулу, представляющую собой конъюнкцию элементарных предложений и отрицаний элементарных предложений. Формула, являющаяся дизъюнкцией элементарных конъюнкций, называется *формулой в дизъюнктивной нормальной форме* (сокращенно *д. н. ф.*). Нами доказана, таким образом

Теорема о приведении к д. н. ф. Для всякой формулы логики предложений существует равносильная ей формула в д. н. ф.

На самом деле доказано больше: мы указали, как практически получить для каждой формулы равносильную ей формулу в д. н. ф. (как обычно говорят — *привести формулу к д.н.ф.*).

Замечания. 1) При приведении формул к д.н.ф. полезно иметь в виду, что из двух одинаковых членов в конъюнкции или в дизъюнкции один можно вычеркнуть (в силу законов идемпотентности).

---

[15] Для большей наглядности мы иногда сохраняем скобки, которые можно опускать.

[16] Этот шаг можно было бы объединить с предыдущим, заметив, что законы Де Моргана легко обобщаются на случай трех (и вообще любого числа) членов.

(Так, в примере 1 можно заменить $\neg X \& \neg X \& \neg Z$ на $\neg X \& \neg Z$, в примере 2 – $X_1 \& X_1$ на $X_1$.

2) Более формальное доказательство теоремы о приведении к д. н. ф. проводится методом математической индукции — например, возвратной индукцией по числу вхождений в исходную формулу пропозициональных связок (см. приложение III). Читатель может при желании проделать это сам.

3. Наряду с дизъюнктивной нормальной формой для формул логики предложений можно получить еще одну нормальную форму, называемую конъюнктивной. Именно, если определить *элементарную дизъюнкцию* как формулу, представляющую собой дизъюнкцию элементарных предложений и отрицаний элементарных предложений, то конъюнкцию элементарных дизъюнкций естественно назвать *формулой в конъюнктивной нормальной форме* (сокращенно *к. н. ф.*). (Здесь, как и выше, допускаются конъюнкции и дизъюнкции из одного члена.) Имеет место

**Теорема о приведении к к. н. ф.** Для всякой формулы логики предложений существует равносильная ей формула в к. н. ф.

Доказательство состоит, аналогично предыдущей теореме, в указании способа приведения формулы к к. н. ф.; именно, формула приводится к к. н. ф. так же, как к д. н. ф., с той только разницей, что на последнем этапе раскрытие скобок производится не по соотношению I 5. а по I 6.

Пример. $(X \leftrightarrow \neg Z) \vee (\neg X \leftrightarrow Y) \equiv$

$$\equiv \big((X \supset \neg Z) \& (\neg Z \supset X)\big) \vee \big((\neg X \supset Y) \& (Y \supset \neg X)\big) \equiv$$

$$\equiv \big((\neg X \vee \neg Z) \& (Z \vee X)\big) \vee \big((X \vee Y) \& (\neg Y \vee \neg X)\big) \equiv$$

$$\equiv (\neg X \vee \neg Z \vee X \vee Y) \& (Z \vee X \vee X \vee Y) \&$$

$$\& (\neg X \vee \neg Z \vee \neg Y \vee \neg X) \& (Z \vee X \vee \neg Y \vee \neg X).$$

Повторяющиеся члены можно здесь опустить.

Заметим, что в примере 1 предыдущего пункта предпоследняя формула находится в к. н. ф. (так что при приведении к к. н. ф. здесь не нужно раскрывать скобки).

Замечание. Вместо «формула в дизъюнктивной (соответственно "конъюнктивной" нормальной форме» часто говорят просто *«дизъюнктивная (конъюнктивная) нормальная форма»*.

Задача. Привести к д. н. ф. и к. н. ф.

(а) $\big(X \supset \neg Y\big) \vee \neg\neg\big(Y \supset (\neg Y \leftrightarrow Y)\big)$;

(б) $\neg \big(X_1 \& \neg (X_2 \vee \neg X_3) \supset X_1\big) \& X_2$.

4. Формула, представляющая тождественно истинную (тождественно ложную) булеву функцию, также называется *тождественно истинной*, соответственно *тождественно ложной*. Все тождественно истинные формулы равносильны между собой — их общей основой является константа *И*; то же верно для тождественно ложных формул, общая основа которых — константа *Л*. Очевидно и обратное — формула, равносильная тождественно истинной (тождественно ложной) формуле, сама является тождественно истинной, соответственно тождественно ложной. Ясно также, что отрицание тождественно истинной формулы есть формула тождественно ложная, а отрицание тождественно ложной — тождественно истинная.

| Примеры. | 1) Формулы | 2) Формулы |
|---|---|---|
| | $X \vee \neg X$, | $X \& \neg X$, |
| | $\neg (X \& \neg X)$, | $X \leftrightarrow \neg X$, |
| | $X \supset X$ | $\neg (X \vee \neg X)$ |
| | тождественно истинны. | тождественно ложны. |

Предложения, выражаемые тождественно истинными формулами, «абсолютно истинны», т. е. истинны вне зависимости от содержания входящих в них элементарных предложений. Некоторые тождественно истинные формулы соответствуют важным логическим законам. В частности, формула $X \vee \neg X$ выражает один из осиовных законов классической логики — *закон исключенного третьего:* всякое суждение либо истинно, либо ложно, «третьего не дано» (по-латыни tertium non datur[17]); формула $\neg (X \& \neg X)$ выражает другой важнейший закон логики — *закон противоречия:* никакое суждение не может быть истинным и ложным одновременно.

Тождественно истинные формулы логики предложений называют также *тавтологиями*, или *тавтологичными формулами* (от греч. ταυτολογέω — повторяю сказанное) — видимо, потому, что некоторые из них выглядят как «повторения одного и того же» ($X \supset X$, $X \leftrightarrow X$, $X \supset X \& X$ и т. п.).

Понятие тождественно истинной формулы позволяет заметить связь между отношением равносильности формул и операцией эквиваленции: формулы $\mathfrak{A}$ и $\mathfrak{B}$ тогда и только тогда равносильны, когда эквиваленция $\mathfrak{A} \leftrightarrow \mathfrak{B}$ тождественно истинна. Действительно, соста-

[17] Иногда этот закон так и называют «принципом tertium non datur».

вив для формул $\mathfrak{A}$, $\mathfrak{B}$ и $\mathfrak{A} \leftrightarrow \mathfrak{B}$ общую истинностную таблицу:

| $X_1 \ldots X_n$ | $\mathfrak{A}$ | $\mathfrak{B}$ | $\mathfrak{A} \leftrightarrow \mathfrak{B}$ |
|---|---|---|---|
| $И \ldots И$ | | | |
| $И \ldots Л$ | | | |
| .. ... .. | ... | ... | ..... |
| .. ... .. | ... | ... | ..... |
| $Л \ldots Л$ | | | |

мы видим, что согласно определению эквиваленции в столбце для $\mathfrak{A} \leftrightarrow \mathfrak{B}$ тогда и только тогда будет всюду стоять $И$, когда столбцы для $\mathfrak{A}$ и для $\mathfrak{B}$ совпадают.

Ввиду соотношения III 4 эквиваленция $\mathfrak{A} \leftrightarrow \mathfrak{B}$ тождественно истинна тогда и только тогда, когда тождественно истинны обе импликации $\mathfrak{A} \supset \mathfrak{B}$ и $\mathfrak{B} \supset \mathfrak{A}$. Итак, тождественная истинность этих двух импликаций необходима и достаточна для равносильности формул $\mathfrak{A}$ и $\mathfrak{B}$.

Задачи. 1) Доказать тождественную истинность формул:

(а) $(X \supset Y) \supset (\neg Y \supset \neg X)$;

(б) $(\neg Y \supset \neg X) \supset (X \supset Y)$;

(в) $(X \supset (Y \supset Z)) \supset (X \,\&\, Y \supset Z)$;

(г) $(X \,\&\, Y \supset Z) \supset (X \supset (Y \supset Z))$;

(д) $(X \supset Y) \,\&\, (Y \supset Z) \supset (X \supset Z)$.

2) Доказать тождественную ложность формул:

(а) $X \,\&\, (X \supset Y) \,\&\, (X \supset \neg Y)$;

(б) $X \,\&\, Y \,\&\, (X \,\&\, Y \supset Z) \,\&\, \neg Z$.

Сейчас мы присоединим к полученным в предыдущем параграфе соотношениям несколько новых; их особенностью будет то, что некоторые из участвующих в них предложений предполагаются тождественно истинными или тождественно ложными. В этих соотношениях буква $\mathfrak{R}$ будет обозначать произвольную тождественно истинную формулу, $\tilde{\mathfrak{o}}$ — произвольную тождественно ложную и $X$ — произвольное предложение.

IV1. $X \,\&\, \mathfrak{R} \equiv X$.

IV2. $X \,\&\, \tilde{\mathfrak{o}} \equiv \tilde{\mathfrak{o}}$.

IV3. $X \vee \mathfrak{R} \equiv \mathfrak{R}$.

IV4. $X \vee \tilde{\mathfrak{o}} \equiv X$.

IV5. $\widetilde{\mathfrak{y}} \supset X \equiv \mathfrak{R}$.

IV6. $X \supset \mathfrak{R} \equiv \mathfrak{R}$.

Доказательства этих соотношений очень просты. Например: если $X$ принимает значение $И$, то, поскольку $\mathfrak{R}$ всегда имеет значение $И$, $X \,\&\, \mathfrak{R}$ тоже принимает значение $И$; если же $X$ принимает значение $Л$, то и $X \,\&\, \mathfrak{R}$ принимает значение $Л$. Аналогично: каково бы ни было $X$, импликация $\widetilde{\mathfrak{y}} \supset X$ принимает значение $И$, поскольку импликация ложна лишь тогда, когда посылка истинна, а заключение ложно. Остальные соотношения читатель докажет сам.

Равносильность IV 5 выражает так называемое правило Дунса Скота[18]) из лжи следует все, что угодно (ex falso quodlibet).

Замечание. Равносильности IV 1—6 остаются справедливыми при замене переменной $X$ любой формулой (ср. замечание на с. 99).

Соотношения IV 1—6 во многих случаях позволяют упрощать формулы, т. е. находить для них равносильные более простого вида. Именно, в силу IV 1,4 в конъюнкциях можно вычеркивать тождественно истинные члены, а в дизъюнкциях — тождественно ложные; в то же время тождественную истинность или тождественную ложность формулы нередко удается установить с помощью соотношений IV 2, 3, 5, 6 (а также законов исключенного третьего и противоречия). Например, формула $(\neg (X \,\&\, \neg X \supset Y) \vee X) \,\&\, (Y \vee Z \vee \neg Z)$ равносильна $X$, поскольку: а) импликация $X \,\&\, \neg X \supset Y$ тождественно истинна (в силу IV5 и тождественной ложности формулы $X \,\&\, \neg X$), так что дизъюнкция $\neg (X \,\&\, \neg X \supset Y) \vee X$ равносильна $X$ (IV 4); б) дизъюнкция $Y \vee Z \vee \neg Z$ тождественно истинна (IV 3 и закон исключенного третьего), так что конъюнкция $X \,\&\, (Y \vee Z \vee \neg Z)$ равносильна $X$ (IV 1). Тем же способом последние формулы примера 1) на с. 103 и примера на с. 104 можно упростить до $(\neg X \,\&\, \neg Y \,\&\, \neg Z) \vee (\neg X \,\&\, \neg Z) \vee (Y \,\&\, \neg X \,\&\, \neg Z)$ и до $(Z \vee X \vee Y) \,\&\, (\neg X \vee \neg Z \vee \neg Y)$ соответственно.

Задача. Упростить:

(а) $(X \vee \neg Y \supset (Z \supset Y \vee \neg Y \vee X)) \,\&\, (X \vee \neg (X \supset X)) \supset Y$;

(б) $((X \,\&\, \neg (X \,\&\, \neg X \supset Y \,\&\, \neg Y)) \supset Z) \vee X \vee (Y \,\&\, Z)$;

(в) $(X_1 \,\&\, (X_2 \vee X_3 \supset X_2 \vee X_3)) \vee (X_1 \,\&\, X_1 \,\&\, \neg X_2) \vee$

$\vee X_1 \vee (X_2 \,\&\, \neg (X_1 \,\&\, \neg X_1))$.

---

[18] Иоанн Дунс Скот (Johannes Duns Scotus, 1265—1308) — один из крупнейших средневековых философов и богословов, монах-францисканец, родом из Шотландии.

## § 3.3. ПРЕДСТАВЛЕНИЕ ПРОИЗВОЛЬНОЙ БУЛЕВОЙ ФУНКЦИИ ФОРМУЛОЙ. СОВЕРШЕННЫЕ НОРМАЛЬНЫЕ ФОРМЫ. ДВОЙСТВЕННОСТЬ

1. Сейчас будет доказана

**Теорема о представлении булевой функции.** Всякая булева функция может быть представлена формулой.

Чтобы доказать эту теорему, введем сначала некоторые новые понятия.

Пусть $X_1, \ldots, X_n$ — элементарные предложения (иначе — переменные), пробегающие $\{И, Л\}$. Мы будем называть *полной элементарной конъюнкцией* от $X_1, \cdots, X_n$ всякую формулу вида $X_1' \,\&\, X_2' \,\&\, \cdots \,\&\, X_n'$, где для каждого $i = 1, \cdots, n$ $X_i'$ есть либо $X_i$, либо $\neg X_i$.

Полных элементарных конъюнкций от $X_1, \cdots, X_n$ имеется ровно $2^n$. (Действительно: а) полных элементарных конъюнкций от $X_1$ ровно две — $X_1$ и $\neg X_1$; б) для каждого $n$ число полных элементарных конъюнкций от $X_1, \cdots, X_{n+1}$ вдвое больше, чем от $X_1, \ldots, X_n$, т. к. каждую конъюнкцию $X_1' \,\&\, \cdots \,\&\, X_n'$ можно дополнить до полной элементарной конъюнкции от $X_1, \cdots, X_{n+1}$ двумя способами — $X_1' \,\&\, \cdots X_n' \,\&\, X_{n+1}$ и $X_1' \,\&\, \cdots \,\&\, X_n' \,\&\, \neg X_{n+1}$. Ср. с подсчетом наборов значений элементарных предложений, с. 74).

Пример. Полных элементарных конъюнкций от $X_1$, $X_2$ имеется четыре:

$$X_1 \& X_2,\ X_1 \& \neg X_2,\ \neg X_1 \& X_2,\ \neg X_1 \& \neg X_2.$$

Мы будем теперь называть *n-мерным булевым вектором* всякую упорядоченную $n$-ку истинностных значений (которую мы будем записывать без скобок и запятых) или, что то же самое, слово длины $n$, состоящее из букв $И$, $Л$. $i$-ю букву этого слова естественно назвать *i-ой координатой* вектора. Например, *ЛИИЛИ* — пятимерный булев вектор с первой координатой $Л$, второй координатой $И$ и т. д. $i$-ю координату вектора $r$ мы будем обозначать через $r^i$.

Очевидно, строки истинностной таблицы от $n$ переменных — это как раз все $n$-мерные булевы векторы, так что число последних равно $2^n$.

Всякую булеву функцию $F(X_1, \cdots, X_n)$ мы можем рассматривать

теперь как векторную: $F(r)$ будет означать то же, что $F(r^1, \ldots, r^n)$. Иногда мы будем также обозначать через $\mathfrak{A}(r)$ истинностное значение, принимаемое формулой $\mathfrak{A}$ на векторе $r$ (т. е. при подстановке $r^1$ вместо $X_1$, $r^2$ вместо $X_2$ и т. д.).

Сопоставим, далее, каждому $n$-мерному булеву вектору $r$ полную элементарную конъюнкцию $K^r$ от переменных $X_1, \ldots, X_n$ следующим образом: $K^r = X_1^r \,\&\, \ldots \,\&\, X_n^r$,

где $X_i^r = \begin{cases} X_i, \text{ если } r^i = И \\ \neg X_i, \text{ если } r^i = Л. \end{cases}$ Например, если $r = ИЛЛИ$, то $K^r = X_1 \,\&\, \neg X_2 \,\&\, \neg X_3 \,\&\, X_4$.

**Лемма.** Если $r$ — $n$-мерный булев вектор, то $K^r(r) = И$ и для любого $n$-мерного булева вектора $r_1 \neq r$ $K^r(r_1) = Л$.

**Доказательство леммы.** а) Из определения формулы $X_i^r$ видно, что при подстановке $r^i$ вместо $X_i$ она принимает значение $И$; поэтому и $K_r$ примет значение $И$, если каждому $X_i$ дать значение $r^i$. б) Если $r_1 \neq r$, то хотя бы для одного $i_0 = 1, \ldots, n$ будет $r_1^{i_0} \neq r^{i_0}$, т. е. $r_1^{i_0} = Л$, если $r^{i_0} = И$, и $r^{i_0} = И$, если $r^{i_0} = Л$. Но тогда формула $X_{i_0}^r$ при подстановке $r_1^{i_0}$ вместо $X_{i_0}$, примет, очевидно, значение $Л$, а поэтому и $K^r$ примет значение $Л$ при подстановке вместо каждого $X_i$ соответствующего $r_1^i$.

**Доказательство теоремы.** Пусть $F(X_1, \ldots, X_n)$ — произвольная булева функция.

Случай 1. Функция $F$ не является тождественно ложной. Обозначим через $M$ множество тех $n$-мерных булевых векторов, на которых $F$ принимает значение $И$; поскольку $F$ не тождественно ложна, это множество не пусто. Пусть $M = \{r_1, \ldots, r_s\}$. Тогда формула $\mathfrak{A} = K^{r_1} \vee \ldots \vee K^{r_s}$ будет представлять нашу функцию. Действительно, для любого $j = 1, \ldots, s$ формула $K^{r_j}$ на векторе $r_j$ принимает значение $И$, так что дизъюнкция $K^{r_1} \vee \ldots \vee K^{r_s}$ также принимает значение $И$ на этом векторе; с другой стороны, на векторе, не принадлежащем $M$, все формулы $K^{r_1}, \ldots, K^{r_s}$ принимают значение $Л$, а поэтому их дизъюнкция также ложна. Итак, формула $\mathfrak{A}$ принимает значение $И$ для тех векторов $r$, для которых $F(r) = И$, и значение $Л$ для тех, для которых $F(r) = Л$.

Случай 2. Если $F(X_1, \ldots, X_n)$ тождественно ложна, она представляется, например, формулой $X_1 \,\&\, \neg X_1 \,\&\, X_2 \neg X_2 \,\&\, \ldots \,\&\, X_n \,\&\, \neg X_n$.

**Пример.** Пусть функция $F(X_1,X_2,X_3)$ задана истинностной таблицей:

| $X_1$ | $X_2$ | $X_3$ | $F(X_1,X_2,X_3)$ |
|---|---|---|---|
| *И* | *И* | *И* | *И* |
| *И* | *И* | *Л* | *Л* |
| *И* | *Л* | *И* | *Л* |
| *И* | *Л* | *Л* | *И* |
| *Л* | *И* | *И* | *И* |
| *Л* | *И* | *Л* | *Л* |
| *Л* | *Л* | *И* | *Л* |
| *Л* | *Л* | *Л* | *Л* |

Выбирая из таблицы те строки, для которых в столбце $F(X_1,X_2,X_3)$ стоит *И*, и составляя для них соответствующие полные элементарные конъюнкции, получаем формулу

$$X_1 \,\&\, X_2 \,\&\, X_3 \vee X_1 \,\&\, \neg X_2 \,\&\, \neg X_3 \vee \neg X_1 \,\&\, X_2 \,\&\, X_3.$$

Заметим, что в случае не тождественно ложной фуикции соответствующая формула является формулой в д. н. ф. Такие формулы — именно, формулы, являющиеся дизъюнкциями полных элементарных конъюнкций от переменных $X_1, \dots, X_n$, причем ни один член в дизъюнкции не повторяется дважды,— называются *формулами в совершенной д. н. ф.* (сокращенно с. д. н. ф.) от $X_1, \dots, X_n$. Таким образом, мы показали, что всякую не тождественно ложную формулу можно привести к с. д. н. ф.[19]). Способ приведения состоит в том, что для формулы строится истинностная таблица, а по этой таблице строится формула в с. д. н. ф., как описано в доказательстве теоремы. (Кстати, заодно мы передоказали теорему о привдении к д. н. ф.)

Можно приводить формулы к с. д. н. ф. и иначе — с помощью тождественных преобразований. Для этого нужно сначала привести формулу к д. н. ф., как описано в § 2, и вычеркнуть а) повторяющиеся члены в конъюнкциях и б) те конъюнкции, в которых какие-либо элементарные предложения встречаются вместе с их отрицаниями (с. 107). Каждую из оставшихся конъюнкций[20]) можно

[19] Для тождественно ложной формулы не существует равносильной формулы в с. д. н. ф., т. к. всякая полная элементарная конъюнкция для какого-то вектора истинна.

[20] Если все конъюнкции оказались вычеркнутыми, формула тождественно ложна.

записать в виде $X_{i_1}' \,\&\, \cdots \,\&\, X_{i_k}'$, где $X_{i_1}, \cdots, X_{i_k}$ — какие-то из входящих в формулу переменных $X_1, \ldots, X_n$, и для каждого $i$ $X_i'$ есть $X_i$ или $\neg X_i$. Если эта конъюнкция — не полная, преобразуем ее так: берем некоторую не входящую в нее переменную $X_l$ $(l = 1, \cdots, n)$ и заменяем $X_{i_1}' \,\&\, \cdots \,\&\, X_{i_k}'$ на $(X_{i_1}' \,\&\, \cdots \,\&\, X_{i_k}') \,\&\, (X_l \vee \neg X_l)$ (соотношение IV 1): раскрывая скобки, получаем $X_{i_1}' \,\&\, \cdots \,\&\, X_{i_k}' \,\&\, X_l) \vee$ $\vee\, (X_{i_1}' \,\&\, \cdots \,\&\, X_{i_k}' \,\&\, \neg X_l)$. Таким образом, одну конъюнкцию мы заменили двумя, содержащими на одну переменную больше. При необходимости каждую из этих конъюнкций снова дополняем, и так до тех пор, пока не получится дизъюнкция полных элементарных конъюнкций — в которой остается вычеркнуть повторяющиеся члены, если таковые окажутся.

Пример. Формула примера 1) на с. 103 после приведения к д. н. ф. и вычеркивания повторений и тождественно ложных конъюнкций получает вид $(\neg X \,\&\, \neg Y \,\&\, \neg Z) \vee (\neg X \,\&\, \neg Z) \vee (Y \,\&\, \neg X \,\&\, \neg Z)$ (с. 107). Первая и третья конъюнкции — уже полные; преобразуя вторую, имеем:

$$\neg X \,\&\, \neg Z \equiv (\neg X \,\&\, \neg Z) \,\&\, (Y \vee \neg Y) \equiv (\neg X \,\&\, Y \,\&\, \neg Z) \vee$$

$$\vee\, (\neg X \,\&\, \neg Y \,\&\, \neg Z).$$

Вставляя полученную дизъюнкцию вместо $\neg X \,\&\, \neg Z$ и устраняя повторения, приходим к формуле $(\neg X \,\&\, \neg Y \,\&\, \neg Z) \vee$ $\vee\, (\neg X \,\&\, Y \,\&\, \neg Z)$.

Задача. Двумя способами привести к с. д. н. ф. формулы задачи на с. 107.

Замечание. Из доказательства теоремы о представлении булевой функции формулой ясно, что формула в с. д. н. ф. от переменных $X_1, \cdots, X_n$ тогда и только тогда тождественно истинна, тогда она содержит все полные элементарные конъюнкции от этих переменных.

2. Пусть $\mathfrak{A}$ — формула, образованная из элементарных предложений с помощью операций конъюнкции, дизъюнкции и отрицания. Сопоставим ей две новые формулы: $\mathfrak{A}^*$, полученную из $\mathfrak{A}$ переменой местами знаков конъюнкции и дизъюнкции, и $\mathfrak{A}^\wedge$, полученную из $\mathfrak{A}^*$ заменой всех неотрицаемых вхождений элементарных предложений отрицаемыми и наоборот. Формулу $\mathfrak{A}^*$ мы будем называть *двойственной* для $\mathfrak{A}$, а $\mathfrak{A}^\wedge$ — *противоположной* для $\mathfrak{A}$. Очевидно, $\mathfrak{A}^{**} = \mathfrak{A}^{\wedge\wedge} = \mathfrak{A}$.

Пример. Если $\mathfrak{A} = X_3 \vee \neg\, (\neg\, (X_2 \vee \neg X_1) \,\&\, \neg\, X_2)$,

то $\mathfrak{A}^* = X_3 \,\&\, \neg\, (\neg\, (X_2 \,\&\, \neg\, X_1) \vee \neg\, X_2)$,

$\mathfrak{A}^\wedge = \neg\, X_3 \,\&\, \neg\, (\neg(\neg\, X_2 \,\&\, X_1) \vee X_2)$.

**Лемма о противоположной формуле.** Формула, противоположная формуле $\mathfrak{A}$, равносильна отрицанию $\mathfrak{A}$.

Доказательство мы проведем с помощью принципа возвратной индукции (см. приложение III, пункт 2).

Пусть $\mathfrak{A}$ — формула, образованная из элементарных предложений и их отрицаний с помощью операций конъюнкции и дизъюнкции. Обозначим через $d(\mathfrak{A})$ общее число вхождений пропозициональных связок в формулу $\mathfrak{A}$. Мы докажем лемму возвратной индукцией по числу $d(\mathfrak{A})$.

Базис. Пусть $d(\mathfrak{A}) = 0$. Тогда $\mathfrak{A}$ есть элементарное предложение $X$; поэтому $\mathfrak{A}^*$ тоже есть $X$, так что $\mathfrak{A}^\wedge = \neg X$.

Индукционный шаг. Пусть $n > 0$ и утверждение теоремы справедливо для всех формул $\mathfrak{B}$, для которых $d(\mathfrak{B}) < n$. Покажем, что тогда оно справедливо и для любой формулы $\mathfrak{A}$, такой, что $d(\mathfrak{A}) = n$.

Если $d(\mathfrak{A}) = n > 0$, то формула $\mathfrak{A}$ содержит хоть одну пропозициональную связку. Поэтому возможны три случая:

а) $\mathfrak{A} = \mathfrak{A}_1 \,\&\, \mathfrak{A}_2$, б) $\mathfrak{A} = \mathfrak{A}_1 \vee \mathfrak{A}_2$, в) $\mathfrak{A} = \neg\, \mathfrak{B}$, причем в случаях а) и б), очевидно, $d(\mathfrak{A}_1)$, $d(\mathfrak{A}_2) < n$, и в случае в) $d(\mathfrak{B}) < n$. Поэтому, в силу индуктивного предположения, в случаях а) и б) $\mathfrak{A}_1^\wedge \equiv \neg\, \mathfrak{A}_1$, $\mathfrak{A}_2^\wedge \equiv \neg\, \mathfrak{A}_2$, и в случае в) $\mathfrak{B}^\wedge \equiv \neg\, \mathfrak{B}$. Но в случае а) имеем, очевидно, $\mathfrak{A}^\wedge = \mathfrak{A}_1^\wedge \vee \mathfrak{A}_2^\wedge$, откуда $\mathfrak{A}^\wedge \equiv \neg\, \mathfrak{A}_1 \vee \neg\, \mathfrak{A}_2$, а эта последняя формула, в свою очередь, равносильна $\neg\, (\mathfrak{A}_1 \,\&\, \mathfrak{A}_2) = \neg\, \mathfrak{A}$, Случай б) рассматривается аналогично. В случае в) $\mathfrak{A}^\wedge = \neg\mathfrak{B}^\wedge \equiv \neg\, \neg\mathfrak{B} = \neg\mathfrak{A}$.

Из доказанной леммы можно вывести, в частности

**Принцип двойственности.** Если две формулы, образованные из элементарных предложений с помощью операций конъюнкции, дизъюнкции и отрицания, равносильны, то двойственные им формулы также равносильны.

**Доказательство.** Назовем булевы векторы $r$ и $r'$ взаимно противоположными, если $r'$ получается из $r$ переменой местами букв *И* и *Л*. (Например, векторы *ИЛЛ* и *ЛИИ* взаимно противоположны.) Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — формулы, удовлетворяющие нужным условиям, $r$ — $n$-мерный булев вектор, где $n$ — общее число элементарных предложений, входящих в $\mathfrak{A}$ и $\mathfrak{B}$, и $r'$ — вектор, противоположный $r$. Из определений двойственной и противоположной формул ясно, что $\mathfrak{A}^*(r) = \mathfrak{A}^\wedge(r')$, $\mathfrak{B}^*(r) = \mathfrak{B}^\wedge(r')$. Но если $\mathfrak{A} \equiv \mathfrak{B}$, то и $\neg\mathfrak{A} \equiv \neg\, \mathfrak{B}$, откуда $\mathfrak{A}^\wedge \equiv \mathfrak{B}^\wedge$; поэтому для любого $r$ имеем $\mathfrak{A}^*(r) = \mathfrak{A}^\wedge(r') = \neg\, \mathfrak{A}(r') = \neg\, \mathfrak{B}(r') = \mathfrak{B}^\wedge(r') = \mathfrak{B}^*(r)$; а это и значит, что $\mathfrak{A}^* \equiv \mathfrak{B}^*$.

**Задача.** Для каждой из основных равиосильностей группы I указать другую равносильность той же группы, которую можно вывести из нее по принципу двойственности.

**3.** Назовем *полной элементарной дизъюнкцией от переменных*

$X_1, \ldots X_n$ формулу вида $X_1' \vee \ldots \vee X_n'$, где для каждого $i = 1, \ldots, n$ $X_i'$ есть либо $X_i$, либо $\neg X_i$. Конъюнкция полных элементарных дизъюнкций от переменных $X_1, \ldots X_n$, в которой ни один член не повторяется дважды, называется *формулой в совершенной к. н. ф.* (сокращенно *с. к. н. ф.*) от $X_1, \ldots, X_n$.

Ясно, что для формулы в с. д. н. ф. двойственная и противоположная являются формулами в с. к. н. ф., и обратно.

Всякую нетождественно истинную формулу можно привести к с. к. н. ф. Для этого достаточно привести ее отрицание к с. д. н. ф., а затем перейти к противоположной формуле. Можно, впрочем, приводить формулы к с. к. н. ф. и непосредственно, с помощью тождественных преобразований — аналогично тому, как это делается для с. д. н. ф. Читателю предоставляется самому восстановить подробности.

Задачи. 1) Двумя способами привести к с. к. н. ф. формулы задачи на с. 107.

2) Вывести теорему о приведении к к. н. ф. из теоремы о приведении к д. н. ф. и леммы о противоположной формуле.

## § 3.4. СЕМАНТИЧЕСКОЕ СЛЕДОВАНИЕ

1. Пусть $\Gamma$ — конечное множество формул, $\mathfrak{B}$ — некоторая формула и $X_1, \ldots, X_n$ — все элементарные предложения, входящие в формулы из множества $\Gamma$ или в формулу $\mathfrak{B}$. Мы будем говорить, что формула $\mathfrak{B}$ есть *семантическое следствие* — или просто *следствие* — множества формул $\Gamma$ (иначе: $\mathfrak{B}$ *(семантически) следует из* $\Gamma$) и писать $\Gamma \Rightarrow \mathfrak{B}$, если для любого набора значений переменных $X_1, \ldots, X_n$, для которого все формулы, входящие в $\Gamma$, принимают значение *И*, формула $\mathfrak{B}$ также принимает значение *И*. (Если при этом в какую-то формулу входят только некоторые из переменных $X_1, \ldots, X_n$ — скажем, $X_1, \ldots, X_s$, $s<n$, — то, говоря, что эта формула принимает значение *И* для набора $X_1^0, \ldots, X_n^0$ значений переменных $X_1, \ldots, X_n$, мы имеем в виду, что она принимает значение *И* для набора $X_1^0, \ldots, X_s^0$ значений входящих в нее переменных.)

В частности, $\varnothing \Rightarrow \mathfrak{B}$ означает, что $\mathfrak{B}$ тождественно истинна.

Если $\Gamma$ не пусто и состоит из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_s$, мы часто будем вместо «$\mathfrak{B}$ следует из множества $\Gamma$» говорить «$\mathfrak{B}$ следует из формул $\mathfrak{A}_1, \ldots, \mathfrak{B}_s$» и писать $\mathfrak{A}_1, \ldots, \mathfrak{A}_s \Rightarrow \mathfrak{B}$ (а не $\{\mathfrak{A}_1, \ldots, \mathfrak{A}_s\} \Rightarrow \mathfrak{B}$).

Для любых формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n, \mathfrak{B}$ можно проверить, является ли $\mathfrak{B}$ следствием $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, составив для них «общую истинностную таблицу», как в следующем примере:

| $X$ | $Y$ | $Z$ | $X \supset Y$ | $Y \supset Z$ | $X \supset Z$ |
|---|---|---|---|---|---|
| *И* | *И* | *И* | *И* | *И* | *И* |
| *И* | *И* | *Л* | *И* | *Л* | *Л* |
| *И* | *Л* | *И* | *Л* | *И* | *И* |
| *И* | *Л* | *Л* | *Л* | *И* | *Л* |
| *Л* | *И* | *И* | *И* | *И* | *И* |
| *Л* | *И* | *Л* | *И* | *Л* | *И* |
| *Л* | *Л* | *И* | *И* | *И* | *И* |
| *Л* | *Л* | *Л* | *И* | *И* | *И* |

Из этой таблицы видно, что формула $X \supset Z$ есть следствие формул $X \supset Y$ и $Y \supset Z$; действительно, в каждой из тех строк, в которых на пересечении со столбцами значений формулы $X \supset Y$ и $Y \supset Z$ стоит *И* (а именно, в 1-й, 5-й, 7-й и 8-й строках), на пересечении со столбцом значений формулы $X \supset Z$ также стоит *И*.

(Установленный только что факт представляет собой очень важный логический закон, широко используемый, в частности, в математических рассуждениях: если из утверждения $X$ следует утверждение $Y$, а из $Y$ следует утверждение $Z$, то из $X$ следует $Z$.)

Задачи. 1) Доказать, что:

(а) $X, X \supset Y \Rightarrow Y$;

(б) $X, Y \Rightarrow X \& Y$;

(в) $X_1 \& X_2, X_2 \& X_3 \Rightarrow X_1 \& X_2 \& X_3$;

(г) каждая из формул X, Y, $X \vee Y$ есть следствие формулы $X \& Y$.

2) Является ли какая-либо из формул $X \supset (Y \supset Z)$ и $(X \supset Y) \supset Z$ следствием другой?

Докажем теперь три совсем простых, но поучительных утверждения.

**Утверждение 1.** Формула $\mathfrak{B}$ тогда и только тогда является следствием формулы $\mathfrak{A}$, когда импликация $\mathfrak{A} \supset \mathfrak{B}$ тождественно истинна.

**Доказательство.** Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — произвольные формулы и $X_1, \ldots, X_n$ — все входящие в них элементарные предложения. Импликация $\mathfrak{A} \supset \mathfrak{B}$ является ложной для тех и только тех наборов значений предложений $X_1, \ldots, X_n$, для которых $\mathfrak{A}$ истинна, а $\mathfrak{B}$ ложна; поэтому тождественная истинность этой импликации означает, что

таких наборов нет, т. е. что для каждого набора, для которого $\mathfrak{A}$ истинна, $\mathfrak{B}$ также истинна — а это как раз и значит, что $\mathfrak{B}$ есть следствие $\mathfrak{A}$.

**Утверждение 2.** Две формулы тогда и только тогда равносильны, когда каждая из них есть следствие другой.

**Доказательство.** Очевидно, тогда и только тогда каждая из двух формул $\mathfrak{A}$ и $\mathfrak{B}$ будет следствием другой, когда при любом наборе входящих в обе формулы значений элементарных предложений, при котором истинна какая-то одна из них, истинна и другая. Но это значит, что истинностные таблицы формул $\mathfrak{A}$ и $\mathfrak{B}$, зависящие от всех входяших в эти формулы переменных, совпадают — т. е. что $\mathfrak{A}$ и $\mathfrak{B}$ равносильны.

**Утверждение 3.** Тогда и только тогда $\mathfrak{A}\Rightarrow\mathfrak{B}$, когда $\neg\mathfrak{B}\Rightarrow\neg\mathfrak{A}$.

**Доказательство.** В силу закона контрапозиции импликация $\mathfrak{A}\Rightarrow\mathfrak{B}$ тогда и только тогда тождественно истинна, когда это же верно для $\neg\mathfrak{B}\supset\neg\mathfrak{A}$. Отсюда и из утверждения 1 сразу следует нужный факт.

2. Семантическое следование допускает простое и наглядное описание с помощью совершенных нормальных форм. Это описание основано на трех леммах:

**Лемма 1.** Если $\mathfrak{A}$ и $\mathfrak{B}$ — формулы в с. д. н. ф. от одних и тех же переменных, то $\mathfrak{A}\Rightarrow\mathfrak{B}$ тогда и только тогда, когда множество дизъюнктивных членов $\mathfrak{A}$ содержится во множестве дизъюнктивных членов $\mathfrak{B}$.

**Доказательство.** Пусть $M_{\mathfrak{A}}$ и $M_{\mathfrak{B}}$ — множества дизъюнктивных членов $\mathfrak{A}$ и $\mathfrak{B}$ соответственно, и $X_1, \ldots, X_n$ — переменные, от которых зависят $\mathfrak{A}$ и $\mathfrak{B}$. Если $r$ — произвольный $n$-мерный булев вектор, то ввиду леммы предыдущего параграфа тогда и только тогда $\mathfrak{A}(r) = И$, когда $K^r \in M_{\mathfrak{A}}$, и аналогично для $\mathfrak{B}$. Пусть теперь $\mathfrak{A}\Rightarrow\mathfrak{B}$. Это значит, что для любого $r$, для которого $\mathfrak{A}(r) = И$, т. е. $K^r \in M_{\mathfrak{B}}$, будет также $\mathfrak{B}(r) = И$, т. е. $K^r \in M_{\mathfrak{B}}$. Таким образом, из $\mathfrak{A}\Rightarrow\mathfrak{B}$ вытекает $M_{\mathfrak{A}} \subset M_{\mathfrak{B}}$. Обратно, если $M_{\mathfrak{A}} \subset M_{\mathfrak{B}}$, то по предыдущему для любого $r$, для которого $\mathfrak{A}(r) = И$, будет также $\mathfrak{B}(r) = И$, что и означает $\mathfrak{A}\Rightarrow\mathfrak{B}$.

**Лемма 2.** Если $\mathfrak{A}$ и $\mathfrak{B}$ — формулы в с. к. н. ф. от одних и тех же переменных, то $\mathfrak{A}\Rightarrow\mathfrak{B}$ тогда и только тогда, когда множество конъюнктивных членов $\mathfrak{A}$ содержит множество конъюнктивных членов $\mathfrak{B}$.

**Доказательство.** Пусть $N_{\mathfrak{A}}$ и $N_{\mathfrak{B}}$ — множества конъюнктивных членов $\mathfrak{A}$ и $\mathfrak{B}$ соответственно. Ввиду утверждения 3 и леммы о противоположной формуле $\mathfrak{A}\Rightarrow\mathfrak{B}$ тогда и только тогда, когда $\mathfrak{B}^\wedge\Rightarrow\mathfrak{A}^\wedge$. Отсюда получаем в силу леммы 1, пользуясь обозначениями из ее доказательства, что $\mathfrak{A}\Rightarrow\mathfrak{B}$ тогда и только тогда, когда $M_{\mathfrak{B}^\wedge} \subset M_{\mathfrak{A}^\wedge}$.

Но последнее включение равносильно $N_{\mathfrak{B}} \subset N_{\mathfrak{A}}$ [21].

**Лемма 3.** Формула $\mathfrak{B}$ является следствием формул $\mathfrak{A}_1, , \ldots, \mathfrak{A}_k$ тогда и только тогда, когда она является следствием их конъюнкции.

Эта лемма непосредственно следует из того, что конъюнкция истинна для тех и только для тех наборов значений переменных, для которых истинны все ее члены.

Лемма 1 дает возможность для произвольной формулы в с. д. н. ф. легко обозреть все следствия из нее (зависящие от тех же переменных): это будут в точности те формулы, которые получаются из данной добавлением в качестве дизъюнктивных членов каких-либо «новых» полных элементарных конъюнкций от тех же переменных (а также, разумеется, сама данная формула). Например, из формулы $(X_1 \& \neg X_2) \vee (\neg X_1 \& \neg X_2)$ получается четыре следствия:

1) она сама; 2) $(X_1 \& \neg X_2) \vee (\neg X_1 \& \neg X_2) \vee (X_1 \& X_2)$; 3) $(X_1 \& \neg X_2) \vee$ $\vee (\neg X_1 \& \neg X_2) \vee (\neg X_1 \& X_2)$; 4) $(X_1 \& \neg X_2) \vee (\neg X_1 \& \neg X_2) \vee (X_1 \& X_2) \vee (\neg X_1 \& X_2)$ (тождественно истинная формула).

Аналогично, в силу леммы 2 для любой формулы в с. к. н. ф. все следствия из нее, зависящие от тех же переменных, получаются вычеркиванием из нее каких-либо конъюнктивных членов (в частности, можно ничего не вычеркивать или вычеркнуть все — в последнем случае считаем, что получилась тождественно истинная формула[22]. Пользуясь леммой 3, можно теперь для любой (конечной) системы формул получить всевозможные следствия из нее: для этого нужно привести все формулы к с. к. н. ф. от всех тех переменных, которые входят хотя бы в одну из них, а затем из полных элементарных дизъюнкций, входящих в полученные с. к. н. ф., составить всевозможные конъюнкции (включая пустую).

Пример. Из формул $(X_1 \vee X_2) \& (X_1 \vee \neg X_2)$ и $(X_1 \vee \neg X_2) \& (\neg X_1 \vee X_2)$ получается 8 следствий:

1) $(X_1 \vee X_2) \& (X_1 \vee \neg X_2) \& (\neg X_1 \vee X_2)$;

2) $(X_1 \vee X_2) \& (X_1 \vee \neg X_2)$;

3) $(X_1 \vee X_2) \& (\neg X_1 \vee X_2)$;

4) $(X_1 \vee \neg X_2) \& (\neg X_1 \vee X_2)$;

---

[21] Это вытекает из следующего очевидного факта: если $\mathfrak{C}$ — произвольная формула в с. к. н. ф. от переменных $X_1, \ldots, X_n$, то полная элементарная дизъюнкция $X_1' \vee \ldots \vee X_n'$ является одним из конъюнктивных членов $\mathfrak{C}$ тогда и только тогда, когда полная элементарная конъюнкция $X_1'' \& \ldots \& X_n''$, где $X_i'' = \neg X_i$, если $X_i' = X_i$, и $X_i' = X_i$, если $X_i'' = \neg X_i$, является одним из дизъюнктивных членов $\mathfrak{C}^\wedge$.

[22] Которая, очевидно, является следствием любой системы формулы (в то же время любая формула — следствие тождественно ложной).

5) $X_1 \vee X_2$;

6) $X_1 \vee \neg X_2$;

7) $\neg X_1 \vee X_2$;

8) тождественно истинная формула.

Задачи. 1) С помощью с. д. н. ф. получить всевозможные следствия из формулы $X \leftrightarrow Y$.

2) С помощью с. к. н. ф. получить всевозможные следствия из формул $X \supset Y$ и $Y \supset Z$.

## § 3.5. ПРИЛОЖЕНИЯ. ФУНКЦИОНАЛЬНАЯ ПОЛНОТА

1. Как уже говорилось во Введении, идеи и методы математической логики находят приложение в некоторых практических задачах. Сейчас мы рассмотрим одну такую задачу, в которой «работает» логика предложений — синтез релейно-контактных схем. Исторически применение методов математической логики к прикладным вопросам началось именно с этой задачи[23].

Начнем с примера. Пусть в каком-нибудь цехе или лаборатории имеется $n$ установок (машин, аппаратов, вспомогательных устройств), работающих на электрическом токе; обозначим их $a_1, \ldots, a_n$. Каждую установку можно включать и выключать. Фиксировав некоторый момент времени, будем обозначать через $A_i$ предложение «Установка $a_i$ в данный момент включена». Булев вектор $r = r^1 \ldots, r^n$, где $r^i$ — истинностное значение предложения $A_i$, мы назовем *режимом работы* системы установок $(a_1, \ldots, a_n)$ (в данный момент времени). Как правило, этот режим должен удовлетворять каким-то специальным условиям, которые обычно легко записываются с помощью формул логики предложений. Например, условие «Установки $a_1$ и $a_2$ не могут работать (т. е. быть включенными) одновременно» означает, что на векторе $r$ должна быть истинна формула $\neg(A_1 \& A_2)$, условие «Если работает хотя бы одна из установок $a_2$, $a_3$, $a_4$, то должна работать также установка $a_{10}$» — что на $r$ истинна

[23] Возможность использования методов логики предложений для синтеза релейно-контактных схем была обнаружена в конце 30-х годов независимо К. Шенноном (Claude E. Shannon) в США и В. И. Шестаковым в СССР.

формула $A_2 \vee A_3 \vee A_4 \supset A_{10}$, и т. п.[24] Таких условий может быть много, но их всегда можно заменить одним — условием истинности конъюнкции формул, отвечающих каждому условию в отдельности. Обозначив эту конъюнкцию через $\mathfrak{A}$, рассмотрим следующую задачу: как построить автоматическое устройство, которое «следило» бы за выполнением условия $\mathfrak{A}$ — например, включало бы при его нарушении звонок или сигнальную лампочку? Для этого достаточно иметь электрическую цепь, в которой идет ток тогда и только тогда, когда $\mathfrak{A}$ выполняется. Посмотрим, как можно реализовать такую цепь.

Допустим, что с каждым устройством $a_i$ мы можем связать некоторое число проводников электрического тока таким образом, что по каждому из них идет ток тогда и только тогда, когда $a_i$ включено, и эти проводники можно соединять между собой в любых комбинациях (технически это вполне осуществимо). Для простоты будем считать, что с каждым устройством можно связать сколько угодно таких проводников, которые мы будем рассматривать как разные экземпляры одного и того же проводника $\alpha_i$; о каждом таком экземпляре мы будем говорить просто «проводник $\alpha_i$» (например, вместо «два экземпляра проводника $\alpha_i$» будем говорить «два проводника $\alpha_i$», вместо «еще один экземпляр проводника $\alpha_i$» — «еще один проводник $\alpha_i$» и т. п.[25] Теперь мы можем каждое предложение $A_i$, поскольку мы интересуемся только его истинностным значением, понимать как «По проводнику $\alpha_i$ идет ток».

Из этих проводников $\alpha_i$ мы и будем строить нашу цепь. Идея построения чрезвычайно проста. Пусть $\alpha$ и $\beta$ — два проводника электрического тока и $A$, $B$ — предложения «По $\alpha$ идет ток» и «По $\beta$ идет ток» соответственно. Тогда, соединив $\alpha$ и $\beta$ последовательно (рис. 3), мы получим проводник, по которому ток идет тогда и только тогда, когда истинна конъюнкция $A\&B$, а соединив $\alpha$ и $\beta$ параллельно (рис. 4), получим проводник, по которому ток идет тогда и только тогда, когда истинна дизъюнкция $A \vee B$. Поскольку для каждой формулы существует равносильная, не содержащая знаков импликации и эквиваленции (см. § 3.2), мы можем считать, что наша формула $\mathfrak{A}$ содержит только знаки конъюнкции, дизъюнкции и отрицания. Поэтому, чтобы «смодели-

[24] Легко понять, какой смысл могут иметь подобные условия в реальных ситуациях. Например, последнее условие потребуется, если $a_{10}$ — вентиляционное устройство, включение которого при работе установок $a_2$, $a_3$, $a_4$ предписывается правилами техники безопасности.

[25] Подобно тому, как говорят «в слове "каша" две буквы $a$» вместо «два вхождения буквы $a$» или «еще один учебник» вместо «еще один экземпляр учебника».

ровать» формулу $\mathfrak{A}$ цепью, составленной из проводников $\alpha_1, \ldots, \alpha_n$, нам остается научиться «конструировать» на основе проводника $\alpha$ другой проводник $\alpha'$, по которому ток будет идти тогда и только тогда, когда по $\alpha$ ток не идет — т. е. когда истинно о т р и ц а н и е предложения «По $\alpha$ идет ток». Это осуществляется с помощью р е л е, подключенного к $\alpha$ и размыкающего $\alpha'$ в точности тогда, когда по $\alpha$ идет ток (рис. 5). Таким образом, мы можем составить из $\alpha_1, \ldots, \alpha_n$ цепь, в которой ток будет идти тогда и только тогда, когда выполнено условие $\mathfrak{A}$. Такая цепь строится с помощью простых со-




Рис. 3

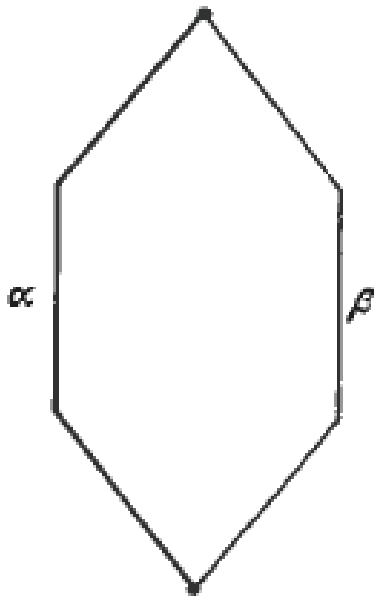



Рис. 4

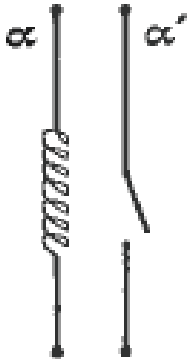



Рис. 5

единений (контактов) и реле; поэтому она называется *релейно-контактной схемой*. Например, схема, изображенная на рис. 6, моделирует формулу $\neg(A_1 \& A_2 \vee A_3) \& (A_3 \vee \neg A_4) \vee (A_1 \& \neg A_2)$: по ней (между «полюсами» $P$ и $Q$) идет ток тогда и только тогда, когда выражаемое этой формулой предложение истинно.

Итак, запись условия на языке логики предложений дает возможность без труда построить — или, как часто говорят, с и н т е з и р о в а т ь — схему устройства, автоматически контролирующего выполнение этого условия. При реальном осуществлении такого устройства важно добиться, чтобы оно было как можно проще, и прежде всего — чтобы для его изготовления требовалось как можно меньше экземпляров всех проводников в совокупности. Здесь приходят на помощь различные приемы упрощения формул. О некоторых самых простых приемах упрощения мы упоминали в § 3.2. Существует много других, более тонких и эффективных приемов; им посвящены многочисленные специальные исследования.

2. Кроме релейно-контактных схем, есть и другой способ модели-

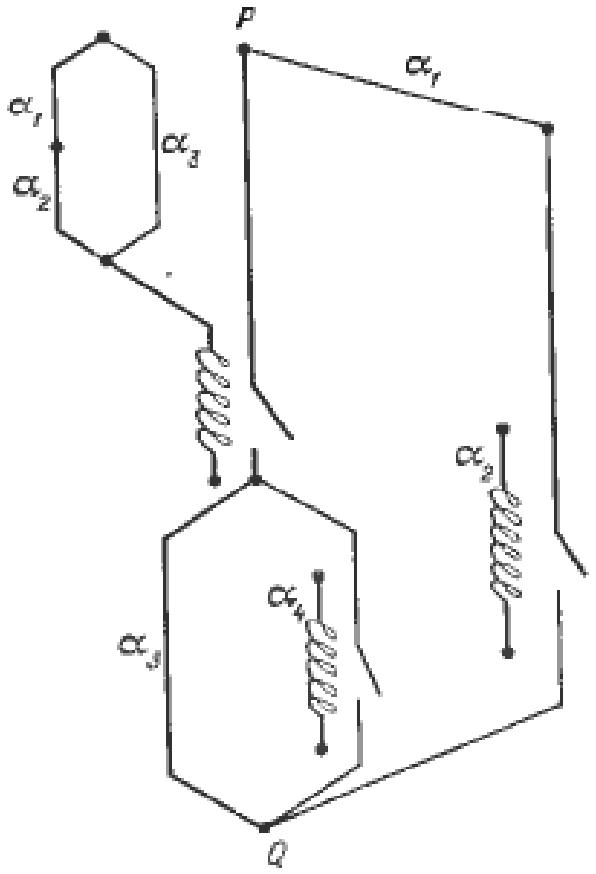



Рис. 6

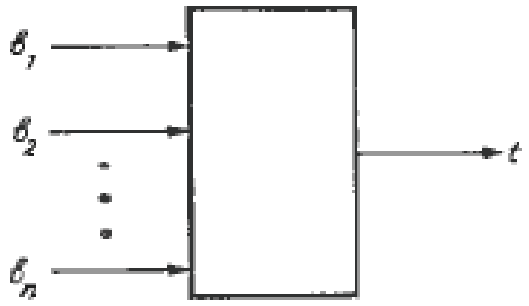



Рис. 7

рования формул логики предложений — с помощью так называемых функциональных элементов.

Пусть $F(X_1, ..., X_n)$ — произвольная булева функция, и пусть у нас имеется некоторое устройство — «ящичек», из которого «торчат» с одной стороны $n$ проводов $b_1, ..., b_n$ — их мы будем называть *входными каналами*, — а с другой еще один провод $t$ — *выходной канал* (рис. 7). Каждый входной канал может быть подключен к источнику тока. Если в канал $b_i$ поступает электрический импульс, мы будем говорить, что в наше устройство *по i-му входному каналу подается истинностное значение И*, а если не поступает — что в него по *i-му входному каналу подается истинностное значение Л*. Если по первому входному каналу в устройство подается истинностное значение $r^1$, по второму — $r^2$ и т. д., мы скажем, что *на вход* нашего устройства *подается вектор* $r = r^1r^2 ... r^n$. В зависимости от того, какой вектор подается на вход, в выходном канале появляется или не появляется электрический импульс; в первом случае мы скажем, что *на выходе* устройства *появляется истинностное значение И*, во втором — что *на выходе появляется Л*. Пусть теперь устройство удовлетворяет следующему условию: каков бы ни был $n$-мерный булев вектор $r$, всякий раз, когда он подается на вход устройства, на выходе появляется значение $F(r)$. Такое устройство называется *функциональным элементом, реализующим функцию F*. (При этом неважно, как устроен «ящичек» внутри.)

Пусть, далее, мы имеем булеву функцию от $k$ переменных $G(Y_1, ..., Y_k)$ и $k$ булевых функций от $n$ переменных: $F_1(X_1, ..., X_n)$, ..., $F_k(X_1, ..., X_n)$, и пусть для каждой из этих функций у нас есть реали-

зующий ее функциональный элемент. (Элемент, реализующий некоторую функцию, мы будем обозначать тем же символом, что и ее самое.) Для каждого $i = 1, \ldots, n$ мы соединим $i$-е входные каналы всех элементов $F_1, \ldots, F_k$ таким образом, что по ним всегда будет подаваться одно и то же истинностное значение, и для каждого $j = 1, \ldots, k$ к выходному каналу элемента $F_j$ подсоединим $j$-й входной канал

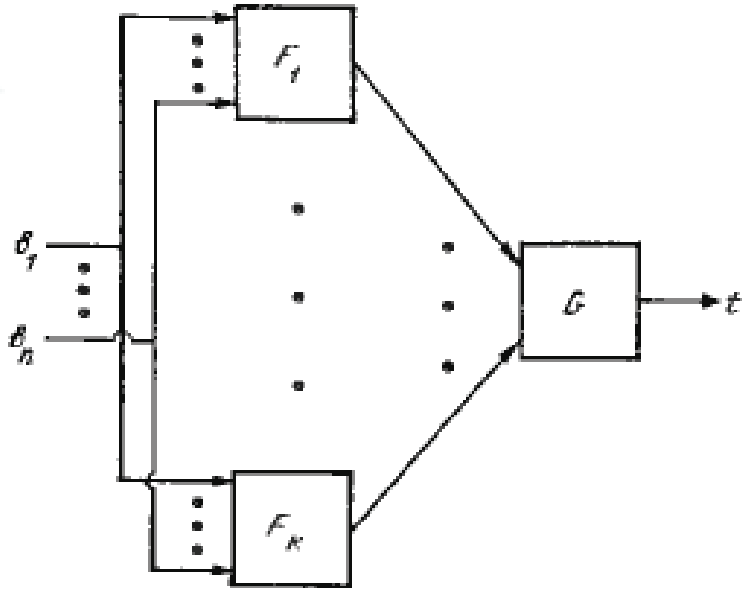



Рис. 8

элемента $G$ (рис. 8). Полученная схема будет, очевидно, работать точно так же, как работал бы элемент, реализующий функцию $G(F_1(X_1, \ldots, X_n), \ldots, F_k(X_1, \ldots, X_n))$, и мы также будем говорить, что эта схема *реализует* названную функцию.

Теперь ясно, что, каков бы ни был набор булевых функций $H_1, \ldots, H_s$, мы можем для любой функции, представимой в виде суперпозиции $H_1, \ldots, H_s$ в каком-либо числе, построить реализующую ее схему из функциональных элементов, реализующих $H_1, \ldots, H_s$. Но всякая формула логики предложений (кроме формул вида $X_i$, не содержащих пропозициональных связок) есть не что иное, как представление некоторой булевой функции в виде суперпозиции функций из набора $H_1, \ldots, H_5$, где

$$H_1(X_1, X_2) = X_1 \& X_2,\ H_2(X_1, X_2) = X_1 \vee X_2,$$

$$H_3(X_1, X_2) = X_1 \supset X_2,\ H_4(X_1, X_2) = X_1 \leftrightarrow X_2,$$

$$H_5(X_1) = \neg X_1,$$

и теорема о представлении булевой функции означает, что любая булева функция представима в виде суперпозиции функций из этого

набора[26]. Поэтому любая булева функция может быть реализована схемой из функциональных элементов, соответствующих перечисленным пяти функциям. Более того, из доказательства упомянутой теоремы ясно, что достаточно даже трех функций — $H_1$, $H_2$, $H_5$.

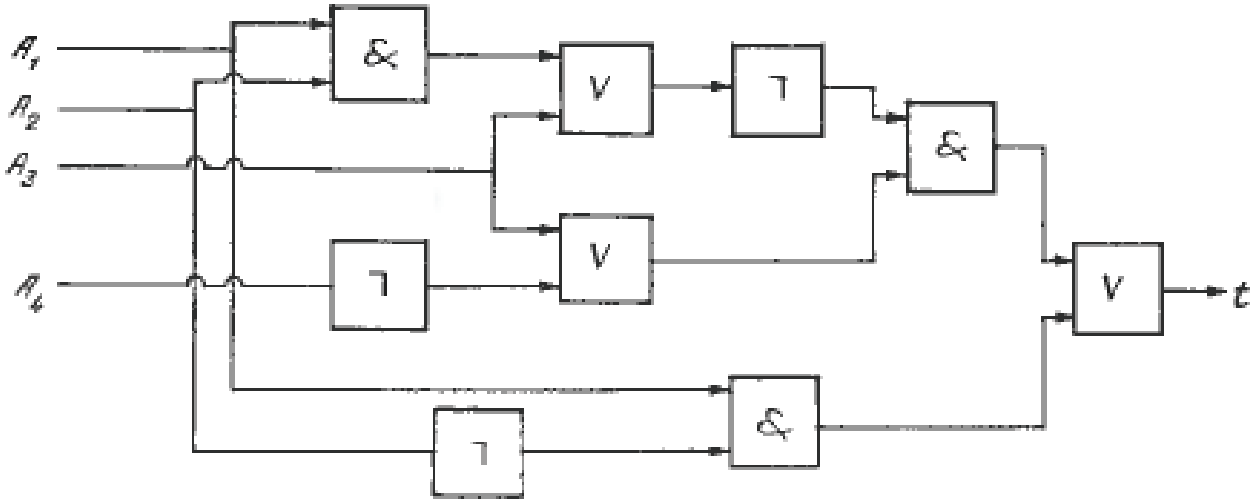



Рис. 9

Пример. Схема, изображенная на рис. 9, отвечает той же формуле, что и схема рис. 6. (Входные каналы обозначены так же, как переменные, значения которых на них подаются.)

3. Множество булевых функций называется *функционально полным* или просто *полным*, если любая булева функция представима в виде суперпозиции функций, принадлежащих этому множеству (иначе говоря — может быть реализована схемой из элементов, отвечающих функциям, входящим в это множество). Примерами полных множеств могут служить $\{H_1, \ldots, H_5\}$ и $\{H_1, H_2, H_5\}$.

Поскольку дизъюнкция представима через конъюнкцию и отрицание, а конъюнкция — через дизъюнкцию и отрицание (законы Де Моргана), множества $\{H_1, H_5\}$ и $\{H_2, H_5\}$ также полны, а ввиду равносильности $X_1 \vee X_2 \equiv \neg X_1 \supset X_2$ полным является и $\{H_3, H_5\}$. Всякое множество булевых функций, содержащее полное подмножество, само полно; поэтому множество булевых функций является полным, если оно содержит хотя бы одно из множеств $\{H_1, H_5\}$, $\{H_2, H_5\}$, $\{H_3, H_5\}$.

Можно было бы показать (см. задачу 28 в конце этой главы), что для множеств, состоящих из пропозициональных связок, т. е. содер-

[26] Это верно и для функций вида $X_i$, т. к. $X_i = \neg\neg X_i$. Можно, впрочем, считать $X_i$ «тривиальной суперпозицией» (ср. конъюнкции и дизъюнкции из одного члена).

жащихся в $\{H_1, ..., H_5\}$, верно и обратное: всякое полное подмножество множества $\{H_1, ..., H_5\}$ содержит хотя бы одно из трех перечисленных множеств.

Существуют и одноэлементные полные множества. Таково множество, единственным элементом которого является *штрих Шеффера* (обозначение $X|Y$) — булева функция, задаваемая следующей таблицей:

| $X$ | $Y$ | $X\|Y$ |
|---|---|---|
| *И* | *И* | *Л* |
| *И* | *Л* | *И* |
| *Л* | *И* | *И* |
| *Л* | *Л* | *И* |

(Очевидно, $X|Y \equiv \neg(X\&Y)$[27].) Читатель проверит, что $X|X \equiv \neg X$ и $(X|Y)\,|\,(X|Y) \equiv X\&Y$, откуда и следует представимость любой булевой функции с помощью суперпозиций через $X|Y$. Этим свойством обладает также, как легко убедиться аналогичным образом, функция $\neg(X \vee Y)$ (иногда обозначаемая через $X \downarrow Y$). Других функций двух переменных, обладающих этим свойством, не существует (см. задачу 29 в конце главы).

Необходимое и достаточное условие полноты множества булевых функций было получено американским математиком Э. Постом (Emil Leon Post, 1897—1954). Доказывать это условие мы не будем; его формулировку см. ниже (сноска 31 в этой главе).

### Задачи и упражнения

1) Построить истинностные таблицы для всех булевых функций от одной переменной $X_1$ и от двух переменных $X_1$, $X_2$.

2) Доказать, что число различных булевых функций от переменных $X_1$ ..., $X_n$ равно $2^{2^n}$.

3) а) Сколько существует приведенных булевых функций от переменных $X_1$, ..., $X_n$?

б) Для каждой приведенной булевой функции от двух переменных $X_1$, $X_2$ указать какую-либо представляющую ее формулу.

4) Доказать, что:

(а) $(X \vee \neg X)\&Y \equiv Y$;

(б) $X \vee (X\&Y) \equiv X$;

(в) $X \supset (Y \supset Z) \equiv Y \supset (X \supset Z)$;

[27] Ср. задачу 7 из гл. 2 (с. 87).

(г) $X_1 \& X_2 \& \ldots \& X_n \supset Y \equiv (X_1 \supset (X_2 \supset \ldots \supset (X_n \supset Y) \ldots))$;

(д) $X_2 \supset X_1 \vee X_2 \equiv \neg X_2 \& \neg X_3 \supset \neg X_2$;

(е) $\overset{k}{\underset{i=1}{\&}} (Z_i \supset Y) \& (\neg Z_1 \& \ldots \& \neg Z_k \supset Y) \equiv Y$[28].

5) Пусть $X$ означает «Иванов — студент», $Y$ — «Петров — студент», $Z$ — «Сидоров — студент». Для каждой из основных равносильностей групп I, II, III построить достаточно приемлемые стилистически русские предложения, выражающие левую и правую части этой равносильности. (Образец: «Или Иванов — студент, или хотя бы один из двоих, Петров или Сидоров — студент»; см. также пример на с. 91.)

6) Показать, что так называемое *симметрическое вычитание* множеств (симметрическая разность между $A$ и $B$ — обозначение $A \div B$ — равна по определению $(A \cup B) \setminus (A \cap B)$) соответствует отрицанию эквиваленции[29] в том смысле, в каком объединение соответствует дизъюнкции и пересечение — конъюнкции (с. 98).

7) Привести к д. н. ф. (с помощью тождественных преобразований) и, если можно, упростить:

(а) $(X \supset Y) \supset (Y \supset X)$;

(б) $X \vee \neg Z \supset Y \& Z$;

(в) $(X \vee \neg Y \supset X \& Z) \supset \neg (X \supset \neg X) \vee Y \& \neg Z$;

(г) $(\neg X \vee Z) \& (Y \supset (U \supset X))$;

(д) $\neg((X \supset \neg(Y \supset \neg Z \vee X)) \& (Y \supset X \& Z))$;

(е) $(X_1 \supset (X_2 \supset \ldots \supset (X_{n-1} \supset X_n) \ldots))$;

(ж) $X_1 \vee \ldots \vee X_n \supset Y_1 \& \ldots \& Y_m$.

8) Привести формулы предыдущей задачи к к. н. ф. (с помощью тождественных преобразований).

9) Доказать тождественную истинность формул:

(а) $Y \supset (X \supset Y)$;

(б) $\neg X \supset (X \supset Y)$;

(в) $(X \supset Y) \supset ((\neg X \supset Y) \supset Y)$;

(г) $(X \supset (Y \supset Z)) \supset ((X \supset Y) \supset (X \supset Z))$.

10) Доказать тождественную ложность формул:

(а) $X \vee \neg X \supset Y \& \neg Y$;

---

[28] Этой равносильностью формализуется широко употребительный в математике прием доказательства разбором случаев: чтобы доказать утверждение $Y$, доказывают его справедливость при каждом из условий $Z_1, \ldots, Z_k, \neg Z_1 \& \ldots \& \neg Z_k$, в совокупности исчерпывающих все возможности. Ср. сноску[5] на с. 93.

[29] Отрицание эквиваленции называют иногда *разделительной дизъюнкцией*.

(б) $7(7(\ldots 7(7(X\&7X\supset Y_1)\supset Y_2)\supset\ldots\supset Y_{n-1})\supset Y_n)\supset Z\&7Z$;

(в) $(X_1\&\ldots\&X_n)\ \&\ (X_1\vee\ldots\vee X_n\supset Y)\ \&\ 7Y$.

11) Вывести равносильности, аналогичные соотношениям IV5 и IV6, с левыми частями $\mathfrak{X}\supset X$ и $X\supset\mathfrak{Y}$.

12) Доказать, что $X\&7Y\supset\mathfrak{Y}\equiv X\supset Y$.

13) Для каждой булевой функции одной и двух переменных (см. задачу 1)) найти представляющую ее формулу способом, использованным в доказательстве теоремы о представлении булевой функции.

14) Двумя способами — с помощью истинностных таблиц и с помощью тождественных преобразований — привести к с. д. н. ф. формулы задачи 7.

15) Булевы функции $F(X_1,\ldots X_n)$ и $F^*(X_1,\ldots,X_n)$ называют *двойственными* друг другу, если $F^*(X_1,\ldots,X_n)=7F(7X_1,\ldots,7X_n)$. Доказать, что двойственные друг другу формулы представляют двойственные друг другу функции.

16) Найти все *самодвойственные*, т.е. двойственные самим себе (см. предыдущую задачу) булевы функции одной и двух переменных.

17) Для произвольного $n$-мерного булева вектора $r$ положим $D^r=\tilde{X}_1^r\vee\ldots\vee\tilde{X}_n^r$, где $\tilde{X}_i^r$ есть $7X_i$ при $r^i=И$ и $X_i$ при $r^i=Л$. Показать, что $D^r(r)=Л$ и $D^r(r')=И$ при $r'\neq r$.

18) Опираясь на результат предыдущей задачи, дать доказательство теоремы о представлении булевой функции, аналогичное приведенному в § 3.3, но с использованием с. к. н. ф. Извлечь из этого доказательства еще один способ приведения формулы к с. к. н. ф. и еще один способ построения формулы по истинностной таблице.

19) Привести формулы задачи 7 к с. к. н. ф. тремя способами: с помощью тождественных преобразований (используя решение задачи 8), с помощью с. д. н. ф. (используя решение задачи 14) и с помощью истинностных таблиц без обращения к с. д. н. ф. (см. задачу 18).

20) Доказать, что:

(а) Каждая из формул $X\vee Y$ и $X\vee7Y$ есть следствие формулы $7(X\supset Y)$;

(б) Формула $X\&Y\vee7X\&Y\vee7X\&7Y$ есть следствие формулы $X\leftrightarrow Y$;

(в) Формула $X\supset Y$ есть следствие формул $7X\vee Y\vee Z$ и $7X\vee Y\vee7Z$;

(г) Формула $7X_1\supset X_2$ есть следствие формул $X_1\vee X_2\vee X_3\vee X_4$, $X_1\vee X_2\vee X_3\vee7X_4$, $X_1\vee X_2\vee7X_3\vee X_4$, $X_1\vee X_2\vee7X_3\vee7X_4$.

21) Доказать (методом математической индукции), что формула $X_1\supset X_n$ есть следствие формул $X_1\supset X_2$, $X_2\supset X_3$, ..., $X_{n-1}\supset X_n$.

22) (а) Доказать, что каждая из формул

$X_1\&\ldots\&X_n\supset Y_1\&\ldots\&Y_m$,

$X_1\vee\ldots\vee X_n\supset Y_1\vee\ldots\vee Y_n$

является следствием формулы

$(X_1\supset Y_1)\&\ldots\&(X_n\supset Y_n)$.

(б) Верны ли обратные утверждения?

23) Изобразить на чертежах релейно-контактные схемы и схемы из функциональных элементов, отвечающие формулам:

(а) $X_2\&\neg X_1 \vee X_2\&\neg X_3$;

(б) $\neg(X_1 \vee \neg X_2)\&(X_3\&\neg X_4 \vee \neg X_1)$;

(в) $(X_1 \vee X_2 \vee \neg X_3)\&(\neg X_1 \vee X_2) \vee (X_2 \vee X_3)$;

24) Определим на множестве $n$-мерных булевых векторов отношение $<$, положив $r_1 < r_2$, если, считая $Л < И$, имеем: $\alpha)$ $r_1^i \le r_2^i$ для каждого $i = 1, \ldots, n$; $\beta)$ хотя бы для одного $i$ $r_1^i < r_2^i$. Булева функция $F(X_1, \ldots, X_n)$ называется *монотонной*, если $r_1 < r_2$ влечет $F(r_1) \le F(r_2)$. Найти все монотонные функции одной и двух переменных.

25) Булева функция $F(X_1, \ldots, X_n)$ называется *линейной*, если она представима в виде $X_{i_1} + \ldots + X_{i_m} + A$, где $1 \le i_1 < \ldots i_k \le n$, $+$ означает разделительную дизъюнкцию (см. сноску 29), и $A$ — константа $И$ или $Л$ [30]. Найти все линейные функции одной и двух переменных.

26) Множество $M$ булевых функций называется *функционально замкнутым*, если суперпозиция функций, принадлежащих $M$, также принадлежит $M$. Доказать, что следующие множества функционально замкнуты:

(а) множество функций, *сохраняющих* $И$, т. е. таких, что $F(И, И, \ldots, И) = И$;

(б) множество функций, сохраняющих $Л$ (определяются аналогично);

(в) множество монотонных функций (см. задачу 24);

(г) множество линейных функций (см. задачу 25);

(д) множество самодвойственных функций (см. задачу 16)[31]

27) Будем говорить, что булева функция $F(X_1, \ldots, X_n)$ обладает свойством $\alpha_n$, если либо $n = 1$, либо число $n$-мерных векторов, на которых $F$ принимает значение $И$, четно. Доказать, что если функции $F(X_1, \ldots, X_k, Y_1, \ldots, Y_l)$ и $G(X_1, \ldots X_k, Z_1, \ldots, Z_m)$ $(k, l, m = 0, 1, \ldots)$ обладают свойствами $\alpha_{k+l}$ и $\alpha_{k+m}$ соответственно, то функция $F(X_1, \ldots, X_k, Y_1, \ldots, Y_l) \Leftrightarrow G(X_1, \ldots, X_k, Z_1, \ldots, Z_m)$ обладает свойством $\alpha_{k+l+m}$.

28) Доказать, что всякое полное множество пропозициональных связок содержит хотя бы одно из множеств $\{H_1, H_5\}$, $\{H_2, H_5\}$, $\{H_3, H_5\}$ (с. 122). [Указание: Сначала доказать, пользуясь задачей 26а, что всякое полное множество пропозициональных связок содержит $H_5$. Затем воспользоваться задачей 27.]

---

[30] Определения этой и предыдущей задач станут прозрачнее, если вместо $И$ писать 1 и вместо $Л$ — 0 (ср. замечание 2) на с. 52). Разделительная дизъюнкция превратится при этом в сложение по модулю 2 (а конъюнкция — в умножение).

[31] Из результата этой задачи немедленно следует, что для полноты множества булевых функций необходимо, чтобы оно для каждого из множеств (а) — (д) содержало хотя бы одну функцию, в него не входящую (поскольку ни одно из этих множеств не исчерпывает всех булевых функций). В действительности сформулированное условие является и достаточным. Это и есть условие Поста (с. 123). Доказательство его достаточности (и необходимости) см. в книге [Гиндикин 1972], § 6.

29) Доказать, что никакая функция двух переменных, отличная от $X|Y$ и $X \downarrow Y$ (с. 123), не образует одна полного множества. [Указание. Воспользоваться задачами 26 и 27.]

30) Назовем систему соотношений вида $\mathfrak{C} \equiv \mathfrak{G}$, где $\mathfrak{C}$ и $\mathfrak{G}$ — формулы, полной, если, каковы бы ни были две равносильные формулы $\mathfrak{A}$ и $\mathfrak{B}$, можно преобразовать $\mathfrak{A}$ в $\mathfrak{B}$, применяя соотношения из данной системы. (Применение соотношений понимается в том же смысле, как применение основных равносильностей при тождественных преобразованиях, описанных в § 3.2.)

(а) Доказать, что система, состоящая из основных равносильностей групп I—III, полна.

(б) Найти все минимальные полные подсистемы этой системы.

ГЛАВА

4

# СЕМАНТИКА ЛОГИКИ ПРЕДИКАТОВ

## § 4.1. ИНТЕРПРЕТАЦИИ И МОДЕЛИ. ВЫПОЛНИМОСТЬ, ИСТИННОСТЬ И РАВНОСИЛЬНОСТЬ ФОРМУЛ

1. Логикой предикатов называется раздел математической логики, в котором изучаются свойства операций над предикатами и выражений, образованных с помощью этих операций — т. е. тех выражений, которые мы назвали формулами логики предикатов. При этом имеются в виду только такие свойства, которые не зависят от природы элементарных предикатов, входящих в формулы[1]. Поэтому при изложении логики предикатов мы будем считать, что входящие в формулы[2] знаки элементарных предикатов могут означать л ю б ы с предикаты от соответствующих переменных; нам будет удобно, таким образом, говорить, что в формулы входят не предикаты, а символы предикатов — иначе, *предикатные символы* — от некоторых переменных и что эти предикатные символы можно замещать любыми предикатами от тех же переменных. (Фактически эти предикатные символы, выступающие вместо конкретных элементарных предикатов, суть переменные, значениями которых служат предикаты — «предикатные перемеиные», в отличие от «предметных переменных», от которых предикаты зависят.)

Пример. Формула $\forall x\, \exists y F(x, y)$ содержит один предикатный сим-

[1] Свойства, зависящие от природы элементарных предикатов, относятся не к логике, а к тем математическим дисциплинам, к которым принадлежат выражаемые этими элементарными предикатами свойства и отношения. Например, истинность предложения $\forall x \forall y \forall z(d(x, y) \& d(y, z) \supset d(x, z))$, где $d(x, y)$ означает «$x$ делится на $y$», есть факт арифметики, а не логики.

[2] Слово «формула» в этой главе всегда, если не оговорено противное, означает «формула логики предикатов».

вол $F$ (от двух переменных). При замещении $F$ определенным на множестве действительных чисел $\mathbf{R}$ предикатом $x < y$ формула превращается в истинное предложение «Для всякого действительного числа существует большее его действительное число», при замещении определенным на $R$ предикатом $x > y$ — в истинное предложение «Для всякого действительного числа существует меньшее его действительное число», при замещении предикатом $x > y$, определенным на этот раз на множестве неотрицательных действительных чисел — в ложное предложение «Для всякого неотрицательного действительного числа существует меньшее его неотрицательное действительное число», при замещении предикатом «$x$ есть корень уравнения $y$» с областью определения $\mathbf{R} \times Eq_2$, где $Eq_2$ есть множество квадратных уравнений с действительными коэффициентами — в истинное предложение «Всякое действительное число служит корнем некоторого квадратного уравнения с действительными коэффициентами», при замещении предикатом «$y$ есть корень уравнения $x$» с областью определения $Eq_2 \times \mathbf{R}$ — в ложное предложение «Всякое квадратное уравнение с действительными коэффициентами имеет действительный корень».

Задача. Найти такие замещения предикатных символов $F$ и $G$ в формуле $\exists y F(x, y) \supset G(x)$ конкретными предикатами, чтобы получился (а) тождественно истинный предикат; (б) тождественно ложный предикат; (в) предикат, не являющийся ни тождественно истинным, ни тождественно ложным. Выразить полученные предикаты словесно.

Итак, мы будем рассматривать формулы, получаемые из предикатных символов с помощью кванторов и пропозициональных связок. (Более точное определение формулы логики предикатов мы отложим до гл. 6.) Каждый предикатный символ имеет определенную *вместимость*: он может быть *одноместным*, *двуместным* и т. д.; ради общности мы будем рассматривать также *нульместные* предикатные символы (фактически играющие роль пропозициональных переменных[3]). Будем предполагать при этом, что предикатные символы разной вместимости всегда различны.

Пусть $M$ — некоторое множество формул. Сопоставим каждому предикатному символу, входящему хотя бы в одну из формул этого множества, некоторый предикат той же вместимости, что и данный символ. (Нульместным предикатным символам сопоставляются предложения[4].) В этом случае мы будем говорить, что задана *интер-*

[3] Таким образом, формулы логики предложений становятся теперь частным случаем формул логики предикатов.

[4] Таким образом, мы формально считаем всякое предложение (истинное или ложное — мы вообще рассматриваем только такие!) «*нульместным предикатом*».

*претация*[5] *множества M*. В частности, если $M$ одноэлементно, будем говорить об *интерпретации формулы*, если двухэлементно (трехэлементно и т. д.) — об *общей интерпретации двух* (*трех* и т. д.) *формул*.

Если все предикаты, сопоставляемые символам, входящим в формулы из $M$, определены на одном и том же множестве $E$, мы будем называть $E$ *основным множеством* данной интерпретации. Впрочем, мы всегда можем считать, что все предикаты определены на одном и том же множестве, рассматривая объединение всех множеств, участвующих в данной интерпретации, и заменяя каждый предикат $F(x_1, ..., x_n)$ предикатом $x_1 \in M_1 \& ... \& x_n \in M_n \& F(x_1, ..., x_n)$, где $M_i$ — область изменения переменной $x_i$. В дальнейшем мы всегда так и будем поступать и без дальнейших пояснений будем говорить об *основном множестве интерпретации*.

Очевидно, всякая интерпретация некоторого множества формул является одновременно интерпретацией любого его подмножества (в частности — любой входящей в него формулы).

Если дана интерпретация формулы, то при замещении каждого предикатного символа сопоставленным ему в данной интерпретации предикатом эта формула превращается в п р е д и к а т (зависящий от всех входящих в нее свободных переменных), если она не замкнута, и в п р е д л о ж е н и е, если она замкнута.

**Пример.** Пусть $\Phi$ — множество всевозможных формул, содержащих трехместные предикатные символы $S$ и $M$, двуместный символ $E$ и одноместные символы $N$ и $I$ и не содержащих никаких других предикатных символов. Рассмотрим следующие интерпретации множества $\Phi$, которые будем обозначать $\Delta_1, ..., \Delta_5, \Delta_6^n$.

$\Delta_1$: Основным множеством служит множество натуральных чисел **N**. Предикатному символу $S$ отвечает предикат $S_1(x, y, z)$, означающий «$x + y = z$», символу $M$ предикат $M_1(x, y, z)$ — «$xy = z$», символу $E$ предикат $E_1(x, y)$ — «$x = y$», символу $N$ предикат $N_1(x)$ — «$x = 0$», символу $I$ предикат $I_1(x)$ — «$x = 1$».

$\Delta_2 — \Delta_5$: Основными множествами служат в $\Delta_2$ множество целых чисел **Z**, в $\Delta_3$ — множество рациональных чисел **Q**, в $\Delta_4$ — множество действительных чисел **R**, в $\Delta_5$ — множество $\{0, 1, 2, ..., 10\}$. Предикаты определяются аналогично $\Delta_1$.

$\Delta_6^n$: Основное множество состоит из всевозможных квадратных матриц размерности $n$ с действительными элементами. Предикаты определяются аналогично $\Delta_1$, но при этом сложение и умножение

[5] От лат. *interpretatio* — «разъяснение, истолкование».

понимаются в «матричном» смысле, 0 заменяется нулевой матрицей и I — единичной матрицей.

Рассмотрим теперь следующие формулы из $\Phi$:

(1) $\exists z(S(x, y, z)\&\forall t(S(x, y, t)\supset E(t, z)))$;

(2) $S(x, y, t)\&S(t, z, u)\&S(y, z, v)\&S(x, v, w)\supset E(u, w)$;

(3) $S(x, y, z)\&N(y)\supset E(x, z)$;

(4) $\exists y\forall z(S(x, y, z)\supset N(z))$;

(5) $S(x, y, z)\&S(y, x, t)\supset E(z, t)$;

(6) $\exists z(M(x, y, z)\&\forall t(M(x, y, t)\supset E(t, z)))$;

(7) $M(x, y, t)\&M(t, z, u)\&M(y, z, v)\&M(x, v, w)\supset E(u, w)$;

(8) $S(x, y, t)\&M(t, z, u)\&M(x, z, v)\&M(y, z, w)\&S(v, w, r)\supset$ $\supset E(u, r)$;

(9) $M(x, y, z)\&I(y)\supset E(x, z)$;

(10) $\neg N(x)\supset\exists y\forall z(M(x, y, z)\supset I(z))$;

(11) $M(x, y, z)\&M(y, x, t)\supset E(z, t)$.

В интерпретации $\Delta_1$ формула (1) превращается в определенный на N двуместный предикат $\exists z((x + y = z)\&\forall t(x + y = t\supset t = z))$ (тождественно истинный, т. к. для любых двух натуральных чисел существует их сумма и она единственна), формула (2) — в семиместный предикат $(x + y = t)\&(t + z = u)\&(y + z = v)\&(x + v = w\supset(v = w)$ (также тождественно истинный ввиду ассоциативности сложения), формула (4) — в одноместный предикат $\exists y\forall z((x + y = z)\supset(z = 0))$ (дающий истинное предложение для $x = 0$ и ложное для $x > 0$). Для остальных формул читатель найдет соответствующие предикаты сам. В интерпретациях $\Delta_2$ — $\Delta_5$ получатся такие же предикаты, но с другими областями определения. При этом, например, предикат $\exists y\forall z((x + y = z)\supset(z = 0))$ в $\Delta_2$ — $\Delta_4$ (но не в $\Delta_5$) будет тождественно истинным, а предикат $\exists z((x + y = z)\&\ \forall t(x + y = t\supset t = z))$ остается тождественно истинным в $\Delta_2$ — $\Delta_4$, но перестает быть таковым в $\Delta_5$. Аналогичные предикаты получатся и в $\Delta_6^n$, только 0 нужно будет заменить нулевой матрицей и I — единичной.

Задача. Поменяв местами сложение и умножение в интерпретациях $\Delta_1$ — $\Delta_6^n$, т. е. при тех же основных множествах сопоставив символам $S$, $M$, $E$, $N$, $I$ предикаты $xy = z$, $x + y = z$, $x = y$, $x = 1$, $x = 0$ соответственно, исследовать формулы (1) — (11) на истинность в полученных интерпретациях.

2. Пусть $\mathfrak{A}$ — произвольная формула и $\Delta$ — некоторая ее интерпретация. Мы будем говорить, что формула $\mathfrak{A}$ *истинна в интерпретации* $\Delta$, если она превращается в этой интерпретации в тождественно истинный предикат (в случае, когда она не замкнута) или в

истинное предложение (в случае, когда она замкнута). Будем говорить, далее, что формула $\mathfrak{A}$ *выполнима в интерпретации* $\Delta$, если она превращается в эти интерпретации в не тождественно ложный предикат (в случае, когда она не замкнута) или в истинное предложение (в случае, когда она замкнута). (Таким образом, для замкнутых формул понятия истинности и выполнимости в интерпретации совпадают.)

Замечания. 1) Очевидно, формула $\mathfrak{A}$ тогда и только тогда истинна в интерпретации $\Delta$, когда ее отрицание невыполнимо в $\Delta$.

2) Если основное множество интерпретации конечно, то эту интерпретацию можно задать (с точностью до истинностных значений предикатов) с помощью таблиц, в которых для любого $n$-местного предикатного символа и любого набора $n$ элементов основного множества указано истинностное значение отвечающего данному символу предиката на данных элементах. При таком задании интерпретации истинность и выполнимость формулы в ней можно проверить простым перебором всевозможных комбинаций значений свободных переменных.

Пусть теперь $M$ — множество формул и $\Delta$ — некоторая его интерпретация. Если каждая формула из $M$ истинна в $\Delta$, говорят, что $\Delta$ является *моделью множества* $M$. (В частном случае, когда $M$ состоит из одной формулы, $\Delta$ называют *моделью* этой *формулы*.)

Возвращаясь к только что рассмотренному примеру, мы видим, что $\Delta_1$ служит моделью для формул (1) — (3), (5) — (9) и (11), $\Delta_2$ — для (1) — (9) и (11), $\Delta_3$ и $\Delta_4$ — для (1) — (11), $\Delta_5$ — для (2), (3), (5), (7) — (9) и (11), $\Delta_6^n$ — для (1) — (9). В $\Delta_1$ не являются истинными формулы (4) и (10), в $\Delta_2$ — формула (10), в $\Delta_5$ — (1), (4), (6) и (10), в $\Delta_6^n$ (при $n > 1$) — (10) и (11). В то же время все формулы (1) — (11) выполнимы во всех этих интерпретациях. Во всем этом читатель немедленно убедится сам. (Например: формула (10) выполнима, но не истинна в $\Delta_6^n$, так как для некоторых, но не для всех, ненулевых матриц существуют обратные.) Примером формулы, невыполнимой в $\Delta_6^n$, может служить отрицание любой из формул (1) — (9); аналогично для остальных интерпретаций.

Еще один пример был фактически рассмотрен выше (с. 128—129); там мы привели пять интерпретаций формулы $\forall x \exists y F(x, y)$, в трех из которых она выполнима (или, что здесь то же самое, истинна) и в двух невыполнима.

Заметим, что формула $\mathfrak{A}(x)$, содержащая свободную переменную $x$, истинна в интерпретации $\Delta$ тогда и только тогда, когда в ней истинна формула $\forall x \mathfrak{A}(x)$. (В самом деле, одноместный предикат $F_0(x)$ тогда и только тогда тождественно истинен, когда $\forall x F_0(x)$ —

истинное предложение; $(k+1)$-местный предикат $F(x, y_1, \ldots, y_n)$ тогда и только тогда тождественно истинен, когда тождественно истинен $k$-местный предикат $\forall x F(x, y_1, \ldots, y_n)$.) Например, вместе с формулой $\exists z S(x, y, z)$, истинной, очевидно, во всех интерпретациях $\Delta_1 - \Delta_4$ и $\Delta_6^7$, в тех же интерпретациях истинны формулы $\forall x \exists z S(x, y, z)$, $\forall y \exists x S(x, y, z)$, $\forall x \forall y \exists z S(x, y, z)$.

Аналогично, формула $\mathfrak{A}(x)$ выполнима в интерпретации тогда и только тогда, когда выполнима формула $\exists x \mathfrak{A}(x)$.

Мы будем называть формулу *всюду истинной*, если она истинна во всякой своей интерпретации, и *выполнимой*, если существует интерпретация, в которой она выполнима.

Замечания. 1) Во избежание недоразумений нужно всегда помнить, что слово «выполнимая» с добавлением слов «в такой-то интерпретации» означает одно, а без добавления — другое. (Можно было бы назвать формулу, выполнимую хотя бы в одной своей интерпретации, «где-нибудь выполнимой», но включать слово «где-нибудь» в состав термина неудобно.)

2) Вместо «всюду истинная» в литературе на русском языке часто употребляется неудачный термин «*общезначимая*»[6].

3) Из предыдущего следует, что формула $\mathfrak{A}(x)$ со свободной переменной $x$ тогда и только тогда всюду истинна, когда всюду истинна формула $\forall x \mathfrak{A}(x)$, и тогда и только тогда выполнима, когда выполнима формула $\exists x \mathfrak{A}(x)$.

4) Очевидно (см. замечание 1 на с. 132), формула тогда и только тогда всюду истинна, когда ее отрицание невыполнимо.

Подобно тождественно истинным формулам логики предложений, всюду истинные формулы логики предикатов выражают «абсолютно истинные» предложения. (Незамкнутая всюду истинная формула становится «абсолютно истинным» предложением, если связать все свободные переменные кванторами общности.)

Примеры. 1) Формула $F(x) \vee \neg F(x)$ всюду истинна. В самом деле, если заместить $F$ произвольным одноместным предикатом $F_0$ и затем дать переменной $x$ произвольное значение, то получится истинное (в силу закона исключенного третьего) предложение $F(x_0) \vee \neg F(x_0)$. Таким образом, при любом замещении $F$ конкретным предикатом наша формула переходит в тождественно истинный предикат.

2) Формула $\forall x(F(x) \vee \neg F(x))$ также всюду истинна (см. выше замечание 3).

3) Формула $\forall x F(x) \supset \exists x F(x)$ всюду истинна, так как для любого предиката $F_0$, для которого предложение $\forall x F_0(x)$ истинно, предложе-

[6] Возникший в результате неправильного перевода немецкого *allgemeingultig*.

ние $\exists x F_0(x)$ также истинно[7], а поэтому истинна и импликация $\forall x F_0(x) \supset \exists x F_0(x)$.

4, 5) Формула $\exists y \forall x F(x, y) \supset \forall x \exists y F(x, y)$ всюду истинна. Действительно, если заместить $F$ произвольным двуместным предикатом $F_0$, выражающим некоторое бинарное отношение, то посылка нашей формулы утверждает, что в области прибытия отношения имеется элемент, связанный этим отношением с каждым элементом области отправления, а заключение — что для каждого элемента области отправления существует — вообще говоря, свой — связанный с ним элемент области прибытия. Очевидно, из истинности посылки вытекает истинность заключения. В то же время при истинном заключении посылка может оказаться ложной; так будет, например, если $F_0$ — определенный на множестве действительных чисел предикат $x < y$ (для каждого действительного числа найдется большее, но нет такого числа, которое было бы больше всех действительных чисел). Следовательно, обратная импликация $\forall x \exists y F(x, y) \supset \exists y \forall x F(x, y)$ не истинна в этой интерпретации и, значит, не всюду истинна. Однако она выполнима (например, она выполнима в интерпретации, в которой $F$ замещается предикатом $x \leq y$, определенным на множестве неположительных действительных чисел).

6) Другим примером выполнимой, но не всюду истинной формулы может служить $\forall x \exists y F(x, y)$: на с. 129 мы указали для нее и такие интерпретации, в которых она выполнима, и такие, в которых она не истинна.

7, 8) Формула $F(x) \& \neg F(x)$ невыполнима: каким бы предикатом $F_0$ мы ни заместили символ $F$, предикат $F_0(x) \& \neg F_0(x)$ будет тождественно ложен. Вместе с этой формулой невыполнима и $\exists x(F(x) \& \& \neg F(x))$ (см. замечание 3).

Задачи. 1) (а) Показать, что формулы

$$\forall x F(x) \vee \forall x G(x) \supset \forall x(F(x) \vee G(x)),$$

$$\exists x(F(x) \& G(x)) \supset \exists x F(x) \& \exists x G(x)$$

всюду истинны.

(б) Показать, что обратные этим формулам импликации не всюду истинны, но выполнимы.

2) Показать, что формулы $F(x) \& \neg \exists x F(x)$ и $\forall x(F(x) \supset G(x)) \& \& \exists x(F(x) \& \neg G(x))$ невыполнимы.

3. В семантике логики предложений главным рабочим инструментом было у нас понятие равносильности формул. Аналогичное

[7] Стоит напомнить, что область определения предиката всегда считается непустой.

понятие мы введем и в логике предикатов; здесь оно также играет первостепенную роль в семантических рассмотрениях. Однако прежде чем определить это понятие, нам придется обобщить понятие равносильности предикатов, которое мы ввели в § 2.2 (конец пункта 2) только для случая, когда предикаты зависят в точности от одних и тех же переменных. Именно: предикаты $F(x_1, \ldots, x_n, y_1, \ldots, y_k)$ и $G(x_1, \ldots, x_n, z_1, \ldots, z_l)$ $(n, k, l = 0, 1, \ldots)$ мы будем называть *равносильными*, если для любого набора $x_1^0, \ldots, x_n^0, y_1^0, \ldots, y_k^0, z_1^0, \ldots, z_l^0$ значений переменных $x_1, \ldots, z_l$ истинностные значения предложений $F(x_1^0, \ldots, x_n^0, y_1^0, \ldots, y_k^0)$ и $G(x_1^0, \ldots, x_n^0, z_1^0, \ldots, z_l^0$ совпадают. (В этом случае функция $F$ в действительности не зависит от $y_1, \ldots, y_k$, а $G$ — от $z_1, \ldots, z_l$, так что эти переменные «несущественны» для соответствующих функций (ср. § 3.1). Можно было бы по аналогии с § 3.1 определить и «основу» предиката.) При $k = l = 0$ это определение переходит в прежнее. Если $n = k = 0$, то равносильность предиката $F$ предикату $G(z_1, \ldots, z_l)$ означает, что этот последний тождественно истинен или тождественно ложен; аналогично для $F(y_1, \ldots, y_k)$ при $n = l = 0$. Поэтому мы могли бы теперь определить тождественно истинный (тождественно ложный) предикат как такой, который равносилен истинному, соответственно ложному предложению. При этом истинное (ложное) предложение оказывается частным случаем тождественно истинного, соответственно тождественно ложного предиката, и, полагая в определении равносильности предикатов $n = k = l = 0$, мы можем назвать два предложения *равносильными*, если совпадают их истинностные значения.

Для обозначения равносильности предикатов в общем случае мы сохраним введенное в § 2.2 обозначение $\equiv$.

Нетрудно доказать — это предоставляется читателю,— что отношение равносильности предикатов является отношением эквивалентности.

**Пример.** Предикаты $Q_1(x, y, z)$ и $Q_2(v, y, z, t)$, определенные на множестве действительных чисел и означающие соответственно $((x < y) \vee (x > y) \vee (x = y)) \& (y < z)$ и $((v = t) \& \neg(v = t)) \vee (y < z)$, равносильны, т. к. каждое из предложений $Q_1(x^0, y^0, z^0)$ и $Q_2(v^0, y^0, z^0, t^0)$ истинно тогда и только тогда, когда $y^0 < z^0$. (Эти предикаты равносильны также предикату $y < z$.)

**Задача.** а) Доказать, что на конечном множестве, состоящем из $m$ элементов, существует ровно $2^m$ попарно неравносильных одноместных предикатов.

б) Сколько существует попарно неравносильных $n$-местных предикатов на конечном множестве, состоящем из $m$ элементов?

Теперь мы можем определить понятие равносильности формул.

Именно, две формулы называются *равносильными*, если в любой общей интерпретации входящих в обе формулы предикатных символов они превращаются в равносильные предикаты.

Для обозначения равносильности формул будет использоваться все тот же знак $\equiv$.

Легко проверить — читатель сделает это сам,— что равносильность формул является отношением эквивалентности.

Примеры. 1) $\neg(F(x)\&G(x)) \equiv \neg F(x) \vee \neg G(x)$.

В самом деле, если мы заместим $F$ и $G$ произвольными одноместными предикатами $F_0$ и $G_0$ и затем дадим переменной $x$ произвольное значение $x_0$, то формула $\neg(F(x)\&G(x))$ превратится в предложение $\neg(F_0(x_0)\&G_0(x_0))$, формула $\neg F(x) \vee \neg G(x)$ — в предложение $\neg F_0(x_0) \vee \neg G_0(x_0)$; но истинностные значения этих предложений совпадают. Таким образом, истинностные значения предикатов $\neg(F_0(x)\&G_0(x))$ и $\neg F_0(x) \vee \neg G_0(x)$ совпадают при любых значениях $x$, т. е. эти предикаты равносильны. Итак, при любом замещении символов $F$ и $G$ конкретными предикатами, т. е. в любой общей интерпретации наших формул, эти формулы превращаются в равносильные предикаты.

2) $\forall x(F(x)\&G(x)) \equiv \forall x F(x) \& \forall x G(x)$.

Действительно, во всякой общей интерпретации этих формул левая часть превращается в истинное предложение, если предикат $F(x)$ & $G(x)$ тождественно истинен, а в противном случае она превращается в ложное предложение. Правая же часть превращается в истинное предложение, если истинны оба предложения $\forall x F(x)$ и $\forall x G(x)$, и в ложное в противном случае. Таким образом, та и другая части превращаются в истинные предложения, когда оба предиката $F$ и $G$ тождественно истинны, и в ложные предложения в противном случае.

3) Если $\mathfrak{A}(x)$ и $\mathfrak{B}(x)$ — произвольные формулы, содержащие свободную переменную $x$, то из $\mathfrak{A}(x) \equiv \mathfrak{B}(x)$ следует $\forall x \mathfrak{A}(x) \equiv \forall x \mathfrak{B}(x)$ и $\exists x \mathfrak{A}(x) \equiv \exists x \mathfrak{B}(x)$.

В самом деле, пусть формула $\mathfrak{A}(x)$ содержит, кроме $x$, свободные переменные $x_1, \ldots, x_n, y_1, \ldots, y_k$, а $\mathfrak{B}(x)$ — $x_1, \ldots, x_n, z_1, \ldots, z_l$ ($n, k, l = 0, 1, \ldots$), причем общими переменными являются только $x, x_1, \ldots, x_n$. Возьмем произвольную общую интерпретацию формул $\mathfrak{A}(x)$ и $\mathfrak{B}(x)$; $\mathfrak{A}(x)$ превратится в ней в некоторый предикат $A(x, x_1, \ldots, x_n, y_1, \ldots, y_k)$, а $\mathfrak{B}(x)$ — в предикат $B(x, x_1, \ldots, x_n, z_1, \ldots, z_l)$. Эти предикаты равносильны; поэтому одноместный предикат $A(x, x_1^0, \ldots, x_n^0, y_1^0, \ldots, y_k^0)$ будет тождественно истинен для тех и только для тех наборов $x_1^0, \ldots, x_n^0, y_1^0, \ldots, y_k^0, z_1^0, \ldots, z_l^0$, для которых тождест-

венно истинен предикат $B(x, x_1^0, \ldots, x_n^0, z_1^0, \ldots, z_l^0$, а это и означает, что $\forall x A(x, x_1, \ldots, x_n, y_1, \ldots, y_k) \equiv \forall x B(x, x_1, \ldots, x_n, z_1, \ldots, z_l)$; аналогично этому, упомянутые одноместные предикаты будут для одних и тех же наборов $x_1^0, \ldots, z_l^0$ не тождественно ложны, что дает $\exists x A(x, x_1, \ldots, x_n, y_1, \ldots, y_k) \equiv \exists x B(x, x_1, \ldots, x_n, z_1, \ldots, z_l)$.

Замечания. 1) Очевидно, что любые две всюду истинные формулы равносильны, и обратно — формула, равносильная всюду истинной формуле, сама всюду истинна. Аналогично для невыполнимых формул.

2) Из определения равносильности предикатов непосредственно следует, что предикаты $F(x_1, \ldots x_n, y_1, \ldots, y_k)$ и $G(x_1, \ldots x_n, z_1, \ldots, z_l)$ тогда и только тогда равносильны, когда тождественно истинна эквиваленция $F(x_1, \ldots y_k) \leftrightarrow G(x_1, \ldots, z_l)$. Поэтому формулы $\mathfrak{A}$ и $\mathfrak{B}$ тогда и только тогда равносильны, когда эквиваленция $\mathfrak{A} \leftrightarrow \mathfrak{B}$ всюду истинна (ср. аналогичный факт в логике предложений, с. 105).

4. Обратимся теперь к способам установления равносильности и всюду-истинности. В логике предложений имеются, как мы знаем, универсальные (и притом очень простые) способы, позволяющие для любой формулы узнавать, является ли она тождественно истинной, и для любых двух формул — равносильны ли они. В логике предикатов подобных способов нет, и пытаться их найти было бы бесполезно: д о к а з а н о, что не может существовать никакого универсального метода, который для любой формулы логики предикатов позволял бы с помощью одних и тех же четко определенных операций — так сказать, «механически» — выяснять, является ли она всюду истинной; аналогичный факт имеет место и для равносильности[8]. Поэтому всюду-истинность и равносильность формул приходится в разных случаях доказывать по-разному; вопрос о том, является ли, скажем, та или иная формула всюду истинной, может оказаться весьма сложной задачей. Но для многих важных частных случаев способы установления равносильности и всюду-истинности можно все же указать.

Самый простой их этих случаев — тот, когда удастся воспользоваться средствами логики предложений. К этому случаю относятся некоторые из приведенных выше примеров (пример 1 на с. 133, пример 1 на с. 136); сейчас мы разберем его в общем виде.

Пусть $\mathfrak{A}$ и $\mathfrak{B}$ — произвольные равносильные формулы логики предложений. Проделаем с ними следующие три операции: (а) вместо каждого элементарного предложения подставим некоторый предикатный символ (причем на место одного и того же элементарного предложения всюду, как в $\mathfrak{A}$, так и в $\mathfrak{B}$, подставляется один и тот же

[8] Точные формулировки и доказательства этих результатов будут приведены ниже (§ 8.5).

символ); (б) каждый предикатный символ заместим некоторым конкретным предикатом (всюду одним и тем же); (в) в полученной формуле фиксируем значения всех свободных переменных. После операции (а) $\mathfrak{A}$ и $\mathfrak{B}$ переходят в формулы логики предикатов $\mathfrak{A}'$ и $\mathfrak{B}'$, после (б) — в предикаты $\mathfrak{A}_0$ и $\mathfrak{B}_0$ и после (в) — в предложения $\mathfrak{A}^*$ и $\mathfrak{B}^*$. Эти предложения либо оба истинны, либо оба ложны (т. к. $\mathfrak{A}^*$ и $\mathfrak{B}^*$ получаются из равносильных формул $\mathfrak{A}$ и $\mathfrak{B}$ заменой переменных элементарных предложений некоторыми конкретными предложениями). Поскольку это верно при любом выборе значений входящих в предикаты $\mathfrak{A}_0$ и $\mathfrak{B}_0$ свободных переменных, эти предикаты равносильны. Последнее, в свою очередь, справедливо при любом замещении входящих в $\mathfrak{A}'$ и $\mathfrak{B}'$ предикатных символов конкретными предикатами; а это значит, что $\mathfrak{A}' \equiv \mathfrak{B}'$.

Итак, мы доказали

**Утверждение 1.** Если в равносильных формулах логики предложений заменить элементарные предложения произвольными предикатными символами так, чтобы одно и то же элементарное предложение заменялось в обеих формулах одним и тем же символом, то возникающие при этом формулы логики предикатов также равносильны.

Пусть, далее, $\mathfrak{A}$ — произвольная тождественно истинная формула логики предложений. Проделав с ней указанные выше операции (а), (б) и (в) и сохраняя прежний смысл обозначений $\mathfrak{A}'$, $\mathfrak{A}_0$ и $\mathfrak{A}^*$, аналогично предыдущему видим, что предложение истинно, и это верно при любом выборе значений свободных переменных, так что $\mathfrak{A}_0$ — тождественно истинный предикат; последнее справедливо при любом замещении входящих в $\mathfrak{A}'$ предикатных символов конкретными предикатами, а это значит, что $\mathfrak{A}'$ — всюду истинная формула.

Итак, доказано

**Утверждение 2.** Если в тождественно истинной формуле логики предложений заменить элементарные предложения произвольными предикатными символами, то возникающая при этом формула логики предикатов всюду истинна.

**5.** В заключение параграфа рассмотрим понятие семантического следования, аналогичное соответствующему понятию логики предложений (§ 3.4).

Введем сначала следующее определение: предикат $F(x_1, \ldots, x_n, y_1, \ldots, y_k)$ *не сильнее* предиката $G(x_1, \ldots, x_n, z_1, \ldots, z_l)$ $(n, k, l = 0, 1 \ldots)$ (иначе: предикат $G$ *не слабее* предиката $F$), если для любого набора $x_1^0, \ldots, z_l^0$ значений переменных $x_1, \ldots, z_l$, для которого $F(x_1^0, \ldots, y_k^0) \equiv И$, будет также $G(x_1^0, \ldots, z_l^0) \equiv И$.

**Примеры.** 1) Если $U$ — произвольное непустое множество и

$F_M(x)$ — характеристический предикат множества $M \subset U$ (см. с. 98), то $F_A(x)$ не сильнее $F_B(x)$ тогда и только тогда, когда $A \subset B$.

2) Очевидно, тождественно истинный предикат не слабее, а тождественно ложный — не сильнее любого предиката.

Мы скажем теперь, что формула $\mathfrak{B}$ есть *семантическое следствие* — или просто *следствие* — конечного множества формул $\Gamma$ (иначе: $\mathfrak{B}$ (*семантически*) *следует из* $\Gamma$), если для любой интерпретации множества $\Gamma \cup \{\mathfrak{B}\}$ тот предикат, в который превращается конъюнкция всех формул из $\Gamma$, не сильнее предиката, в который превращается $\mathfrak{B}$.

В частности, при пустом $\Gamma$ это означает, что в любой интерпретации формулы $\mathfrak{B}$ она должна превращаться в предикат, истинный для всех значений своих аргументов,— т. е. что $\mathfrak{B}$ всюду истинна.

Обозначаться семантическое следование будет так же, как в логике предложений: $\Gamma \Rightarrow \mathfrak{B}$.

Если множество $\Gamma$ не пусто и состоит из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$, мы часто будем вместо «$\mathfrak{B}$ следует из $\Gamma$» говорить «$\mathfrak{B}$ следует из $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$» и писать $\mathfrak{A}_1, \ldots, \mathfrak{A}_k \Rightarrow \mathfrak{B}$.

Примеры. 1) $\forall x(F(x, y) \supset G(x, y)), F(z, y) \Rightarrow G(z, y)$. В самом деле: заместим $F$ и $G$ произвольными конкретными предикатами $F_0$ и $G_0$. Если при этом для некоторых значений $z_0, y_0$ переменных $z, y$ конъюнкция $\forall x(F_0(x, y_0) \supset G_0(x, y_0)) \& F_0(z_0, y_0)$ принимает значение $И$, то $\forall x(F_0(x, y_0) \supset G_0(x, y_0))$ и $F_0(z_0, y_0)$ — истинные предложения; вместе с первым из них истинно и предложение $F_0(z_0, y_0) \supset G_0(z_0, y_0)$, но из истинности импликации и ее посылки следует истинность заключения — в данном случае предложения $G_0(z_0, y_0)$. Таким образом, предикат $\forall x(F_0(x, y) \supset G_0(x, y)) \& F_0(x, y)$ не сильнее предиката $G_0(z, y)$.

2) Очевидно, $\forall x F(x) \Rightarrow \exists x F(x)$ (ср. пример 3 на с. 133).

3) Повторяя рассуждения, приведенные при разборе примеров 4, 5 на с. 134, читатель легко докажет, что $\exists y \forall x F(x, y) \Rightarrow \forall x \exists y F(x, y)$, а обратное неверно.

4) Очевидно, всюду истинная формула следует из любой формулы, и любая формула следует из невыполнимой.

Задачи. 1) Доказать, что $F(x) \vee G(x), \neg \exists y G(y) \Rightarrow F(x)$.

2) Доказать, что

$$\forall x F(x) \vee \forall x G(x) \Rightarrow \forall x(F(x) \vee G(x));$$

$$\exists x(F(x) \& G(x)) \Rightarrow \exists x F(x) \& \exists x G(x),$$

а обратные следования не имеют места (ср. задачу 1 на с. 134).

Из определений непосредственно ясно, что: (а) предикат $F$ не

сильнее предиката $G$ тогда и только тогда, когда импликация $F \supset G$ является тождественно истинным предикатом; (б) два предиката тогда и только тогда равносильны, когда каждый из них не сильнее другого. Из (а) и (б), в свою очередь, сразу вытекает, что в логике предикатов справедливы аналоги утверждений 1 и 2 из § 3.4, а именно:

**Утверждение 3.** Формула $\mathfrak{B}$ тогда и только тогда является следствием формулы $\mathfrak{A}$, когда импликация $\mathfrak{A} \supset \mathfrak{B}$ всюду истинна.

**Утверждение 4.** Две формулы тогда и только тогда равносильны, когда каждая из них есть следствие другой.

Справедливо также и утверждение, аналогичное утверждению 3 из § 3.4:

**Утверждение 5.** Тогда и только тогда $\mathfrak{A} \Rightarrow \mathfrak{B}$, когда $\neg\mathfrak{B} \Rightarrow \neg\mathfrak{A}$.

**Доказательство.** Ввиду утверждения 1 (см. предыдущий пункт) $\mathfrak{A} \supset \mathfrak{B} \equiv \neg\mathfrak{B} \supset \neg\mathfrak{A}$. Поэтому импликация $\mathfrak{A} \supset \mathfrak{B}$ тогда и только тогда всюду истинна, когда то же верно для $\neg\mathfrak{B} \supset \neg\mathfrak{A}$. Остается воспользоваться утверждением 3.

## § 4.2. ОСНОВНЫЕ РАВНОСИЛЬНОСТИ. ТОЖДЕСТВЕННЫЕ ПРЕОБРАЗОВАНИЯ. ПРЕФИКСНАЯ НОРМАЛЬНАЯ ФОРМА

1. Если при доказательстве равносильности формул не удается обойтись средствами логики предложений (см. пункт 4 предыдущего параграфа), пользуются свойствами кванторов. Наиболее важные из этих свойств (часто называемые *основными равносильностями логики предикатов*), будут сейчас доказаны; для удобства запоминания мы разобьем их на четыре группы.

Группа 1: перестановка одноименных кванторов.

11. $\forall x \forall y F(x, y) \equiv \forall y \forall x F(x, y)$.

12. $\exists x \exists y F(x, y) \equiv \exists y \exists x F(x, y)$.

Для доказательства соотношения 11 достаточно заметить, что при замещении символа $F$ любым конкретным двуместным предикатом $F_0$ как левая, так и правая его части превращаются в истинные предложения в том и только в том случае, когда $F_0$ — тождественно истинный предикат. Соотношение 12 предоставляется доказать читателю.

Группа II: связь между разноименными кванторами.

II1. $\neg\forall x F(x) \equiv \exists x \neg F(x)$.

II2. $\neg\exists x F(x) \equiv \forall x \neg F(x)$.

**Доказательство соотношения II1.** Заместим предикатный символ $F$ произвольным одноместным предикатом $F_0$. Если предложение $\neg\forall x F_0$ истинно, то $\forall x F_0(x)$ ложно; следовательно, предикат $F_0$ не является тождественно истинным и, стало быть, $\neg F_0$ не является тождественно ложным, т. е. для какого-то значения переменной $x$ он принимает значение *И*, так что $\exists x \neg F_0(x)$ — истинное предложение. С другой стороны, если предложение $\neg\forall x F_0(x)$ ложно, то $\forall x F_0(x)$ истинно; поэтому предикат $F_0(x)$ тождественно истинен, а $\neg F_0(x)$ тождественно ложен, так что $\exists x \neg F_0(x)$ — ложное предложение.

**Доказательство соотношения II2.** Заместим $F$ произвольным одноместным предикатом $F_0$. Предложение $\neg\exists x F_0(x)$ тогда и только тогда истинно, когда $\exists x F_0(x)$ ложно, т. е. предикат $F_0(x)$ тождественно ложен; а это имеет место тогда и только тогда, когда предикат $\neg F_0(x)$ тождественно истинен, т. е. истинно предложение $\forall x \neg F_0(x)$.

**Замечание.** Если некоторый (одноместный) предикат $P(x)$ определен на конечном множестве $\{a_1, \ldots, a_n\}$, то $\forall x P(x)$ означает то же, что $P(a_1) \& \ldots \& P(a_n)$, а $\exists x P(x)$ — то же, что $P(a_1) \vee \ldots \vee P(a_n)$. В общем случае кванторы общности и существования можно понимать как «бесконечную конъюнкцию» и «бесконечную дизъюнкцию». Тогда соотношения группы II оказываются обобщениями на «бесконечный случай» законов Де Моргана.

Группа III: вынесение кванторов за скобки.

Для произвольной формулы $\mathfrak{A}$, не содержащей свободных вхождений переменной $x$, справедливы соотношения:

III1. $\mathfrak{A} \& \forall x F(x) \equiv \forall x (\mathfrak{A} \& F(x))$.

III2. $\mathfrak{A} \vee \forall x F(x) \equiv \forall x (\mathfrak{A} \vee F(x))$.

III3. $\mathfrak{A} \& \exists x F(x) \equiv \exists x (\mathfrak{A} \& F(x))$.

III4. $\mathfrak{A} \vee \exists x F(x) \equiv \exists x (\mathfrak{A} \vee F(x))$.

Доказательства проведем сначала для случая, когда $\mathfrak{A}$ — замкнутая формула. Заместим $F$ произвольным одноместным предикатом $F_0$ и все предикатные символы, входящие в $\mathfrak{A}$ — произвольными предикатами (соответствующей вместимости); формула $\mathfrak{A}$ перейдет при этом в некоторое предложение $\mathfrak{A}^*$. Тогда имеем:

1) Если предложение $\mathfrak{A}^* \& \forall x F_0(x)$ истинно, то истинны оба пред-

ложения $\mathfrak{A}^*$ и $\forall x F_0(x)$; из истинности $\forall x F_0(x)$ следует, что предикат $F_0(x)$ тождественно истинен; поэтому предикат $\mathfrak{A}^* \& F_0(x)$ также тождественно истинен, так что $\forall x(\mathfrak{A}^* \& F_0(x))$ — истинное предложение. С другой стороны, если $\mathfrak{A}^* \& \forall x F_0(x))$ ложно, то ложно либо $\mathfrak{A}^*$, либо $\forall x F_0(x)$; в первом случае $\mathfrak{A}^* \& F_0(x)$ — тождественно ложный предикат, во втором предикат $F_0(x)$ не тождественно истинен, и, стало быть, не тождественно истинен также и предикат $\mathfrak{A}^* \& F_0(x)$. В обоих случаях предложение $\forall x(\mathfrak{A}^* \& F_0(x))$ ложно.

2) Если $\mathfrak{A}^* \vee \forall x F_0(x)$ истинно, то истинно либо $\mathfrak{A}^*$, либо $\forall x F_0(x)$. Из истинности $\mathfrak{A}^*$ сразу следует тождественная истинность предиката $\mathfrak{A}^* \vee F_0(x)$; если истинно $\forall x F_0(x)$, то предикат $F_0(x)$ тождественно истинен, а отсюда опять-таки следует тождественная истинность предиката $\mathfrak{A}^* \vee F_0(x)$. Следовательно, предложение $\forall x(\mathfrak{A}^* \vee F_0(x))$ истинно. Если же $\mathfrak{A}^* \vee \forall x F_0(x)$ ложно, то ложны оба предложения $\mathfrak{A}^*$ и $\forall x F_0(x)$; поэтому предикат $F_0(x)$ не тождественно истинен, но он ввиду ложности $\mathfrak{A}^*$ равносилен $\mathfrak{A}^* \vee F_0(x)$. Таким образом, предложение $\forall x(\mathfrak{A}^* \vee F_0(x))$ ложно.

3) Если $\mathfrak{A}^* \& \exists x F_0(x)$ истинно, то истинны оба предложения $\mathfrak{A}^*$ и $\exists x F_0(x)$; значит, предикат $F_0(x)$ не тождественно ложен, но он ввиду истинности $\mathfrak{A}^*$ равносилен $\mathfrak{A}^* \& F_0(x)$; поэтому предложение $\exists x(\mathfrak{A}^* \& F_0(x))$ истинно. Если $\mathfrak{A}^* \& \exists x F_0(x)$ ложно, то ложно либо $\mathfrak{A}^*$, либо $\exists x F_0(x)$. Из ложности $\mathfrak{A}^*$ сразу следует тождественная ложность $\mathfrak{A}^* \& F_0(x)$, из ложности $\exists x F_0(x)$ — тождественная ложность $F_0(x)$ и тем более $\mathfrak{A}^* \& F_0(x)$. Поэтому предложение $\exists x(\mathfrak{A}^* \& F_0(x))$ ложно.

4) Соотношение 1114 читатель докажет самостоятельно.

Перейдем к случаю, когда $\mathfrak{A}$ не замкнута. Заместим $F$ произвольным одноместным предикатом $F_0$ и все предикатные символы в $\mathfrak{A}$ — произвольными предикатами; формула $\mathfrak{A}$ перейдет теперь в некоторый предикат $\mathfrak{A}_0$. Если в этом предикате дать свободным переменным произвольные значения, получится некоторое предложение $\mathfrak{A}^*$; рассуждая точно так же, как в предыдущем случае, видим, что предложения $\mathfrak{A}^* \& \forall x\, F_0(x)$ и $\forall x(\mathfrak{A}^* \& F_0(x))$ имеют одинаковые истинностные значения; а поскольку это справедливо при любом выборе значений свободных переменных, предикаты $\mathfrak{A}_0 \& \forall x F_0(x)$ и $\forall x(\mathfrak{A}_0 \& F_0(x))$ равносильны. Тем самым доказано 1111. Остальные соотношения доказываются так же.

Если формула $\mathfrak{A}$ содержит свободные вхождения $x$, так рассуждать нельзя, т. к. тогда при фиксировании значений свободных переменных истинностное значение предиката $F_0$ также фиксируется.

При нарушении нашего условия соотношения группы III могут нарушаться. Например, формулы $G(x, y)\&\forall xF(x)$ и $\forall x(G(x, y)\&F(x))$ не равносильны; чтобы это показать, заместим $F$ и $G$ предикатами, определенными на множестве целых положительных чисел и означающими соответственно $x \geq 1$ и $x < y$. Тогда первая формула перейдет в двуместный предикат $(x < y)\&\forall x(x \geq 1)$, равносильный $x < y$, а вторая — в тождественно ложный одноместный предикат $\forall x(x < y\& \&x \geq 1)$.

Другие примеры см. в задаче 17 в конце главы.

Группа IV: переименование связанных переменных.

IV1. $\forall xF(x) \equiv \forall yF(y)$.

IV2. $\exists xF(x) \equiv \exists yF(y)$.

Эти соотношения следуют из того, что, как было отмечено еще в гл. 2 (с. 60), предложения $\forall xF_0(x)$ и $\forall yF_0(y)$ имеют одинаковые истинностные значения, каков бы ни был предикат $F_0$, и то же самое верно для $\exists xF_0(x)$ и $\exists yF_0(y)$.

Замечания. 1) Во всех выведенных сейчас равносильностях можно, разумеется, вместо $x$ и $y$ взять любые другие переменные.

2) Равносильности групп I—III останутся справедливыми, если заменить в них $F(x)$ и $F(x, y)$ любыми формулами.

Покажем это, например, для равносильности III; для остальных равносильностей групп I—III рассуждения в точности такие же.

Пусть сначала формула $\mathfrak{A}$, на которую мы заменили $F(x)$, не содержит свободных переменных, отличных от $x$. Тогда при замещении предикатных символов конкретными предикатами $\mathfrak{A}$ превращается в одноместный предикат $G_0(x)$[9], и в силу III предложения $\neg\forall xG_0(x)$ и $\exists x\neg G_0(x)$ имеют одинаковые истинностные значения; а поскольку это верно при любом замещении, формулы $\neg\forall x\mathfrak{A}$ и $\exists x\neg\mathfrak{A}$ равносильны.

Пусть теперь $\mathfrak{A}$ содержит, кроме $x$, свободные переменные $y_1, \ldots, y_n$. При замещении предикатных символов конкретными предикатами $\mathfrak{A}$ превращается в $(n + 1)$-местный предикат $G_0(x, y_1, \ldots, y_n)$; этот последний при фиксировании значений $y_1, \ldots, y_n$ становится одноместным предикатом $G_0(x, y_1^0, \ldots, y_n^0)$, и, как в предыдущем случае, мы видим, что предложения $\neg\forall xG_0(x, y_1^0, \ldots, y_n^0)$ и $\exists x\neg G(x, y_1^0, \ldots, y_n^0)$ имеют одинаковые истинностные значения; по-

[9] Это верно даже тогда, когда $\mathfrak{A}$ не содержит свободных вхождений $x$; предикат $G_0(x)$ в этом случае тождественно истинен или тождественно ложен.

поскольку это справедливо при любом выборе значений $y_1, \ldots, y_n$, предикаты $\neg\forall x G_0(x, y_1, \ldots, y_n)$ и $\exists x \neg G_0(x, y_1, \ldots, y_n)$ равносильны, а так как это верно при любом замещении, имеем $\neg\forall x\mathfrak{A} = \exists x\neg\mathfrak{A}$.

3) Аналогичный факт имеет место и для равносильностей группы IV, но с одной оговоркой. Именно, эти равносильности остаются справедливыми, если $F(x)$ заменить произвольной формулой $\mathfrak{A}$, такой, что (а) $\mathfrak{A}$ не содержит свободных вхождений $y$ и (б) никакое свободное вхождение $x$ в $\mathfrak{A}$ не находится в области действия какого-либо квантора по $y$, а $F(y)$ заменить формулой $\mathfrak{A}|^x_y$, полученной из $\mathfrak{A}$ заменой всех свободных вхождений $x$ вхождениями $y$. Покажем это сначала для случая, когда $\mathfrak{A}$ не содержит свободных переменных, отличных от $x$. Тогда при замещении предикатных символов предикатами формула $\mathfrak{A}$ перейдет в некоторый одноместный предикат $G_0(x)$, а формула $\mathfrak{A}|^x_y$ — в предикат $G_0(y)$, отличающийся от $G_0(x)$ только обозначением независимой переменной. Поэтому предложения $\forall x G_0(x)$ и $\forall y G_0(y)$ принимают одинаковые истинностные значения, и то же верно для $\exists x G_0 x$ и $\exists y G_0(y)$. Если $\mathfrak{A}$ содержит, кроме $x$[10], еще свободные переменные $z_1, \ldots, z_k$, то при замещении предикатных символов предикатами и фиксировании значений переменных $z_1, \ldots, z_k$ формула $\mathfrak{A}$ превратится в одноместный предикат $G_0(x, z_1^0, \ldots, z_k^0)$, а формула $\mathfrak{A}|^x_y$ — поскольку среди переменных $z_1, \ldots, z_k$ нет $y$ и ввиду условия (б) всякое свободное вхождение $x$ превращается в свободное вхождение $y$,— превратится в предикат $G_0(y, z_1^0, \ldots, z_k^0)$, отличающийся от $G_0(x, z_1^0, \ldots, z_k^0)$ только обозначением независимой переменной. Поэтому истинностные значения предложений $\forall x G_0(x, z_1^0, \ldots, z_k^0)$ и $\forall y G_0(y, z_1^0, \ldots, z_k^0)$ совпадают, а поскольку это верно при любых значениях $z_1, \ldots, z_k$, предикаты $\forall x G_0(x, z_1, \ldots, z_k)$ и $\forall y G_0(y, z_1, \ldots, z_k)$ равносильны; аналогично для квантора существования. Но если условие (а) или (б) не выполняется, то при замене $F(x)$ на $\mathfrak{A}$ и $F(y)$ на $\mathfrak{A}|^x_y$ соотношения IV1 и IV2 могут нарушиться. Например, если $\mathfrak{A}$ есть $G(x, y)$ (не выполняется условие (а)), то левая часть соотношения IV1 превратится в $\forall x G(x, y)$, а правая — в $\forall y G(y, y)$; эти формулы, очевидно, не равносильны. Если $\mathfrak{A}$ есть $\forall y H(x, y)$ (не выполняется условие (б)), получаются формулы $\forall x \forall y H(x, y)$ и $\forall y \forall y H(y, y)$, также не равносильные.

Итак: в формуле $\forall x\mathfrak{A}$ можно переименовать $x$ в $y$, если выполняются условия (а) и (б).

2. С помощью соотношений I—IV мы можем, учитывая только что сделанные замечания, производить над формулами логики пре-

[10] $\mathfrak{A}$ может и не содержать $x$ (ср. предыдущую сноску).

дикатов *тождественные преобразования*, причем ввиду утверждения 1 из предыдущего параграфа в этих преобразованиях можно использовать также любые равносильности логики предложений. Но, как и в логике предложений, возникает вопрос о допустимости замены формулы на равносильную внутри более сложной формулы (ср. начало § 3.2). Решается этот вопрос так же, как там — с помощью понятия подформулы и теоремы о замене равносильных формул. Прежде всего, аналогично тому, как сделано в § 3.2, мы будем называть *подформулой* формулы $\mathfrak{A}$ всякую формулу $\mathfrak{B}$, «входящую в состав» $\mathfrak{A}$, т. е. такую, что формулу $\mathfrak{A}$ можно получить из некоторой формулы $\mathfrak{C}$ заменой некоторого вхождения формулы вида $F(z_1, \ldots, z_k)$, где $z_1, \ldots, z_k$ $(k \geq 0)$ — все входящие в $\mathfrak{B}$ свободные переменные и $F$ — предикатный символ вместимости $k$, вхождением формулы $\mathfrak{B}$. Например, формула

$$\mathfrak{A}_0 = \forall x(\neg(G(x)) \supset (\exists y(\exists z(F(z, y)))))^{11}$$

может быть получена из $\forall x(\neg(G(x)) \supset (\exists y(H(y))))$ заменой (единственного) вхождения формулы $H(y)$ вхождением формулы $\exists z(F(z, y))$ или из $\forall x(\neg G(x)) \supset (L))$ (где $L$ — нульместный предикатный символ) заменой $L$ на $\exists y(\exists z(F(z, y)))$; таким образом, формулы $\exists z(F(z, y))$ и $\exists y(\exists z(F(z, y)))$ являются подформулами $\mathfrak{A}_0$. Остальные 5 подформул $\mathfrak{A}_0$ читатель легко найдет сам.

Мы будем теперь называть формулу $\mathfrak{B}$ *непосредственной составляющей* формулы $\mathfrak{A}$, если $\mathfrak{A}$ имеет либо вид $\neg(\mathfrak{B})$, либо вид $(\mathfrak{B})\alpha(\mathfrak{C})$ или $(\mathfrak{C})\alpha(\mathfrak{B})$, где $\alpha$ — один из знаков $\&$, $\vee$, $\supset$, $\leftrightarrow$, либо, наконец, вид $Q(\mathfrak{B})$, где $Q$ — квантор[12] С помощью понятия непосредственной составляющей можно теперь определить понятие *глубины вхождения подформулы в формулу*, дословно повторив формулировку соответствующего определения из § 3.2. После этого может быть сформулирована и доказана

**Теорема о замене равносильных формул (логики предикатов).** Ее формулировка дословно совпадает с формулировкой соответствующей теоремы логики предложений (§ 3.2). Доказательство ее также очень похоже на доказательство этой теоремы: оно ведется индукцией по глубине заменяемого вхождения $\mathfrak{B}_0$, причем базис слово в слово совпадает с прежним, а индукционный шаг точно так же, как прежде, сводится к доказательству того, что формула перейдет в равносильную, если заменить в ней вхождение непосредствен-

[11] Здесь мы намеренно сохраняем все скобки.

[12] При этом формула $\mathfrak{B}$ может и не содержать подкванторной переменной — в определении формулы нет такого ограничения. Ясно, что в этом случае формулы $\mathfrak{B}$ и $Q(\mathfrak{B})$ равносильны.

ной составляющей $\mathfrak{C}_1$ вхождением формулы $\mathfrak{C}_1'$, равносильной $\mathfrak{C}_1$. Однако при этом возможны не три случая, как в логике предложений, а пять: случаи (а), (б), (в), такие же, как прежде, и, кроме того, (г) $\mathfrak{A} = \forall x(\mathfrak{C}_1)$ и (д) $\mathfrak{A} = \exists x(\mathfrak{C}_1)$. В случае (а), если, например, $\alpha$ есть $\&$, беря произвольную интерпретацию формулы $\mathfrak{A}$ и обозначая соответственно через $G$, $G'$ и $H$ предикаты, в которые в этой интерпретации переходят формулы $\mathfrak{C}_1$, $\mathfrak{C}_1'$ и $\mathfrak{D}$, видим, что формула $\mathfrak{A}$ перейдет в той же интерпретации в предикат $G\&H$, а $\mathfrak{A}'$ — в $G'\&H$. А так как $G$ и $G'$ равносильны, $G\&H$ и $G'\&H$ тоже равносильны, откуда, поскольку это верно для любой интерпретации, $\mathfrak{A} \equiv \mathfrak{A}'$. Точно так же рассуждаем при $\alpha = \vee, \supset, \leftrightarrow$ и в случаях (б) и (в). Случаи (г) и (д) мы фактически уже рассмотрели (см. пример 3 на с. 135).

**3.** Теперь мы в самом деле можем производить над формулами логики предикатов тождественные преобразования с помощью соотношений групп I—IV и равносильностей логики предложений. Производя такие преобразования в определенном порядке, можно для каждой формулы получить равносильную, имеющую особенно простое строение. Делается это так:

1) С помощью соотношений III 1, 2, 4 из § 3.1 устраняем все знаки импликации и эквиваленции (если таковые имеются).

2) К полученной формуле последовательно применяем — в произвольном возможном порядке — преобразования следующих двух типов:

Преобразование типа *А*. Находим в формуле некоторую подформулу $\mathfrak{C}$, имеющую вид $\mathfrak{A}\&\forall x\mathfrak{B}(x)$, или $\mathfrak{A}\vee\forall x\mathfrak{B}(x)$, или $\mathfrak{A}\&\exists x\mathfrak{B}(x)$, или $\mathfrak{A}\vee\exists x\mathfrak{B}(x)$, где $\mathfrak{A}$, $\mathfrak{B}(x)$ — какие-то формулы[13]. Пусть для определенности $\mathfrak{C} = \mathfrak{A}\&\forall x\mathfrak{B}(x)$ (в остальных случаях все делается точно так же). Преобразуем $\mathfrak{C}$ следующим образом: проверяем, содержит ли $\mathfrak{A}$ свободно переменную $x$, и если нет — заменяем $\mathfrak{C}$ на $\forall x(\mathfrak{A}\&\mathfrak{B}(x))$ (соотношение III 1), если да — заменяем все вхождения $x$ в $\forall x\mathfrak{B}(x)$ вхождениями какой-либо новой переменной, скажем, $z$, не встречающейся в нашей «большой» формуле вовсе (соотношение IV 1) и затем заменяем $\mathfrak{A}\&\forall z\mathfrak{B}(z)$ на $\forall z(\mathfrak{A}\&\mathfrak{B}(z))$. Таким же образом поступаем с подформулами вида $\forall x\mathfrak{B}(x)\&\mathfrak{A}$ и т. п. (это возможно ввиду коммутативности конъюнкции и дизъюнкции).

Преобразование типа Б. Находим в формуле некоторую часть, имеющую вид $\neg\forall x\mathfrak{B}(x)$ или $\neg\exists x\mathfrak{B}(x)$, и заменяем ее на $\exists x\neg\mathfrak{B}(x)$, соответственно на $\forall x\neg\mathfrak{B}(x)$ (III, 2).

Применяя преобразования типов А и Б, мы шаг за шагом «вытаскиваем наружу» все кванторы и в конце концов приходим к формуле, в которой ни один квантор не стоит внутри конъюнкции или дизъ-

---

[13] $\mathfrak{B}(x)$ может даже и не содержать свободных вхождений $x$ (ср. сноску 12).

юнкции или вслед за отрицанием; но в такой формуле квантор может стоять только либо вслед за другим квантором, либо в самом начале — иначе говоря, формула должна иметь вид $Q_1x_1Q_2x_2 \dots Q_sx_s\mathfrak{B}$, где $Q_1x_1, Q_2x_2, \dots, Q_sx_s$ — какие-то кванторы и $\mathfrak{B}$ — бескванторная формула. Формула, имеющая такой вид, называется *формулой в префиксной нормальной форме* (сокращенно п. н. ф.). Выражение $Q_1x_1 \dots Q_sx_s$ называется здесь *кванторным префиксом*[14] (или *кванторной приставкой*), формула $\mathfrak{B}$ — *матрицей*[15] данной формулы. Кроме того, всякую бескванторную формулу естественно также считать формулой в п. н. ф.

Итак, доказана

Теорема. Для всякой формулы логики предикатов существует равносильная ей формула в п. н. ф.

Более того, мы указали практический способ «приведения к п. н. ф.» (ср. доказательство теоремы о приведении к д. н. ф. в § 3.2).

При фактическом приведении формул к п. н. ф. удобно «по пути» устранять двойные отрицания всякий раз, когда они возникают (а также производить любые другие упрощения, если они возможны).

Пример.

$$\neg\exists y\neg\exists u((\exists xF(x, y, z)\supset\forall xG(x, y))\&\neg\forall zF(z, u, z)) \equiv$$

$$\equiv \forall y\neg\neg\exists u((\neg\exists xF(x, y, z)\vee\forall xG(x, y))\&\exists z\neg F(z, u, z)) \equiv$$

$$\equiv \forall y\exists u((\forall x\neg F(x, y, z)\vee\forall tG(t, y))\&\exists v\neg F(v, u, v)) \equiv$$

$$\equiv \forall y\exists u(\forall t(\forall x\neg F(x, y, z)\vee G(t, y))\&\exists v\neg F(v, u, v)) \equiv$$

$$\equiv \forall y\exists u(\forall t\forall x(\neg F(x, y, z)\vee G(t, y))\&\exists v\neg F(v, u, v)) \equiv$$

$$\equiv \forall y\exists u\forall t\forall x((\neg F(x, y, z)\vee G(t, y))\&\exists v\neg F(v, u, v)) \equiv$$

$$\equiv \forall y\exists u\forall t\forall x\exists v|(\neg F(x, y, z)\vee G(t, y))\&\neg F(v, u, v)|.$$

Задача. Привести к п. и. ф.:

(а) $\neg\exists xF(x, z)\&(G(x, y)\supset\forall zH(z, x))$;

(б) $\forall x\neg\exists yF(x, y, z)\&\exists x\exists yG(y, x)\supset\exists zH(z)$;

(в) $\forall x_1 \dots \forall x_nF(x_1, \dots, x_n)\supset\exists x_1, \dots \exists x_nG(x_1, \dots, x_n)$.

---

[14] От лат. *praefixus* — «прикрепленный спереди».

[15] Это слово, как и омонимичные ему алгебраический и типографский термины, происходит от латинского слова *matrix*, первоначальное значение которого — «матка» (например, пчелиная); от этого значения идет, видимо, типографский термин. Наш термин произошел, скорее всего, от одного из производных значений латинского слова — «ствол, из которого растут ветви», а алгебраический от другого производного значения — «список, перечень».

Полезно заметить, что в силу соотношений группы II отрицание формулы $Q_1x_1 \ldots Q_sx_s\mathfrak{B}$, где $Q_1x_1, \ldots, Q_sx_s$ — кванторы, равносильно формуле $Q_1'x_1 \ldots Q_s'x_s\neg\mathfrak{B}$, где $Q_i'x_i$ — квантор, «противоположный» $Q_ix_i$. Например:

$$\neg\forall x\exists y\exists z\forall u F(x, y, z, u) \equiv \exists x\forall y\forall z\exists u\neg F(x, y, z, u).$$

Образовывать отрицания формул в п. н. ф. с тремя, четырьмя и более кванторами приходится, например, в анализе, когда нужно подробно формулировать утверждения вроде: «Данное число не является пределом данной последовательности», «Данная функция имеет разрыв в некоторой точке» и т. п. Указанное сейчас правило может в этом помочь; однако необходимо решительно предостеречь от попыток пользоваться правилом вместо размышления. Строить отрицания нужно всегда по смыслу, а правило использовать только для самоконтроля.

## § 4.3. ПРЕДМЕТНЫЕ ФУНКЦИИ И КОНСТАНТЫ

**1.** Для приложений полезно расширить запас выразительных средств логики предикатов, присоединив к нему символы «*предметных функций*» (например, числовых: $x + 1$, $\sin x$, $x + y$ и т. п.) и «предметных констант» (таких, как 0, 1 и т. п.). Аргументные места в предикатах смогут занимать тогда не только предметные переменные, но и всевозможные выражения, образованные из предметных переменных, предметных констант и символов предметных функций с помощью подстановки (суперпозиции) — так называемые *термы*[16]. Например, если $E$ — двуместный предикат, означающий равенство действительных чисел, то при такой записи $E(x + 0, x)$ будет означать $x + 0 = x$, а свойство ассоциативности сложения запишется в виде $E((x + y) + z, x + (y + z))$; сравнение с формулой (2) на с. 131 показывает, что этот способ записи много проще. Мы, однако, будем использовать не символы конкретных функций и констант, а абстрактные *функциональные символы* и *символы констант* — аналогично тому, как мы делаем, начиная с § 4.1, для предикатов; эти символы могут обозначать любые предметные

[16] От нем. *Term* или англ. *term* — «член математического выражения» (то и другое от лат. *terminus* — «граница, пограничный знак, цель»; отсюда же русское слово «термин»).

функции и любые предметные константы. В отличие от предикатных символов, в качестве которых обычно используют прописные латинские буквы, функциональными символами и символами констант у нас будут строчные латинские буквы (иногда с индексами), причем для функциональных символов чаще всего берутся буквы $f$, $g$, $h$, а для символов констант — $a$, $b$, $c$, $d$.

Теперь в число формул логики предикатов войдут, например, такие выражения, как $F(g_1(a, b, c), g_2(c, a, b))$, $\forall x \exists y (F(a, f(g(x, f))) \& \& \neg G(g(b_1, (g(b_2 y)))))$ и т. п. Свободное и связанное вхождения переменной, свободная и связанная переменная, замкнутая формула определяются так же, как прежде. (В кванторы могут входить, разумеется, только переменные.)

**2.** Расширив запас формул логики предикатов, мы должны, само собой, дополнить и определение интерпретации. Именно, задавая *интерпретацию множества формул* $M$, мы будем теперь не только сопоставлять каждому входящему в одну из формул $M$ предикатному символу некоторый предикат той же вместимости, но также и каждому входящему в одну из формул $M$ функциональному символу некоторую функцию той же вместимости, а каждому входящему в одну из формул $M$ символу константы — некоторый фиксированный объект. Обычно мы будем считать, что все входящие в интерпретацию предикаты и функции определены на одном и том же множестве, и этому же множеству принадлежат все значения функций и все объекты, сопоставленные символам констант (ср. с. 130); это множество мы будем называть *основным множеством* данной интерпретации.

Как и прежде, незамкнутая формула превращается в интерпретации в предикат, а замкнутая — в предложение. Определения *формулы, истинной в интерпретации, формулы, выполнимой в интерпретации, модели, всюду истинной формулы, выполнимой формулы, равносильности формул* не меняются. Утверждения 1 и 2 пункта 4 § 4.1, как легко проверить, остаются в силе, равно как и все утверждения пункта 5 и все содержание § 4.2.

Пример. Пусть $\Psi$ — множество всевозможных формул, содержащих двуместный предикатный символ $E$, двуместный функциональный символ $f$, одноместный функциональный символ $g$ и символ константы $a$. Рассмотрим следующие интерпретации $\Xi_1, \ldots, \Xi_5$ множества формул $\Psi$:

$\Xi_1$: Основным множеством служит множество натуральных чисел $\mathbb{N}$. Символу $E$ отвечает предикат равенства, символам $f$ и $g$ — функции $x + y$ и $x + 1$, символу $a$ — число 0.

$\Xi_2$: Основным множеством служит множество целых чисел $\mathbb{Z}$.

Символу $E$ отвечает предикат равенства, символам $f$ и $g$ — функции $x + y$ и $-x$, символу $a$ — число 0.

$\Xi_3$ отличается от $\Xi_2$ тем, что вместо $\mathbf{Z}$ берется множество рациональных чисел $\mathbf{Q}$.

$\Xi_4$ отличается от $\Xi_3$ тем, что вместо $x + y$, $-x$ и 0 берутся соответственно $x \cdot y$, $\varphi(x) = \begin{cases} \frac{1}{x} & \text{при } x \neq 0 \\ 0 & \text{при } x = 0 \end{cases}$ и 1.

$\Xi_5$: как $\Xi_2$, с той только разницей, что символу $E$ сопоставляется предикат $x < y$.

Рассмотрим, далее, следующие формулы из $\Psi$:

(1) $\exists z(E(f(x, y), z) \& \forall t(E(f(x, y), t) \supset E(t, z)))$;

(2) $E(f(f(x, y), z), f(x, f(y, z)))$;

(3) $E(f(x, a), x)$;

(4) $E(f(x, y), f(y, x))$;

(5) $E(f(x, (g(x)), a)$;

(6) $E(x, g(x))$.

Читателю предоставляется самому выяснить, какие из этих формул истинны и какие выполнимы в каждой из интерпретаций $\Xi_1 - \Xi_5$.

## Задачи и упражнения

1) Найти такие два замещения предикатного символа $F$ конкретным предикатом в формуле $\exists x F(x) \supset \forall x F(x)$, чтобы при одном замещении получилось истинное предложение, при другом — ложное.

2) (а) Пусть $\Psi$ — множество всевозможных формул, содержащих двуместные предикатные символы $G_1$ и $G_2$ и трехместный предикатный символ $H$ и не содержащих никаких других предикатных символов. Обозначим через $\Gamma_1, \ldots, \Gamma_4$ следующие интерпретации множества $\Psi$:

$\Gamma_1$: Основным множеством служит множество натуральных чисел $\mathbf{N}$; символам $G_1$, $G_2$ и $H$ отвечают соответственно предикаты $E(x, y)$, $M(x, y)$ и $C(x, y, z)$, означающие «$x = y$», «$x < y$» и «$y$ расположено между $x$ и $z$»;

$\Gamma_2$: Основным множеством служит множество действительных чисел $\mathbf{R}$, предикаты определяются так же, как в $\Gamma_1$;

$\Gamma_3$: Основным множеством служит $\mathbf{N}$; символам $G_1$, $G_2$ и $H$ отвечают соответственно предикаты $E(x, y)$, $d(x, y)$ и $D(x, y, z)$, означающие «$x = y$», «$x$ делится на $y$» и «$z$ есть наибольший общий делитель $x$ и $y$»;

$\Gamma_4$: Основным множеством служит множество всех плоскостей в трехмерном евклидовом пространстве, символам $G_1$, $G_2$ и $H$ отвечают

соответственно предикаты $E(x, y)$, $\Pi(x, y)$ и $I(x, y, z)$, означающие «$x$ совпадает с $y$», «$x$ и $y$ параллельны» и «$x$, $y$ и $z$ проходят через одну точку».

Рассмотрим следующие формулы из $\Psi$.

($\alpha$) $G_2(x, y)\&G_2(y, z)\supset H(x, y, z)$;

($\beta$) $G_2(x, y)\&G_2(y, z)\supset\neg H(x, y, z)$;

($\gamma$) $\forall y(\neg G_1(x, y)\supset G_2(y, x))$;

($\delta$) $\forall y G_2(y, x))$;

($\varepsilon$) $H(x, y, z)\leftrightarrow G_2(x, z)\&G_2(y, z)\&$

$\&\forall t(G_2(x, t)\&G_2(y, t)\supset G_2(z, t))$.

Для каждой из формул ($\alpha$) — ($\varepsilon$) и каждой из интерпретаций $\Gamma_1$ — $\Gamma_4$ выяснить, истинна ли эта формула в данной интерпретации, и если нет — выполнима ли она в ней.

(б) Пусть $\Gamma_5$ — интерпретация множества $\Psi$, в которой основным множеством служит множество людей, а символами $G_1$, $G_2$ и $H$ отвечают соответственно предикаты $A(x, y)$, $B(x, y)$ и $P'(x, y, z)$, означающие «$x$ — мужского пола, а $y$ — женского», «$x$ старше $y$-а» и «$x$ и $y$ — родители $z$-а» (не смешивать с предикатом $P$ из примера 3 в § 2.4, пункт 6).

Рассмотрим следующие формулы:

($\alpha$) $\neg G_2(x, y)\&\neg G_2(y, x)\&\exists z\exists t(H(z, t, x)\&H(z, t, y))$;

($\beta$) $H(x, y, z)\&G_1(x, y)$;

($\gamma$) $H(x, y, z)\supset G_2(x, z)\&G_2(y, z)$;

($\delta$) $\neg\exists x\exists y H(x, y, z)$;

($\varepsilon$) $\neg\exists y\exists z H(x, y, z)$.

Выразить на русском языке предикаты, в которые переходят формулы ($\alpha$) — ($\varepsilon$) в интерпретации $\Gamma_5$. Какие из этих формул истинны в $\Gamma_5$? Какие выполнимы?

3) Пусть $\Psi'$ получается из $\Psi$ (см. задачу 2) заменой символа $H$ четырехместным предикатным символом $K$. Обозначим через $\Gamma_1'$, $\Gamma_2'$, $\Gamma_3'$ интерпретации множества $\Psi'$, в которых основное множество и предикаты, отвечающие $G_1$ и $G_2$ — те же, что в $\Gamma_1$ из задачи 2а, а символу $K$ отвечают соответственно предикаты $\Pi_1(x, y, z, t)$, $\Pi_2(x, y, z, t)$, $\Pi_3(x, y, z, t)$, означающие «числа $x$, $y$ пропорциональны числам $z$, $t$», «числа $x$, $y$, $z$, $t$ взаимно просты» и «$x = y = z = t$».

Рассмотрим формулы:

($\alpha$) $K(x, y, z, t)\supset(G_1(x, y)\supset G_1(z, t))$;

($\beta$) $K(x, y, z, t)\supset(G_2(x, y)\supset G_2(z, t))$;

($\gamma$) $\exists x\exists y(G_1(x, z)\&G_2(y, t)\&K(x, y, z, t))$.

Задание то же, что в задаче 2а.

4) Доказать, что следующие формулы всюду истинны:

а) $\forall x(F(x)\supset F(x))$;

б) $\forall x F(x) \supset F(y)$;

в) $F(y) \supset \exists x F(x)$;

г) $\exists y G(x, x) \supset \exists y \exists z G(y, z)$;

д) $\exists x \exists y \exists z H(x, y, z) \vee \exists z \forall y \forall x \neg H(z, y, x))$.

5) Доказать, что следующие формулы невыполнимы:

а) $\exists x((G(x) \supset \neg G(x)) \& (\neg G(x) \supset G(x)))$;

б) $\exists y \forall x \neg F(y, x) \& \forall x \exists y F(x, y)$;

в) $(H(x) \supset H(y)) \& \exists x H(x) \& \exists x \neg H(x)$.

6) Доказать, что следующие формулы выполнимы, но не всюду истинны:

а) $\exists y F(x, y)$;

б) $F(y) \supset \forall x F(x)$;

в) $\exists x F(x) \supset F(y)$;

г) $\exists x(G(x) \supset \neg G(x)) \& \exists x(\neg G(x) \supset G(x))$;

д) $\forall y \exists x H(x, y) \& \neg \exists x \forall y H(x, y)$.

е) $\exists x F(x, y) \& \exists x F(y, x)$;

ж) $\forall x F(x, y) \vee \forall x F(y, x)$;

з) $F(x) \& (\exists x F(x) \supset \forall x F(x))$.

7) Доказать, что если формула (з) предыдущей задачи в какой-либо интерпретации выполнима, то она в ней истинна.

8) (а) Доказать, что формула

$$\forall x \neg M(x, x) \& \forall x \forall y \forall z (M(x, y) \& M(y, z) \supset M(y, z)) \&$$

$$\& \exists x \exists y M(x, y) \& \forall y (M(x, y) \vee M(y, x) \supset M(y, x))$$

выполнима, но ни в какой интерпретации не истинна.

(б) Доказать, что формула

$$\forall x \neg M(x, x) \& \forall x \forall y \forall z (M(x, y) \& M(y, z) \supset M(x, z)) \& \forall x \exists y M(x, y)$$

выполнима, но не является выполнимой ни в какой интерпретации с конечным основным множеством.

9) Доказать, что следующие предикаты, заданные на множестве действительных чисел R, равносильны:

а) $\exists x(x^2 = z^2 - 2z - 15) \equiv (z \leq -3) \vee (z \geq 5)$;

б) $(xy \geq 3x) \& (x < 0) \vee (xy \leq 3x) \& (x > 0) \vee (y \leq 3) \& (x = 0) \equiv y \leq 3$.

10) Доказать, что:

а) $\exists x(F(x) \vee G(x)) \equiv \exists x F(x) \vee \exists x G(x)$;

б) $\exists x(F(x) \supset G(x)) \equiv \forall x F(x) \supset \exists x G(x)$;

в) $\forall x \forall y F(x, y) \supset \exists z \exists t F(t, z) \equiv G(z) \vee \neg G(z)$;

г) $\forall x\forall y\exists z(F(x,z)\&F(z,y))\&\forall x\forall y\forall z(F(x,y)\&F(y,z)\supset F(x,z))\equiv\forall x\forall y F(x,y)$.

11) (а) Доказать, что $\exists x\forall y(F(x)\&G(y))\equiv\forall y\exists x(F(x)\&G(y))$.

(б) То же с заменой $\&$ на $\vee$.

(в) Можно ли в (а) и (б) заменить $F(x)$ $G(y)$ произвольными формулами?

12) Доказать, что:

а) $\exists x F(x,y)\supset\neg\exists x F(y,x)\Rightarrow\neg\exists x F(x,x)$;

б) $\forall x\forall y\forall z(F(x,y)\&F(y,z)\supset F(x,z))$, $\neg\exists x F(x,x)$,

$\exists x\exists y F(x,y)\Rightarrow\neg\exists x\exists y(F(x,y)\&F(y,x))$.

в) $\forall x\forall y\exists z(F(x,z)\&F(z,y)\vee F(y,z)\&F(z,x))$,

$\forall x\forall y\forall z(F(x,y)\&F(y,z)\supset F(x,z))\Rightarrow\forall x\forall y(F(x,y)\vee F(y,x))$.

13) Для следования а) предыдущей задачи показать подходящим подбором интерпретации, что обратное следование неверно.

14) (а) Доказать, что для любой формулы логики предикатов можно построить равносильную, не содержащую кванторов существования.

(б) То же с заменой кванторов существования на кванторы общности.

15) Вывести соотношение II2 из II1.

16) Используя соотношения II1,2, вывести III2 из III3 и III4 из III1.

17) (а) Показать, что формулы $G(x,y)\vee\forall x F(x)$ и $\forall x(G(x,y)\vee F(x))$ не равносильны.

(б) То же для формул $G(x,y)\&\exists x F(x)$ и $\exists x(G(x,y)\&F(x))$.

(в) То же для формул $G(x,y)\vee\exists x F(x)$ и $\exists x(G(x,y)\vee F(x))$.

[Указание. В (а) и (б) заместить $F$ и $G$ предикатами, определенными на множестве всех целых чисел и означающими соответственно «$x>0$», «$x<y$». В (в) использовать замещение из примера после доказательства соотношений группы III, заменив в нем предикат $x\geq 1$ на $x<1$.]

18) Привести к п. н. ф.:

а) $(\neg\exists x F(x,y,z)\supset\forall x F(x,x,x))\vee F(x,z,y)$;

б) $\neg(\exists z\neg\forall x(G(x,y)\&F(x,z))\supset\forall y H(y,z))$;

в) $\forall x(\neg F(x)\supset\forall y(\neg F(y)\supset(\neg\forall z F(z)\supset\forall u F(u))))$;

г) $F(x_1,x_2)\&\forall x_2 G(x_1,x_2,x_3)\&\neg\exists x_1 F(x_1,x_1)$;

д) $\forall x_1 F(x_1,\ldots,x_n)\supset(\forall x_2 F(x_1,\ldots,x_n)\supset\ldots\supset(\forall x_n F(x_1,\ldots,x_n)\supset G(y))\ldots)$.

ГЛАВА

5

# СИНТАКСИС ЛОГИКИ ПРЕДЛОЖЕНИЙ

## § 5.1. ОБЩЕЕ ПОНЯТИЕ ЛОГИЧЕСКОГО ИСЧИСЛЕНИЯ

1. В настоящей главе мы будем изучать отношения между формулами логики предложений — а именно, отношение выводимости и некоторые производные от него,— отвлекаясь от истинностных значений этих формул. Строение связей между единицами того или иного языка, рассматриваемыми в плане выражения, т. е. безотносительно к их смыслу, называют синтаксисом[1] этого языка. Таким образом, мы будем сейчас заниматься синтаксисом языка логики предложений; слово «языка» здесь обычно опускают и говорят просто о синтаксисе логики предложений (ср. начало гл. 3).

Что же такое отношение выводимости? «Материально», т. е. по объему, оно совпадает с рассматривавшимся в гл. 3 отношением семантического следования. Но задается оно совсем иначе — как результат «процесса вывода», аналогичного процессу доказательства в «обычной математике», пользующейся естественным (а не символическим) языком, но происходящего в соответствии с некоторыми четко сформулированными правилами — настолько четко, что ведущийся по этим правилам процесс вывода в принципе может быть механизирован. Совокупность этих «правил вывода» называют иногда логическим исчислением. Чаще, однако, последний термин понимают в более широком смысле, включая в логическое исчисление не только правила вывода, или, как еще говорят, правила преобразова-

[1] От греч. σύνταξις — «строй, устройство, сочетание, связь, система». Соответствующий аспект исследования языка, а также раздел языковедения, в котором изучаются связи между языковыми единицами безотносительно к их смыслу, называют иногда *синтактикой*.

ния формул, но и правила их образования, позволяющие строго формально описать само понятие формулы. А чтобы это можно было сделать, исчисление должно содержать еще одну компоненту — перечень элементарных символов, из которых формулы строятся. (Разумеется, при построении конкретного исчисления компоненты должны вводиться в обратном порядке — сначала перечень элементарных символов, затем правила образования и, наконец, правила преобразования.) В дальнейшем мы будем понимать логические исчисления именно в таком расширенном смысле; это тем более уместно, что до сих пор мы не дали еще строгого определения формулы логики предложений, равно как и формулы логики предикатов[2].

2. Итак, *логическое исчисление* есть система, состоящая из трех компонент, которые мы сейчас охарактеризуем более подробно.

I. Первая компонента — перечень *элементарных символов*, в совокупности образующих *алфавит* данного исчисления. С формальной точки зрения это просто некоторое множество, но оно должно быть задано достаточно конструктивно — либо просто перечислением элементов, либо «как бы перечислением» вроде $a_1, \cdots, a_n$ или $a_1, a_2, \cdots$ (поэтому мы и говорим о «перечне»). В принципе можно было бы обойтись исчислениями с конечным алфавитом, но это приводит к не вызываемому необходимостью усложнению вида формул; поэтому чаще рассматриваются исчисления с бесконечными алфавитами.

Следует иметь в виду, что элемент алфавита — это не какой-то конкретный «экземпляр» символа, а «символ-образец», с которого можно изготовить сколько угодно «копий». (Это согласуется и с обычным «нематематическим» употреблением слова «алфавит»: под алфавитом, как правило, понимают именно множество образцов букв.)

Из элементарных символов, как из «букв» алфавита, можно составлять «слова» — конечные последовательности элементарных символов, или, точнее, «копий» элементарных символов; эти «копии» называются вхождениями элементарных символов в слово. Например, «парапсихоэкстрасенсобред» — слово в русском алфавите, содержащее два вхождения буквы «п», три вхождения буквы «а» и т. д. (Формально слово в алфавите $A$ можно определить как отображение конечного отрезка натурального ряда $\{1, \cdots, n\}$ в $A$, а вхождение символа в слово — как упорядоченную пару $\langle k, f(k)\rangle$, где $f$ — упомянутое отображение и $k \in \{1, \cdots, n\}$. Напрнмер, вхож -

[2] В качестве синонима термина «логическое исчисление» в расширенном смысле иногда употребляются термины *формальная система* и *формальная теория*. (Эти словосочетания используются и вне математической логики — разумеется, в других значениях.)

дения буквы «а» в только что приведенное слово суть (2,а), (4,а) и (15,а).) Число вхождений символов в слово (т. е. мощность отображаемого отрезка) называется *длиной* этого слова. Например, длина только что приведенного слова равна 24.

II. Вторая компонента — совокупность *правил образования формул*, выделяющих из множества всех слов в алфавите исчисления некоторые «отмеченные» слова, называемые *правильно построенными формулами* — или просто *формулами* — этого исчисления. Правила образования должны быть таковы, чтобы по каждому слову в алфавите исчисления можно было распознать, является ли оно формулой. Чаще всего используются так называемые индуктивные системы правил образования, позволяющие строить формулы «шаг за шагом», переходя от более простых к более сложным. Пример такой системы будет приведен в следующем параграфе.

III. Третья компонента — это совокупность *правил преобразования формул*, иначе называемых *правилами вывода*. С помощью этих правил определяется *отношение выводимости* — бинарное отношение, областью отправления которого является множество всевозможных конечных множеств формул данного исчисления[3], а областью прибытия — множество всевозможных его формул. Если в исчислении $I$ формула $\mathfrak{A}$ выводима из множества формул $\Gamma$, пишут $\Gamma \vdash_I \mathfrak{A}$; если при этом исчисление $I$ заранее известно и подразумевается, то знак $I$ часто опускают и пишут просто $\Gamma \vdash \mathfrak{A}$. При этом для обозначения множества, заданного перечислением его элементов, используется их перечень — т. е. пишут, например, $\mathfrak{A}, \mathfrak{B} \vdash \mathfrak{C}$ или $\mathfrak{A} \vdash \mathfrak{B}$ (а не $\{\mathfrak{A}, \mathfrak{B}\} \vdash \mathfrak{C}$ и не $\{\mathfrak{A}\} \vdash \mathfrak{B}$). Если множество $\Gamma$ пусто, пишут $\vdash_I \mathfrak{A}$ (а не $\varnothing \vdash_I \mathfrak{A}$) или $\vdash \mathfrak{A}$.

Содержательный смысл выводимости $\Gamma \vdash \mathfrak{A}$ состоит в том, что а) формула $\mathfrak{A}$ истинна при условиях $\Gamma$ и б) этот факт установлен с помощью формального вывода. В частности, формула, выводимая из пустого множества, истинна без всяких условий, и имеется формальный вывод, позволяющий установить ее истинность. Поэтому такие формулы естественно называть *теоремами* — или *доказуемыми формулами* — данного исчисления. Вывод формулы из пусто-

[3] Чаще здесь говорят не о конечных множествах, а о конечных последовательностях формул. Это обыкновение возникло в свое время в связи с так называемой «финитной установкой» Д. Гильберта, надеявшегося дать обоснование математики, исходя из реально выписываемых последовательностей символов; эти надежды не оправдались, и в настоящее время определение отношения выводимости для последовательностей, а не для множеств сохраняется в основном по традиции, которую мы позволяем себе нарушить, поскольку изменения при этом не так уж велики, но все же многие формулировки становятся проще и естественнее.

го множества мы будем иногда называть *доказательством* этой формулы.

Более конкретно выводимость формулы $\mathfrak{A}$ из множества формул $\Gamma$ означает существование так называемого *вывода* $\mathfrak{A}$ из $\Gamma$, представляющего собой либо конечную последовательность формул, либо дерево, в узлах которого стоят формулы, и служащего изображением «процесса выведения $\mathfrak{A}$ из $\Gamma$». Каждый шаг этого процесса состоит в применении того или иного правила. В разных исчислениях правила вывода устроены по-разному, но при всем их разнообразии можно выделить два основных типа: *структурные правила*, отвечающие чисто формальным шагам вывода (например, правило, устанавливающее, что всякая формула выводима из любого содержащего ее множества формул) и *логические правила*, отвечающие шагам, основанным на свойствах логических операций и логических констант (например, правило, устанавливающее, что из формул $\mathfrak{A}$ и $\mathfrak{B}$ выводима формула $\mathfrak{A}\&\mathfrak{B}$). Особое место занимают правила, устанавливающие выводимость каких-либо формул из пустого множества. Такие формулы — выводимые из пустого множества непосредственно в силу какого-то одного правила — называются *аксиомами*[4] данного исчисления. (Таким образом, аксиома в логическом исчислении есть частный случай теоремы — «исходная» теорема.) Правила этого типа чаще всего формулируют отдельно от остальных, просто перечисляя аксиомы (если их множество конечно) или указывая их общий вид. Иногда аксиомы считают отдельной, четвертой компонентой логического исчисления.

3. Несколько слов о классификации логических исчислений. Прежде всего, различают *чистые логические исчисления* (лучше было бы говорить «чисто логические исчисления»), предназначенные для формализации логического вывода безотносительно к предметной области, в которой он применяется, и *прикладные логические исчисления* (иначе — *логико-математические исчисления*), служащие для формализации вывода теорем в тех или иных разделах математики. Прикладные исчисления получаются из чистых сужением алфавита и добавлением специальных математических аксиом. В этой главе мы будем иметь дело исключительно с чистыми логическими исчислениями; с прикладными исчислениями мы столкнемся в § 6.3 и в гл. 8.

Логические исчисления делят также на исчисления *гильбертов-*

[4] От греч. ἀξίωμα — «основное положение» (собственно, «нечто достойное признания» — от ἄξιος — «достойный, заслуживающий»).

*ского типа*[5] и *генценовского типа*[6]. Первые характеризуются тем, что почти все логические правила формулируются в виде аксиом, во вторых аксиом почти нет или даже нет вовсе. В исчислениях гильбертовского типа выводимость описывается технически проще, зато исчисления генценовского типа более естественны — вывод в них больше похож на то, как на самом деле рассуждают математики. Поэтому мы будем вести основное изложение на базе «генценовских» исчислений. (О «гильбертовских» см. в §§ 5.5 и 6.4.)

**4.** В заключение параграфа заметим, что слово «теорема» будет использоваться в этой главе (и в главах 6 и 8) в двух значениях: для обозначения формального объекта — теоремы логического исчисления — и в обычном «неформальном» смысле. Можно было бы, конечно, избежать омонимии — например, называть теоремы логических исчислений «формальными теоремами» или, наоборот, переименовать «обычные» теоремы в «метатеоремы»,— но мы этого не делаем, поскольку читатель вряд ли спутает два столь разных значения слова.

## § 5.2. ОПРЕДЕЛЕНИЕ ИСЧИСЛЕНИЯ $G_0$

Сейчас мы рассмотрим логическое исчисление, предназначенное для описания отношения выводимости в логике предложений. Это исчисление, построенное Г. Генценом[7] и известное под названием *исчисления естественного вывода*, мы будем обозначать $G_0$. В соответствии со сказанным в предыдущем параграфе определение исчисления $G_0$ будет состоять в описании его алфавита, правил образования и правил вывода.

I. А л ф а в и т исчисления $G_0$ есть объединение следующих трех попарно непересекающихся множеств:

$\{X_1, X_2, \ldots\}$ (множество *переменных*);

$\{\&, \vee, \supset, \neg, \Lambda\}$ (множество *логических символов*);

$\{(,)\}$ (множество *синтаксических символов*).

[5] По имени предложившего их немецкого математика Д. Гильберта (David Hilbert, 1862—1943). Гильберт, крупнейший математик своего времени, внес, в частности, существенный вклад в развитие математической логики.

[6] По имени придумавшего их ученика Д. Гильберта немецкого математика Г. Генцена (Gerhard Gentzen, 1909—1945).

[7] Рассматриваемое нами исчисление не в точности совпадает с исчислением Г. Генцена; различия, однако, несущественны.

Пояснения: а) $Л$ означает логическую константу «ложь».

б) Константа «истина» и знак эквиваленции не включены в алфавит во избежание мало оправданного усложнения правил вывода. (Вместо константы «истина» можно использовать выражение $\neg Л$; по поводу эквиваленции см. задачу 5 в конце главы.)

в) Скобки названы синтаксическими символами потому, что они служат исключительно для описания того, как построена формула, т. е. выполняют чисто синтаксические функции.

II. Правила образования формул в исчислении $G_0$ имеют следующий вид:

(а) Каждая переменная есть формула.

(б) $Л$ есть формула.

(в) Если $\mathfrak{A}$ и $\mathfrak{B}$ — формулы, то $(\mathfrak{A})\&(\mathfrak{B})$, $(\mathfrak{A})\vee(\mathfrak{B})$, $(\mathfrak{A})\supset(\mathfrak{B})$ — также формулы.

(г) Если $\mathfrak{A}$ — формула, то $\neg(\mathfrak{A})$ — также формула.

(д) Всякая формула является таковой в силу одного из правил (а) — (г). (Иначе говоря, не существует никаких формул, кроме построенных по правилам (а) — (г).)

Мы сформулировали, таким образом, систему правил, состоящую из нескольких «положительных», или, как обычно говорят, *прямых* правил, указывающих, какие бывают формулы, и одного «отрицательного», или *косвенного* правила, утверждающего, что никаких других формул не бывает. При этом прямые правила делятся на *безусловные*, утверждающие просто, что такие-то и такие-то объекты являются формулами (правила (а) и (б)), и *условные*, утверждающие, что если какие-то объекты суть формулы, то и некоторые другие объекты, построенные определенным образом из исходных, тоже будут формулами (правила (в) и (г)). Так устроенные системы правил, служащие для определения некоторого понятия, называются *индуктивными*. (Часто им дают имя *индуктивных определений*; отдельные правила называют тогда *пунктами* определения и говорят о *прямых пунктах* и *косвенном пункте*. Сформулированная нами система правил — это индуктивное определение формулы исчисления $G_0$.)

Число вхождений в формулу логических символов, отличных от $Л$ (т. е. пропозициональных связок), мы будем называть *сложностью* этой формулы. Когда нужно доказать, что все формулы обладают некоторым общим свойством, это делается чаще всего с помощью возвратной индукции по сложности формулы. (Мы уже пользовались этим методом при доказательстве леммы о противоположной формуле в § 3.3.)

Для упрощения записи формул мы обычно будем опускать некоторые (или все) скобки, следуя тому же соглашению о порядке действий, которого мы придерживались в предыдущих главах.

III. Правила вывода — самая сложная и самая интересная часть всякого логического исчисления. Формулируя эти правила, мы всегда будем использовать для обозначения произвольных формул прописные готические буквы и для обозначения произвольных конечных множеств формул — прописные греческие (так что, например, запись $\mathfrak{A}$, $\mathfrak{A}\supset\mathfrak{B}\vdash\mathfrak{B}$ будет означать: «Каковы бы ни были формулы $\mathfrak{A}$ и $\mathfrak{B}$, из формул $\mathfrak{A}$ и $\mathfrak{A}\supset\mathfrak{B}$ выводима формула $\mathfrak{B}$».

В исчислении $G_0$ правила вывода следующие:

A. Прямые правила

A1. Структурные правила

1) Если $\mathfrak{A}\in\Gamma$, то $\Gamma\vdash\mathfrak{A}$ (*правило тривиальной выводимости*, сокращенно ТВ);

2) Если $\Gamma_1\vdash\mathfrak{A}_1$, .... $\Gamma_k\vdash\mathfrak{A}_k$ и $\mathfrak{A}_1$, ..., $\mathfrak{A}_k$, $\mathfrak{B}_1$, ..., $\mathfrak{B}_l\vdash\mathfrak{C}$ ($k = 1, 2, ...$, $l = 0, 1, ...$), то $\Gamma_1$, ..., $\Gamma_k$, $\mathfrak{B}_1$, ..., $\mathfrak{B}_l\vdash\mathfrak{C}$ (*правило транзитивности*, сокращено Т).

Пояснение. Мы пишем $\Gamma_1$, ..., $\Gamma_k$, $\mathfrak{B}_1$, ..., $\mathfrak{B}_l$ вместо $\Gamma_1\cup\cdots\cup\Gamma_k\cup\{\mathfrak{B}_1, ..., \mathfrak{B}_l\}$. Подобными обозначениями мы будем пользоваться и дальше (например, $\Gamma, \mathfrak{A}$ вместо $\Gamma\cup\{\mathfrak{A}\}$.

Содержательный смысл структурных правил очевиден.

Правило транзитности мы могли бы сформулировать в более простом и изящном виде: Если $\Gamma_1\vdash\mathfrak{A}$, ..., $\Gamma_k\vdash\mathfrak{A}_k$ и $\mathfrak{A}_1$, ..., $\mathfrak{A}_k\vdash\mathfrak{C}$, то $\Gamma_1$, ..., $\Gamma_k\vdash\mathfrak{B}$; из этой формулировки вместе с правилом ТВ очевидным образом получается наша, которую мы предпочли потому, что она удобнее в работе (см. ниже).

A2. Логические правила

Исчисление $G_0$ содержит десять логических правил. Восемь из них — так называемые правила введения и удаления логических символов, играющие, в сущности, роль определений пропозициональных связок. Каждой пропозициональной связке отвечают два правила — правило введения и правило удаления этой связки. Мы расположим эти правила в два столбца:

1) $\mathfrak{A}, \mathfrak{B}\vdash\mathfrak{A}\&\mathfrak{B}$

(*введение конъюнкции*);

2) $\mathfrak{A}\&\mathfrak{B}\vdash\mathfrak{A}$
$\mathfrak{A}\&\mathfrak{B}\vdash\mathfrak{B}$

(*удаление конъюнкции*);

3) $\mathfrak{A}\vdash\mathfrak{A}\vee\mathfrak{B}$
$\mathfrak{B}\vdash\mathfrak{A}\vee\mathfrak{B}$

(*введение дизъюнкции*);

4) Если $\Gamma, \mathfrak{A}\vdash\mathfrak{C}$ и $\Gamma, \mathfrak{B}\vdash\mathfrak{C}$, то $\Gamma, \mathfrak{A}\vee\mathfrak{B}\vdash\mathfrak{C}$

(*удаление дизъюнкции*);

5) Если $\Gamma, \mathfrak{A}\vdash\mathfrak{B}$, то $\Gamma\vdash\mathfrak{A}\supset\mathfrak{B}$

(*введение импликации*);

6) $\mathfrak{A}, \mathfrak{A}\supset\mathfrak{B}\vdash\mathfrak{B}$

(*удаление импликации*);

7) Если $\Gamma, \mathfrak{A} \vdash Л$, то $\Gamma \vdash \neg\mathfrak{A}$ (*введение отрицания*);

8) $\mathfrak{A}, \neg\mathfrak{A} \vdash Л$ (*удаление отрицания*).

Сокращенно эти правила будут обозначаться ВК, УК, ВД, УД, ВИ, УИ, ВО, УО.

Кроме правил введения и удаления, имеются еще два особых логических правила:

9) $Л \vdash \mathfrak{B}$ (*правило Дунса Скота*, сокращенно ДС);

10) $\vdash \mathfrak{A} \vee \neg\mathfrak{A}$ (*закон исключенного третьего*, сокращенно ИТ).

**Пояснение.** Логические правила исчисления $G_0$ представляют собой формализацию простейших «правил логического вывода», которыми пользуются математики в своих рассуждениях. Так, доказав два утверждения $A$ и $B$, математик выводит из этого, что истинно также утверждение «$A$ и $B$» (введение конъюнкции); обратно, если доказано «$A$ и $B$», считается истинным каждое из предложений $A$ и $B$ по отдельности (удаление конъюнкции). Если доказано хотя бы одно из утверждений $A$, $B$, отсюда выводится истинность утверждения «$A$ или $B$» (введение дизъюнкции). Удаление дизъюнкции — это *доказательство разбором случаев*: если в какой-то ситуации (описываемой множеством предложений $\Gamma$) возможны два случая $A$ и $B$ (не обязательно взаимоисключающие) и в каждом из этих случаев удается доказать утверждение $C$, то это утверждение можно считать вообще доказанным для данной ситуации. Далее, если из $A$ можно вывести $B$, то считается доказанным условное утверждение «Если $A$, то $B$» (введение импликации); обратно, из истинности условного утверждения и его посылки выводится истинность заключения (удаление импликации). Введение отрицания — это прием доказательства, который в старых учебниках математики назывался *приведением к нелепости* (по-латыни *reductio ad absurdum*): если, допустив, что (при некотором условии $\Gamma$) предложение $A$ истинно, мы приходим к заведомо ложному выводу, то мы можем считать доказанным, что (при условии $\Gamma$) предложение $A$ ложно (т. е. что истинно его отрицание)[8]. Удаление отрицания — это закон противоречия (ср. с. 105). Правило Дунса Скота, позволяющее вывести из ложного утверждения все, что угодно (ср. другую формулировку того правила на с. 107), в математике используется, когда считают доказанным условное утверждение, если его посылка опровергнута (ср. соображения, приведенные в § 2.3 при определении импликации); в исчислении $G_0$ это означает применение ДС в сочетании с введением импликации (см. ниже пример (9)). В обычных математических рассуж-

[8] Приведение к нелепости не следует смешивать с доказательством от противного (о нем см. ниже, с. 173).

дениях правило Дунса Скота часто используется также при доказательстве разбором случаев: если, доказывая, что при некотором условии $\Gamma$ справедливо утверждение $C$, мы рассматриваем различные случаи и при этом оказывается, что с одним из них условие несовместимо (т. е. в этом случае из $\Gamma$ выводится заведомая ложь), то мы считаем, что и в этом случае $C$ истинно при условии $\Gamma$. (Типичный пример — когда при доказательстве какого-либо свойства элементов множества в одном из случаев множество оказывается пустым.) В формальных выводах в исчислении $G_0$ правило Дунса Скота также часто применяется в сочетании с разбором случаев, т. е. удалением дизъюнкции (см. ниже примеры (14) и (23).

Особняком стоит закон исключенного третьего — единственное правило, справедливость которого ставится частью математиков под сомнение[9]. Эти математики считают, что всякое математическое доказательство должно быть «конструктивным»; в частности, утверждение о существовании объекта с определенными свойствами может считаться доказанным лишь при условии, что известно, как такой объект построить, а дизъюнкция обоснована только тогда, когда известен способ узнать, какой ее член верен, и найти обоснование его верности. Поэтому если, например, $A$ есть утверждение о существовании объекта с теми или иными свойствами, то дизъюнкция «$A$ или не $A$» может считаться обоснованной лишь в двух случаях: когда указан способ построения такого объекта и когда доказано, что его не существует.

Впервые с этого рода критикой закона исключенного третьего выступили в начале нынешнего столетия сторонники интуиционистского направления в философии математики (см. Введение) — Л. Э. Я. Брауэр (Luitzen Egbertus Jan Brouwer, 1881—1966) и Г. Вейль (Hermann Weyl, 1885—1955). Таких же взглядов относительно конструктивности в математических рассуждениях и роли закона исключенного третьего придерживаются сторонники возникшего в середине века конструктивного направления, основоположниками которого были А.А. Марков (1903—1979) и Н.А. Шанин (род. в 1919 г.). Логическое исчисление, формализующее допустимые с интуиционистской точки зрения методы рассуждения, было построено в 1930 г. учеником Брауэра А. Гейтингом (Arend Heiting). В отличие от *классической логики*, используемой в обычных матема-

[9] Подвергалось критике также правило Дунса Скота, но эта критика не нашла сколько-нибудь заметного отклика. Последовательное проведение основанной на этой критике точки зрения требует отказа от операции отрицания и, стало быть, от всех связанных с ней правил. Попытки обосновать математику без использования отрицания предпринимались (см. [Френкель — Бар-Хиллел 1966], с. 289—291), но вряд ли можно говорить здесь о существенных успехах.

тических рассуждениях, логику, описываемую исчислением Гейтинга, принято называть *интуиционистской* или *конструктивной логикой*[10]. Исчисление $G_0$ без закона исключенного третьего равносильно «пропозициональной части» исчисления Гейтинга[11].

В дальнейшем изложении неконструктивные формальные выводы — т. е. те, в которых используется закон исключенного третьего — будут отмечаться звездочкой.

Заметим еще, что закон исключенного третьего занимает среди правил исчисления $G_0$ особое место и в отношении формы: он дает единственную в этом исчислении *схему аксиом*. [Вообще *схемой формул* принято называть выражение, содержащее «формульные переменные» (у нас эту роль играют прописные готические буквы) и превращающееся при замене этих переменных произвольными формулами также в формулу (например, $\mathfrak{A} \supset \mathfrak{B}$, $\neg\mathfrak{A} \vee \neg\mathfrak{B}$ и т. п.). Если каждая формула, возникающая таким образом из некоторой схемы формул, является аксиомой соответствующего логического исчисления, эту схему называют *схемой аксиом* данного исчисления. Точно так же говорят о *схемах теорем*.]

Б. К о с в е н н о е п р а в и л о. Отношение выводимости между множеством формул и формулой может иметь место только в силу одного из прямых правил.

Таким образом, определение отношения выводимости по своей формальной структуре аналогично определению формулы: оно является индуктивным.

Заметим, наконец, что прямые правила вывода, аналогично прямым правилам образования формул, можно разделить на *безусловные* и *условные*. Правила Т, УД, ВИ, ВО — условные, все остальные — безусловные[12].

---

[10] Конструктивной логикой занимаются не только интуиционисты и конструктивисты, но и «классики». Образцами «классического» подхода к конструктивной логике могут служить работа К. Гёделя [Gödel 1933] и курс лекций П.С. Новикова [Новиков 1977].

[11] Исчисление, равносильное гейтинговскому исчислению в полном объеме, будет построено ниже, в § 6.1.

[12] Почему мы относим к безусловным правило ТВ — ведь оно имеет вид условного предложения? Дело в том, что в посылке этого предложения нет речи о выводимости.

## § 5.3. ФОРМАЛЬНЫЕ ВЫВОДЫ В ИСЧИСЛЕНИИ $G_0$

1. Посмотрим теперь, как «работает» исчисление $G_0$, т. е. как в нем доказывается выводимость. Когда нужно доказать, что в том или ином логическом исчислении из некоторого множества формул $\Gamma$ выводима некоторая формула $\mathfrak{A}$, это делается обычно путем последовательного применения правил вывода. Такое «прямое» доказательство выводимости принято называть *выводом* $\mathfrak{A}$ из $\Gamma$ в данном исчислении.

Приведем для начала четыре простых примера выводов в исчислении $G_0$.

(1) Легко видеть, что $(\mathfrak{A}\&\mathfrak{B})\&\mathfrak{C}\vdash\mathfrak{A}$. В самом деле, по правилу УК имеем $(\mathfrak{A}\&\mathfrak{B})\&\mathfrak{C}\vdash\&\mathfrak{C}\vdash\mathfrak{A}\&\mathfrak{B}$ и $(\mathfrak{A}\&\mathfrak{B})\vdash\mathfrak{A}$, откуда по правилу Т получаем $(\mathfrak{A}\&\mathfrak{B})\&\mathfrak{C}\vdash\mathfrak{A}$.

(2) Покажем, что $\mathfrak{A}, \mathfrak{B}, \mathfrak{A}\&\mathfrak{B}\vee\mathfrak{C}\supset\mathfrak{G}\vdash\mathfrak{G}$. Имеем $\mathfrak{A}, \mathfrak{B}\vdash\mathfrak{A}\&\mathfrak{B}$ (правило ВК), $\mathfrak{A}\&\mathfrak{B}\vdash\mathfrak{A}\&\mathfrak{B}\vee\mathfrak{C}$ (правило ВД), откуда $\mathfrak{A}, \mathfrak{B}\vdash\mathfrak{A}\&\mathfrak{B}\vee\mathfrak{C}$ (правило Т). Но $\mathfrak{A}\&\mathfrak{B}\vee\mathfrak{C}, \mathfrak{A}\&\mathfrak{B}\vee\mathfrak{C}\supset\mathfrak{G}\vdash\mathfrak{G}$ (правило УИ), так что по правилу Т получается $\mathfrak{A}, \mathfrak{B}, \mathfrak{A}\&\mathfrak{B}\vee\mathfrak{C}\supset\mathfrak{G}\vdash\mathfrak{G}$.

(3) $\mathfrak{A}\&\mathfrak{B}\vdash\mathfrak{B}\&\mathfrak{A}$. По УК имеем $\mathfrak{A}\&\mathfrak{B}\vdash\mathfrak{B}$ и $\mathfrak{A}\&\mathfrak{B}\vdash\mathfrak{A}$, а по ВК $\mathfrak{B}, \mathfrak{A}\vdash\mathfrak{B}\&\mathfrak{A}$. Отсюда по Т получаем $\mathfrak{A}\&\mathfrak{B}\vdash\mathfrak{B}\&\mathfrak{A}$.

(4) $\mathfrak{A}, \mathfrak{B}\vdash\mathfrak{A}\vee\mathfrak{B}$. Имеем $\mathfrak{A}, \mathfrak{B}\vdash\mathfrak{A}$ (по ТВ) и $\mathfrak{A}\vdash\mathfrak{A}\vee\mathfrak{B}$ (по ВД), откуда $\mathfrak{A}, \mathfrak{B}\vdash\mathfrak{A}\vee\mathfrak{B}$ (по Т).

Очень удобно изображать вывод формулы $\mathfrak{A}$ из множества $\Gamma$ в виде дерева, в котором $\mathfrak{A}$ служит «корнем», а элементы $\Gamma$ — «листьями». Например, только что приведенные выводы представляются в виде деревьев следующим образом:

(1)
$$\begin{array}{l} 1\ \dfrac{(\mathfrak{A}\&\mathfrak{B})\&\mathfrak{C}}{\mathfrak{A}\&\mathfrak{B}}\ \text{УК} \\ 2\ \dfrac{\mathfrak{A}\&\mathfrak{B}}{\mathfrak{A}}\ \text{УК} \end{array}$$

(2)
$$\begin{array}{l} 1\ \dfrac{\mathfrak{A}\quad\mathfrak{B}}{\mathfrak{A}\&\mathfrak{B}}\ \text{ВК} \\ 2\ \dfrac{\mathfrak{A}\&\mathfrak{B}}{\mathfrak{A}\&\mathfrak{B}\vee\mathfrak{C}}\ \text{ВД} \qquad \mathfrak{A}\&\mathfrak{B}\vee\mathfrak{C}\supset\mathfrak{G} \\ 3\ \dfrac{\qquad\qquad\qquad\qquad}{\mathfrak{G}}\ \text{УИ} \end{array}$$

(3) $$\dfrac{\dfrac{\mathfrak{A}\&\mathfrak{B}}{\mathfrak{A}}\,\text{УК} \qquad \dfrac{\mathfrak{A}\&\mathfrak{B}}{\mathfrak{B}}\,\text{УК}}{\mathfrak{B}\&\mathfrak{A}}\,\text{ВК}$$

(4) $$\dfrac{\dfrac{\mathfrak{A} \quad \mathfrak{B}}{\mathfrak{A}}\,\text{ТВ}}{\mathfrak{A}\vee\mathfrak{B}}\,\text{ВД}$$

Из этих примеров должно быть уже понятно, как устроены *«деревья вывода»* в простейшем случае, когда применяются только безусловные правила и правило транзитивности. Нетрудно было бы дать и точное определение такого дерева, но мы отложим это до того времени, когда будет рассмотрен общий случай, а пока ограничимся следующими неформальными пояснениями:

1) Каждой горизонтальной черте отвечает применение некоторого (безусловного) правила: над чертой стоят посылки этого правила, под чертой — заключение. Дерево, содержащее только одну черту — это «элементарное» дерево; его «корень» выводим из множества «листьев» непосредственно в силу соответствующего правила[13].

2) Каждое неэлементарное дерево «собирается» из других «меньших» деревьев, и эта «сборка» есть не что иное, как применение правила транзитивности. В самом деле, всякое неэлементарное дерево имеет вид

$$\frac{\delta_1 \cdots \delta_k \quad \mathfrak{A}_1 \cdots \mathfrak{A}_l}{\mathfrak{B}}\ (k = 1, 2, \ldots;\ l = 0, 1, \ldots),$$

где $\delta_1, \ldots, \delta_k$ — деревья и $\mathfrak{A}_1, \ldots, \mathfrak{A}_l, \mathfrak{B}$ — формулы[14].

Пусть $\mathfrak{C}_i$ и $\Delta_i$ — соответственно «корень» и множество «листьев» дерева $\delta_i$ $(i = 1, \ldots, k)$. Тогда, если $\mathfrak{C}_1, \ldots, \mathfrak{C}_k, \mathfrak{A}_1, \ldots, \mathfrak{A}_l \vdash \mathfrak{B}$ и для каждого $i = 1, \ldots, k$ справедливо $\Delta_i \vdash \mathfrak{C}_i$, имеем по правилу транзитивности $\Delta_1, \ldots, \Delta_k, \mathfrak{A}_1, \ldots, \mathfrak{A}_l \vdash \mathfrak{B}$; но $\Delta_1, \ldots, \Delta_k, \mathfrak{A}_1, \ldots, \mathfrak{A}_l$ — это как раз множество «листьев» нашего «большого» дерева.

---

[13] Множество «листьев» «элементарного» дерева для безусловного логического правила состоит или из двух элементов (для ВК, УИ и УО), или из одного (для УК, ВД и ДС), или пусто (для ИТ). В случае ТВ листьев может быть сколько угодно (но хоть один лист должен быть).

[14] Поскольку мы рассматриваем выводы из множеств, а не из последовательностей формул (в отличие от того, как излагал свое исчисление сам Генцен), мы можем не различать деревья, отличающиеся друг от друга только порядком поддеревьев, «корни» которых расположены непосредственно над одной чертой.

3) Каждое применение правила, отличного от правила транзитивности, мы будем в дальнейшем называть *элементарным шагом* или просто *шагом* вывода. Шаги вывода мы нумеруем (номер ставится слева от черты). Пока что без номеров можно было бы обойтись, но потом они нам понадобятся. Номера присваиваются шагам таким образом, чтобы в каждом поддереве самая нижняя черта имела наибольший номер[15]; в остальном нумерация произвольна. Справа от черты мы пишем сокращенное название правила. Впрочем, в дальнейшем мы будем писать его не всегда, так же как и номер.

Задача. а) Доказать, что всякая теорема исчисления $G_0$ выводима в нем из любого конечного множества формул. [Указание: воспользоваться правилами ТВ, ВК и УК ].

б) Доказать, что в $G_0$ справедливо «правило расширения»: если $\Gamma\vdash\mathfrak{A}$ и $\Gamma\subset\Delta$, то $\Delta\vdash\mathfrak{A}$.

Перейдем теперь к выводам, содержащим условные логические правила. Для чего эти правила служат? В математических рассуждениях часто прибегают к введению *промежуточных гипотез*, которые потом устраняются. Примером может служить доказательство от противного: чтобы доказать некоторое утверждение, мы принимаем гипотезу, что оно неверно, которая в дальнейшем устраняется. То же происходит при доказательстве разбором случаев: рассматривая каждый отдельный случай, мы принимаем гипотезу, что этот случай имеет место, а когда все случаи разобраны, мы больше не нуждаемся в этих гипотезах. Для формализации таких доказательств — с введением промежуточных гипотез, которые потом устраняются — как раз и служат условные логические правила. При применении каждого из этих правил устраняется некоторая гипотеза или гипотезы (устраняемые гипотезы были обозначены на с. 160—161 через $\mathfrak{A}$, $\mathfrak{B}$ в правиле УД и через $\mathfrak{A}$ в правилах ВИ и ВО). В дереве вывода гипотезы — это те формулы, которые являются его «листьями». Поэтому устранение гипотезы можно представлять себе как «обрыв» или «увядание» листа. (Из дальнейшего будет видно, что «увядание» — более точный образ.) При «сборке» большего дерева из меньших[16] некоторые их листья могут «увядать»; те листья, которые не «увянут» до конца, образуют множество исходных посылок вывода, т. е. то множество $\Gamma$, которое стоит слева от знака $\vdash$ в выводимости $\Gamma\vdash\mathfrak{A}$, доказываемой с помощью данного дерева; «увядшие» листья — это промежуточные гипотезы. Может случиться, что «увянут» все листья;

[15] Мы делаем так, впрочем, только ради удобства; на самом деле существенно только то, чтобы номера разных шагов были различны.

[16] Хотелось бы, конечно, говорить здесь о «выращивании» дерева, но тогда ему пришлось бы расти от листьев к корню.

тогда мы получим вывод из пустого множества — иначе говоря, корень дерева будет теоремой.

В соответствии со сказанным применение условных логических правил изображается в дереве вывода следующим образом:

а) Применению правила ВИ отвечает горизонтальная черта, снизу от которой записывается формула $\mathfrak{A} \supset \mathfrak{B}$, а сверху — формула $\mathfrak{B}$, причем эта последняя должна быть корнем дерева вывода, среди «неувядших» листьев которого имеются все формулы, составляющие $\Gamma$, и формула $\mathfrak{A}$. При «достройке» дерева с корнем $\mathfrak{B}$ до дерева с корнем $\mathfrak{A} \supset \mathfrak{B}$ лист $\mathfrak{A}$ «увядает». «Увядшие листья» — т. е. устраненные гипотезы — мы будем заключать в квадратные скобки, указывая при них номера шагов, на которых они устранены (номер пишется в круглых скобках справа).

б) Применение правила ВО изображается точно так же с заменой $\mathfrak{B}$ на $\Lambda$ и $\mathfrak{A} \supset \mathfrak{B}$ на $\neg\mathfrak{A}$.

в) Применению правила УД отвечает горизонтальная черта, снизу от которой записывается формула $\mathfrak{C}$, а сверху — $\mathfrak{A} \vee \mathfrak{B}$ и два раза та же формула $\mathfrak{C}$, причем одно из верхних вхождений $\mathfrak{C}$ должно быть корнем дерева, среди неувядших листьев которого имеются формула $\mathfrak{A}$ и все формулы, составляющие $\Gamma$, а другое — корнем дерева, среди неувядших листьев которого имеются формула $\mathfrak{B}$ и все формулы, составляющие $\Gamma$. (Формула $\mathfrak{A} \vee \mathfrak{B}$ тоже может быть здесь корнем какого-то дерева.) При «сборке» «большого» дерева листья $\mathfrak{A}$ и $\mathfrak{B}$ «увядают».

Проиллюстрируем применение условных логических правил на примерах.

(5) $\vdash \mathfrak{A} \supset \mathfrak{A}$.

Доказательство:

$$1\ \frac{[\mathfrak{A}](2)}{\mathfrak{A}}\ \text{ТВ}$$
$$2\ \frac{\mathfrak{A}}{\mathfrak{A} \supset \mathfrak{A}}\ \text{ВИ}$$

(На шаге 2 применяется ВИ с пустым $\Gamma$.)

(6) $\mathfrak{A} \vdash \neg\neg\mathfrak{A}$.

Доказательство:

$$1\ \frac{\mathfrak{A}\ [\neg\mathfrak{A}](2)}{\Lambda}\ \text{УО}$$
$$2\ \frac{\Lambda}{\neg\neg\mathfrak{A}}\ \text{ВО}$$

(На шаге 2 применяется ВО с $\Gamma = \mathfrak{A}$.)

(7) $\mathfrak{A} \vee \mathfrak{B} \vdash \mathfrak{B} \vee \mathfrak{A}$.

Доказательство:

$$\begin{array}{l} 1\ \dfrac{[\mathfrak{A}](3)}{\mathfrak{B}\vee\mathfrak{A}}\ \text{ВД} \quad 2\ \dfrac{[\mathfrak{B}](3)}{\mathfrak{B}\vee\mathfrak{A}}\ \text{ВД} \\ 3\ \dfrac{\mathfrak{A}\vee\mathfrak{B}}{\mathfrak{B}\vee\mathfrak{A}}\ \text{УД} \end{array}$$

(На шаге 3 применяется УД с пустым $\Gamma$.)

Теперь мы можем сформулировать точное определение дерева вывода. Деревья, которые мы будем определять, не содержат номеров шагов и имен правил; эти компоненты можно восстановить по остальным, и мы пишем их в примерах только для облегчения понимания (да и то не всегда).

Предварительно определим *элементарное дерево вывода* (*в исчислении* $G_0$). Так мы будем называть выражение, состоящее из горизонтальной черты, снизу от которой записано заключение некоторого б е з у с л о в н о г о правила исчисления $G_0$, а сверху в произвольном порядке — все посылки этого правила. (В частности, в случае правила ТВ над чертой записывается произвольный конечный набор формул, а под чертой — любая формула из этого набора; в случае правила ИТ над чертой не пишется ничего.)

Определение *дерева вывода* в исчислении $G_0$ будет индуктивным. Одновременно будут определяться *корень* дерева вывода, его *зеленые листья*, его *увядшие листья* и его *высота*.

Определение состоит из следующих шести пунктов:

1) Всякое элементарное дерево вывода есть дерево вывода высоты 1. Его корнем служит формула, записанная под чертой, зелеными листьями — формулы, записанные над чертой; увядших листьев у него нет.

2) Пусть $r$ — элементарное дерево вывода, в котором над чертой записаны формулы $\mathfrak{A}_1, \ldots, \mathfrak{A}_k, \mathfrak{B}_1, \ldots, \mathfrak{B}_l$ ($k = 1, 2, \ldots$; $l = 0, 1, \ldots$) и под чертой — формула $\mathfrak{C}$, и пусть $\delta_1, \ldots, \delta_k$ — деревья вывода с корнями $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$, множествами зеленых листьев $\Gamma_1, \ldots, \Gamma_k$ и множествами увядших листьев $\Delta_1, \ldots, \Delta_k$ соответственно, причем наибольшая из высот этих деревьев равна $n$. Тогда выражение, полученное из $r$ заменой каждой формулы $\mathfrak{A}_i$ ($i = 1, \ldots, k$) деревом $\delta_i$, будет деревом вывода высоты $n + 1$ с корнем $\mathfrak{C}$, множеством зеленых листьев $\Gamma_1 \cup \cdots \cup \Gamma_k \cup \{\mathfrak{B}_1, \ldots, \mathfrak{B}_l\}$ и множеством увядших листьев $\Delta_1 \cup \ldots \cup \Delta_k$.

3) Пусть $\delta$ — дерево вывода высоты $n$ с корнем $\mathfrak{B}$, множеством зеленых листьев $\Gamma$ и множеством увядших листьев $\Delta$, причем $\Gamma$ содержит формулу $\mathfrak{A}$. Тогда выражение, состоящее из горизонтальной черты, снизу от которой записана формула $\mathfrak{A} \supset \mathfrak{B}$, а сверху — дерево $\delta$, будет деревом вывода высоты $n + 1$ с корнем $\mathfrak{A} \supset \mathfrak{B}$, множеством зеленых листьев $\Gamma \setminus \{\mathfrak{A}\}$ и множеством увядших листьев $\Delta \cup \{\mathfrak{A}\}$.

4) Аналогично предыдущему пункту с заменой $\mathfrak{B}$ на $\Pi$ и $\mathfrak{A}\supset\mathfrak{B}$ на $\neg\mathfrak{A}$.

5) а) Пусть $\delta_1$ и $\delta_2$ — деревья вывода, каждое из которых имеет корнем формулу $\mathfrak{C}$, с множествами зеленых листьев $\Gamma_1$ и $\Gamma_2$ и множествами увядших листьев $\Delta_1$ и $\Delta_2$ соответственно, причем $\Gamma_1$ содержит формулу $\mathfrak{A}$, а $\Gamma_2$ — формулу $\mathfrak{B}$, и наибольшая из высот деревьев $\delta_1$, $\delta_2$ равна $n$. Тогда выражение, состоящее из горизонтальной черты, снизу от которой записана формула $\mathfrak{C}$, а сверху в произвольном порядке деревья $\delta_1$ и $\delta_2$ и формула $\mathfrak{A}\vee\mathfrak{B}$, будет деревом вывода высоты $n+1$ с корнем $\mathfrak{C}$, множеством зеленых листьев $(\Gamma_1\setminus\{\mathfrak{A}\})\cup(\Gamma_2\setminus\{\mathfrak{B}\}\cup\cup\{\mathfrak{A}\vee\mathfrak{B}\}$ и множеством увядших листьев $\Delta_1\cup\Delta_2\cup\{\mathfrak{A},\mathfrak{B}\}$.

б) Аналогично а) со следующими изменениями: вместо формулы $\mathfrak{A}\vee\mathfrak{B}$ над чертой записывается некоторое дерево вывода $\delta$ с корнем $\mathfrak{A}\vee\mathfrak{B}$, множеством зеленых листьев $\Gamma$ и множеством увядших листьев $\Delta$; $n$ есть наибольшая из высот деревьев $\delta_1$, $\delta_2$, $\delta$; множество зеленых листьев нового дерева есть $(\Gamma\setminus\{\mathfrak{A}\})\cup(\Gamma\setminus\{\mathfrak{B}\})\cup\Gamma$, множество увядших листьев — $\Delta_1\cup\Delta_2\cup\Delta\cup\{\mathfrak{A},\mathfrak{B}\}$.

6) Всякое дерево вывода является таковым в силу одного из пунктов 1) — 5).

Часть дерева вывода, состоящую из горизонтальной черты и формул, записанных непосредственно над ней и под ней, мы будем называть *шагом вывода*.

Заметим еще, что корень — это формула, под которой нет черты, а листья — формулы, над которыми нет черты.

Теперь, определив понятие дерева вывода, мы можем сказать, что формула $\mathfrak{A}$ выводима из множества формул $\Gamma$ тогда и только тогда, когда существует дерево вывода с корнем $\mathfrak{A}$ и множеством зеленых листьев $\Gamma$. Это вытекает непосредственно из правил вывода исчисления $G_0$ и определения дерева вывода.

Замечание. Одно из правил $G_0$ — правило транзитивности — «работает» в деревьях вывода не так, как остальные: оно обеспечивает самую возможность построения дерева, тогда как другие правила обеспечивают элементарные шаги. Поэтому, если бы мы вместо индуктивного определения выводимости сразу определили ее с помощью деревьев вывода, правило транзитивности было бы не нужно. Можно было бы обойтись также без правила тривиальной выводимости, так как его можно вывести из остальных правил. В самом деле, поскольку мы рассматриваем лишь конечные множества формул, это правило можно заменить следующими двумя:

($\alpha$) $\mathfrak{A}\vdash\mathfrak{A}$; ($\beta$) если $\Gamma\vdash\mathfrak{A}$, то $\Gamma,\mathfrak{B}\vdash\mathfrak{A}$.

Но во-первых, если $\dfrac{\Gamma}{\mathfrak{A}}$ дерево вывода с корнем $\mathfrak{A}$ и множеством зеленых листьев $\Gamma$, то

$$\delta_1 = \dfrac{\dfrac{\Gamma}{\mathfrak{A}} \quad \mathfrak{B}}{\dfrac{\mathfrak{A}\&\mathfrak{B}}{\mathfrak{A}}\ \text{УК}}\ \text{ВК}$$

есть дерево вывода с корнем $\mathfrak{A}$ и множеством зеленых листьев $\Gamma \cup \{\mathfrak{B}\}$; во-вторых, дерево

$$\dfrac{\dfrac{\mathfrak{A} \quad \mathfrak{A}}{\mathfrak{A}\ \&\ \mathfrak{A}}\ \text{ВК}}{\mathfrak{A}}\ \text{УК}$$

имеет корнем $\mathfrak{A}$ и множеством зеленых листьев $\{\mathfrak{A}\}$. Таким образом, определив выводимость с помощью деревьев вывода, мы могли бы обойтись без структурных правил (как и сделано в изложении самого Генцена).

2. Рассмотрим теперь еще ряд примеров выводов — или, что то же самое, деревьев вывода.

(8) $\mathfrak{B} \vdash \mathfrak{A} \supset \mathfrak{B}$.

Доказательство:

$$\begin{array}{ll} 1 & \dfrac{[\mathfrak{A}]^{(2)} \quad \mathfrak{B}}{\mathfrak{B}}\ \text{ТВ} \\ 2 & \dfrac{\mathfrak{B}}{\mathfrak{A}\supset\mathfrak{B}}\ \text{ВИ} \end{array}$$

(9) $\neg\mathfrak{A} \vdash \mathfrak{A} \supset \mathfrak{B}$.

Доказательство:

$$\begin{array}{ll} 1 & \dfrac{[\mathfrak{A}]^{(3)} \quad \neg\mathfrak{A}}{\Lambda}\ \text{УО} \\ 2 & \dfrac{\Lambda}{\mathfrak{B}}\ \text{ДС} \\ 3 & \dfrac{\mathfrak{B}}{\mathfrak{A}\supset\mathfrak{B}}\ \text{ВИ} \end{array}$$

(10) $\mathfrak{A} \vee (\mathfrak{B} \vee \mathfrak{C}) \vdash (\mathfrak{A} \vee \mathfrak{B}) \vee \mathfrak{C}$.

Доказательство:

$$\begin{array}{lll} 1 & \dfrac{[\mathfrak{B}]^{(4)}}{\mathfrak{A}\vee\mathfrak{B}}\ \text{ВД} & \\ 2 & \dfrac{\mathfrak{A}\vee\mathfrak{B}}{(\mathfrak{A}\vee\mathfrak{B})\vee\mathfrak{C}}\ \text{ВД} & 3\ \dfrac{[\mathfrak{C}]^{(4)}}{\mathfrak{B}\vee\mathfrak{C}}\ \text{ВД} \\ 4 & \dfrac{(\mathfrak{A}\vee\mathfrak{B})\vee\mathfrak{C} \quad (\mathfrak{A}\vee\mathfrak{B})\vee\mathfrak{C} \quad [\mathfrak{B}\vee\mathfrak{C}]^{(7)}}{(\mathfrak{A}\vee\mathfrak{B})\vee\mathfrak{C}}\ \text{УД} & 5\ \dfrac{[\mathfrak{A}]^{(7)}}{\mathfrak{A}\vee(\mathfrak{B}\vee\mathfrak{C})}\ \text{ВД} \\ 6 & & \dfrac{\mathfrak{A}\vee\mathfrak{B}}{(\mathfrak{A}\vee\mathfrak{B})\vee\mathfrak{C}\quad \mathfrak{A}\vee(\mathfrak{B}\vee\mathfrak{C})}\ \text{УД} \\ 7 & \dfrac{(\mathfrak{A}\vee\mathfrak{B})\vee\mathfrak{C}}{(\mathfrak{A}\vee\mathfrak{B})\vee\mathfrak{C}}\ \text{УД} & \end{array}$$

(11) $(\mathfrak{A} \vee \mathfrak{B}) \vee \mathfrak{C} \vdash \mathfrak{A} \vee (\mathfrak{B} \vee \mathfrak{C})$.

(12) $\mathfrak{A} \& (\mathfrak{B} \& \mathfrak{C}) \vdash (\mathfrak{A} \& \mathfrak{B}) \& \mathfrak{C}$.

(13) $(\mathfrak{A} \& \mathfrak{B}) \& \mathfrak{C} \vdash \mathfrak{A} \& (\mathfrak{B} \& \mathfrak{C})$.

Эти три выводимости читатель докажет самостоятельно.

(14) $\mathfrak{A} \vee \mathfrak{B}, \neg\mathfrak{A} \vdash \mathfrak{B}$.

Доказательство:

$$\dfrac{1\ \dfrac{[\mathfrak{A}](4) \quad \neg\mathfrak{A}}{2\ \dfrac{\Lambda}{\mathfrak{B}}\ \text{ДС}} \text{УО} \qquad 3\ \dfrac{[\mathfrak{B}](4) \quad \neg\mathfrak{A}}{\mathfrak{B}}\ \text{ТВ} \qquad \mathfrak{A} \vee \mathfrak{B}}{4\ \dfrac{}{\mathfrak{B}}}\ \text{УД}$$

(15) $\mathfrak{A} \vee (\mathfrak{B} \& \mathfrak{C}) \vdash (\mathfrak{A} \vee \mathfrak{B}) \& (\mathfrak{A} \vee \mathfrak{C})$.

Доказательство:

$$\dfrac{\dfrac{1\ \dfrac{[\mathfrak{A}](9)}{\mathfrak{A} \vee \mathfrak{B}} \qquad 2\ \dfrac{[\mathfrak{A}](9)}{\mathfrak{A} \vee \mathfrak{C}}}{3\ \dfrac{}{(\mathfrak{A} \vee \mathfrak{B}) \& (\mathfrak{A} \vee \mathfrak{C})}} \qquad \dfrac{4\ \dfrac{[\mathfrak{B} \& \mathfrak{C}](9)}{5\ \dfrac{\mathfrak{B}}{\mathfrak{A} \vee \mathfrak{B}}} \qquad 6\ \dfrac{[\mathfrak{B} \& \mathfrak{C}](9)}{7\ \dfrac{\mathfrak{C}}{\mathfrak{A} \vee \mathfrak{C}}}}{8\ \dfrac{}{(\mathfrak{A} \vee \mathfrak{B}) \& (\mathfrak{A} \vee \mathfrak{C})}} \qquad \mathfrak{A} \vee (\mathfrak{B} \& \mathfrak{C})}{9\ \dfrac{}{(\mathfrak{A} \vee \mathfrak{B}) \& (\mathfrak{A} \vee \mathfrak{C})}}$$

(16) $(\mathfrak{A} \vee \mathfrak{B}) \& (\mathfrak{A} \vee \mathfrak{C}) \vdash \mathfrak{A} \vee (\mathfrak{B} \& \mathfrak{C})$.

Доказательство:

$$\dfrac{1\ \dfrac{(\mathfrak{A} \vee \mathfrak{B}) \& (\mathfrak{A} \vee \mathfrak{C})}{5\ \dfrac{\mathfrak{A} \vee \mathfrak{B} \quad \mathfrak{A} \vee (\mathfrak{B} \& \mathfrak{C}) \quad \mathfrak{A} \vee (\mathfrak{B} \& \mathfrak{C})}{\mathfrak{A} \vee (\mathfrak{B} \& \mathfrak{C})}\ \text{УД}} \qquad 2\ \dfrac{[\mathfrak{A}](5)}{} \qquad 3\ \dfrac{[\mathfrak{B}](5) \quad [\mathfrak{C}](8)}{4\ \dfrac{\mathfrak{B} \& \mathfrak{C}}{}} \qquad 6\ \dfrac{[\mathfrak{A}](8)}{\mathfrak{A} \vee (\mathfrak{B} \& \mathfrak{C})} \qquad 7\ \dfrac{(\mathfrak{A} \vee \mathfrak{B}) \& (\mathfrak{A} \vee \mathfrak{C})}{\mathfrak{A} \vee \mathfrak{C}}\ \text{УД}}{8\ \dfrac{}{\mathfrak{A} \vee (\mathfrak{B} \& \mathfrak{C})}}$$

(17) $\mathfrak{A} \& (\mathfrak{B} \vee \mathfrak{C}) \vdash (\mathfrak{A} \& \mathfrak{B}) \vee (\mathfrak{A} \& \mathfrak{C})$.

Доказательство:

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathfrak{A} \& (\mathfrak{B} \vee \mathfrak{C})}{\mathfrak{A} \qquad [\mathfrak{B}]}}{\mathfrak{A} \& \mathfrak{B}}}{(\mathfrak{A} \& \mathfrak{B}) \vee (\mathfrak{A} \& \mathfrak{C})} \qquad \dfrac{\dfrac{\dfrac{\mathfrak{A} \& (\mathfrak{B} \vee \mathfrak{C})}{\mathfrak{A} \qquad [\mathfrak{C}]}}{\mathfrak{A} \& \mathfrak{C}}}{(\mathfrak{A} \& \mathfrak{B}) \vee (\mathfrak{A} \& \mathfrak{C})} \qquad \dfrac{\mathfrak{A} \& (\mathfrak{B} \vee \mathfrak{C})}{\mathfrak{B} \vee \mathfrak{C}}}{(\mathfrak{A} \& \mathfrak{B}) \vee (\mathfrak{A} \& \mathfrak{C})}$$

(18) $(\mathfrak{A} \& \mathfrak{B}) \vee (\mathfrak{A} \& \mathfrak{C}) \vdash \mathfrak{A} \& (\mathfrak{B} \vee \mathfrak{C})$.

Эту выводимость читатель докажет самостоятельно.

(19) $\mathfrak{A} \vdash \mathfrak{A} \vee \mathfrak{A}$.

(20) $\mathfrak{A} \vee \mathfrak{A} \vdash \mathfrak{A}$.

(21) $\mathfrak{A} \vdash \mathfrak{A} \& \mathfrak{A}$.

(22) $\mathfrak{A} \& \mathfrak{A} \vdash \mathfrak{A}$.

(19), (21) и (22) — частные случаи правил ВД, ВК и УК. (20) доказывается так:

$$\dfrac{\dfrac{[\mathfrak{A}]}{\mathfrak{A}}\ \text{ТВ} \quad \dfrac{[\mathfrak{A}]}{\mathfrak{A}}\ \text{ТВ} \qquad \mathfrak{A} \vee \mathfrak{A}}{\mathfrak{A}}\ \text{УД}$$

Все рассмотренные до сих пор выводы были конструктивными, т. е. ни в одном из них не использовался закон исключенного третьего. (Без сомнения, выводимости (11), (12), (13) и (18) читатель доказал — или докажет — также конструктивно.) При этом среди наших примеров были аналоги всех основных равносильностей логики предложений из группы I (см. § 3.1) — в том смысле, что для каждой из этих равносильностей ее правая часть выводима в $G_0$ из левой, а левая из правой. Далее мы получим такие аналоги и для прочих основных равносильностей из § 3.1, но не все они будут конструктивны. В частности, закон исключенного третьего нужен, чтобы получить аналог равносильности III — точнее, одну из «половин» этого аналога (другую «половину» мы уже доказали — см. выше пример (6)). В § 3.1 мы назвали равносильность III «правилом снятия двойного отрицания». Однако при переходе к двум выводимостям $\neg\neg\mathfrak{A} \vdash \mathfrak{A}$ и $\mathfrak{A} \vdash \neg\neg\mathfrak{A}$ естественно называть так только первую из них — второй скорее подошло бы название «правила постановки двойного отрицания»; впредь мы ее так и будем называть. Итак:

*(23) $\neg\neg\mathfrak{A} \vdash \mathfrak{A}$.

(Напоминаем, что звездочкой мы договорились отмечать неконструктивные выводы.)

Доказательство:

$$\dfrac{1\ \dfrac{\neg\neg\mathfrak{A} \quad [\mathfrak{A}](5)}{\mathfrak{A}}\ \text{ТВ} \qquad 2\ \dfrac{\neg\neg\mathfrak{A}\ [\neg\mathfrak{A}](5)}{3\ \dfrac{\Lambda}{\mathfrak{A}}\ \text{ДС}}\ \text{УО} \qquad 4\ \dfrac{}{\mathfrak{A} \vee \neg\mathfrak{A}}\ \text{ИТ}}{5\ \mathfrak{A}}\ \text{УД}$$

Комментарий: а) Ниже (с. 174) мы покажем, что из конструктивных правил исчисления $G_0$ и правила снятия двойного отрицания можно, в свою очередь, вывести закон исключенного третьего.

б) Неконструктивный характер правила снятия двойного отрица-

ния можно пояснить так. Если $A$ — утверждение о существовании объекта с теми или иными свойствами, то с конструктивной точки зрения оно считается истинным лишь тогда, когда указан способ построения нужного объекта, в то время как двойное отрицание утверждения $A$ означает только неверность утверждения, что такого способа не существует. Если мы опровергли утверждение о несуществовании способа построить какой-то объект, это еще не позволяет нам указать конкретный способ его построения.

в) На правиле снятия двойного отрицания основано *доказательство от противного*. Оно состоит в следующем: желая доказать утверждение $A$, мы принимаем гипотезу, что оно неверно — иначе говоря, что истинно его отрицание,— и пытаемся привести эту гипотезу к нелепости, т. е. вывести из нее два противоречащих друг другу утверждения — скажем, $B$ и «не $B$»[17]. Если это удалось, то мы можем заключить, пользуясь правилом введения отрицания, что гипотеза неверна, т. е. что справедливо утверждение «Неверно, что $A$ неверно», откуда по правилу снятия двойного отрицания следует, что $A$ истинно. Таким образом, доказательство от противного сложнее, чем приведение к нелепости, и в отличие от него неконструктивно. Приведением к нелепости мы лишь опровергаем некоторую гипотезу, а от противного доказывается «положительное» утверждение.

Займемся теперь аналогами законов Де Моргана. Эту роль выполняют четыре выводимости:

(24) $\neg\mathfrak{A}\&\neg\mathfrak{B} \vdash \neg(\mathfrak{A}\vee\mathfrak{B})$.

(25) $\neg(\mathfrak{A}\vee\mathfrak{B}) \vdash \neg\mathfrak{A}\&\neg\mathfrak{B}$.

(26) $\neg\mathfrak{A}\vee\neg\mathfrak{B} \vdash \neg(\mathfrak{A}\&\mathfrak{B})$.

*(27) $\neg(\mathfrak{A}\&\mathfrak{B}) \vdash \neg\mathfrak{A}\vee\neg\mathfrak{B}$.

Первые три выводимости мы докажем приведением к нелепости:

$$\dfrac{\dfrac{\dfrac{1\ \dfrac{\neg\mathfrak{A}\&\neg\mathfrak{B}}{\neg\mathfrak{A}}\text{УК}\quad [\mathfrak{A}]\,(5)}{2}\text{УО}\qquad \dfrac{3\ \dfrac{\neg\mathfrak{A}\&\neg\mathfrak{B}}{\neg\mathfrak{B}}\text{УК}\quad [\mathfrak{B}]\,(5)}{4}\text{УО}}{5\ \dfrac{Л\qquad\qquad Л}{6\ \dfrac{Л}{\neg(\mathfrak{A}\vee\mathfrak{B})}\text{ВО}}\qquad [\mathfrak{A}\vee\mathfrak{B}]\,(6)}\text{УД}$$

[17] В роли $B$ часто оказывается само $A$. Тогда утверждение «не $B$» вытекает из гипотезы тривиальным образом, так как совпадает с ней (формально — выводится из гипотезы по правилу тривиальной выводимости).

$$\dfrac{\dfrac{[\mathfrak{A}]}{\mathfrak{A}\vee\mathfrak{B}} \quad \neg(\mathfrak{A}\vee\mathfrak{B})}{\dfrac{Л}{\neg\mathfrak{A}}} \qquad \dfrac{\dfrac{[\mathfrak{B}]}{\mathfrak{A}\vee\mathfrak{B}} \quad \neg(\mathfrak{A}\vee\mathfrak{B})}{\dfrac{Л}{\neg\mathfrak{B}}}}{\neg\mathfrak{A}\&\neg\mathfrak{B}}$$

$$1\,\dfrac{[\mathfrak{A}\&\mathfrak{B}](3)}{2\,\dfrac{\mathfrak{A}}{3\,\dfrac{Л}{7\,\dfrac{\neg(\mathfrak{A}\&\mathfrak{B})}{\neg(\mathfrak{A}\&\mathfrak{B})}}}}\qquad\qquad 4\,\dfrac{[\mathfrak{A}\&\mathfrak{B}](6)}{5\,\dfrac{\mathfrak{B}}{6\,\dfrac{Л}{\neg(\mathfrak{A}\&\mathfrak{B})}}}\qquad\dfrac{[\neg\mathfrak{B}](7)}{\neg\mathfrak{A}\vee\neg\mathfrak{B}}$$

Содержательный смысл этих выводов понятен. Например, выводя $\neg(\mathfrak{A}\&\mathfrak{B})$ из $\neg\mathfrak{A}\vee\neg\mathfrak{B}$, мы рассматриваем два случая: $\neg\mathfrak{A}$ и $\neg\mathfrak{B}$, и в каждом из них приводим к противоречию (т.е. к нелепости) гипотезу, что конъюнкция $\mathfrak{A}\&\mathfrak{B}$ истинна. Обратный вывод (т. е. доказательство соотношения (27)) мы также проведем разбором случаев, но теперь это будут случаи $\mathfrak{B}$ и $\neg\mathfrak{B}$, для разбора которых необходим закон исключенного третьего. В случае $\mathfrak{B}$ мы введем еще одну промежуточную гипотезу $\mathfrak{A}$, которую уже имеющиеся гипотезы $\neg(\mathfrak{A}\&\mathfrak{B})$ (основная) и $\mathfrak{B}$ (промежуточная) позволяют легко привести к нелепости, т. е. доказать $\neg\mathfrak{A}$, откуда уже сразу выводится $\neg\mathfrak{A}\vee\neg\mathfrak{B}$. В случае $\neg\mathfrak{B}$ вывод дизъюнкции $\neg\mathfrak{A}\vee\neg\mathfrak{B}$ очевиден. Формальный вывод выглядит так:

$$1\,\dfrac{[\mathfrak{A}](3)\qquad[\mathfrak{B}](7)}{2\,\dfrac{\mathfrak{A}\&\mathfrak{B}\qquad\neg(\mathfrak{A}\&\mathfrak{B})}{3\,\dfrac{Л}{\neg\mathfrak{A}}}}$$

$$4\,\dfrac{\neg\mathfrak{A}}{\neg\mathfrak{A}\vee\neg\mathfrak{B}}\qquad 5\,\dfrac{[\neg\mathfrak{B}](7)}{\neg\mathfrak{A}\vee\neg\mathfrak{B}}\qquad 6\,\dfrac{}{\mathfrak{B}\vee\neg\mathfrak{B}}$$

$$7\,\dfrac{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}{\neg\mathfrak{A}\vee\neg\mathfrak{B}}$$

Итак, «три четверти» законов Де Моргана удается доказать конструктивно. Неконструктивность последней «четверти» связана с тем, что с конструктивной точки зрения дизъюнкция $\neg\mathfrak{A}\vee\neg\mathfrak{B}$ считается обоснованной лишь тогда, когда хотя бы для одного ее члена предъявлено обоснование, в то время как истинность формулы $\neg(\mathfrak{A}\&\mathfrak{B})$ означает только, что доказана невозможность обосновать одновременно $\mathfrak{A}$ и $\mathfrak{B}$.

Покажем теперь, что закон исключенного третьего будет теоремой в исчислении, полученном из $G_0$ заменой этого закона правилом снятия двойного отрицания. Очевидно, достаточно установить, что формула $\neg\neg(\mathfrak{A}\vee\neg\mathfrak{A})$ доказуема в $G_0$ без применения правила ИТ. Для

этого, в свою очередь, достаточно привести к нелепости формулу $\neg(\mathfrak{A} \vee \neg\mathfrak{A})$. Но из этой последней ввиду (25) выводима в $G_0$ без ИТ конъюнкция $\neg\mathfrak{A} \& \neg\neg\mathfrak{A}$, из которой по УК можно вывести $\neg\mathfrak{A}$ и $\neg\neg\mathfrak{A}$, что по УО дает $\Lambda$. (Построение дерева не представляет никаких трудностей.)

Теперь мы должны получить аналоги основных равносильностей группы III из § 3.1, т. е. следующие шесть выводимостей:

(28) $\neg\mathfrak{A} \vee \mathfrak{B} \vdash \mathfrak{A} \supset \mathfrak{B}$.

*(29) $\mathfrak{A} \supset \mathfrak{B} \vdash \neg\mathfrak{A} \vee \mathfrak{B}$.

*(30) $\neg(\mathfrak{A} \& \neg\mathfrak{B}) \vdash \mathfrak{A} \supset \mathfrak{B}$.

(31) $\mathfrak{A} \supset \mathfrak{B} \vdash \neg(\mathfrak{A} \& \neg\mathfrak{B})$.

(32) $\mathfrak{A} \supset \mathfrak{B} \vdash \neg\mathfrak{B} \supset \neg\mathfrak{A}$ (*закон контрапозиции*).

*(33) $\neg\mathfrak{B} \supset \neg\mathfrak{A} \vdash \mathfrak{A} \supset \mathfrak{B}$ (*обратный закон контрапозиции*).

Деревьев вывода для (28) — (33) мы не будем выписывать; ограничимся указаниями, по которым нетрудно их построить. Чтобы получить (28), достаточно вывести $\mathfrak{B}$ из $\neg\mathfrak{A} \vee \mathfrak{B}$ и $\mathfrak{A}$ (чтобы можно было воспользоваться правилом ВИ), а это легко делается разбором случаев. Правая часть (29) очевидным образом выводится из левой с добавлением одной из гипотез $\mathfrak{A}$, $\neg\mathfrak{A}$; далее пользуемся правилом ИТ. Для доказательства (30) достаточно получить $\neg(\mathfrak{A} \& \neg\mathfrak{B}), \mathfrak{A} \vdash \mathfrak{B}$; но, принимая гипотезу $\neg\mathfrak{B}$, из нее и из $\mathfrak{A}$ выводим $\mathfrak{A} \& \neg\mathfrak{B}$, что дает противоречие; поэтому $\neg(\mathfrak{A} \& \neg\mathfrak{B}), \mathfrak{A} \vdash \neg\neg\mathfrak{B}$. (31) легко доказать приведением к нелепости. Чтобы получить (32), достаточно вывести $\neg\mathfrak{A}$ из $\mathfrak{A} \supset \mathfrak{B}$ и $\neg\mathfrak{B}$, а это можно сделать, приведя к нелепости гипотезу $\mathfrak{A}$. В точности так же из $\neg\mathfrak{B} \supset \neg\mathfrak{A}$ и $\mathfrak{A}$ выводится $\neg\neg\mathfrak{B}$; отсюда, пользуясь правилом снятия двойного отрицания и введением импликации, получаем (33).

Неконструктивность соотношений (29), (30) и (33) связана с тем, что импликация с конструктивной точки зрения считается обоснованной тогда, когда указан способ, позволяющий по любому обоснованию посылки построить обоснование заключения. Неконструктивность (29) означает, что из существования такого способа не следует, что мы умеем опровергнуть посылку или обосновать заключение. С другой стороны, если мы доказали, что $\mathfrak{A}$ и отрицание $\mathfrak{B}$ не могут одновременно быть истинными, это еще не дает нам способа по всякому доказательству $\mathfrak{A}$ строить доказательство $\mathfrak{B}$; в этом смысл неконструктивности (30). Наконец, значение неконструктивности (33) легче всего пояснить на примере случая, когда $\mathfrak{A}$ и $\mathfrak{B}$ — утверждения о существовании объектов, обладающих некоторыми свойствами $\alpha$ и $\beta$ соответственно. Тогда импликация $\neg\mathfrak{B} \supset \neg\mathfrak{A}$ с конструктивной точки зрения будет обоснована, если имеется способ по любо-

му доказательству невозможности существования объекта со свойством $\beta$ построить доказательство невозможности существования объекта со свойством $\alpha$; но такой способ вовсе не обязательно позволит по любому объекту со свойством $\alpha$ строить объект со свойством $\beta$, что как раз и необходимо для конструктивного обоснования импликации $\mathfrak{A} \supset \mathfrak{B}$.

Замечание. Тот факт, что закон исключенного третьего и правило снятия двойного отрицания нельзя вывести из конструктивных правил исчисления $G_0$, может быть строго доказан. В задаче 17 в конце этой главы будет указано построение, позволяющее провести это доказательство.

В заключение отметим еще несколько выводимостей, которые часто бывают полезны:

(34) $\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{C}) \vdash \mathfrak{B} \supset (\mathfrak{A} \supset \mathfrak{C})$
(*правило перестановки посылок*);

(35) $\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{C}) \vdash \mathfrak{A} \& \mathfrak{B} \supset \mathfrak{C}$
(*правило соединения посылок*);

(36) $\mathfrak{A} \& \mathfrak{B} \supset \mathfrak{C} \vdash \mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{C})$
(*правило разъединения посылок*);

(37) $\mathfrak{A} \supset \mathfrak{B}, \mathfrak{B} \supset \mathfrak{C} \vdash \mathfrak{A} \supset \mathfrak{C}$
(*закон транзитивности импликации*);

(38) $\mathfrak{A}_1 \supset \mathfrak{B}_1, \ldots, \mathfrak{A}_n \supset \mathfrak{B}_n \vdash \mathfrak{A}_1 \& \ldots \& \mathfrak{A}_n \supset \mathfrak{B}_1 \& \ldots \& \mathfrak{B}_n$
(*правило соединения импликаций*).

Эти выводимости читатель без труда докажет сам.

3. Отметим теперь три очевидных, но важных факта.

Лемма 1. Тогда и только тогда $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$, когда $\Gamma \vdash \mathfrak{A} \supset \mathfrak{B}$.

Доказательство. $\Gamma \vdash \mathfrak{A} \supset \mathfrak{B}$ следует из $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$ по правилу ВИ, а $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$ из $\Gamma \vdash \mathfrak{A} \supset \mathfrak{B}$ — по правилу УИ.

Например, следующие формулы будут теоремами исчисления $G_0$:

$\mathfrak{A} \vee (\mathfrak{B} \vee \mathfrak{C}) \supset (\mathfrak{A} \vee \mathfrak{B}) \vee \mathfrak{C}$ (из (10)),

$(\mathfrak{A} \vee \mathfrak{B}) \vee \mathfrak{C} \supset \mathfrak{A} \vee (\mathfrak{B} \vee \mathfrak{C})$ (из (11)), и т. д.

Лемма 2. Если $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$, то $\Gamma, \neg\mathfrak{B} \vdash \neg\mathfrak{A}$.

Доказательство. Из $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$, применяя правило УО, получаем $\Gamma, \mathfrak{A}, \neg\mathfrak{B} \vdash L$ и далее, применяя ВО — $\Gamma, \neg\mathfrak{B} \vdash \neg\mathfrak{A}$.

При доказательстве лемм 1 и 2 мы не пользовались законом исключенного третьего. Но он понадобился бы для доказательства утверждения, обратного лемме 2, и понадобится для доказательства следующей леммы:

Лемма 3. Если $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$ и $\Gamma, \neg\mathfrak{A} \vdash \mathfrak{B}$, то $\Gamma \vdash \mathfrak{B}$.

**Доказательство.** Достаточно применить закон исключенного третьего и правило УД.

4. Будем говорить теперь, что формулы $\mathfrak{A}$ и $\mathfrak{B}$ *дедуктивно эквивалентны*, если каждая из них выводима из другой. (Ввиду леммы 1 это равносильно доказуемости двух импликаций $\mathfrak{A} \supset \mathfrak{B}$ и $\mathfrak{B} \supset \mathfrak{A}$.)

Доказанные выше аналоги основных равносильностей из § 3.1 позволяют предположить, что при «синтаксическом» построении логики предложений дедуктивная эквивалентность играет такую же роль, как равносильность при «семантическом» построении. Это действительно так, и в следующем параграфе мы выясним, в чем здесь дело. А пока что заметим, что для дедуктивной эквивалентности имеет место теорема о замене, совершенно аналогичная доказанной в § 3.2 теореме о замене равносильных формул.

**Теорема о замене дедуктивно эквивалентных формул (в исчислении $G_0$).** Если в формуле $\mathfrak{A}$ заменить вхождение подформулы $\mathfrak{B}$ вхождением формулы $\mathfrak{B}'$, дедуктивно эквивалентной $\mathfrak{B}$, то полученная формула $\mathfrak{A}'$ будет дедуктивно эквивалентна $\mathfrak{A}$.

Доказательство проводится индукцией по глубине заменяемого вхождения подформулы $\mathfrak{B}$ и строится совершенно аналогично доказательству упомянутой теоремы из § 3.2. Базис можно воспроизвести слово в слово. В индукционном шаге, рассуждая опять-таки точно так же, как в § 3.2, нетрудно убедиться, что достаточно доказать следующее: если формула $\mathfrak{A}$ имеет один из трех видов (а) $\mathfrak{A} = (\mathfrak{C})\alpha(\mathfrak{D})$, (б) $\mathfrak{A} = (\mathfrak{D})\alpha(\mathfrak{C})$ и (в) $\mathfrak{A} = \neg(\mathfrak{C})$, где в случаях (а) и (б) $\alpha = \&, \vee, \supset$, то формула $\mathfrak{A}'$, получаемая из $\mathfrak{A}$ заменой выделенного вхождения $\mathfrak{C}$ вхождением формулы $\mathfrak{C}'$, дедуктивно эквивалентной $\mathfrak{C}$, будет дедуктивно эквивалентна $\mathfrak{A}$. А это последнее утверждение доказывается следующим образом. В случае (а) при $\alpha = \&$, поскольку по условию $\mathfrak{C} \vdash \mathfrak{C}'$, применением правил УК, ВК и Т получаем $(\mathfrak{C})\&(\mathfrak{D}) \vdash (\mathfrak{C}')\&(\mathfrak{D})$; обратная выводимость доказывается так же. При $\alpha = \vee$ поступаем аналогично, пользуясь правилами ВД, УД и Т. При $\alpha = \supset$ из условия $\mathfrak{C} \vdash \mathfrak{C}'$ применением правил УИ и Т получаем $\mathfrak{C}, \mathfrak{C}' \supset \mathfrak{D} \vdash \mathfrak{D}$, откуда по правилу ВИ следует, что $\mathfrak{C}' \supset \mathfrak{D} \vdash \mathfrak{C} \supset \mathfrak{D}$; обратное получаем так же. В случае (б) при $\alpha = \&$, $\vee$ рассуждаем точно так же, как в случае (а); при $\alpha = \supset$ условие $\mathfrak{C} \vdash \mathfrak{C}'$ вместе с правилами УИ и Т дает $\mathfrak{D}, \mathfrak{D} \supset \mathfrak{C} \vdash \mathfrak{C}'$, откуда по ВИ получается $\mathfrak{D} \supset \mathfrak{C} \vdash \mathfrak{D} \supset \mathfrak{C}'$, и так же доказывается обратное. Наконец, в случае (в) из $\mathfrak{C} \vdash \mathfrak{C}'$ получаем $\vdash \mathfrak{C} \supset \mathfrak{C}'$, откуда в силу (32) и Т вытекает $\vdash \neg(\mathfrak{C}') \supset \neg(\mathfrak{C})$ и далее $\neg(\mathfrak{C}') \vdash \neg(\mathfrak{C})$; обратное — так же.

**Замечание.** При доказательстве теоремы о замене мы нигде не пользовались законом исключенного третьего. Следовательно, эта теорема справедлива и в конструктивном варианте исчисления $G_0$.

## § 5.4. СЕМАНТИЧЕСКАЯ ПРИГОДНОСТЬ И ПОЛНОТА ИСЧИСЛЕНИЯ $G_0$

1. В самом начале этой главы, прежде чем определить отношение выводимости, мы говорили, что по объему оно совпадает с изучавшимся в гл. 3 отношением семантического следования. Теперь, располагая строгим определением выводимости и многочисленными примерами, мы можем доказать это утверждение (для исчисления $G_0$). Одновременно мы покажем, что понятие теоремы в $G_0$ совпадает по объему с понятием тождественно истинной формулы.

Предварительно введем два технических термина. Именно, мы будем называть логическое исчисление *семантически пригодным*[18], если всякая его теорема истинна, и *полным* — или *семантически полным*[19] — если всякая истинная формула в его алфавите является в нем теоремой. Эти термины оправдываются тем, что если в логическом исчислении можно доказать теорему, не являющуюся истинной в некоторой содержательной математической теории, то это исчисление, безусловно, не годится для описания данной теории, а если в исчислении доказуемы только предложения, истинные в содержательной теории, но не все такие предложения, тогда естественно сказать, что исчисление описывает теорию, но не полностью. Конечно, так сформулированные определения семантической пригодности и полноты — не настоящие математические определения, потому что в них участвует понятие «истинной формулы», не имеющее строго определенного смысла и для разных исчислений уточняемое поразному. Но если ограничиться исчислениями с тем же алфавитом и тем же множеством формул, как в логике предложений (а в этой главе мы так и делаем), то естественно понимать «истинную формулу» как тождественно истинную[20], и тогда понятия семантической пригодности и полноты получают точный смысл.

Заметим еще, что обычно в семантически пригодном исчислении выводимость влечет семантическое следование, а в полном семантическое следование влечет выводимость.

2. Займемся сначала семантической пригодностью. Справедлива

**Теорема о семантической пригодности исчисления $G_0$.** Если

[18] Этот термин введен А.А. Марковым.

[19] В отличие от дедуктивной полноты, которая будет определена в § 6.2. В настоящей главе мы называем семантическую полноту просто полнотой.

[20] В гл. 3 мы определили тождественную истинность для формул, не содержащих константы $\Lambda$, но ясно, что это определение можно без всяких изменений перенести на формулы, содержащие ее. То же верно для семантического следования.

формула $\mathfrak{A}$ выводима в исчислении $G_0$ из множества формул $\Gamma$, то $\mathfrak{A}$ семантически следует из $\Gamma$.

**Доказательство** проведем возвратной индукцией по высоте дерева вывода $\mathfrak{A}$ из $\Gamma$.

Базис. Пусть $\mathfrak{A}$ выводится из $\Gamma$ с помощью дерева высоты 1, т. е. элементарного дерева вывода. Тогда $\mathfrak{A}$ — заключение некоторого безусловного правила вывода, все посылки которого входят в $\Gamma$. Поэтому достаточно для каждого из этих правил проверить, что для всякого набора значений пропозициональных переменных, для которого истинны его посылки, заключение также истинно; а такую проверку легко провести непосредственно. (Например, для УИ достаточно заметить, что в силу определения импликации для любого набора значений, для которого формулы $\mathfrak{A}\supset\mathfrak{B}$ и $\mathfrak{A}$ истинны, формула $\mathfrak{B}$ также истинна.)

Индукционный шаг. Пусть $n > 1$ и для деревьев, высоты которых меньше $n$, утверждение доказано. Рассмотрим формулу $\mathfrak{A}$, выводимую из множества $\Gamma$ с помощью дерева высоты $n$. Тогда возможны следующие случаи:

а) Дерево образовано по пункту 2 определения (см. с. 168) из деревьев $\delta_1, \ldots, \delta_k$ с корнями $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ и множествами зеленых листьев $\Gamma_1, \ldots, \Gamma_k$, а также (быть может) формул $\mathfrak{B}_1, \ldots, \mathfrak{B}_l$, причем $\Gamma = \Gamma_1 \cup \cdots \Gamma_k \cup \{\mathfrak{B}_1, \ldots, \mathfrak{B}_l\}$. В этом случае, поскольку высоты деревьев $\delta_1, \ldots, \delta_k$ меньше $n$, по предположению индукции для каждого $i = 1, \ldots, k$ формула $\mathfrak{A}_i$ семантически следует из $\Gamma_i$. С другой стороны, рассуждая так же, как в базисе, видим, что $\mathfrak{A}$ семантически следует из $\mathfrak{A}_1, \ldots, \mathfrak{A}_k, \mathfrak{B}_1, \ldots, \mathfrak{B}_l$. Поэтому $\mathfrak{A}$ семантически следует из $\Gamma$.

б) Дерево образовано по пункту 3 определения. Тогда $\mathfrak{A}$ имеет вид $\mathfrak{C}\supset\mathfrak{D}$ и существует дерево вывода формулы $\mathfrak{D}$ из множества $\Gamma\cup\{\mathfrak{C}\}$, имеющее высоту $n-1$. По предположению индукции $\mathfrak{D}$ семантически следует из $\Gamma\cup\{\mathfrak{C}\}$, т. е. всякий раз, когда все формулы из $\Gamma$ и формула $\mathfrak{C}$ принимают значение $И$, формула $\mathfrak{D}$ также принимает значение $И$; поэтому импликация $\mathfrak{C}\supset\mathfrak{D}$ должна быть истинной, когда все формулы из $\Gamma$ истинны (ср. доказательство утверждения 1 из § 3.4), а это и значит, что $\mathfrak{A} = \mathfrak{C}\supset\mathfrak{D}$ семантически следует из $\Gamma$.

в) Дерево образовано по пункту 4. Тогда $\mathfrak{A}$ имеет вид $\neg\mathfrak{B}$ и существует дерево вывода константы $Л$ из $\Gamma\cup\{\mathfrak{C}\}$, имеющее высоту $n-1$. По предположению индукции $\Gamma\cup\{\mathfrak{C}\}\Rightarrow Л$. Это означает, что все формулы из $\Gamma$ и формула $\mathfrak{C}$ не могут быть истинны одновременно — иначе говоря, что всякий раз, когда все формулы из $\Gamma$ истинны, формула $\mathfrak{C}$ ложна и, стало быть, формула $\neg\mathfrak{C}$ истинна. Таким образом, и в этом случае $\Gamma\Rightarrow\mathfrak{A}$.

г) Дерево образовано по пункту 5а. Тогда множество $\Gamma$ можно

представить в виде $\Gamma = \Gamma' \cup \Gamma'' \cup \{\mathfrak{C} \vee \mathfrak{D}\}$ таким образом, что существуют деревья вывода формулы $\mathfrak{A}$ из множеств $\Gamma' \cup \{\mathfrak{C}\}$ и $\Gamma'' \cup \{\mathfrak{D}\}$, высоты которых меньше $n$. По предположению индукции $\Gamma' \cup \{\mathfrak{C}\} \Rightarrow \mathfrak{A}$ и $\Gamma'' \cup \{\mathfrak{D}\} \Rightarrow \mathfrak{A}$. Но отсюда немедленно вытекает, что формула $\mathfrak{A}$ будет истинна всякий раз, когда истинны все формулы, входящие в объединение $\Gamma' \cup \Gamma''$, и хотя бы одна из формул $\mathfrak{C}$ и $\mathfrak{D}$ — иначе говоря, когда истинны все формулы, входящие в $\Gamma' \cup \Gamma''$, и дизъюнкция $\mathfrak{C} \vee \mathfrak{D}$. А это как раз и значит, что $\mathfrak{A}$ семантически следует из множества $\Gamma' \cup \Gamma'' \cup \{\mathfrak{C} \vee \mathfrak{D}\} = \Gamma$.

д) Дерево образовано по пункту 5б. В этом случае начинаем рассуждение так же, как в предыдущем, с той разницей, что $\Gamma$ представляется не в виде $\Gamma' \cup \Gamma'' \cup \{\mathfrak{C} \vee \mathfrak{D}\}$, а в виде $\Gamma' \cup \Gamma'' \cup \Gamma^*$, где $\Gamma^*$ — множество зеленых листьев некоторого дерева вывода $\delta^*$ высоты $< n$ с корнем $\mathfrak{C} \vee \mathfrak{D}$. Заменяя в исходном дереве поддерево $\delta^*$ формулой $\mathfrak{C} \vee \mathfrak{D}$, оказываемся в условиях предыдущего пункта и заключаем, что $\Gamma' \cup \Gamma'' \cup \mathfrak{C} \vee \mathfrak{D} \Rightarrow \Gamma$. Но в силу предположения индукции $\Gamma^* \Rightarrow \{\mathfrak{C} \vee \mathfrak{D}\}$, и поэтому[21] $\Gamma' \cup \Gamma'' \cup \Gamma^* \Rightarrow \mathfrak{A}$. Теорема доказана.

Вспомнив, что формула, семантически следующая из пустого множества, тождественно истинна, немедленно получаем

Следствие. Всякая теорема исчисления $G_0$ тождественно истинна.

3. Сложнее доказывается

**Теорема о полноте исчисления $G_0$.** Всякая тождественно истинная формула в алфавите исчисления $G_0$ является теоремой этого исчисления.

Для доказательства этой теоремы[22] введем предварительно следующее обозначение.

Пусть $\mathfrak{A}$ — произвольная формула (в алфавите исчисления $G$), $n$ — целое положительное число, такое, что $\mathfrak{A}$ не содержит переменных с номерами, бо́льшими $n$, и $r$ — произвольный $n$-мерный булев вектор. Будем обозначать через $\mathfrak{A}^r$ саму формулу $\mathfrak{A}$, если $\mathfrak{A}(r) = И$, и формулу $\neg\mathfrak{A}$, если $\mathfrak{A}(r) = Л$. В частности, если $i$, $n$ — целые положительные числа, такие, что $i \leq n$, и $r = r_1 \ldots r_n$ — произвольный $n$-мерный булев вектор, то $X_i^r$ есть $X_i$, если $r_i = И$, и $\neg X_i$, если $r_i = Л$. (Таким образом, обозначение $X_i^r$ имеет здесь тот же смысл, что и в § 3.3.)

Основную роль в доказательстве теоремы будет играть

Лемма. Для любой формулы $\mathfrak{A}$, любого целого положительного числа $n$, такого, что $\mathfrak{A}$ не содержит переменных с номерами, бо́льши-

---

[21] Непосредственно из определения семантического следования ясно, что если $\Gamma \cup \Delta \Rightarrow \mathfrak{A}$ и $\Gamma \cup \mathfrak{A} \Rightarrow \mathfrak{B}$, то $\Gamma \cup \Delta \Rightarrow \mathfrak{B}$.

[22] Метод, которым мы пользуемся при доказательстве теоремы о полноте, предложен венгерским математиком Л. Кальмаром (Kalmár László, 1905—1976).

ми $n$, и любого $n$-мерного булева вектора $r$ формула $\mathfrak{A}^r$ выводима из формул $X_1^r, \ldots, X_n^r$.

Доказательство леммы проведем возвратной индукцией по сложности формулы $\mathfrak{A}$.

Базис. Пусть сложность формулы $\mathfrak{A}$ равна нулю, т. е. $\mathfrak{A}$ не содержит пропозициональных связок. Тогда $\mathfrak{A}$ есть либо переменная $X_i$, $1 \leq i \leq n$, либо константа $Л$. Но $X_1^r, \ldots, X_n^r \vdash X_i^r$ по правилу ТВ; если же $\mathfrak{A} = Л$, то $\mathfrak{A}^r = \neg Л$, а эта формула выводима из любого множества формул. (В самом деле, $\Gamma, Л \vdash Л$, откуда по ВО $\Gamma \vdash \neg Л$.)

Индукционный шаг. Допустим, что утверждение леммы справедливо для всех формул, сложности которых меньше некоторого положительного $s$. Рассмотрим произвольную формулу $\mathfrak{A}$ сложности $s$ и докажем, что утверждение верно и для нее.

Фиксируем подходящее число $n$ и произвольный булев вектор $r$. Поскольку $s > 0$, формула $\mathfrak{A}$ содержит хотя бы одну пропозициональную связку и, следовательно, возможны четыре случая: (1) $\mathfrak{A} = (\mathfrak{B})\&(\mathfrak{C})$; (2) $\mathfrak{A} = (\mathfrak{B}) \vee (\mathfrak{C})$; (3) $\mathfrak{A} = (\mathfrak{B}) \supset (\mathfrak{C})$; (4) $\mathfrak{A} = \neg(\mathfrak{B})$. Во всех этих случаях сложности формул $\mathfrak{B}$ и $\mathfrak{C}$ меньше $s$, так что по предположению индукции $\mathfrak{B}^r$ и $\mathfrak{C}^r$ выводимы из $X_1^r, \ldots, X_n^r$. Рассмотрим теперь каждый случай отдельно.

В случае (1), если $\mathfrak{B}(r) = \mathfrak{C}(r) = И$, имеем $\mathfrak{B}^r = \mathfrak{B}$, $\mathfrak{C}^r = \mathfrak{C}$, $\mathfrak{A}(r) = И$, $\mathfrak{A}^r = \mathfrak{A}$. Поэтому из $X_1^r, \cdots, X_n^r$ выводимы $\mathfrak{B}$ и $\mathfrak{C}$, а из них по ВК выводится $\mathfrak{B}\&\mathfrak{C} = \mathfrak{A} = \mathfrak{A}^r$. Если же хотя бы одно из значений $\mathfrak{B}(r)$ и $\mathfrak{C}(r)$ есть $Л$ — для определенности пусть первое,— то $\mathfrak{B}^r = \neg\mathfrak{B}$, $\mathfrak{A}(r) = Л$, $\mathfrak{A}^r = \neg\mathfrak{A}$. Но $\neg\mathfrak{B} \vdash \neg(\mathfrak{B}\&\mathfrak{C})$ (по УК и лемме 2 из предыдущего параграфа), так что из $X_1^r, \cdots, X_n^r$ выводима формула $\neg(\mathfrak{B}\&\mathfrak{C}) = \neg\mathfrak{A} = \mathfrak{A}^r$.

В случае (2), если хотя бы одно из значений $\mathfrak{B}(r)$ и $\mathfrak{C}(r)$ — пусть первое — есть $И$, то $\mathfrak{B}^r = \mathfrak{B}$, $\mathfrak{A}(r) = И$, $\mathfrak{A}^r = \mathfrak{A}$, и из $X_1^r, \cdots, X_n^r$ выводима формула $\mathfrak{B}$, из которой по ВД выводится $\mathfrak{B} \vee \mathfrak{C} = \mathfrak{A} = \mathfrak{A}^r$. Если же $\mathfrak{B}(r) = \mathfrak{C}(r) = Л$, то $\mathfrak{B}^r = \neg\mathfrak{B}$, $\mathfrak{C}^r = \neg\mathfrak{C}$, $\mathfrak{A}(r) = Л$, $\mathfrak{A}^r = \neg\mathfrak{A}$, а так как $\neg\mathfrak{C}, \neg\mathfrak{C} \vdash \neg(\mathfrak{B} \vee \mathfrak{C})$ (по ВК $\neg\mathfrak{B}, \neg\mathfrak{C} \vdash \neg\mathfrak{B}\&\neg\mathfrak{C}$, а в силу (24) из предыдущего параграфа $\neg\mathfrak{B}\&\neg\mathfrak{C} \vdash \neg(\mathfrak{B} \vee \mathfrak{C})$), то из $X_1^r, \cdots, X_n^r$ выводится $\neg(\mathfrak{B} \vee \mathfrak{C}) = \mathfrak{A}^r$.

В случае (3) нам придется рассмотреть три подслучая: (а) $\mathfrak{A}(r) = Л$; (б) $\mathfrak{C}(r) = И$; (в) $\mathfrak{B}(r) = И$, $\mathfrak{C}(r) = Л$[23]. В подслучае (а) $\mathfrak{B}^r = \neg\mathfrak{B}$, $\mathfrak{A}(r) = И$, $\mathfrak{A}^r = \mathfrak{A}$, а так как $\neg\mathfrak{B} \vdash (\mathfrak{B} \supset \mathfrak{C})$ (см. в предыдущем параграфе пример (9)), то из $X_1^r, \cdots, X_n^r$ выводима формула $\mathfrak{B} \supset \mathfrak{C} = \mathfrak{A} = \mathfrak{A}^r$. В подслучае (б) рассуждаем так же, используя при-

[23] Разумеется, подслучаи (а) и (б) не исключают друг друга.

мер (8) из предыдущего параграфа. В подслучае (в) $\mathfrak{B}^r = \mathfrak{B}$, $\mathfrak{C}^r = \neg\mathfrak{C}$, $\mathfrak{A}(r) = Л$, $\mathfrak{A}^r = \neg\mathfrak{A}$. Но по УИ $\mathfrak{B}$, $\mathfrak{B} \supset \mathfrak{C} \vdash \mathfrak{C}$, откуда по лемме 2 из предыдущего параграфа $\mathfrak{B}$, $\neg\mathfrak{C} \vdash \neg(\mathfrak{B} \supset \mathfrak{C})$. Поэтому из $X_1^r$, ..., $X_n^r$ выводима формула $\neg(\mathfrak{B} \supset \mathfrak{C}) = \neg\mathfrak{A} = \mathfrak{A}^r$.

Наконец, в случае (4), если $\mathfrak{B}(r) = И$, то $\mathfrak{B}^r = \mathfrak{B}$, $\mathfrak{A}(r) = Л$, $\mathfrak{A}^r = \neg\mathfrak{A}$, и из $X_1^r$, ..., $X_n^r$ выводима формула $\mathfrak{B}$, из которой по правилу постановки двойного отрицания выводится $\neg\neg\mathfrak{B} = \neg\mathfrak{A} = \mathfrak{A}^r$. Если же $\mathfrak{B}(r) = Л$, то $\mathfrak{B}^r = \neg\mathfrak{B}$, $\mathfrak{A}(r) = И$, $\mathfrak{A}^r = \mathfrak{A}$, и $X_1^r$, ..., $X_n^r \vdash \neg\mathfrak{B} = \mathfrak{A} = \mathfrak{A}^r$.

Лемма доказана.

Доказательство теоремы. Пусть $\mathfrak{A}$ — произвольная тождественно истинная формула. Фиксируем раз навсегда подходящее число $n$. Тогда для любого $n$-мерного булева вектора $r$ будет $\mathfrak{A}^r = \mathfrak{A}$, и по только что доказанной лемме $X_1^r, \cdots, X_n^r \vdash \mathfrak{A}$. Сопоставим теперь произвольному $n$-мерному булеву вектору $r$ конечную последовательность множеств формул $\Gamma_1^r$, ..., $\Gamma_n^r$, $\Gamma_{n+1}^r$ следующим образом: если $1 \leq i \leq n$, то $\Gamma_i^r = \{X_i^r, X_{i+1}^r, ..., X_n^r\}$; $\Gamma_{n+1}^r = \varnothing$. Покажем теперь индукцией по $i$, что для любого $i = 1, ..., n + 1$ и любого $n$-мерного булева вектора $r$ имеет место $\Gamma_i^r \vdash \mathfrak{A}$. Сделав это[24], мы убедимся, в частности, что $\Gamma_{n+1}^r \vdash \mathfrak{A}$, т. е. $\vdash \mathfrak{A}$, и доказательство теоремы о полноте будет завершено. Базис индукции у нас уже готов; остается провести индукционный шаг.

Итак, пусть для некоторого $i = 1, ..., n$ справедливо следующее утверждение: для любого $n$-мерного булева вектора $r$ имеет место $\Gamma_i^r \vdash \mathfrak{A}$ или, что то же самое, $\Gamma_{i+1}^r, X_i^r \vdash \mathfrak{A}$. Фиксировав произвольный вектор $r$, изменим его $i$-ю координату; обозначим полученный таким образом вектор через $r'$. Тогда наряду с выводимостью $\Gamma_{i+1}^r, X_i^r \vdash \mathfrak{A}$ будет иметь место $\Gamma_{i+1}^{r'}, X_i^{r'} \vdash \mathfrak{A}$. Но так как всякая формула $X_j^{r'}$ зависит только от $j$-й координаты вектора $r'$, а у $r$ и $r'$ все координаты, кроме $i$-й, совпадают, имеем $X_{i+1}^r = X_{i+1}^{r'}$, ..., $X_n^r = X_n^{r'}$, т. е. $\Gamma_{i+1}^r = \Gamma_{i+1}^{r'}$ (так при $i < n$; равенство $\Gamma_{n+1}^r = \Gamma_{n+1}^{r'}$ выполняется тривиальным образом). Таким образом, $\Gamma_{i+1}^r, X_i^{r'} \vdash \mathfrak{A}$. А поскольку одна из формул $X_i^r$, $X_i^{r'}$ есть $X_i$, а другая $\neg X_i$, имеем $\Gamma_{i+1}^r, X_i \vdash \mathfrak{A}$, $\Gamma_{i+1}^r, \neg X_i \vdash \mathfrak{A}$, откуда по лемме 3 из предыдущего параграфа $\Gamma_{i+1}^r \vdash \mathfrak{A}$. Этим заканчивается индукционный шаг и вместе с ним доказательство теоремы.

---

[24] Об индукции по конечному отрезку натурального ряда см. в Приложении II (замечание 2 на с. 461).

Замечание. Тот вывод произвольной тождественно истинной формулы из пустого множества формул, способ построения которого был сейчас указан, является, вообще говоря, неконструктивным (поскольку лемма 3 предыдущего параграфа зависит от закона исключенного третьего).

Следствие. Если формула $\mathfrak{A}$ в алфавите исчисления $G_0$ семантически следует из множества $\Gamma$ формул в том же алфавите, то $\mathfrak{A}$ выводима в $G$ из $\Gamma$.

Доказательство. Пусть $\Gamma$ — конечное множество формул и $\Gamma \Rightarrow \mathfrak{A}$. Если $\Gamma$ пусто, формула $\mathfrak{A}$ тождественно истинна, и по только что доказанной теореме $\vdash \mathfrak{A}$, т. е. $\Gamma \vdash \mathfrak{A}$. Если $\Gamma$ не пусто, $\Gamma = \{\mathfrak{C}_1, \ldots, \mathfrak{C}_n\}$, то формула $\mathfrak{C}_1 \supset (\mathfrak{C}_2 \supset \ldots \supset (\mathfrak{C}_k \supset \mathfrak{A}) \ldots)$ тождественно истинна. (В самом деле, легко видеть, что она могла бы принимать значение $\Lambda$ только на таком векторе, на котором все $\mathfrak{C}_i$ истинны и $\mathfrak{A}$ ложна, что несовместимо с условием.) Поэтому в силу теоремы о полноте $\vdash \mathfrak{C}_1 \supset (\mathfrak{C}_2 \supset \ldots \supset (\mathfrak{C}_k \supset \mathfrak{A}) \ldots)$, откуда, применяя $k$ раз УИ, получаем $\mathfrak{C}_1, \ldots, \mathfrak{C}_k \vdash \mathfrak{A}$.

4. Мы убедились теперь, что синтаксическое понятие выводимости в $G_0$ совпадает по объему с понятием семантического следования, и то же верно для понятий теоремы в $G_0$ и тождественно истинной формулы. Синтаксические понятия математической логики часто называют *формальными*, так как они, во-первых, относятся к форме, а не к смыслу ее выражений (именно в таком значении —«относящийся к форме»— употребляется слово «формальный» в языковедении) и, во-вторых, связаны со строгим соблюдением некоторых четко сформулированных правил (что отвечает одному из главных значений слова «формальный» в обиходном русском языке: «сделанный с соблюдением всех принятых правил, в установленном, законном порядке»; исторически именно это значение было исходным). Может возникнуть соблазн распространить на синтаксический и семантический подходы к понятиям математической логики обычное противопоставление формы и содержания и считать первый подход «менее содержательным», чем второй (соблазн этот тем сильнее, что в современном языке у слова «формальный» есть еще одно значение: «существующий только по видимости, по форме», которое воспринимается сейчас едва ли не как основное). На самом же деле для такого заключения нет ни малейших оснований. Скорее уж наоборот: синтаксическая система понятий моделирует реальный процесс логического вывода и потому дает гораздо больше сведений о его содержании, чем семантическая, имеющая дело с уже готовыми результатами процесса безотносительно к тому, как они получены. В действительности эти системы понятий необходимым образом дополняют друг друга, и именно наличие их обеих и тесная взаимосвязь между

ними[25] обеспечивают математической логике то важное место в здании математики, которое она сейчас занимает.

**5.** Одно из важнейших требований, предъявляемых к логическим исчислениям, претендующим на значимость для логики или математики — *непротиворечивость*, т. е. невозможность доказать две противоречащие друг другу теоремы[26]. (Разумеется, это требование имеет смысл только для тех исчислений, алфавиты которых содержат логический символ, интерпретируемый как отрицание — ср. сноску на с. 162). Удовлетворяет этому требованию и изучаемое нами исчисление: справедлива

**Теорема о непротиворечивости исчисления $G_0$.** Ни для какой формулы исчисления $G_0$ невозможно, чтобы и она, и ее отрицание были в этом исчислении теоремами.

**Доказательство.** Допустим, что для некоторой формулы $\mathfrak{A}$ одновременно $\vdash \mathfrak{A}$ и $\vdash \neg\mathfrak{A}$. Тогда по теореме о семантической пригодности обе формулы $\mathfrak{A}$ и $\neg\mathfrak{A}$ должны быть тождественно истинны, что невозможно, т. к. из тождественной истинности $\mathfrak{A}$ следует тождественная ложность $\neg\mathfrak{A}$.

Таким образом, непротиворечивость $G_0$ оказывается простым следствием семантической пригодности.

## § 5.5. ДРУГИЕ ВАРИАНТЫ ИСЧИСЛЕНИЯ ПРЕДЛОЖЕНИЙ

**1.** Сейчас мы приведем пример исчисления гильбертовского типа для логики предложений с тем же объемом понятий выводимости и теоремы, что и в $G_0$. Но сначала необходимо сделать несколько общих замечаний о гильбертовских исчислениях.

Как было уже сказано в § 5.1, в этих исчислениях почти все логические правила формулируются в виде аксиом. Но у них есть еще одна особенность — отсутствие условных логических правил. Кроме того, в них по традиции используется другой, технически более простой способ описания вывода. (При наличии условных правил этот способ неприменим.) Именно, *выводом* формулы $\mathfrak{A}$ из мно-

[25] Эта взаимосвязь основана прежде всего на семантической пригодности и полноте логических исчислений.

[26] Правда, сейчас можно услышать о попытках строить нетривиальные исчисления, не удовлетворяющие этому условию (ради приложений к нематематическим системам, функционирующим несмотря на наличие в них противоречий — как, например, в юриспруденции). Однако здесь еще, видимо, рано говорить о существенных результатах.

жества формул $\Gamma$ в исчислении гильбертовского типа принято называть конечную последовательность $\mathfrak{C}_1, \ldots, \mathfrak{C}_l$ формул этого исчисления, такую, что $\mathfrak{C}_l = \mathfrak{A}$ и каждая формула $\mathfrak{C}_i$ удовлетворяет хотя бы одному из трех условий: ($\alpha$) $\mathfrak{C}_i \in \Gamma$; ($\beta$) $\mathfrak{C}_i$ есть аксиома; ($\gamma$) $i > 1$ и $\mathfrak{C}_i$ является заключением некоторого правила, все посылки которого содержатся среди формул $\mathfrak{C}_1, \ldots, \mathfrak{C}_{i-1}$[27]. (Аксиомы здесь не включаются в число правил.) Число $l$ называется *длиной вывода*. Формула называется *выводимой* из $\Gamma$, если существует ее вывод из $\Gamma$. Теорема и доказуемость определяются, как обычно.

Иногда в литературе встречаются «гибридные» исчисления с большим числом аксиом и условными правилами (пример см. в задаче 20 в конце гл. 6). Для таких исчислений выводимость приходится определять индуктивно.

Разными авторами предложено много различных исчислений гильбертовского типа с разными наборами аксиом; но в отношении правил разнообразие значительно меньше. Едва ли не все исчисления этого типа, предназначенные для логики предложений, содержат либо одно правило — удаление импликации, либо два — удаление импликации и подстановку. Первое из этих правил в традиционной (не математической) логике обозначается латинским термином modus ponens, т. е. «положительный способ» (умозаключения)[28]; так же обычно называют его и в логических исчислениях гильбертовского типа (термин «удаление импликации» используется только в контексте системы правил введения и удаления). Правило подстановки состоит в том, что формула, полученная из некоторой теоремы заменой всех переменных произвольными формулами, также считается теоремой (например, вместе с формулой $X_1 \vee \neg X_1$ считается теоремой формула $(X_1 \& X_2) \vee \neg(X_1 \& X_2)$. Это правило используется в тех исчислениях, в которых аксиомы задаются простым перечислением, как конкретные формулы (например, $X_1 \& X_2 \supset X_1$, $X_1 \vee \neg X_1$ и т. п.). В исчислениях, в которых аксиомы задаются в виде схем (например: «Всякая формула вида $\mathfrak{A} \& \mathfrak{B} \supset \mathfrak{A}$ есть аксиома»), правило подстановки не нужно.

---

[27] Подчеркнем еще раз, что исходная простота достигается здесь за счет сложности. В реальных математических рассуждениях логические аксиомы (кроме закона исключенного третьего) не используются, зато постоянно встречаются промежуточные гипотезы, т. е. применяются условные логические правила. Кроме того, дерево дает гораздо более естественную модель структуры логического вывода, чем линейная последовательность.

[28] В противоположность «отрицательному способу» (modus tollens), т. е. выводу из предложений $A \supset B$ и $\neg B$ предложения $\neg A$.

2. Рассмотрим теперь исчисление $H_0$, предложенное П.С. Новиковым [Новиков 1959][29]. Оно определяется так:

Алфавит $H_0$ состоит из тех же символов, что и алфавит $G_0$, кроме $\Lambda$.

Правила образования формул в $H_0$ те же, что в $G_0$, кроме правила (б).

Единственное правило вывода в $H_0$ есть modus ponens (сокращенно MP): $\mathfrak{A}$, $\mathfrak{A}\supset\mathfrak{B} \vdash \mathfrak{B}$.

Аксиомами $H_0$ являются всевозможные формулы следующих видов:

I

1. $\mathfrak{A}\supset(\mathfrak{B}\supset\mathfrak{A})$;

2. $(\mathfrak{A}\supset(\mathfrak{B}\supset\mathfrak{C}))\supset((\mathfrak{A}\supset\mathfrak{B})\supset(\mathfrak{A}\supset\mathfrak{C}))$;

II

1. $\mathfrak{A}\&\mathfrak{B}\supset\mathfrak{A}$;

2. $\mathfrak{A}\&\mathfrak{B}\supset\mathfrak{B}$;

3. $(\mathfrak{A}\supset\mathfrak{B})\supset((\mathfrak{A}\supset\mathfrak{C})\supset(\mathfrak{A}\supset\mathfrak{B}\&\mathfrak{C}))$;

III

1. $\mathfrak{A}\supset\mathfrak{A}\vee\mathfrak{B}$;

2. $\mathfrak{B}\supset\mathfrak{A}\vee\mathfrak{B}$;

3. $(\mathfrak{A}\supset\mathfrak{C})\supset((\mathfrak{B}\supset\mathfrak{C})\supset(\mathfrak{A}\vee\mathfrak{B}\supset\mathfrak{C}))$;

IV

1. $(\mathfrak{A}\supset\mathfrak{B})\supset(\neg\mathfrak{B}\supset\neg\mathfrak{A})$;

2. $\mathfrak{A}\supset\neg\neg\mathfrak{A}$;

3. $\neg\neg\mathfrak{A}\supset\mathfrak{A}$.

Приведем два примера выводов в $H_0$. Мы будем записывать выводы «столбиком», нумеруя входящие в них формулы и при каждой из них указывая (в скобках), на каком основании она включена в вывод.

(1) Покажем, что $\vdash \mathfrak{A}\supset\mathfrak{A}$.

[29] Строго говоря, $H_0$ в нашем изложении не полностью совпадает с исчислением П.С. Новикова: там используются конкретные аксиомы и правило подстановки, а у нас — схемы аксиом.

1. $\mathfrak{A}\supset((\mathfrak{A}\supset\mathfrak{A})\supset\mathfrak{A})$ (аксиома по схеме I1) [30]

2. $(\mathfrak{A}\supset((\mathfrak{A}\supset\mathfrak{A}\supset\mathfrak{A}))\supset((\mathfrak{A}\supset(\mathfrak{A}\supset\mathfrak{A}))\supset(\mathfrak{A}\supset\mathfrak{A}))$ (аксиома по схеме I2)

3. $(\mathfrak{A}\supset(\mathfrak{A}\supset\mathfrak{A}))\supset(\mathfrak{A}\supset\mathfrak{A})$ (по MP из 1 и 2)

4. $(\mathfrak{A}\supset(\mathfrak{A}\supset\mathfrak{A})$ (аксиома по схеме I1)

5. $\mathfrak{A}\supset\mathfrak{A}$ (по MP из 4 и 3)

(2) Покажем, что $\mathfrak{A}\&\mathfrak{B}\vdash\mathfrak{B}\&\mathfrak{A}$.

1. $\mathfrak{A}\&\mathfrak{B}\supset\mathfrak{B}$ (аксиома по схеме I12)

2. $(\mathfrak{A}\&\mathfrak{B}\supset\mathfrak{B})\supset((\mathfrak{A}\&\mathfrak{B}\supset\mathfrak{A})\supset(\mathfrak{A}\&\mathfrak{B}\supset\mathfrak{B}\&\mathfrak{A}))$ (аксиома по схеме I1 3)

3. $(\mathfrak{A}\&\mathfrak{B}\supset\mathfrak{A})\supset(\mathfrak{A}\&\mathfrak{B}\supset\mathfrak{B}\&\mathfrak{A})$ (по MP из 1 и 2)

4. $\mathfrak{A}\&\mathfrak{B}\supset\mathfrak{A}$ (аксиома по схеме I11)

5. $\mathfrak{A}\&\mathfrak{B}\supset\mathfrak{B}\&\mathfrak{A}$ (по MP из 4 и 3)

6. $\mathfrak{A}\&\mathfrak{B}$ (исходная формула)

7. $\mathfrak{B}\&\mathfrak{A}$ (по MP из 6 и 5)

Задача. Доказать, что в $H_0$:

(а) $\mathfrak{A}\vee\mathfrak{B}\vdash\mathfrak{B}\vee\mathfrak{A}$;

(б) $\vdash((\mathfrak{A}\supset\mathfrak{B})\supset(\mathfrak{A}\supset\mathfrak{C}))\supset((\mathfrak{A}\supset\mathfrak{B})\supset(\mathfrak{A}\supset\mathfrak{B}\&\mathfrak{C}))$.

Доказательства выводимости путем непосредственного построения выводов часто оказываются очень громоздкими. Поэтому обычно пользуются *производными правилами*, выводимыми[31] из правила MP и аксиом. В частности, следующая теорема дает возможность пользоваться в $H_0$ правилом введения импликации:

**Теорема о дедукции.** Если $\Gamma,\mathfrak{A}\vdash\mathfrak{B}$, то $\Gamma\vdash\mathfrak{A}\supset\mathfrak{B}$.

Доказательство. Выводимость $\mathfrak{B}$ из $\Gamma,\mathfrak{A}$ означает, что существует вывод $\mathfrak{B}$ из $\Gamma,\mathfrak{A}$, представляющий собой последовательность формул $\mathfrak{C}_1,\ldots,\mathfrak{C}_s=\mathfrak{B}$. Докажем возвратной индукцией по $s$, что при этом условии $\Gamma\vdash\mathfrak{A}\supset\mathfrak{B}$.

Базис. Пусть $s=1$, т. е. данный вывод состоит из одной формулы $\Gamma_1=\mathfrak{B}$. Эта формула должна либо быть аксиомой, либо принадлежать $\Gamma$, либо совпадать с $\mathfrak{A}$. В первых двух случаях вывод $\mathfrak{A}\supset\mathfrak{B}$ из $\Gamma$

---

[30] Сама по себе з а п и с ь $\mathfrak{A}\supset((\mathfrak{A}\supset\mathfrak{A})\supset\mathfrak{A})$ — это, конечно, не аксиома, а схема аксиом, да и последовательность формул, которую мы выписываем — не вывод, а «схема выводов». Но если понимать под $\mathfrak{A}$ произвольную конкретную формулу, мы имеем право говорить «аксиома $\mathfrak{A}\supset((\mathfrak{A}\supset\mathfrak{A})\supset\mathfrak{A})$» и т. п. (как говорят, скажем, «число $x+y$»).

[31] Разумеется, в неформальном смысле. Слова «вывод», «выводимый», «выводимость» так же омонимичны, как слово «теорема» (см. выше, § 5.1, пункт 4).

имеет вид $\mathfrak{B}$. $\mathfrak{B}\supset(\mathfrak{A}\supset\mathfrak{B})$ (аксиома по схеме II), $\mathfrak{A}\supset\mathfrak{B}$. В третьем случае $\mathfrak{A}\supset\mathfrak{B}$ совпадает с $\mathfrak{A}\supset\mathfrak{A}$, а эта формула, как мы только что показали, выводима из пустого множества и тем более из $\Gamma$[42].

Индукционный шаг. Пусть $s > 1$ и для любой формулы $\mathfrak{B}'$, выводимой из $\Gamma$, $\mathfrak{A}$ с помощью вывода длины $< s$, формула $\mathfrak{A}\supset\mathfrak{B}'$ выводима из $\Gamma$. Рассмотрим произвольную формулу $\mathfrak{B}$, выводимую из $\Gamma$, $\mathfrak{A}$ с помощью вывода длины $s$; пусть $\mathfrak{C}_1, \ldots, \mathfrak{C}_s = \mathfrak{B}$ — этот вывод. Формула $\mathfrak{B}$ должна либо быть аксиомой, либо принадлежать $\Gamma$, либо совпадать с $\mathfrak{A}$, либо получаться по MP из некоторых формул $\mathfrak{C}_i$ и $\mathfrak{C}_j$, где $i$, $j < s$. В первых трех случаях можно рассуждать так же, как в базисе. В четвертом случае одна из формул $\mathfrak{C}_i$, $\mathfrak{C}_j$ — импликация с заключением $\mathfrak{B}$, а другая — посылка этой импликации. Пусть для определенности $\mathfrak{C}_j = \mathfrak{C}_i\supset\mathfrak{B}$. Последовательности $\mathfrak{C}_1, \ldots, \mathfrak{C}_i$ и $\mathfrak{C}_1, \ldots, \mathfrak{C}_j$ являются, очевидно, выводами своих последних формул из $\Gamma$, $\mathfrak{A}$; поэтому по предположению индукции из $\Gamma$ выводимы формулы $\mathfrak{A}\supset\mathfrak{C}_i$ и $\mathfrak{A}\supset\mathfrak{C}_j = \mathfrak{A}\supset(\mathfrak{C}_i\supset\mathfrak{B})$. Это даст возможность построить вывод формулы $\mathfrak{A}\supset\mathfrak{B}$ из $\Gamma$ следующим образом: записываем вывод формулы $\mathfrak{A}\supset\mathfrak{C}_i$ и вслед за ним вывод формулы $\mathfrak{A}\supset(\mathfrak{C}_i\supset\mathfrak{B})$, далее пишем аксиому $(\mathfrak{A}\supset(\mathfrak{C}_i\supset\mathfrak{B}))\supset((\mathfrak{A}\supset\mathfrak{C}_i)\supset(\mathfrak{A}\supset\mathfrak{B}))$ (по схеме I2), потом получаемую из этой аксиомы и формулы $\mathfrak{A}\supset(\mathfrak{C}_i\supset\mathfrak{B})$ формулу $(\mathfrak{A}\supset\mathfrak{C}_i)\supset(\mathfrak{A}\supset\mathfrak{B})$ и, наконец, получаемую из предыдущей формулы и $\mathfrak{A}\supset\mathfrak{C}_i$ формулу $\mathfrak{A}\supset\mathfrak{B}$.

В качестве следствия из теоремы о дедукции легко получить еще одно производное правило: *закон транзитивности импликации* (сокращенно ТИ): $\mathfrak{A}\supset\mathfrak{B}, \mathfrak{B}\supset\mathfrak{C} \vdash \mathfrak{A}\supset\mathfrak{C}$.

Доказательство. Ввиду теоремы о дедукции достаточно показать, что $\mathfrak{A}\supset\mathfrak{B}, \mathfrak{B}\supset\mathfrak{C}, \mathfrak{A} \vdash \mathfrak{C}$. Но $\mathfrak{A}, \mathfrak{A}\supset\mathfrak{B} \vdash \mathfrak{B}$, а $\mathfrak{B}, \mathfrak{B}\supset\mathfrak{C} \vdash \mathfrak{C}$.

Очень полезно также *правило устранения теоремы* (сокращенно УТ): Если $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$ и $\vdash \mathfrak{A}$, то $\Gamma \vdash \mathfrak{B}$.

Доказательство. Заменив в выводе формулы $\mathfrak{B}$ из $\Gamma$, $\mathfrak{A}$ первое вхождение $\mathfrak{A}$ доказательством[43] $\mathfrak{A}$, получим, очевидно, вывод $\mathfrak{B}$ из $\Gamma$. (Впрочем, правило УТ — частный случай правила транзитивности.)

Рассмотрим теперь несколько примеров доказательств выводимости с использованием производных правил.

(3) $\vdash (\neg\mathfrak{B}\supset\neg\mathfrak{A})\supset(\mathfrak{A}\supset\mathfrak{B})$.

---

[42] Из определения вывода в исчислении гильбертовского типа непосредственно ясно, что в любом таком исчислении справедливо «правило расширения» (ср. задачу на с. 166): если $\Gamma \vdash \mathfrak{A}$ и $\Gamma\subset\Lambda$, то $\Lambda \vdash \mathfrak{A}$ (а также правила тривиальной выводимости и транзитивности).

[43] Мы видим здесь, что слово «доказательство» так же омонимично, как «теорема» и «вывод».

Доказательство. Имеем $\vdash (\neg\mathfrak{B}\supset\neg\mathfrak{A})\supset(\neg\neg\mathfrak{A}\supset\neg\neg\mathfrak{B})$ (аксиома по схеме IV1); поэтому, если мы докажем, что $\vdash (\neg\neg\mathfrak{A}\supset\neg\neg\mathfrak{B})\supset(\mathfrak{A}\supset\mathfrak{B})$, то, воспользовавшись правилом ТИ, получим нужную теорему. Но $\mathfrak{A}\supset\neg\neg\mathfrak{A}$, $\neg\neg\mathfrak{A}\supset\neg\neg\mathfrak{B}$, $\neg\neg\mathfrak{B}\supset\mathfrak{B}\vdash\mathfrak{A}\supset\mathfrak{B}$ (два раза ТИ), откуда $\neg\neg\mathfrak{A}\supset\neg\neg\mathfrak{B}\vdash\mathfrak{A}\supset\mathfrak{B}$ (два раз УТ) и по теореме о дедукции $\vdash(\neg\neg\mathfrak{A}\supset\neg\neg\mathfrak{B})\supset(\mathfrak{A}\supset\mathfrak{B})$.

(4) $\vdash\neg\mathfrak{A}\supset(\mathfrak{A}\supset\mathfrak{B})$.

Доказательство. Нужная теорема получается по ТИ из $\neg\mathfrak{A}\supset(\neg\mathfrak{B}\supset\neg\mathfrak{A})$ (это аксиома по схеме II) и (3).

С помощью примера (4) можно вывести еще одно производное правило: если $\Gamma,\mathfrak{A}\vdash\mathfrak{B}$ и $\Gamma,\mathfrak{A}\vdash\neg\mathfrak{B}$, то $\Gamma\vdash\neg\mathfrak{A}$. В самом деле, пусть $\Gamma,\mathfrak{A}\vdash\mathfrak{B}$ и $\Gamma,\mathfrak{A}\vdash\neg\mathfrak{B}$, и пусть $\mathfrak{C}$ — произвольная (формальная) теорема. Так как по (4) $\vdash\neg\mathfrak{B}\supset(\mathfrak{B}\supset\neg\mathfrak{C})$, имеем $\Gamma,\mathfrak{A}\vdash\neg\mathfrak{C}$, откуда по теореме о дедукции $\Gamma\vdash\mathfrak{A}\supset\neg\mathfrak{C}$, и далее $\Gamma\vdash\neg\neg\mathfrak{C}\supset\neg\mathfrak{A}$ (ввиду IV1 и MP). Поэтому $\Gamma,\neg\neg\mathfrak{C}\vdash\neg\mathfrak{A}$, а отсюда, поскольку (ввиду IV2) $\neg\neg\mathfrak{C}$ — теорема, по правилу УТ получаем $\Gamma\vdash\neg\mathfrak{A}$.

Из только что доказанного правила легко получить еще одно: если $\Gamma,\mathfrak{A}\vdash\mathfrak{B}$ и $\Gamma,\neg\mathfrak{A}\vdash\mathfrak{B}$, то $\Gamma\vdash\mathfrak{B}$. Действительно, из $\Gamma,\mathfrak{A}\vdash\mathfrak{B}$ следует $\Gamma,\neg\mathfrak{B}\vdash\neg\mathfrak{A}$ (ввиду теоремы о дедукции, IV1 и MP) и точно так же из $\Gamma,\neg\mathfrak{A}\vdash\mathfrak{B}$ следует $\Gamma,\neg\mathfrak{B}\vdash\neg\neg\mathfrak{A}$. Но из $\Gamma,\neg\mathfrak{B}\vdash\neg\mathfrak{A}$ и $\Gamma,\neg\mathfrak{B}\vdash\neg\neg\mathfrak{A}$ по предыдущему правилу вытекает $\Gamma\vdash\neg\neg\mathfrak{B}$, откуда ввиду IV3 $\Gamma\vdash\mathfrak{B}$.

(5) $\vdash\mathfrak{A}\vee\neg\mathfrak{A}$.

Доказательство. По III 1,2 имеем $\vdash\mathfrak{A}\supset\mathfrak{A}\vee\neg\mathfrak{A}$ и $\neg\mathfrak{A}\supset\mathfrak{A}\vee\neg\mathfrak{A}$ и потому $\mathfrak{A}\vdash\mathfrak{A}\vee\neg\mathfrak{A}$ и $\neg\mathfrak{A}\vdash\mathfrak{A}\vee\neg\mathfrak{A}$. Отсюда по только что выведенному правилу $\vdash\mathfrak{A}\vee\neg\mathfrak{A}$.

Задача. Пользуясь производными правилами, доказать, что в $H_0$:

(а) $\mathfrak{A}\vee\mathfrak{B},\neg\mathfrak{A}\vdash\mathfrak{B}$;

(б) $\neg\mathfrak{A}\&\neg\mathfrak{B}\vdash\neg(\mathfrak{A}\vee\mathfrak{B})$;

(в) $\neg(\mathfrak{A}\vee\mathfrak{B})\vdash\neg\mathfrak{A}\&\neg\mathfrak{B}$;

(г) $\neg\mathfrak{A}\vee\neg\mathfrak{B}\vdash\neg(\mathfrak{A}\&\mathfrak{B})$;

(д) $\neg(\mathfrak{A}\&\mathfrak{B})\vdash\neg\mathfrak{A}\vee\neg\mathfrak{B}$.

Мы могли бы теперь доказать для исчисления $H_0$ теоремы о замене дедуктивно эквивалентных формул, о семантической пригодности и о полноте аналогично тому, как это было сделано для $G_0$; доказательства потребовали бы сравнительно небольших изменений (например, вместо правил введения и удаления конъюнкции и

дизъюнкции пришлось бы пользоваться аксиомами групп II и III в сочетании с MP и теоремой о дедукции) и кое-где упростились бы. Но вместо этого мы покажем, что исчисления $G_0$ и $H_0$ равносильны в следующем смысле: если в $G_0$ рассматривать только формулы, не содержащие константы $Л$, то понятия выводимости и теоремы для ограниченного таким образом исчисления будут совпадать по объему с соответствующими понятиями для $H_0$. Отсюда будут немедленно следовать и теоремы о замене, о семантической пригодности и о полноте для $H_0$.

Перейдем к точным формулировкам и доказательству. Рассмотрим прежде всего исчисление, получающееся из $G_0$ следующим образом: из алфавита изымается символ $Л$, из системы правил образования формул — правило (б) и из системы правил вывода — УО, ВО и ДС и взамен вводятся два новых правила: если $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$ и $\Gamma, \mathfrak{A} \vdash \neg\mathfrak{B}$, то $\Gamma \vdash \neg\mathfrak{A}$ (ВО'); $\mathfrak{A}, \neg\mathfrak{A} \vdash \mathfrak{B}$ (ДС'). Обозначим это исчисление $G_0'$. Покажем, что если $\Gamma$ — конечное множество формул исчисления $G_0$ и $\mathfrak{A}$ — формула $G_0$, то $\Gamma \underset{G_0'}{\vdash} \mathfrak{A}$ тогда и только тогда, когда $\Gamma \underset{G_0}{\vdash} \mathfrak{A}$ (и, в частности, формула исчисления $G_0'$ является в $G_0'$ теоремой тогда и только тогда, когда она — теорема в $G_0$). В самом деле: (а) Произвольное дерево вывода в $G_0'$ легко переделать в дерево вывода в $G_0$, заменяя каждое применение ВО' последовательным применением УО и ВО, а каждое применение ДС' — последовательным применением УО и ДС. (б) Пусть $\delta$ — дерево вывода в $G_0$, у которого корень и зеленые листья не содержат символа $Л$. Если и остальные формулы, входящие в $\delta$, не содержат $Л$, то $\delta$ уже является деревом вывода в $G_0'$. В противном случае заменим все вхождения $Л$ в формулы, фигурирующие в $\delta$, вхождениями конъюнкции $X_1 \& \neg X_1$. При этом все применения правила УО превратятся в применения ДС', а элементарные поддеревья, отвечающие применениям правил ВО и ДС, превратятся в «неправильные» элементарные поддеревья, которые можно устранить следующим образом. Возьмем самое верхнее «неправильное» элементарное поддерево, т.е. такое, выше которого нет других «неправильных» поддеревьев (если таких несколько, берем любое из них). Пусть это поддерево есть $\varepsilon$; обозначим через $\lambda$ то поддерево дерева $\delta$, которое служит деревом вывода корня дерева $\varepsilon$ (т. е. то «полное» поддерево $\delta$, которое «растет» из корня $\varepsilon$). Дерево $\varepsilon$ имеет вид $\dfrac{X_1 \& \neg X_1}{\mathfrak{C}}$, где $\mathfrak{C}$ — некоторая формула, а $\lambda$ есть $\dfrac{\mu}{\mathfrak{C}}$, где $\mu$ — некоторое дерево вывода в $G_0$ с корнем $X_1 \& \neg X_1$. Заменим в дереве $\delta$ поддерево $\lambda$ поддеревом

$$\lambda' = \dfrac{\dfrac{\Gamma}{X_i}\ \text{УК} \qquad \dfrac{\Gamma}{\neg X_i}\ \text{УК}}{\mathfrak{C}}.$$

Ясно, что $\lambda'$ есть дерево вывода в $G_0$, причем на самом нижнем шаге в $\lambda'$ применяется ВО′, если $\varepsilon$ отвечало применению ВО, и ДС′, если $\varepsilon$ отвечало применению ДС. Дерево, полученное из $\delta$ заменой $\lambda$ на $\lambda'$, будет содержать одним «неправильным» элементарным поддеревом меньше; множество зеленых листьев при этом не меняется. Устранив таким образом все «неправильности», мы получим дерево вывода в $G_0$ с тем же корнем и тем же множеством зеленых листьев, что и $\delta$.

Докажем теперь, что формула в алфавите исчисления $H_0$ тогда и только тогда выводима в $H_0$ из множества формул в том же алфавите, когда это имеет место в $G_0$.

(а) Покажем, что если $\Gamma \underset{H_0}{\vdash} \mathfrak{A}$, то $\Gamma \underset{G_0}{\vdash} \mathfrak{A}$. Достаточно убедиться, что всякая теорема $H_0$ является теоремой и в $G_0$; действительно, тогда при непустом $\Gamma = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_k\}$ из $\mathfrak{B}_1, \ldots, \mathfrak{B}_k \underset{H_0}{\vdash} \mathfrak{A}$ получим, применяя $k$ раз теорему о дедукции, $\underset{H_0}{\vdash} \mathfrak{B}_1 \supset (\mathfrak{B}_2 \supset \ldots \supset (\mathfrak{B}_k \supset \mathfrak{A}) \ldots)$, откуда $\underset{G_0}{\vdash} \mathfrak{B}_1 \supset (\mathfrak{B}_2 \supset \ldots \supset (\mathfrak{B}_k \supset \mathfrak{A}) \ldots)$ и далее по УИ $\mathfrak{B}_1, \ldots, \mathfrak{B}_k \underset{G_0}{\vdash} \mathfrak{A}$. А поскольку единственное правило исчисления $H_0$ действует и в $G_0$, остается проверить, что все аксиомы $H_0$ доказуемы в $G_0$ — или в $G_0$, так как аксиомы $H_0$ не содержат вхождений $A$. Для схемы I1 мы это фактически уже сделали (пример (8) из § 5.3). Для схем II1,2, III1,2 и IV1,2,3 достаточно воспользоваться соответственно правилами УК и ВД и примерами (32), (6) и (23) из § 5.3 в сочетании с леммой 1 из того же параграфа. Для схемы III3 рассуждаем так: поскольку $\mathfrak{A} \supset \mathfrak{C}$, $\mathfrak{A} \vdash \mathfrak{C}$ и $\mathfrak{B} \supset \mathfrak{C}$, $\mathfrak{B} \vdash \mathfrak{C}$, по правилу УД имеем $\mathfrak{A} \supset \mathfrak{C}$, $\mathfrak{B} \supset \mathfrak{C}$, $\mathfrak{A} \vee \mathfrak{B} \vdash \mathfrak{C}$, а отсюда, применив три раза ВИ, получаем $\vdash (\mathfrak{A} \supset \mathfrak{C}) \supset ((\mathfrak{B} \supset \mathfrak{C}) \supset (\mathfrak{A} \vee \mathfrak{B} \supset \mathfrak{C}))$. Сходным образом можно рассуждать для I2 и I3; читатель сделает это сам.

(б) Чтобы показать, что $\Gamma \underset{G_0}{\vdash} \mathfrak{A}$ влечет $\Gamma \underset{H_0}{\vdash} \mathfrak{A}$, достаточно установить, что в $H_0$ действуют все правила исчисления $G_0$. Мы уже заметили (см. сноску к доказательству теоремы о дедукции), что в любом исчислении гильбертовского типа справедливы правила тривиальной выводимости и транзитивности. Что касается логических правил, то: УК и ВД непосредственно следуют из схем II1,2 и III1,2 (в сочетании с МР); УИ есть МР; справедливость ВИ обеспечивается

мер (8) из предыдущего параграфа. В подслучае (в) $\mathfrak{B}' = \mathfrak{B}$, $\mathfrak{C}' = \neg\mathfrak{C}$, $\mathfrak{A}(r) = Л$, $\mathfrak{A}' = \neg\mathfrak{A}$. Но по УИ $\mathfrak{B}$, $\mathfrak{B} \supset \mathfrak{C} \vdash \mathfrak{C}$, откуда по лемме 2 из предыдущего параграфа $\mathfrak{B}$, $\neg\mathfrak{C} \vdash \neg(\mathfrak{B} \supset \mathfrak{C})$. Поэтому из $X'_1, \ldots, X'_n$ выводима формула $\neg(\mathfrak{B} \supset \mathfrak{C}) = \neg\neg\mathfrak{A} = \mathfrak{A}'$.

Наконец, в случае (4), если $\mathfrak{B}(r) = И$, то $\mathfrak{B}' = \mathfrak{B}$, $\mathfrak{A}(r) = Л$, $\mathfrak{A}' = \neg\mathfrak{A}$, и из $X'_1, \ldots, X'_n$ выводима формула $\mathfrak{B}$, из которой по правилу постановки двойного отрицания выводится $\neg\neg\mathfrak{B} = \neg\mathfrak{A} = \mathfrak{A}'$. Если же $\mathfrak{B}(r) = Л$, то $\mathfrak{B}' = \neg\mathfrak{B}$, $\mathfrak{A}(r) = И$, $\mathfrak{A}' = \mathfrak{A}$, и $X'_1, \ldots, X'_n \vdash \neg\mathfrak{B} = \mathfrak{A} = \mathfrak{A}'$.

Лемма доказана.

**Доказательство теоремы.** Пусть $\mathfrak{A}$ — произвольная тождественно истинная формула. Фиксируем раз навсегда подходящее число $n$. Тогда для любого $n$-мерного булева вектора $r$ будет $\mathfrak{A}' = \mathfrak{A}$, и по только что доказанной лемме $X'_1, \cdots, X'_n \vdash \mathfrak{A}$. Сопоставим теперь произвольному $n$-мерному булеву вектору $r$ конечную последовательность множеств формул $\Gamma'_1, \ldots, \Gamma'_n, \Gamma'_{n+1}$ следующим образом: если $1 \leq i \leq n$, то $\Gamma'_i = \{X'_i, X'_{i+1}, \ldots, X'_n\}$; $\Gamma'_{n+1} = \varnothing$. Покажем теперь индукцией по $i$, что для любого $i = 1, \ldots, n+1$ и любого $n$-мерного булева вектора $r$ имеет место $\Gamma'_i \vdash \mathfrak{A}$. Сделав это[24], мы убедимся, в частности, что $\Gamma'_{n+1} \vdash \mathfrak{A}$, т. е. $\vdash \mathfrak{A}$, и доказательство теоремы о полноте будет завершено. Базис индукции у нас уже готов; остается провести индукционный шаг.

Итак, пусть для некоторого $i = 1, \ldots, n$ справедливо следующее утверждение: для любого $n$-мерного булева вектора $r$ имеет место $\Gamma'_i \vdash \mathfrak{A}$ или, что то же самое, $\Gamma'_{i+1}, X'_i \vdash \mathfrak{A}$. Фиксировав произвольный вектор $r$, изменим его $i$-ю координату; обозначим полученный таким образом вектор через $r'$. Тогда наряду с выводимостью $\Gamma'_{i+1}, X'_i \vdash \mathfrak{A}$ будет иметь место $\Gamma'_{i+1}, X'_i \vdash \mathfrak{A}$. Но так как всякая формула $X'_j$ зависит только от $j$-й координаты вектора $r'$, а у $r$ и $r'$ все координаты, кроме $i$-й, совпадают, имеем $X'_{i+1} = X'_{i+1}, \ldots, X'_n = X'_n$, т. е. $\Gamma'_{i+1} = \Gamma'_{i+1}$ (так при $i < n$; равенство $\Gamma'_{n+1} = \Gamma'_{n+1}$ выполняется тривиальным образом). Таким образом, $\Gamma'_{i+1}, X'_i \vdash \mathfrak{A}$. А поскольку одна из формул $X'_i$, $X'_i$ есть $X_i$, а другая $\neg X_i$, имеем $\Gamma'_{i+1}, X_i \vdash \mathfrak{A}$, $\Gamma'_{i+1}, \neg X_i \vdash \mathfrak{A}$, откуда по лемме 3 из предыдущего параграфа $\Gamma'_{i+1} \vdash \mathfrak{A}$. Этим заканчивается индукционный шаг и вместе с ним доказательство теоремы.

---

[24] Об индукции по конечному отрезку натурального ряда см. в Приложении III (примечание 2 на с. 461).

Заметим еще, что для описания конструктивной логики исчисления в «неполных» алфавитах непригодны, так как в ней не выполняются классические соотношения между пропозициональными связками.

4. Кроме исчислений гильбертовского типа и исчислений естественного вывода существует еще одна широко употребительная разновидность логических исчислений — так называемые *секвенциальные исчисления*. Они относятся к генценовскому типу и были введены в той же работе Г. Генцена [Генцен 1967][35], в которой впервые появились исчисления естественного вывода. Аналогично последним, в них используется представление вывода в виде дерева, но здесь при движении вниз по дереву переходят не от формулы к формуле, а от выводимости к выводимости, причем листьями дерева служат тривиальные выводимости вида $\mathfrak{A} \vdash \mathfrak{A}$, а корнем — та выводимость, которую нужно доказать. Таким образом, в этих исчислениях происходит «вывод выводимостей». Все правила в них должны быть условными; например, правила введения и удаления конъюнкции заменяются такими правилами: «Если $\Gamma \vdash \mathfrak{A}$ и $\Gamma \vdash \mathfrak{B}$, то $\Gamma \vdash \mathfrak{A}\&\mathfrak{B}$», «Если $\Gamma, \mathfrak{A} \vdash \Delta$, то $\Gamma, \mathfrak{A}\&\mathfrak{B} \vdash \Delta$»; «Если $\Gamma, \mathfrak{B} \vdash \Delta$, то $\Gamma, \mathfrak{A}\&\mathfrak{B} \vdash \Delta$». С помощью этих правил можно следующим образом доказать выводимость $\mathfrak{A}\&\mathfrak{B} \vdash \mathfrak{B}\&\mathfrak{A}$:

$$\dfrac{\dfrac{\dfrac{\mathfrak{B} \vdash \mathfrak{B}}{\mathfrak{A}\&\mathfrak{B} \vdash \mathfrak{B}} \quad \dfrac{\mathfrak{A} \vdash \mathfrak{A}}{\mathfrak{A}\&\mathfrak{B} \vdash \mathfrak{A}}}{\mathfrak{A}\&\mathfrak{B} \vdash \mathfrak{B}\&\mathfrak{A}}}$$

При таком способе вывода оказывается удобно обобщить понятие выводимости, рассматривая случаи, когда из данного множества формул выводима хотя бы одна из двух формул $\mathfrak{A}_1$, $\mathfrak{A}_2$ или хотя бы одна из трех формул $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{A}_3$ и т. д.— иначе говоря, когда из истинности в с е х формул, входящих в некоторое конечное множество, следует истинность х о т я б ы о д н о й из формул, входящих в другое конечное множество (и этот факт устанавливается путем формального вывода). Разумеется, выводимость хотя бы одной из нескольких формул содержательно означает то же, что выводимость их дизъюнкции — но точно так же выводимость и з нескольких формул содержательно равносильна выводимости из их конъюнкции. Возникает, таким образом, своеобразная симметрия левой и правой частей выводимости. Однако за термином «выводимость» желательно все же сохранить его прежнее значение; поэтому мы будем, следуя Г. Генцену, называть «обобщенную выводимость» *секвен-*

[35] В нашем списке литературы указан год опубликования русского перевода. В подлиннике эта работа впервые была опубликована в 1934—1935 гг.

*цией*[36] и для ее обозначения пользоваться не знаком $\vdash$, а новым символом $\to$. Точнее, мы будем называть секвенцией выражение вида $\mathfrak{A}_1, \ldots, \mathfrak{A}_k \to \mathfrak{B}_1, \ldots, \mathfrak{B}_l$, где $\mathfrak{A}_1, \ldots, \mathfrak{A}_k, \mathfrak{B}_1, \ldots, \mathfrak{B}_l$ — формулы и $k$, $l = 0, 1, \ldots$. Часть секвенции слева от стрелки называется ее *антецедентом*, справа — *сукцедентом*[37]. Поскольку мы допускаем случаи $k = 0$ и $l = 0$, антецедент и сукцедент могут быть и пустыми. Содержательно пустота антецедента означает, что сукцедент истинен, пустота сукцедента — что антецедент ложен; секвенция, у которой обе части пусты, противоречива[38]. Подчеркнем, что антецедент и сукцедент секвенции — последовательности, а не множества формул; принципиального значения это не имеет (ср. сноску на с. 156), но форма секвенции такова, что было бы неестественно считать ее состоящей из множеств.

Теперь мы можем описать секвенциальный вариант исчисления предложений, который мы будем обозначать $S_0$. Алфавит и правила образования формул будут в $S_0$ те же, что в $H_0$. Правила вывода будут иметь вид *фигур заключения*; каждая такая фигура состоит из горизонтальной черты, снизу от которой записана некоторая секвенция (*нижняя секвенция* данной фигуры), а сверху — одна или две секвенции (*верхние секвенции* фигуры). Точнее, правила будут представлять собой *схемы фигур заключения*, содержащие *схемы секвенций*; в этих схемах прописные готические буквы будут обозначать, как и прежде, формулы, а прописные греческие — последовательности формул (а не множества, как раньше). Собственно *фигура заключения* есть выражение, полученное из схемы фигур заключения заменой схем секвенций конкретными секвенциями.

Далее следует перечень схем фигур заключения.

Структурные фигуры заключения:

1) *Разбавление*[39] *в антецеденте*:

$$\frac{\Gamma \to \Theta}{\mathfrak{D}, \Gamma \to \Theta}$$

2) *Разбавление*[39] *в сукцеденте*:

$$\frac{\Gamma \to \Theta}{\Gamma \to \Theta, \mathfrak{D}}$$

---

[36] От лат. *sequens* — «следующий».

[37] От лат. *antecedens* — «предшествующий» и *succedens* — «идущий вслед».

[38] Если сукцедент состоит из формул $\mathfrak{B}_1, \ldots, \mathfrak{B}_l$, это означает, что при условии истинности антецедента имеет место хотя бы один из случаев, описываемых этими формулами. Если же сукцедент пуст, это значит, что при истинности антецедента «никакой случай невозможен». А если при этом пуст и антецедент, это значит, что «никакой случай невозможен» даже без всяких условий.

[39] По-немецки *Verdünnung*, что может означать также «утончение». В литературе на русском языке эту фигуру до сих пор так и называли «утончением», хотя это, конечно, ошибка: антецедент или сукцедент здесь именно разбавляется, а не делается тоньше.

3) *Сокращение в антецеденте:*

$$\frac{\mathfrak{D},\ \mathfrak{D},\ \Gamma \to \Theta}{\mathfrak{D},\ \Gamma \to \Theta}$$

4) *Сокращение в сукцеденте:*

$$\frac{\Gamma \to \Theta,\ \mathfrak{D},\ \mathfrak{D}}{\Gamma \to \Theta,\ \mathfrak{D}}$$

5) *Перестановка в антецеденте:*

$$\frac{\Delta,\ \mathfrak{D},\ \mathfrak{E},\ \Gamma \to \Theta}{\Delta,\ \mathfrak{E},\ \mathfrak{D},\ \Gamma \to \Theta}$$

6) *Перестановка в сукцеденте:*

$$\frac{\Gamma \to \Theta,\ \mathfrak{D},\ \mathfrak{E},\ \Delta}{\Gamma \to \Theta,\ \mathfrak{E},\ \mathfrak{D},\ \Delta}$$

7) *Сечение* (вывод по транзитивности):

$$\frac{\Gamma \to \Theta,\ \mathfrak{D} \qquad \mathfrak{D},\ \Delta \to \Lambda}{\Gamma,\ \Delta \to \Theta,\ \Lambda}$$

Логические фигуры заключения:

1) *Введение конъюнкции в антецедент:*

$$\frac{\mathfrak{A},\ \Gamma \to \Delta}{\mathfrak{A}\&\mathfrak{B},\ \Gamma \to \Delta} \qquad \frac{\mathfrak{B},\ \Gamma \to \Delta}{\mathfrak{A}\&\mathfrak{B},\ \Gamma \to \Delta}$$

2) *Введение конъюнкции в сукцедент:*

$$\frac{\Gamma \to \Delta,\ \mathfrak{A} \qquad \Gamma \to \Delta,\ \mathfrak{B}}{\Gamma \to \Delta,\ \mathfrak{A}\&\mathfrak{B}}$$

3) *Введение дизъюнкции в антецедент:*

$$\frac{\mathfrak{A},\ \Gamma \to \Delta \qquad \mathfrak{B},\ \Gamma \to \Delta}{\mathfrak{A} \vee \mathfrak{B},\ \Gamma \to \Delta}$$

4) *Введение дизъюнкции в сукцедент:*

$$\frac{\Gamma \to \Delta,\ \mathfrak{A}}{\Gamma \to \Delta,\ \mathfrak{A} \vee \mathfrak{B}} \qquad \frac{\Gamma \to \Delta,\ \mathfrak{B}}{\Gamma \to \Delta,\ \mathfrak{A} \vee \mathfrak{B}}$$

5) *Введение импликации в антецедент:*

$$\frac{\Gamma \to \Delta,\ \mathfrak{A} \qquad \mathfrak{B},\ \Theta \to \Lambda}{\mathfrak{A} \supset \mathfrak{B},\ \Gamma,\ \Theta \to \Delta,\ \Lambda}$$

6) *Введение импликации в сукцедент:*

$$\frac{\mathfrak{A},\ \Gamma \to \Delta,\ \mathfrak{B}}{\Gamma \to \Delta,\ \mathfrak{A} \supset \mathfrak{B}}$$

7) *Введение отрицания в антецедент:*

$$\frac{\Gamma \to \Delta,\ \mathfrak{A}}{\neg\mathfrak{A},\ \Gamma \to \Delta}$$

8) *Введение отрицания в сукцедент:*

$$\frac{\mathfrak{A},\ \Gamma \to \Delta}{\Gamma \to \Delta,\ \neg\mathfrak{A}}$$

Иногда мы будем сокращенно обозначать фигуры заключения аналогично тому, как обозначились правила $G_0$, например РА, ПС, ВКА, ВДС.

Легко заметить, что правилам введения логических символов исчисления $G_0$ отвечают здесь фигуры введения в сукцедент, а правилам удаления — фигуры введения в антецедент (последнее особенно очевидно в случае, когда сукцеденты верхних и нижних секвенций содержат не более чем по одной формуле).

Определим теперь *дерево вывода в исчислении* $S_0$. Одновременно будут определяться *корень*, *листья* и *высота* дерева. Определение будет состоять из трех пунктов:

1) Всякая секвенция есть дерево вывода, корнем и единственным листом которого служит она сама. Высота такого дерева равна нулю.

2) Выражение, получаемое из фигуры заключения $r$ заменой ее верхних секвенций деревьями вывода, корнями которых служат эти секвенции, есть дерево вывода; корнем этого дерева служит нижняя секвенция дерева $r$, а листьями — все листья деревьев, которыми заменены верхние секвенции. Высота такого дерева на единицу больше наибольшей из высот деревьев, из которых оно получено.

3) Всякое дерево вывода является таковым в силу пункта 1 или 2.

Мы будем теперь называть секвенцию *выводимой*, если она либо имеет вид $\mathfrak{A} \to \mathfrak{A}$, либо является корнем некоторого дерева вывода, все листья которого — секвенции вида $\mathfrak{A} \to \mathfrak{A}$.

Приведем несколько примеров выводов секвенций.

1) Вывод закона коммутативности дизъюнкции:

$$\dfrac{\dfrac{\dfrac{\mathfrak{A} \to \mathfrak{A}}{\mathfrak{A} \to \mathfrak{B} \vee \mathfrak{A}}\,\text{ВДС} \qquad \dfrac{\mathfrak{B} \to \mathfrak{B}}{\mathfrak{B} \to \mathfrak{B} \vee \mathfrak{A}}\,\text{ВДС}}{\mathfrak{A} \vee \mathfrak{B} \to \mathfrak{B} \vee \mathfrak{A}}\,\text{ВДА}$$

2) Вывод закона исключенного третьего:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathfrak{A} \to \mathfrak{A}}{\to \mathfrak{A},\ \neg\mathfrak{A}}\,\text{ВОС}}{\to \mathfrak{A},\ \mathfrak{A} \vee \neg\mathfrak{A}}\,\text{ВДС}}{\to \mathfrak{A} \vee \neg\mathfrak{A},\ \mathfrak{A}}\,\text{ПС}}{\to \mathfrak{A} \vee \neg\mathfrak{A},\ \mathfrak{A} \vee \neg\mathfrak{A}}\,\text{ВДС}}{\to \mathfrak{A} \vee \neg\mathfrak{A}}\,\text{СС}$$

3) Вывод правила снятия двойного отрицания:

$$\dfrac{\dfrac{\mathfrak{A} \to \mathfrak{A}}{\to \mathfrak{A},\ \neg\mathfrak{A}}\,\text{ВОС}}{\neg\neg\mathfrak{A} \to \mathfrak{A}}\,\text{ВОА}$$

4) Вывод секвенции $\neg\mathfrak{A} \vee \neg\mathfrak{B} \to \neg(\mathfrak{A}\&\mathfrak{B})$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathfrak{A} \to \mathfrak{A}}{\mathfrak{A}\&\mathfrak{B} \to \mathfrak{A}}\,\text{ВКА}}{\neg\mathfrak{A},\ \mathfrak{A}\&\mathfrak{B} \to}\,\text{ВОА}}{\mathfrak{A}\&\mathfrak{B},\ \neg\mathfrak{A} \to}\,\text{ПА}}{\neg\mathfrak{A} \to \neg(\mathfrak{A}\&\mathfrak{B})}\,\text{ВОС} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathfrak{B} \to \mathfrak{B}}{\mathfrak{A}\&\mathfrak{B} \to \mathfrak{B}}\,\text{ВКА}}{\neg\mathfrak{B},\ \mathfrak{A}\&\mathfrak{B} \to}\,\text{ВОА}}{\mathfrak{A}\&\mathfrak{B},\ \neg\mathfrak{B} \to}\,\text{ПА}}{\neg\mathfrak{B} \to \neg(\mathfrak{A}\&\mathfrak{B})}\,\text{ВОС}}{\neg\mathfrak{A} \vee \neg\mathfrak{B} \to \neg(\mathfrak{A}\&\mathfrak{B})}\,\text{ВДА}$$

5) Вывод секвенции $\neg(\mathfrak{A}\&\mathfrak{B}) \to \neg\mathfrak{A} \vee \neg\mathfrak{B}$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathfrak{A} \to \mathfrak{A}}{\mathfrak{B},\ \mathfrak{A} \to \mathfrak{A}}\,\text{РА}}{\mathfrak{A},\ \mathfrak{B} \to \mathfrak{A}}\,\text{ПС} \qquad \dfrac{\mathfrak{B} \to \mathfrak{B}}{\mathfrak{A},\ \mathfrak{B} \to \mathfrak{B}}\,\text{РА}}{\mathfrak{A},\ \mathfrak{B} \to \mathfrak{A}\&\mathfrak{B}}\,\text{ВКС}}{\mathfrak{B} \to \mathfrak{A}\&\mathfrak{B},\ \neg\mathfrak{A}}\,\text{ВОС}}{\to \mathfrak{A}\&\mathfrak{B},\ \neg\mathfrak{A},\ \neg\mathfrak{B}}\,\text{ВОС}}{\neg(\mathfrak{A}\&\mathfrak{B}) \to \neg\mathfrak{A},\ \neg\mathfrak{B}}\,\text{ВОА}}{\neg(\mathfrak{A}\&\mathfrak{B}) \to \neg\mathfrak{A},\ \neg\mathfrak{A} \vee \neg\mathfrak{B}}\,\text{ВДС}}{\neg(\mathfrak{A}\&\mathfrak{B}) \to \neg\mathfrak{A} \vee \neg\mathfrak{B},\ \neg\mathfrak{A}}\,\text{ПС}}{\neg(\mathfrak{A}\&\mathfrak{B}) \to \neg\mathfrak{A} \vee \neg\mathfrak{B},\ \neg\mathfrak{A} \vee \neg\mathfrak{B}}\,\text{ВДС}}{\neg(\mathfrak{A}\&\mathfrak{B}) \to \neg\mathfrak{A} \vee \neg\mathfrak{B}}\,\text{СС}$$

6) Вывод секвенции $\mathfrak{A},\ \mathfrak{A}\supset\mathfrak{B},\ \mathfrak{B}\supset\mathfrak{C} \to \mathfrak{C}$:

$$\dfrac{\dfrac{\dfrac{\mathfrak{A} \to \mathfrak{A} \quad \mathfrak{B} \to \mathfrak{B}}{\mathfrak{A}\supset\mathfrak{B},\ \mathfrak{A} \to \mathfrak{B}}\,\text{ВИА}}{\mathfrak{A},\ \mathfrak{A}\supset\mathfrak{B} \to \mathfrak{B}}\,\text{ПА} \qquad \dfrac{\dfrac{\mathfrak{B} \to \mathfrak{B} \quad \mathfrak{C} \to \mathfrak{C}}{\mathfrak{B}\supset\mathfrak{C},\ \mathfrak{B} \to \mathfrak{C}}\,\text{ВИА}}{\mathfrak{B},\ \mathfrak{B}\supset\mathfrak{C} \to \mathfrak{C}}\,\text{ПА}}{\mathfrak{A},\ \mathfrak{A}\supset\mathfrak{B},\ \mathfrak{B}\supset\mathfrak{C} \to \mathfrak{C}}\,\text{сечение}$$

**Замечание.** Выводы примеров 1, 4 и 6, принадлежащие конструктивной логике, отличаются от неконструктивных выводов примеров 2, 3 и 5 тем, что в них сукцеденты всех секвенций содержат не более чем по одной формуле. Далее мы увидим, что это не случайно.

Просматривая фигуры заключения исчисления $S_0$, можно заметить, что все они, кроме сечения, обладают следующим свойством: каждая формула, входящая в верхнюю секвенцию, либо входит также и в нижнюю, либо является непосредственной составляющей (подформулой глубины 1) некоторой формулы, входящей в нижнюю секвенцию. Поэтому если дерево вывода не содержит сечений, то все участвующие в выводе формулы являются подформулами формул, входящих в заключительную секвенцию — т. е. в ту секвенцию, которая служит корнем дерева (*свойство подформульности*). Оказывается, однако, что для любой секвенции, выводимой в $S_0$, существует дерево вывода, не содержащее сечений, и такое дерево можно эффективно построить по произвольному дереву вывода данной секвенции. Это так называемая **основная теорема Генцена**[40] (доказывать ее мы не будем). Таким образом, для всякой выводимой секвен-

[40] Точнее, основной теоремой Генцена называется соответствующее утверждение для узкого исчисления предикатов в секвенциальной форме (см. ниже, § 6.4), для которого только что сформулированная теорема фактически является частным случаем.

ции найдется дерево вывода, обладающее свойством подформульности. Содержательно это означает, что для всякого доказуемого математического утверждения можно найти «прямое» доказательство — «прямое» в том смысле, что все участвующие в нем промежуточные утверждения являются «частями» доказываемого. Практически такое «прямое» доказательство далеко не всегда проще «косвенного», т. к., с одной стороны, оно может быть длиннее, с другой — что случается особенно часто,— большой кусок «косвенного» доказательства может уже находиться в нашем распоряжении (например, когда нужное утверждение — частный случай или простое следствие известной или ранее доказанной нами теоремы) и тогда удобнее воспользоваться этим доказательством, даже если все целиком оно длиннее «прямого». Однако теоретическое значение основной теоремы очень велико. В частности, она позволила Генцену доказать непротиворечивость арифметики[41]. Широко используется эта теорема в современных исследованиях по теории логического вывода и по его автоматизации (см. в настоящем параграфе пункт 5). Ее доказательство можно найти в статье [Генцен 1967], в книге [Клини 1957] и в приложении I (написанном редактором перевода Г.Е. Минцем) к книге [Клини 1973].

Задачи. 1) Построить деревья вывода для следующих секвенций:

(а) $\to \mathfrak{B} \supset (\mathfrak{A} \supset \mathfrak{B})$;

(б) $\mathfrak{A} \supset \mathfrak{B},\ \mathfrak{A},\ \neg\mathfrak{B} \to$;

(в) $\mathfrak{A} \supset \mathfrak{B} \to \neg\mathfrak{B} \supset \neg\mathfrak{A}$;

(г) $\neg\mathfrak{A} \& \neg\mathfrak{B} \to \neg(\mathfrak{A} \vee \mathfrak{B})$;

(д) $\neg(\mathfrak{A} \vee \mathfrak{B}) \to \neg\mathfrak{A} \& \neg\mathfrak{B}$.

2) Вывести секвенцию примера 6 без сечения.

Теперь нам остается показать, что исчисление $S_0$ равносильно ранее построенным исчислениям $G_0$ и $H_0$. Достаточно установить, что секвенция $\Gamma \to \Delta$ тогда и только тогда выводима в $S_0$, когда $\Gamma' \vdash_{\overline{G_0}} \widetilde{\mathfrak{A}}^{\Delta}$, где $\Gamma'$ — множество формул, входящих в $\Gamma$, и $\widetilde{\mathfrak{A}}^{\Delta}$ есть формула $\mathfrak{B}_1 \vee \dots \vee B_k$, если $\Delta = \mathfrak{B}_1, \dots, \mathfrak{B}_k$ $(k = 1, 2, \dots)$, а если $\Delta$ — пустая последовательность, то $\widetilde{\mathfrak{A}}^{\Delta} = X_1 \& \neg X_1$. (Об исчислении $G_0$ см. выше,

[41] С привлечением средств, лежащих вне ее пределов. Доказать непротиворечивость арифметики ее собственными средствами невозможно (см. ниже, § 8.4, пункт 5).

В генценовском доказательстве непротиворечивости арифметики используется основная теорема в общем виде — для исчисления предикатов (см. предыдущую сноску). Это доказательство изложено в статьях [Генцен (а)] и [Генцен (б)].

пункт 2 этого параграфа.) В доказательстве мы опустим бо́льшую часть технических подробностей, предоставив восстановить их читателю. Далее вместо $\vdash_{G_0}$ будем писать просто $\vdash$.

а) Тот факт, что из выводимости секвенции $\Gamma \to \Delta$ следует $\Gamma' \vdash \widetilde{\mathfrak{A}}^{\wedge}$, доказывается возвратной индукцией по высоте дерева вывода секвенции. Базис очевиден, т. к. при нулевой высоте секвенция имеет вид $\mathfrak{A} \to \mathfrak{A}$. Индукционный шаг распадается на случаи, зависящие от вида нижней фигуры заключения. Случаи, отвечающие разбавлению, сокращению и перестановке, очевидны. Если нижняя фигура есть сечение, то при пустом $\Theta$ из $\Gamma \to \mathfrak{D}$ и $\mathfrak{D}, \Delta \to \Lambda$ вытекает по предположению индукции $\Gamma' \vdash \mathfrak{D}$ и $\mathfrak{D}, \Delta' \vdash \widetilde{\mathfrak{B}}^{\wedge}$, откуда $\Gamma', \Delta' \vdash \widetilde{\mathfrak{B}}^{\wedge}$ по правилу транзитивности исчисления $G_0$. При непустом $\Theta$ рассуждаем так: из $\Gamma \to \Theta$, $\mathfrak{D}$ разбавлением в антецеденте получается $\neg\widetilde{\mathfrak{B}}^{\Theta}$, $\Gamma \to \Theta, \mathfrak{D}$; отсюда в силу предположения индукции и уже проведенного индукционного шага для разбавления следует $\neg\widetilde{\mathfrak{B}}^{\Theta}, \Gamma' \vdash \widetilde{\mathfrak{B}}^{\Theta} \vee \mathfrak{D}$; но $\neg\widetilde{\mathfrak{B}}^{\Theta}, \widetilde{\mathfrak{B}}^{\Theta} \vee \mathfrak{D} \vdash \mathfrak{D}$ (см. пример (14) из § 5.3). Поэтому $\neg\widetilde{\mathfrak{B}}^{\Theta}, \Gamma' \vdash \mathfrak{D}$, а поскольку по предположению индукции справедливо также $\mathfrak{D}, \Delta' \vdash \widetilde{\mathfrak{B}}^{\wedge}$, имеем $\neg\widetilde{\mathfrak{B}}^{\Theta}, \Gamma', \Delta' \vdash \widetilde{\mathfrak{A}}^{\wedge}$, откуда $\neg\widetilde{\mathfrak{B}}^{\Theta}, \Gamma', \Delta' \vdash \widetilde{\mathfrak{A}}^{\Theta} \vee \widetilde{\mathfrak{B}}^{\wedge}$. В то же время очевидно, что $\widetilde{\mathfrak{B}}^{\Theta}, \Gamma', \Delta' \vdash \widetilde{\mathfrak{B}}^{\Theta} \vee \widetilde{\mathfrak{B}}^{\wedge}$. Далее пользуемся правилом удаления дизъюнкции и законом исключенного третьего.

Случаи, отвечающие логическим фигурам заключения, читатель разберет сам. Для всех фигур, кроме ВКА и ВДА, при непустом $\Delta$ следует рассуждать аналогично тому, как было сделано для сечения при непустом $\Theta$.

б) Обратное утверждение доказывается тоже возвратной индукцией — по высоте дерева вывода в $G_0$. И базис, и индукционный шаг распадаются здесь на случаи в зависимости от вида самого нижнего элементарного дерева — иначе говоря, от того, какое правило применялось на последнем шаге вывода. В каждом из случаев индукционного шага для каждого из деревьев, из которых данное дерево непосредственно «собирается» на последнем шаге вывода, имеется по предположению индукции соответствующее секвенциальное дерево вывода, и к этим секвенциальным деревьям вывода нужно «пристроить» снизу некоторое — для каждого случая стандартное — дерево вывода в $S_0$. Такое же стандартное секвенциальное дерево строится для соответствующего случая в базисе. Например, для правила УИ это будет дерево

$$\dfrac{\dfrac{\Gamma' \to \mathfrak{A}\supset\mathfrak{B}}{\Gamma', \Gamma'' \to \mathfrak{B}}\ \text{сечение}}{\vdots\ \text{перестановки и сокращения}}$$
$$\Gamma \to \mathfrak{B}$$

$$\dfrac{\dfrac{\Gamma'' \to \mathfrak{A} \qquad \mathfrak{B} \to \mathfrak{B}}{\mathfrak{A}\supset\mathfrak{B}, \Gamma'' \to \mathfrak{B}}\ \text{ВИА}}{}$$

(здесь $\Gamma$ — последовательность, получаемая из $\Gamma'$, $\Gamma''$ вычеркиванием повторений, если они есть), для правила ВО′ (возможного только в индукционном шаге) — дерево

$$\mathfrak{A},\ \Gamma' \to 7\mathfrak{B} \qquad \frac{\mathfrak{A},\ \Gamma'' \to \mathfrak{B}}{7\mathfrak{B},\ \mathfrak{A},\ \Gamma'' \to}\ \text{ВОА}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \text{ сечения, перестановки и сокращения}$$

$$\frac{\mathfrak{A},\ \Gamma \to}{\Gamma \to 7\mathfrak{A}}\ \text{ВОС}$$

(где $\Gamma$ имеет тот же смысл, что и в предыдущем дереве); для правила ИТ (возможного только в базисе) соответствующим секвенциальным деревом будет дерево вывода закона исключенного третьего (см. выше пример 2). Построение остальных стандартных деревьев предоставляется читателю.

**Замечание.** Проведя все опущенные рассуждения, читатель сможет убедиться, что в первой части доказательства закон исключенного третьего применяется лишь тогда, когда сукцедент содержит больше одной формулы, а во второй части единственное стандартное дерево, в котором встречаются секвенции более чем с одной формулой в сукцеденте, отвечает закону исключенного третьего. Поэтому конструктивный вариант $G_0$ равносилен исчислению $S_0$ с дополнительным условием, что сукцедент каждой секвенции содержит не более одной формулы.

5. Вскоре после появления быстродействующих цифровых вычислительных машин — которые, как известно, позволяют автоматизировать не только арифметические вычисления, но и формальные преобразования символических выражений — возникла идея использовать эти машины для автоматического построения выводов в логических исчислениях. Начиная с 50-х годов в этом направлении ведутся непрекращающиеся исследования[42]. Основная трудность связана здесь с тем, что процесс вывода в логическом исчислении — недетерминированный: после очередного шага его можно, как правило, продолжать по-разному, и поэтому построение формальных выводов требует интуиции и сообразительности точно так же, как любая математическая задача (в чем читатель, без сомнения, уже убедился). Можно, конечно, думать о том, чтобы перебирать все выводы подряд — сначала, скажем, все деревья высоты 1, потом высоты 2 и т. д.,— и отбирать те из них, которые окажутся доказательствами интересных теорем. Это, в сущности, та самая идея, на которой был основан проект механического сочинения книг «по философии, поэзии, праву, математике и богословию», предложенный одним из

[42] С методами автоматического доказательства теорем можно познакомиться по книге [Чень — Ли 1983]. См. также [Маслов 1986], гл. 8.

профессоров Академии прожектеров в Лагадо в «Путешествиях Гулливера» Свифта: выписывать подряд всевозможные комбинации слов, а среди них окажутся и все нужные книги. Несостоятельность такого подхода обнаружилась очень скоро, и с начала 60-х годов основные усилия в этом направлении сосредоточены на том, чтобы попытаться с помощью машины в какой-то мере имитировать процесс поиска вывода человеком. В частности, ищутся критерии «естественности» вывода и способы построения выводов, удовлетворяющих этим критериям. Примером такого критерия может служить упоминавшееся выше свойство подформульности; поэтому теорема Генцена находит в работах по «машинному доказательству теорем» широкое применение.

Какое же значение имеют эти исследования для математической логики и для математики в целом? Прежде всего следует сказать, что вряд ли можно рассчитывать на сколько-нибудь широкое практическое использование машин для поиска доказательств, по крайней мере в обозримом будущем. (Другое дело — автоматизация необходимых для доказательства технических выкладок. Примеры такого использования ЭВМ уже имеются: самый известный из них — решение проблемы четырех красок.) А если бы «машинное доказательство» оказалось практически возможным, вряд ли математикам стоило бы этому радоваться. Ведь новые математические идеи и методы чаще всего возникают не только и не столько благодаря новым результатам, сколько благодаря усилиям, приложенным для их получения; и если бы эти усилия стали ненужными и «ручное» (лучше сказать, «головное») доказательство теорем сохранилось бы только в виде развлечения или «гимнастики для ума», то профессия математика исчезла бы, и вслед за ней исчезла бы математическая культура (что нанесло бы непоправимый урон и общей культуре человечества, ибо математическая культура — ее неотъемлемая часть). Развитие математической науки прекратилось бы, и вскоре не осталось бы людей, способных понимать сделанное ею прежде. Надо думать, впрочем, что этого никогда не произойдет. (Для уверенности в этом есть, кроме сложности задачи, и другие основания — см. ниже, § 8.4, пункт 4.) А если так, то исследования по «автоматизации вывода» полезны, потому что благодаря им удается глубже понять природу процесса логического вывода — иначе говоря, они способствуют развитию его теории; более того, они сами ей принадлежат. Кроме того, они могут иметь значение для понимания психологии математического творчества и других творческих процессов (см. [Маслов 1986], гл. 9).

Напрашивается аналогия между автоматизацией логического вывода и автоматизацией перевода с одного естественного языка на другой. Правда, сейчас существуют уже автоматические системы,

способные более или менее удовлетворительно переводить тексты, относящиеся к определенной специальной области (например, по электротехнике)[43]; однако конкурировать с настоящим хорошим переводчиком, знающим не только оба языка, но и предмет, о котором идет речь, эти системы не могут и вряд ли смогут когда-нибудь. Что же касается автоматического перевода художественной литературы, да и вообще таких текстов, где важна не только «информация», но и стиль (а он далеко не безразличен на самом деле и в научной книге), то такого перевода не видно и в отдаленной перспективе — и это очень хорошо, потому что если бы автоматизация перевода продвинулась до такой степени, что изучение иностранных языков стало бы ненужным (о чем втайне мечтают в наше время многие «работники умственного труда» и в том числе «ученые»). это неизбежно обернулось бы таким упадком культуры, последствия которого трудно предвидеть. Но эта опасность, скорее всего, нам не грозит, а исследования по автоматизации перевода вносят определенный вклад в развитие лингвистической науки, способствуя лучшему пониманию ряда аспектов языка и выработке новых методов (в частности, экспериментальных). И в лингвистике, и в математике, и в других областях умственной деятельности человека автоматизация желательна лишь постольку, поскольку она облегчает громоздкие и однообразные операции; автоматизация творческой работы принесла бы с собой неисчислимые опасности — но она, надо надеяться, несосуществима.

Задачи и упражнения

1) Изменить правила образования формул исчисления $G_0$ так, чтобы:

(а) не было скобок вокруг элементарных подформул (т. е. переменных и $\mathit{И}$), но были наружные скобки вокруг каждой неэлементарной формулы;

(б) не было ни скобок вокруг элементарных подформул, ни наружных скобок;

(в) скобки были расставлены в соответствии с обычным соглашением о порядке действий. [Указание. Одновременно с формулой определять ее «главную связку».]

2) Иногда в математической логике используется так называемая бесскобочная запись формул[44], при которой знаки бинарных операций ставятся не между аргументами, а перед ними; например, вместо $X\&(Y \vee Z)$ пишется $\&XVYZ$, вместо $X\&Y \vee Z$ — $\vee\&XYZ$, вместо $\neg X \vee Y \supset \exists\neg(\neg X\&\neg Z)$ — $\exists\vee\neg X Y\neg\&\neg X\neg Z$. При таком способе записи формула всегда читается однозначно и скобки не нужны. Изменить алфавит и правила образования формул исчисления $G_0$ применительно к этой записи.

---

[43] См. [Апресян и др. 1989].

[44] Предложенная польским логиком Я. Лукасевичем (Jan Łukasiewicz, 1878–1956).

3) Показать, что каждое безусловное логическое правило исчисления $G_0$, кроме ИТ, можно заменить условным по следующему образцу: правило ВК приобретает вид «Если $\Gamma \vdash \mathfrak{A}$ и $\Gamma \vdash \mathfrak{B}$, то $\Gamma \vdash \mathfrak{A} \& \mathfrak{B}$». («Можно заменить» означает, что при такой замене объем понятия выводимости остается прежним.)

4) Убедиться, что правило УД равносильно следующему правилу: Если $\Gamma, \mathfrak{A} \vdash \mathfrak{C}$ и $\Gamma, \mathfrak{B} \vdash \mathfrak{C}$, а также $\Gamma' \vdash \mathfrak{A} \vee \mathfrak{B}$, то $\Gamma, \Gamma' \vdash \mathfrak{C}$.

5) Показать, что если присоединить к алфавиту $G_0$ символ $\leftrightarrow$, соответствующим образом дополнить правила образования формул и добавить правила вывода: «Если $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$ и $\Gamma, \mathfrak{B} \vdash \mathfrak{A}$, то $\Gamma \vdash \mathfrak{A} \leftrightarrow \mathfrak{B}$» (введение эквиваленции) и «$\mathfrak{A} \leftrightarrow \mathfrak{B}, \mathfrak{A} \vdash \mathfrak{B}$», «$\mathfrak{A} \leftrightarrow \mathfrak{B}, \mathfrak{B} \vdash \mathfrak{A}$» (удаление эквиваленции), то в полученном исчислении:

а) $\mathfrak{A} \supset \mathfrak{B}, \mathfrak{B} \supset \mathfrak{A} \vdash \mathfrak{A} \leftrightarrow \mathfrak{B}$;

б) $\mathfrak{A} \leftrightarrow \mathfrak{B} \vdash \mathfrak{A} \supset \mathfrak{B}$;

в) $\mathfrak{A} \leftrightarrow \mathfrak{B} \vdash \mathfrak{B} \supset \mathfrak{A}$;

г) $\mathfrak{A} \leftrightarrow \mathfrak{B} \vdash \mathfrak{B} \leftrightarrow \mathfrak{A}$

и все эти выводимости можно установить без использования закона исключенного третьего.

6) Показать, что в исчислении $G_0$:

а) $\vdash \neg(\mathfrak{A} \& \neg\mathfrak{A})$;

б) $\vdash (\neg\mathfrak{B} \supset \neg\mathfrak{A}) \supset ((\neg\mathfrak{B} \supset \mathfrak{A}) \supset \mathfrak{B})$;

в) $\vdash \mathfrak{A} \& \mathfrak{B} \vee \mathfrak{A} \& \neg\mathfrak{B} \vee \neg\mathfrak{A} \& \mathfrak{B} \vee \neg\mathfrak{A} \& \neg\mathfrak{B}$;

г) $(\mathfrak{A} \vee \mathfrak{B}) \& (\mathfrak{A} \vee \neg\mathfrak{B}) \& (\neg\mathfrak{A} \vee \mathfrak{B}) \& (\neg\mathfrak{A} \vee \neg\mathfrak{B}) \vdash \Lambda$.

7) Показать, что следующие формулы дедуктивно эквивалентны в $G_0$:

а) $\mathfrak{A} \& \neg\Lambda$ и $\mathfrak{A}$;

б) $\mathfrak{A} \& \Lambda$ и $\Lambda$;

в) $\mathfrak{A} \vee \Lambda$ и $\mathfrak{A}$;

г) $\mathfrak{A} \vee \neg\Lambda$ и $\neg\Lambda$;

д) $\mathfrak{A} \supset \Lambda$ и $\neg\mathfrak{A}$;

е) $\neg\Lambda \supset \mathfrak{A}$ и $\mathfrak{A}$;

ж) $\mathfrak{A} \supset \neg\mathfrak{A}$ и $\neg\mathfrak{A}$;

з) $\mathfrak{A}_1 \& \mathfrak{A}_2 \& \ldots \& \mathfrak{A}_n \supset \mathfrak{B}$ и $\mathfrak{A}_1 \supset (\mathfrak{A}_2 \supset \ldots \supset (\mathfrak{A}_n \supset \mathfrak{B}) \ldots)$.

8) Показать, что формула в алфавите $G_0$ тогда и только тогда является в $G_0$ теоремой, когда она дедуктивно эквивалентна $\neg\Lambda$.

9) а) Показать, что в конструктивном варианте $G_0$ из соотношения (29) параграфа 5.3 выводим закон исключенного третьего.

б,в) То же для соотношений (30), (33) параграфа 5.3.

г) Показать, что соотношение (27) параграфа 5.3 равносильно в конструктивном варианте $G_0$ *ослабленному закону исключенного третьего*: $\vdash \neg\mathfrak{A} \vee \neg\neg\mathfrak{A}$.

10) Доказать, что в конструктивном варианте $G_0$ справедливы следующие выводимости.

а) $\neg\neg\neg\mathfrak{A} \vdash \neg\mathfrak{A}$ («правило снятия тройного отрицания»);

б) $\vdash \neg\neg(\mathfrak{A} \vee \neg\mathfrak{A})$;

в) $\neg\neg Л \vdash Л$.

Попытаться дать содержательное истолкование этих фактов.

11) Показать, что в $G_0$ можно заменить закон исключенного третьего и правило Дунса Скота правилом снятия двойного отрицания (т. е. что если изъять из $G_0$ правила ИТ и ДС и добавить правило снятия двойного отрицания, то в таком исчислении можно вывести не только ИТ (с. 174), но и ДС). [Замечание. Можно доказать (подобрав подходящую модель), что ДС нельзя вывести из остальных аксиом $G_0$. Таким образом, правило снятия двойного отрицания в некотором смысле сильнее закона исключенного третьего.]

12) Доказать теорему Гливенко[45]: Если формула $\mathfrak{A}$ является теоремой в $G_0$, то формула $\neg\neg\mathfrak{A}$ — теорема в конструктивном варианте $G_0$. [Указание. Доказать, что если $\Gamma$ — множество, полученное из $\Gamma$ заменой каждой входящей в него формулы ее двойным отрицанием, то из $\Gamma \vdash_{G_0} \mathfrak{A}$ следует, что $\bar{\Gamma} \vdash \neg\neg\mathfrak{A}$ в конструктивном варианте $G_0$.]

13) Показать, что в $G_0$ можно заменить правило введения отрицания и закон исключенного третьего одним правилом: «Если $\Gamma, \neg\mathfrak{A} \vdash Л$, то $\Gamma \vdash \mathfrak{A}$» («правило доказательства от противного»).

14) а) Доказать, что всякая тождественно истинная формула в алфавите $G_0$, не содержащая знаков $\&$ и $\vee$, является теоремой в исчислении, полученном из $G_0$ изъятием знаков конъюнкции и дизъюнкции и отвечающих им правил (с соответствующим изменением правил образования формул).

б) Аналогичная задача для формул, не содержащих знака $\supset$.

15) Не пользуясь теоремой о полноте, показать, что любые две равносильные формулы в алфавите исчисления $G_0$ дедуктивно эквивалентны в $G_0$. [Указание. Воспользоваться результатом задачи 30а в конце гл. 3 и выводимостями из § 5.3.]

16) Пользуясь выводимостями из § 5.3, показать, что формула в с. д. н. ф. от переменных $X_1, \ldots, X_n$, содержащая все полные элементарные конъюнкции от этих переменных, является теоремой в $G_0$.

Замечание. Результаты задач 15 и 16 вместе с замечанием в конце пункта 1 § 3.3 дают еще одно доказательство теоремы о полноте $G_0$.

17) Сопоставим каждому логическому символу $s$ исчисления $G_0$ функцию $\varphi_s$, отображающую множество $\{0, \frac{1}{2}, 1\}$ в себя, следующим образом: $(\alpha)\varphi_{\&}(X, Y) = \min(X, Y)$; $(\beta)\ \varphi_{\vee}(X, Y) = \max(X, Y)$;

[45] Валерий Иванович Гливенко (1897—1940) — советский математик, был профессором Московского педагогического института им. К. Либкнехта.

(γ) $\varphi_{\supset}$ определяется таблицей:

| x \ y | 0 | $\frac{1}{2}$ | 1 |
|---|---|---|---|
| 0 | 1 | 1 | 1 |
| $\frac{1}{2}$ | 0 | 1 | 1 |
| 1 | 0 | $\frac{1}{2}$ | 1 |

(δ) $\varphi_{\neg}(0) = 1$, $\varphi_{\neg}\left(\frac{1}{2}\right) = \varphi_{\neg}(1) = 0$; (ε) $\varphi_{\mathfrak{J}}$ есть константа 0 («нульместная функция»). Далее, каждой формуле $\mathfrak{A}$ исчисления $G_0$ сопоставим функцию $\varphi_{\mathfrak{A}}$, полученную соответствующей суперпозицией функций, отвечающих входящим в $\mathfrak{A}$ логическим символам. (Например, если $\mathfrak{A} = \neg(X_1 \supset X_2 \& X_3)$, то $\varphi_{\mathfrak{A}}(X_1, X_2, X_3) = \varphi_{\neg}(\varphi_{\supset}(X_1, \varphi_{\&}(X_2, X_3)))$; если $\mathfrak{A} = X_1 \vee \mathfrak{J}$, то $\varphi_{\mathfrak{A}}(X_1) = \varphi_{\vee}(X_1, 0)$.

а) Доказать (возвратной индукцией по высоте дерева вывода), что если $\Gamma \vdash \mathfrak{A}$ в конструктивном варианте $G_0$, то при $\Gamma \neq \emptyset$ для любого набора значений переменных, входящих в $\mathfrak{A}$ и в формулы из $\Gamma$, в $\Gamma$ найдется такая формула $\mathfrak{B}$, что значение $\varphi_{\mathfrak{B}}$ для этого набора не превосходит значения $\varphi_{\mathfrak{A}}$, а если $\Gamma$ пусто, то $\varphi_{\mathfrak{A}}$ тождественно равна единице.

б) Пользуясь результатом пункта а), показать, что закон исключенного третьего и правило снятия двойного отрицания в конструктивном варианте $G_0$ не выполняются.

в) Аналогично предыдущему пункту показать, что в конструктивном варианте $G_0$ не имеют места выводимости (29), (30) и (33) из § 5.3.

18) Показать, что следующие формулы дедуктивно эквивалентны в исчислении $H_0$:

а) $\mathfrak{A} \supset \mathfrak{B}$ и $\neg\mathfrak{A} \vee \mathfrak{B}$;

б) $\mathfrak{A} \supset \mathfrak{B}$ и $\neg(\mathfrak{A} \& \neg\mathfrak{B})$;

в) $\mathfrak{A} \vee \mathfrak{B}$ и $\neg\mathfrak{A} \supset \mathfrak{B}$;

г) $\mathfrak{A} \& \mathfrak{B}$ и $\neg(\mathfrak{A} \supset \neg\mathfrak{B})$;

д) $\mathfrak{A} \& \mathfrak{B} \supset \mathfrak{C}$ и $\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{C})$;

е) $\mathfrak{A} \supset (\mathfrak{B} \supset \mathfrak{C})$ и $\mathfrak{B} \supset (\mathfrak{A} \supset \mathfrak{C})$.

19) Показать, что исчисления $H_0$ и $H_0'$ равносильны в каждом из следующих двух смыслов:

а) Формула в алфавите $H_0'$ выводима в $H_0'$ из множества формул в $H_0$ тогда и только тогда, когда она выводима из него в $H_0$.

б) Формула в алфавите $H_0$ выводима в $H_0$ из множества формул в $H_0$ тогда и только тогда, когда она выводима из него в исчислении, полученном из $H_0'$ соответствующим расширением алфавита и правил

образования формул и добавлением четырех новых схем аксиом: $\mathfrak{A} \vee \mathfrak{B} \supset (\neg\mathfrak{A} \supset \mathfrak{B})$; $(\neg\mathfrak{A} \supset \mathfrak{B}) \supset \mathfrak{A} \vee \mathfrak{B}$; $\mathfrak{A} \& \mathfrak{B} \supset \neg(\mathfrak{A} \supset \neg\mathfrak{B})$; $\neg(\mathfrak{A} \supset \neg\mathfrak{B}) \supset \mathfrak{A} \& \mathfrak{B}$.

20) а) Показать, что исчисление, полученное из $H_0$ заменой схем аксиом 2 и 3 одной схемой $(\neg\mathfrak{B} \supset \neg\mathfrak{A}) \supset ((\neg\mathfrak{B} \supset \mathfrak{A}) \supset \mathfrak{B})$, равносильно $H_0$.

б) То же для исчисления, полученного из $H_0$ заменой схем 2 и 3 схемой $\neg\neg\mathfrak{A} \supset \mathfrak{A}$.

21) Показать, что в исчислении $S_0$ (и даже в его конструктивном варианте) из секвенции $\rightarrow \mathfrak{A} \& \neg\mathfrak{A}$ выводима пустая секвенция $\rightarrow$, и обратно.

22) Пользуясь основной теоремой Генцена, показать, что

а) в $S_0$ невыводима пустая секвенция (ввиду результата предыдущей задачи это означает, что $S_0$ непротиворечиво);

б) если в конструктивном варианте $S_0$ выводима секвенция вида $\rightarrow \mathfrak{A} \vee \mathfrak{B}$, то в нем выводима хотя бы одна из секвенций $\rightarrow \mathfrak{A}$ и $\rightarrow \mathfrak{B}$ (**теорема Генцена о дизъюнкции**, показывающая, что в конструктивном исчислении предложений дизъюнкция ведет себя в соответствии с ее содержательным конструктивным пониманием).

23) Пользуясь теоремой Генцена о дизъюнкции (см. предыдущую задачу), доказать невыводимость в конструктивном варианте $S_0$ закона исключенного третьего (без использования интерпретаций — в отличие от задачи 17).

ГЛАВА 6

# СИНТАКСИС ЛОГИКИ ПРЕДИКАТОВ

## § 6.1. ИСЧИСЛЕНИЕ $G_1$

1. Для изучения синтаксиса логики предикатов мы будем пользоваться тем же аппаратом, с помощью которого в предыдущей главе изучался синтаксис логики предложений — логическими исчислениями. Основное изложение будем вести на базе построенного Г. Генценом исчисления естественного вывода, которое будет обозначаться $G_1$. Это исчисление предназначено для формализации логики предикатов в расширенном варианте, описанном в § 4.3 — с функциональными символами и символами констант.

2.1. А л ф а в и т исчисления $G_1$ есть объединение следующих шести попарно непересекающихся множеств:

$\{F_n^k \mid n, k = 1, 2, \ldots\}$ (множество *предикатных символов*);

$\{f_n^k \mid n, k = 1, 2, \ldots\}$ (множество *функциональных символов*);

$\{x_1, x_2, \ldots\}$ (множество (*предметных*) *переменных*);

$\{a_1, a_2, \ldots\}$ (множество *символов предметных констант*);

$\{\&, \vee, \supset, \neg, \forall, \exists, \Lambda\}$ (множество *логических символов*);

$\{(,), ,\}$ (множество *синтаксических символов*).

Пояснения. а) Верхние индексы при предикатных и функциональных символах означают их вместимости. Поэтому символы с верхним индексом $k$ мы будем называть *$k$-местными*.

б) Переменные, являющиеся элементами нашего алфавита, мы печатаем курсивным шрифтом в отличие от «неформальных» переменных, для которых мы используем прямой шрифт.

в) Запятую — элемент нашего алфавита мы печатаем здесь жирным шрифтом, чтобы не смешивать ее с «неформальной» запятой. В дальнейшем, однако, опасность такого смешения возникать не будет, и «формальная» запятая будет печататься обычным шрифтом.

II. Поскольку в формулы нашего исчисления могут входить слож-

ные термы, правилам образования формул нужно предпослать п р а в и л а о б р а з о в а н и я т е р м о в. Вот они:

($\alpha$) Каждая переменная есть терм.

($\beta$) Каждая предметная константа есть терм.

($\gamma$) Если $f_n^k$ — $k$-местный функциональный символ и $t_1, \ldots, t_k$ — термы, то $f_n^k(t_1, \ldots, t_k)$ также есть терм.

($\delta$) Всякий терм является таковым в силу одного из правил ($\alpha$), ($\beta$), ($\gamma$).

Теперь мы можем сформулировать правила образования формул исчисления $G_1$:

(а) Если $F_n^k$ — $k$-местный предикатный символ и $t_1, \ldots, t_k$ — термы, то $F_n^k(t_1, \ldots, t_k)$ есть формула.

(б) $A$ есть формула.

(в) Если $\mathfrak{A}$ и $\mathfrak{B}$ — формулы, то $(\mathfrak{A})\&(\mathfrak{B})$, $(\mathfrak{A})\vee(\mathfrak{B})$, $(\mathfrak{A})\supset(\mathfrak{B})$ — также формулы.

(г) Если $\mathfrak{A}$ — формула, то $\neg(\mathfrak{A})$ — также формула.

(д) Если $\mathfrak{A}$ — формула и $x$ — переменная, то $\forall x\mathfrak{A}$ и $\exists x\mathfrak{A}$ — также формулы.

(е) Всякая формула является таковой в силу одного из правил (а) — (д).

Таким образом, системы правил образования термов и формул — индуктивные; каждая из них содержит несколько прямых правил и одно косвенное.

Формулы, образованные по правилам (а) и (б), называются *атомными*.

Обычно мы будем опускать в формулах часть скобок, придерживаясь прежнего соглашения о порядке действий.

*Сложность формулы* определяется как число вхождений в нее логических символов, отличных от $A$.

Если существуют свободные, соответственно связанные вхождения переменной $x$ в формулу $\mathfrak{A}$, мы будем говорить, что $x$ *входит* в $\mathfrak{A}$ *свободно (связанно)*.

Через $\mathfrak{A}\frac{t}{x}$, где $\mathfrak{A}$ — формула, $x$ — переменная и $t$ — терм, будет обозначаться *результат подстановки* $t$ *вместо* $x$ *в* $\mathfrak{A}$, т. е. формула, полученная из $\mathfrak{A}$ замещением всех свободных вхождений $x$ вхождениями $t$. Но вместо этого обозначения мы обычно будем пользоваться другим, более традиционным. Именно, произвольную формулу $\mathfrak{A}$ мы будем иногда обозначать $\mathfrak{A}(x)$, где $x$ — переменная (не обязательно входящая в $\mathfrak{A}$!), и тогда в пределах «области действия» этого обозначения вместо $\mathfrak{A}\frac{t}{x}$ будем писать $\mathfrak{A}(t)$. В частности, если $x$ не входит свободно в $\mathfrak{A}$, то $\mathfrak{A}(t) = \mathfrak{A}(x)$ (в другой записи: $\mathfrak{A}\frac{t}{x} = \mathfrak{A}$). Понятен также смысл обозначения $\mathfrak{A}(x, y)$ и вслед за ним $\mathfrak{A}(t_1, t_2)$ и т. п.

Следует заметить, что в очень ясном на первый взгляд понятии подстановки терма в формулу вместо переменной таится «подводный камень». Допустим ради простоты, что в формулу $\mathfrak{A}(x)$ не входят свободно никакие переменные, кроме $x$, а терм $t$ есть просто другая переменная, скажем, $y$. Тогда в произвольной интерпретации формула $\mathfrak{A} = \mathfrak{A}(x)$ перейдет в одноместный предикат $\Phi(x)$, и естественно ожидать, что $\mathfrak{A}(y)$ перейдет в тот же самый предикат, только с другим обозначением аргумента. Так оно и будет, например, для формулы $\mathfrak{A}(x_2) = \exists x_1 F_1^2(x_1, x_2) \& F_1^1(x_2)$ при $x = x_2$, $y = x_3$; если мы возьмем в качестве основного множества интерпретации, скажем, множество всех действительных чисел и будем интерпретировать $F_1^2(a, b)$ и $F_1^1(a)$ как предикаты $a^2 = b$ и $a \leq 0$, то формула $\mathfrak{A}(x_2)$ превратится в предикат $\exists x_1(x_1^2 = x_2) \& (x_2 \leq 0)$, истинностное значение которого есть *И* при $x_2 = 0$ и *Л* при $x_2 \neq 0$, и в точно такой же предикат, только от $x_3$, превратится формула $\mathfrak{A}(x_3)$. Но если в качестве $y$ взять $x_1$, картина изменится: в той же интерпретации формула $\mathfrak{A}(x_1)$ превращается в предикат $\exists x_1(x_1^2 = x_1) \& (x_1 \leq 0)$, равносильный предикату $x_1 \leq 0$. Произошло это потому, что свободное вхождение $x_2$ превратилось после замены в связанное вхождение $x_1$. Подобный нежелательный эффект может возникнуть и при подстановке сложного терма; так, если в том же примере подставить вместо $x_2$ терм $f_1^1(x_i)$ и истолковать $f_1^1(a)$ как $a + 2$, то при $i \neq 1$ получится предикат, истинностное значение которого есть *И* при $x_i = -2$ и *Л* при $x_i \neq -2$, а при $i = 1$ — тождественно ложный предикат (т. к. ни один из корней уравнения $x_1^2 = x_1 + 2$ не удовлетворяет неравенству $x_1 + 2 \leq 0$). На такие «неправильные подстановки» необходимо наложить запрет[1], что и будет сделано при формулировке правил вывода: в эти правила войдет условие, чтобы ни одно свободное вхождение заменяемой переменной $x$ в формулу $\mathfrak{A}$ не содержалось в области действия квантора по какой-либо переменной, входящей в терм $t$. Если это условие выполняется, говорят, что *терм $t$ свободен для подстановки вместо $x$ в формулу $\mathfrak{A}$*.

[1] В естественном языке аналогом этого запрета (правда, неполным) служит невозможность использовать местоимения в качестве собственных имен. В правилом у многих народов (в том числе и у русских) едва ли не любое существительное и прилагательное могло быть личным именем, но местоимения, кажется, никогда или почти никогда не употреблялись для этой цели, потому что высказывание, содержащее такое имя, было бы очень легко понять неправильно. (Например, услышав в ответ на вопрос «Кто это сделал?» имя «Никто», спрашивающий может решить, что виновника не существует. Этим, как известно, воспользовался хитроумный Одиссей, чтобы спастись от циклопа Полифема.)

Замечание. Очевидно, что (а) всякая переменная свободна для подстановки вместо самой себя в любую формулу; (б) терм, не содержащий переменных, свободен для подстановки вместо любой переменной в любую формулу; (в) переменная, не входящая в формулу связанно, свободна для подстановки в эту формулу вместо любой переменной.

III. Система правил вывода исчисления $G_1$ получается из соответствующей системы исчисления $G_0$ добавлением четырех новых логических правил:

| | |
|---|---|
| 11) Если $\Gamma \vdash \mathfrak{A}$ и переменная $x$ не входит свободно ни в одну формулу из $\Gamma$, то $\Gamma \vdash \forall x \mathfrak{A}$ (*введение общности*); | 12) $\forall x \mathfrak{A}(x) \vdash \mathfrak{A}(t)$, где $x$ — переменная и $t$ — терм, свободный для подстановки вместо $x$ в $\mathfrak{A}$ (*удаление общности*); |
| 13) $\mathfrak{A}(t) \vdash \exists x \mathfrak{A}(x)$, где $x$ — переменная и $t$ — терм, свободный для подстановки вместо $x$ в $\mathfrak{A}$ (*введение существования*); | 14) Если $\Gamma, \mathfrak{A} \vdash \mathfrak{C}$ и переменная $x$ не входит свободно ни в одну формулу из $\Gamma$ и в $\mathfrak{C}$, то $\Gamma, \exists x \mathfrak{A} \vdash \mathfrak{C}$ (*удаление существования*). |

Сокращенно эти правила будут обозначаться В∀, У∀, В∃, У∃.

Пояснение. В § 5.2 мы видели, что каждое логическое правило исчисления $G_0$ представляет собой формализацию одного из простейших «правил логического вывода», используемых в обычных математических рассуждениях. То же верно и для новых правил: если, фиксировав произвольный элемент $x$ заданного множества, мы доказали, что он (при некотором условии $\Gamma$) обладает свойством $A$, то мы можем заключить, что этим свойством (при условии $\Gamma$) обладают все элементы множества (В∀)[2]; из утверждения «Все элементы данного множества обладают свойством $A$» следует, что для любого элемента $t$ этого множества справедливо утверждение «$t$ обладает свойством $A$» (У∀), и из справедливости этого утверждения хотя бы для одного элемента множества вытекает утверждение «В данном множестве существует элемент, обладающий свойством $A$» (У∃); наконец, если для фиксированного, но произвольного элемента множества из того, что он обладает свойством $A$, следует (при условии $\Gamma$) утверждение $C$, то это утверждение будет следовать (при условии $\Gamma$) также из существования в данном множестве элемента, обладающего свойством $A$ (У∃).

Содержащееся в правилах В∀ и У∃ требование, чтобы переменная $x$ не входила свободно в формулы из $\Gamma$, обеспечивает произволь-

[2] Это пояснение будет понятнее, если вместо $\mathfrak{A}$ писать $\mathfrak{A}(x)$, на что мы всегда имеем право. То же относится к пояснению правила У∃ (см. ниже).

ность элемента $x$: если бы какая-нибудь формула $\mathfrak{B}\in\Gamma$ содержала свободные вхождения $x$, то речь шла бы уже не о произвольном $x$, а только о таком, который удовлетворяет условию $\mathfrak{B}(x)$. Понятно, почему в УЭ $x$ не должно входить свободно и в $\mathfrak{C}$: в противном случае выводимость $\Gamma, \mathfrak{A} \vdash \mathfrak{C}$ будет означать только то, что если элемент $x$ обладает свойством $A$, то т о т ж е с а м ы й $x$ должен обладать и свойством $C$. О смысле требования, чтобы в УВ и ВЭ терм $t$ был свободен для подстановки вместо $x$ в $\mathfrak{A}$, мы уже говорили: при несоблюдении этого требования $\mathfrak{A}(x)$ и $\mathfrak{A}(t)$ могут просто-напросто оказаться разными предикатами.

Задача. а) Убедиться, что при отказе от ограничения в одном из новых правил стали бы доказуемыми (без изменения остальных правил $G_i$) следующие формулы:

$\forall y(F_1^1(y)\supset\forall xF_1^1(x))$ — для ВВ;

$\forall x\exists yF_1^2(x, y)\supset\exists yF_1^2(y, y)$ — для УВ;

$\forall yF_1^2(y, y)\supset\exists x\forall yF_1^2(x, y)$ — для ВЭ;

$\forall x((F_1^1(x)\supset F_2^1(x))\supset(\exists xF_1^1(x)\supset F_2^1(x)))$ — для УЭ.

б) Подобрав для формул пункта а) подходящие интерпретации, убедиться, что из них можно получить следующие утверждения: «Всякое натуральное число равно нулю» — из первой и из четвертой; «Существует натуральное число, которое больше самого себя» — из второй; «Существует натуральное число, равное всем натуральным числам» — из третьей.

Замечание. Если вспомнить, что кванторы общности и существования можно понимать как «бесконечную конъюнкцию» и «бесконечную дизъюнкцию» (см. замечание на с. 141), то станет ясно, что правила введения и удаления общности существования — это, в сущности, распространенные на «бесконечный случай» правила введения и удаления конъюнкции и дизъюнкции. (Чтобы убедиться в этом для правила ВК, нужно взять его в форме, указанной в задаче 3 в конце гл. 5.)

3. Теперь нам нужно дополнить данное в § 5.3 определение дерева вывода — указать, как изображается в нем применение новых правил. Для безусловных правил УВ и ВЭ это совсем просто: соответствующие элементарные шаги вывода будут изображаться так же, как для прочих безусловных правил. Сходным образом изобразится и применение ВВ: ему будет соответствовать горизонтальная черта, сверху от которой пишется формула $\mathfrak{A}$, а снизу — формула $\forall x\mathfrak{A}$; однако в отличие от безусловных правил здесь придется следить, чтобы зеленые листья дерева с корнем $\mathfrak{A}$ не содержали свободных вхождений $x$. Остается правило УЭ, которое мы изобразим аналогич-

но УД: его применению будет отвечать горизонтальная черта, снизу от которой записывается формула $\mathfrak{C}$, а сверху — $\exists x\mathfrak{A}$ и та же формула $\mathfrak{C}$, причем она должна быть корнем дерева вывода, среди зеленых листьев которого имеются все формулы, составляющие $\Gamma$, и формула $\mathfrak{A}$; при «достройке» меньшего дерева до большего лист $\mathfrak{A}$ увядает.

Теперь мы можем получить точное определение дерева вывода в исчислении $G_1$ из соответствующего определения для $G_0$ (§ 5.3, пункт 1), переименовав косвенный пункт 6 в пункт 8 и добавив два новых прямых пункта:

6) Пусть $\delta$ — дерево вывода высоты $n$ с корнем $\mathfrak{A}$, множеством зеленых листьев $\Gamma$ и множеством увядших листьев $\Delta$, и $x$ — переменная, не входящая свободно ни в одну формулу из $\Gamma$. Тогда выражение, состоящее из горизонтальной черты, снизу от которой записана формула $\forall x\mathfrak{A}$, а сверху — дерево $\delta$, будет деревом вывода высоты $n+1$ с корнем $\forall x\mathfrak{A}$, множеством зеленых листьев $\Gamma$ и множеством увядших листьев $\Delta$.

7) а) Пусть $\delta$ — дерево вывода высоты $n$ с корнем $\mathfrak{C}$, множеством зеленых листьев $\Gamma$ и множеством увядших листьев $\Delta$, причем $\Gamma$ содержит формулу $\mathfrak{A}$ и переменная $x$ не входит свободно ни в одну формулу из $\Gamma$, кроме $\mathfrak{A}$, и в формулу $\mathfrak{C}$. Тогда выражение, состоящее из горизонтальной черты, снизу от которой записана формула $\mathfrak{C}$, а сверху в произвольном порядке дерево $\delta$ и формула $\exists x\mathfrak{A}$, будет деревом вывода высоты $n+1$ с корнем $\mathfrak{C}$, множеством зеленых листьев $(\Gamma\setminus\{\mathfrak{A}\})\cup\{\exists x\mathfrak{A}\}$ и множеством увядших листьев $\Delta\cup\{\mathfrak{A}\}$.

б) Аналогично а) со следующими изменениями: вместо формулы $\exists x\mathfrak{A}$ над чертой записывается некоторое дерево вывода $\delta'$ с корнем $\exists x\mathfrak{A}$, множеством зеленых листьев $\Gamma'$ и множеством увядших листьев $\Delta'$; $n$ есть наибольшая из высот деревьев $\delta$ и $\delta'$, множество зеленых листьев нового дерева есть $(\Gamma\setminus\{\mathfrak{A}\})\cup\Gamma'$, множество увядших листьев — $\Delta\cup\Delta'\cup\{\mathfrak{A}\}$.

Следует также иметь в виду, что, введя два новых безусловных правила, мы расширили объем понятия элементарного дерева вывода и тем самым фактически изменили пункты 1) и 2) нашего определения.

4. Перейдем теперь к примерам формальных выводов в $G_1$. Заметим прежде всего, что — поскольку в $G_1$ действуют все правила вывода исчисления $G_0$ — приведенные в § 5.3 «схемы выводов» для $G_0$ годятся и для $G_1$[3]; поэтому сейчас нас будут интересовать только выводы с применением новых правил.

---

[3] Отсюда следует, между прочим, что всякая формула исчисления $G_1$, являющаяся частным случаем теоремы исчисления $G_0$, есть теорема $G_1$ и может быть доказана в $G_1$ без применения новых правил.

Во всех примерах буквы $x$, $y$ будут означать произвольные переменные.

(1) $\forall x\forall y\mathfrak{A} \vdash \forall y\forall x\mathfrak{A}$.

Доказательство:

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall x\forall y\mathfrak{A}(x, y)}{\forall y\mathfrak{A}(x, y)}\,\text{У}\forall}{\mathfrak{A}(x, y)}\,\text{У}\forall}{\forall x\mathfrak{A}(x, y)}\,\text{В}\forall}{\forall y\forall x\mathfrak{A}(x, y)}\,\text{В}\forall$$

(2) $\exists x\exists y\mathfrak{A} \vdash \exists y\exists x\mathfrak{A}$.

Доказательство:

$$\dfrac{\dfrac{1\ \dfrac{[\mathfrak{A}(x, y)]^{(3)}}{\exists x\mathfrak{A}(x, y)}\,\text{В}\exists}{2\ \exists y\exists x\mathfrak{A}(x, y)}\,\text{В}\exists \qquad [\exists y\mathfrak{A}(x, y)]^{(4)}}{3\ \exists y\exists x\mathfrak{A}(x, y)}\,\text{У}\exists \qquad \exists x\exists y\mathfrak{A}(x, y)}{4\ \exists y\exists x\mathfrak{A}(x, y)}\,\text{У}\exists$$

(3) $\forall x\neg\mathfrak{A} \vdash \neg\exists x\mathfrak{A}$.

Доказательство:

$$\dfrac{1\ \dfrac{\forall x\neg\mathfrak{A}(x)}{\neg\mathfrak{A}(x)}\,\text{У}\forall \qquad [\mathfrak{A}(x)]^{(3)}}{2\ \dfrac{\mathit{Л}}{3\ \dfrac{\mathit{Л}}{\neg\exists x\mathfrak{A}(x)}\,\text{В}\neg}\,\text{У}\neg \qquad [\exists x\mathfrak{A}(x)]^{(4)}}\,\text{У}\exists$$

(4) $\neg\exists x\mathfrak{A} \vdash \forall x\neg\mathfrak{A}$.

Доказательство:

$$\dfrac{1\ \dfrac{[\mathfrak{A}(x)]^{(3)}}{\exists x\mathfrak{A}(x)} \qquad \neg\exists x\mathfrak{A}(x)}{2\ \dfrac{\mathit{Л}}{3\ \dfrac{\neg\mathfrak{A}(x)}{\forall x\neg\mathfrak{A}(x)}}\,\text{В}\forall}\,\text{В}\neg$$

(5) $\exists x\neg\mathfrak{A} \vdash \neg\forall x\mathfrak{A}$.

Доказательство:

$$\dfrac{\dfrac{\dfrac{|\forall x\mathfrak{A}(x)\ |(3)}{\mathfrak{A}(x)}\qquad |\neg\mathfrak{A}(x)\ |(4)}{\dfrac{\dfrac{Л}{\neg\forall x\mathfrak{A}(x)}\qquad \exists x\neg\mathfrak{A}(x)}{\neg\forall x\mathfrak{A}(x)}}}{}\ \begin{matrix}1\\2\\3\\4\end{matrix}$$

*(6) $\neg\forall x\mathfrak{A} \vdash \exists x\neg\mathfrak{A}$.

Доказательство:

$$\dfrac{\dfrac{\dfrac{|\neg\mathfrak{A}(x)\ |(3)}{\exists x\neg\mathfrak{A}(x)}\qquad |\neg\exists x\neg\mathfrak{A}(x)\ |(k)}{\dfrac{\dfrac{Л}{\neg\neg\mathfrak{A}(x)}}{\dfrac{\mathfrak{A}(x)}{\forall x\mathfrak{A}(x)}\qquad \neg\forall x\mathfrak{A}(x)}}}{k\ \dfrac{Л}{\neg\neg\exists x\neg\mathfrak{A}(x)}}\ \begin{matrix}1\\2\\3\end{matrix}$$
$$\exists x\neg\mathfrak{A}(x)$$

Опущенные фрагменты дерева (заменяющие пунктирными линиями) аналогичны примеру (23) из § 5.3. Шагу, на котором устраняется промежуточная гипотеза $\neg\exists x\neg\mathfrak{A}(x)$, для большей ясности приписан условный номер k.

Читателю рекомендуется, учитывая замечание в конце пункта 2 этого параграфа, убедиться, что доказательства выводимостей (3), (4), (5) совершенно аналогичны доказательствам выводимостей (24), (25), (26) из § 5.3. (Но для (6) мы дали доказательство, непохожее на пример (27) из § 5.3 и более сложное. Полезно попытаться объяснить, почему аналогия здесь «не проходит», а также дать для примера (27) из § 5.3 доказательство, аналогичное только что приведенному для примера (6).)

Доказанные шесть выводимостей были аналогами равносильностей групп I и II из § 4.2; следующие восемь будут аналогами равносильностей группы III. Из них (8) — (13) имеют место лишь при условии, что формула $\mathfrak{B}$ не содержит свободных вхождений $x$; (7) и (14) справедливы без ограничений.

(7) $\forall x(\mathfrak{A}\&\mathfrak{B}) \vdash \forall x\mathfrak{A}\&\mathfrak{B}$.

(8) $\forall x\mathfrak{A}\&\mathfrak{B} \vdash \forall x(\mathfrak{A}\&\mathfrak{B})$.

*(9) $\forall x(\mathfrak{A}\vee\mathfrak{B}) \vdash \forall x\mathfrak{A}\vee\mathfrak{B}$.

(10) $\forall x\mathfrak{A}\vee\mathfrak{B} \vdash \forall x(\mathfrak{A}\vee\mathfrak{B})$.

(11) $\exists x(\mathfrak{A}\&\mathfrak{B}) \vdash \exists x\mathfrak{A}\&\mathfrak{B}$.

(12) $\exists x\mathfrak{A}\&\mathfrak{B} \vdash \exists x(\mathfrak{A}\&\mathfrak{B})$.

(13) $\exists x(\mathfrak{A}\vee\mathfrak{B}) \vdash \exists x\mathfrak{A}\vee\mathfrak{B}$.

(14) $\exists x\mathfrak{A}\vee\mathfrak{B} \vdash \exists x(\mathfrak{A}\vee\mathfrak{B})$.

Мы докажем четыре из этих выводимостей: (7), (9), (11) и (12). Доказательство остальных предоставляется читателю.

Доказательство выводимости (7):

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall x(\mathfrak{A}(x)\&\mathfrak{B})}{\mathfrak{A}(x)\&\mathfrak{B}}}{\mathfrak{A}(x)}}{\forall x\mathfrak{A}(x)} \qquad \dfrac{\dfrac{\forall x(\mathfrak{A}(x)\&\mathfrak{B})}{\mathfrak{A}(x)\&\mathfrak{B}}}{\mathfrak{B}}}{\forall x\mathfrak{A}(x)\&\mathfrak{B}}$$

Доказательство выводимости (9):

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall x(\mathfrak{A}(x)\vee\mathfrak{B})}{\mathfrak{A}(x)\vee\mathfrak{B}}\,\text{УВ} \quad |\neg\mathfrak{B}|}{\dfrac{\mathfrak{A}(x)}{\forall x\mathfrak{A}(x)}\,\text{ВВ}}\,\text{ВД}}{\forall x\mathfrak{A}(x)\vee\mathfrak{B}} \qquad \dfrac{\dfrac{\dfrac{\forall x(\mathfrak{A}(x)\vee\mathfrak{B}) \quad |\mathfrak{B}|}{\mathfrak{B}}\,\text{ТВ}}{\forall x\mathfrak{A}(x)\vee\mathfrak{B}}\,\text{ВД} \quad \dfrac{}{\mathfrak{B}\vee\neg\mathfrak{B}}\,\text{ИТ}}{\forall x\mathfrak{A}(x)\vee\mathfrak{B}}\,\text{УД}$$

Опущенная часть дерева (замененная пунктирной линией) аналогична примеру (14) из § 5.3.

Доказательство выводимости (11):

$$\dfrac{\dfrac{\dfrac{\dfrac{1\ \dfrac{|\mathfrak{A}(x)\&\mathfrak{B}|(5)}{\mathfrak{A}(x)}\,\text{УК}}{2\ \dfrac{\mathfrak{A}(x)}{\exists x\mathfrak{A}(x)}\,\text{ВЭ}} \quad 3\ \dfrac{|\mathfrak{A}(x)\&\mathfrak{B}|(5)}{\mathfrak{B}}\,\text{УК}}{4\ \dfrac{\exists x\mathfrak{A}(x)\quad\mathfrak{B}}{\exists x\mathfrak{A}(x)\&\mathfrak{B}}\,\text{ВК}} \qquad \dfrac{\exists x(\mathfrak{A}(x)\&\mathfrak{B})}{\exists x\mathfrak{A}(x)\&\mathfrak{B}}}{5\ \dfrac{\exists x\mathfrak{A}(x)\&\mathfrak{B}}{\exists x\mathfrak{A}(x)\&\mathfrak{B}}}$$

Доказательство выводимости (12):

$$\dfrac{\dfrac{\dfrac{\dfrac{1\ \dfrac{\exists x\mathfrak{A}(x)\&\mathfrak{B}}{\mathfrak{B}}\,\text{УК}}{2\ \dfrac{\mathfrak{B}\quad|\mathfrak{A}(x)|(5)}{\mathfrak{A}(x)\&\mathfrak{B}}\,\text{ВК}}}{3\ \dfrac{\mathfrak{A}(x)\&\mathfrak{B}}{\exists x(\mathfrak{A}(x))\&\mathfrak{B}}\,\text{ВЭ}} \qquad 4\ \dfrac{\exists x(\mathfrak{A}(x)\&\mathfrak{B})}{\exists x\mathfrak{A}(x)}\,\text{УК}}{5\ \dfrac{\exists x(\mathfrak{A}(x)\&\mathfrak{B})}{\exists x(\mathfrak{A}(x)\&\mathfrak{B})}\,\text{УЭ}}$$

В выводе (9) отсутствие свободных вхождений $x$ в $\mathfrak{B}$ необходимо для применимости ВВ, в (11) и (12) — для применимости УЭ.

**Задача.** Для каждой из выводимостей (8) — (13) убедиться, подобрав подходящие формулы и интерпретации (аналогично задаче в конце пункта 2 этого параграфа), что если бы она была справедлива без ограничений, то из нее следовало бы некоторое заведомо ложное утверждение.

Следующие две выводимости, служащие аналогами основных равносильностей группы IV из § 4.2, справедливы при условии, что $y$ не входит в $\mathfrak{A}(x)$ свободно и никакое свободное вхождение $x$ в $\mathfrak{A}(x)$ не находится в области действия квантора по $y$:

(15) $\forall x\mathfrak{A}(x) \vdash \forall y\mathfrak{A}(y)$.

(16) $\exists x\mathfrak{A}(x) \vdash \exists y\mathfrak{A}(y)$.

Доказательство выводимости (15):

$$\frac{\dfrac{\forall x\mathfrak{A}(x)}{\mathfrak{A}(y)}\ \forall\forall}{\forall y\mathfrak{A}(y)}\ B\forall$$

Выводимость (16) читатель докажет сам.

Добавим теперь к полученному запасу выводимостей еще одну:

(17) $\forall x\mathfrak{A} \vdash \exists x\mathfrak{A}$.

Доказательство предоставляется читателю.

**Задача.** Доказать, что в исчислении $G_1$:

(а) $\exists y\forall x\mathfrak{A} \vdash \forall x\exists y\mathfrak{A}$;

(б) $\forall x(\mathfrak{A}\&\mathfrak{B}) \vdash \forall x\mathfrak{A}\&\forall x\mathfrak{B}$;

(в) $\forall x\mathfrak{A}\&\forall x\mathfrak{B} \vdash \forall x(\mathfrak{A}\&\mathfrak{B})$;

(г) $\exists x(\mathfrak{A}\vee\mathfrak{B}) \vdash \exists x\mathfrak{A}\vee\exists x\mathfrak{B}$;

(д) $\exists x\mathfrak{A}\vee\exists x\mathfrak{B} \vdash \exists x(\mathfrak{A}\vee\mathfrak{B})$;

(е) $\forall x\mathfrak{A}\vee\forall x\mathfrak{B} \vdash \forall x(\mathfrak{A}\vee\mathfrak{B})$;

(ж) $\exists x(\mathfrak{A}\&\mathfrak{B}) \vdash \exists x\mathfrak{A}\&\exists x\mathfrak{B}$;

(з) $\forall x(\mathfrak{A}\supset\mathfrak{B}) \vdash \forall x\mathfrak{A}\supset\forall x\mathfrak{B}$;

(и) $\forall x(\mathfrak{A}\supset\mathfrak{B}) \vdash \exists x\mathfrak{A}\supset\exists x\mathfrak{B}$.

5. В заключение параграфа отметим некоторые простые свойства исчисления $G_1$.

1) Для $G_1$ сохраняют силу леммы 1, 2, 3 из § 5.3 (пункт 3); их доказательства можно повторить слово в слово.

2) Для исчисления $G_1$ можно ввести понятие *дедуктивной эквивалентности* формул, дословно повторив соответствующее определение для $G_0$ (§ 5.3, пункт 4). Имеет место для $G_1$ и теорема о замене

дедуктивно эквивалентных формул. Формулируется она так же, как соответствующая теорема для $G_0$ (§ 5.3, пункт 4), и так же доказывается, с той только разницей, что в индукционном шаге к случаям (а), (б), (в) добавляется еще случай (г) $\mathfrak{A} = Qx(\mathfrak{C})$, где $Q$ — один из знаков $\forall$, $\exists$ и $x$ — переменная. При $Q = \forall$ дедуктивная эквивалентность формул $\mathfrak{A} = \forall x(\mathfrak{C})$ и $\mathfrak{A}' = \forall x(\mathfrak{C}')$ (при условии, что $\mathfrak{C}$ и $\mathfrak{C}'$ дедуктивно эквивалентны) доказывается так: поскольку $\mathfrak{C} \vdash \mathfrak{C}'$ по условию и $\forall x(\mathfrak{C}) \vdash \mathfrak{C}$ по У$\forall$, имеем $\forall x(\mathfrak{C}) \vdash \mathfrak{C}'$, откуда $\forall x(\mathfrak{C}) \vdash \forall(\mathfrak{C}')$ по В$\forall$: так же получается обратная выводимость. При $Q = \exists$ рассуждаем аналогично, пользуясь правилами В$\exists$ и У$\exists$.

3) Теорема о приведении формул к префиксной нормальной форме (см. § 4.2) может быть усилена теперь следующим образом: для всякой формулы в алфавите исчисления $G_1$ можно построить формулу в префиксной нормальной форме (в том же алфавите), равносильную и дедуктивно эквивалентную данной.

В самом деле, просмотрев доказательство теоремы из § 4.2, мы легко убедимся, пользуясь выводимостями (3) — (16) и теоремой о замене дедуктивно эквивалентных формул, что каждое из преобразований, производимых при приведении к п. н. ф., переводит формулу в дедуктивно эквивалентную. (Добавление к алфавиту логической константы $\Lambda$ ничего не меняет в доказательстве.)

## § 6.2. СЕМАНТИЧЕСКАЯ ПРИГОДНОСТЬ И ПОЛНОТА ИСЧИСЛЕНИЯ $G_1$

1. **Теорема 1 (о семантической пригодности исчисления $G_1$).** Если формула $\mathfrak{A}$ выводима в исчислении $G_1$ из множества формул $\Gamma$, то $\mathfrak{A}$ семантически следует из $\Gamma$.

Доказательство очень похоже на то, которое было дано в § 5.4 для соответствующей теоремы об исчислении $G_0$, и также проводится возвратной индукцией по высоте дерева вывода $\mathfrak{A}$ из $\Gamma$.

Базис. Если высота дерева равна 1, то $\mathfrak{A}$ — заключение некоторого безусловного правила вывода, все посылки которого входят в $\Gamma$. Поэтому достаточно для каждого из этих правил проверить, что, какова бы ни была интерпретация множества формул $\Gamma \cup \{\mathfrak{A}\}$, если для некоторого набора значений свободных переменных, входящих в формулы из этого множества, все предикаты, отвечающие в данной интерпретации формулам из $\Gamma$, становятся истинными предложениями, то предикат, отвечающий формуле $\mathfrak{A}$, для этого набора значений переменных также станет истинным предложением. Для

старых правил эта проверка проводится точно так же, как в случае исчисления $G_0$. Нетрудно провести ее и для новых безусловных правил — УУ и ВЭ. В самом деле, пусть в некоторой интерпретации формула $\mathfrak{A}$ переходит в предикат $F(x, y_1, \cdots, y_k)$ и терм $t$ — в функцию $f(z_1, \cdots, z_l)$, где $x, y_1, \cdots, y_k$ и $z_1, \cdots, z_l$ — все свободные переменные, входящие в $\mathfrak{A}$ и в $t$ соответственно, $k, l = 0, 1, \ldots$ и некоторые из переменных $z_1, \cdots, z_l$ (или все они) могут содержаться среди переменных $x, y_1, \cdots, y_k$. (Мы можем считать, что $x$ входит свободно в $\mathfrak{A}$, поскольку в противном случае формулы $\forall x\mathfrak{A}(x)$ и $\exists x\mathfrak{A}(x)$ переходят в любой интерпретации в тот же предикат, что и $\mathfrak{A}(x)$, а формула $\mathfrak{A}(t)$ совпадает с $\mathfrak{A}(x)$, так что наше утверждение для обоих правил тривиальным образом верно.) Тогда: формула $\forall x\mathfrak{A}(x)$ перейдет в этой интерпретации в предикат $G(y_1, \cdots, y_k)$, такой, что для любых допустимых значений $y_1^0, \cdots, y_k^0$ переменных $y_1, \cdots, y_k$ тогда и только тогда $G(y_1^0, \cdots, y_k^0) \equiv И$, когда $F(x^0, y_1^0, \cdots, y_k^0) \equiv И$ для любого допустимого значения $x^0$ переменной $x$; формула $\exists x\mathfrak{A}(x)$ перейдет в предикат $H(y_1, \cdots, y_k)$, такой, что $H(y_1^0, \ldots, y_k^0) \equiv И$ тогда и только тогда, когда $F(x^0, y_1^0, \cdots, y_k^0) \equiv И$ хотя бы для одного допустимого значения $x^0$; формула $\mathfrak{A}(t)$ перейдет в предикат $F(f(z_1^0, \ldots, z_l^0), y_1, \ldots, y_k)$. Но очевидно, что: а) если для каких-то $y_1^0, \ldots, y_k^0$ имеем $G(y_1^0, \ldots, y_k^0) \equiv И$, то $F(f(z_1^0, \cdots, z_l), y_1^0, \cdots, y_k^0) \equiv И$, каковы бы ни были $z_1^0, \cdots, z_l^0$; б) если $F(f(z_1^0, \cdots, z_l^0), y_1^0, \cdots, y_k^0) \equiv И$ для некоторых $y_1^0, \cdots, y_k^0, z_1^0, \cdots, z_l^0$, то $H(y_1^0, \cdots, y_k^0) \equiv И$.

Индукционный шаг проводится по той же схеме, что и для $G_0$, и в случаях, когда дерево образовано по одному из старых пунктов определения (т. е. пунктов 2, 3, 4, 5), можно рассуждать точно так же. Остается рассмотреть еще три случая:

*е)* Дерево образовано по пункту 6 определения из § 6.1. Тогда $\mathfrak{A}$ имеет вид $\forall x\mathfrak{D}$, причем существует дерево вывода формулы $\mathfrak{D}$ из $\Gamma$, имеющее высоту $n-1$, и $x$ не входит свободно ни в одну формулу из $\Gamma$. По предположению индукции $\mathfrak{D}$ семантически следует из $\Gamma$, т. е. в любой общей интерпретации $\Gamma$ и $\mathfrak{D}$ всякий раз, когда для какого-то набора значений входящих в формулы из $\Gamma$ и в формулу $\mathfrak{D}$ свободных переменных все предикаты, отвечающие формулам из $\Gamma$, истинны[4], предикат $F$, отвечающий $\mathfrak{D}$, также истинен. Пусть $y_1, \cdots, y_k$ — все переменные, входящие свободно в формулы из $\Gamma$; ни одна из них не совпадает с $x$. По только что сказанному для всякого набора значений $y_1, \ldots, y_k$, для которого истинны все предикаты, отвечающие форму-

[4] Т. е. их значения являются истинными предложениями.

лам из $\Gamma$, предикат $F$ будет истинен при любых значениях остальных свободных переменных формулы $\mathfrak{D}$, в том числе и $x$; поэтому при любом наборе значений переменных, входящих свободно в формулы из $\Gamma$ и в формулу $\forall x\mathfrak{D}$, при котором все предикаты, отвечающие формулам из $\Gamma$, истинны, будет истинен и предикат $\forall xF$, отвечающий формуле $\forall x\mathfrak{D}$. Таким образом, $\forall x\mathfrak{D}$ семантически следует из $\Gamma$.

ж) Дерево образовано по пункту 7а. Тогда $\Gamma$ можно представить в виде $\Gamma'\cup\{\exists x\mathfrak{D}\}$ таким образом, что существует дерево вывода формулы $\mathfrak{A}$ из множества $\Gamma'\cup\{\mathfrak{D}\}$ высоты $n-1$ и $x$ не входит свободно ни в одну формулу из $\Gamma'$ и в $\mathfrak{A}$. По предположению индукции $\mathfrak{A}$ семантически следует из $\Gamma'\cup\{\mathfrak{D}\}$. Пусть $z_1, \ldots, z_m$ — все переменные, входящие свободно в формулы из $\Gamma'$, в $\mathfrak{A}$ и в $\mathfrak{D}$ и отличные от $x$. В любой общей интерпретации $\Gamma'$, $\mathfrak{D}$ и $\mathfrak{A}$ для всякого набора значений переменных $z_1, \ldots, z_m$, $x$, для которого истинны все предикаты, отвечающие формулам из $\Gamma'$, и предикат $G$, отвечающий формуле $\mathfrak{D}$, будет истинен и предикат $F$, отвечающий формуле $\mathfrak{A}$. А это значит, поскольку $x$ не входит свободно в формулы из $\Gamma$ и в $\mathfrak{A}$, что для любого набора значений $z_1, \ldots, z_m$, для которого истинны все предикаты, отвечающие формулам из $\Gamma'$, и сверх того предикат $G$ истинен хотя бы при одном значении $x$ — иначе говоря, истинен предикат $\exists xG$, отвечающий формуле $\exists x\mathfrak{D}$,— предикат $F$ также истинен. Итак, формула $\mathfrak{A}$ семантически следует из $\Gamma'\cup\{\exists x\mathfrak{D}\}$.

з) Дерево образовано по пункту 7б. Этот случай легко сводится к предыдущему; подробности читатель восстановит сам.

Теорема доказана.

Следствие 1. Всякая теорема исчисления $G$ всюду истинна.

Это непосредственно вытекает из доказанной теоремы, потому что формула, семантически следующая из пустого множества, является всюду истинной.

Следствие 2. Исчисление $G_1$ непротиворечиво, т. е. никакая формула не может быть в нем теоремой одновременно со своим отрицанием.

В самом деле, если бы формулы $\mathfrak{A}$ и $\neg\mathfrak{A}$ были теоремами в $G_1$, то по следствию 1 обе они были бы всюду истинны, что невозможно.

Вопрос. Где в доказательстве теоремы о семантической пригодности $G_1$ используется условие свободы терма для подстановки в правилах У$\forall$ и В$\exists$?

Задача. Пользуясь теоремой 1, доказать, что для выводимости (17) из § 6.1 и выводимостей (а), (е), (ж), (з), (и) из задачи в конце пункта 4 §6.1 обратные выводимости не имеют места.

2. На теореме о семантической пригодности аналогия между $G_0$ и $G_1$ кончается. Полнота $G_1$ доказывается значительно сложнее, чем для $G_0$ — что вполне естественно, поскольку в $G_0$ достаточно иссле-

довать поведение формулы на конечном и просто устроенном множестве $n$-мерных булевых векторов, а в $G_1$ приходится иметь дело с произвольными интерпретациями, вообще говоря, бесконечными. Первое доказательство полноты исчисления предикатов (без функциональных символов и констант) было опубликовано в 1930 г. К. Гёделем [Gödel 1930][5]. Это доказательство, очень красивое, хотя и довольно сложное, имеется в книгах [Гильберт — Аккерман 1947] и [Чёрч 1960]. Мы изложим сейчас другое, более простое доказательство, найденное позднее американским математиком Л. Генкиным [Henkin 1949] (и упрощенное немецким математиком Г. Хазенъегером [Hasenjäger 1953])[6].

(Существуют и другие доказательства этой теоремы. Особого упоминания заслуживают «табличные» доказательства, основанные на идеях голландского математика Э. Бета (Evert Willem Beth, 1909—1964). См., например, [Smullyan 1968].

Прежде чем доказывать теорему о полноте, мы введем некоторые новые понятия и установим некоторые факты, представляющие и самостоятельный интерес.

Будем называть *тривиальным ограничением* исчисления $G_1$ всякое логическое исчисление $G'$, удовлетворяющее следующим условиям: ($\alpha$) алфавит $G'$ содержится в алфавите $G_1$ и содержит все переменные, все логические и синтаксические символы и хотя бы один предикатный символ; ($\beta$) множество формул состоит из всех формул $G_1$, являющихся словами в алфавите $G_1'$; ($\gamma$) правила $G'$ совпадает с правилами $G_1$.

Непосредственной проверкой легко убедиться, что в любом тривиальном ограничении $G_1$ сохраняют силу все выводимости из § 6.1, равно как и выводимости, доказанные в предыдущей главе для $G_0$, а также леммы 1, 2, 3 из § 5.3 и теорема о замене дедуктивно эквивалентных формул.

Пусть теперь $L$ и $L'$ — логические исчисления с одним и тем же множеством формул. Мы будем говорить, что $L'$ есть *простое расширение $L$ с помощью множества формул $\Delta$*, если множество правил $L'$ есть объединение множества правил $L$ с множеством всевозможных правил вида $\vdash \mathfrak{A}$, где $\mathfrak{A} \in \Delta$ — иначе говоря, если $L'$ получается из $L$ присоединением всех элементов $\Delta$ в качестве аксиом. Если $\Delta$

[5] К. Гедель (Kurt Gödel, 1906—1979) — австрийский математик (с 1938 г. жил в США). Математическая логика обязана ему очень глубокими идеями и необыкновенно сильными результатами, и мы в этой книге еще не раз встретимся с его именем.

[6] Генкин, как и Гёдель, рассматривал не наше исчисление $G_1$, а исчисление предикатов гильбертовского типа, однако выбор конкретного исчисления здесь не играет роли.

состоит из одной формулы $\mathfrak{A}$ или из двух формул $\mathfrak{A}$, $\mathfrak{B}$ и т. п., мы будем говорить о простом расширении $L$ с помощью формулы $\mathfrak{A}$, соответственно с помощью формул $\mathfrak{A}$ и $\mathfrak{B}$ и т. п.

*Лемма* 1. Если $L'$ — простое расширение $L$ с помощью множества замкнутых формул $\Delta$, то: (а) всякая теорема $L$ является теоремой и в $L'$; (б) формула в алфавите $L$ тогда и только тогда является теоремой в $L'$, когда она выводима в $L$ из некоторого конечного подмножества $\Delta$. (Если $\Delta$ конечно, это равносильно выводимости формулы из самого $\Delta$.)

*Доказательство.* Утверждение (а) очевидно. Докажем (б). Назовем накрытием листа дерева операцию, состоящую в проведении над ним горизонтальной черты (над которой ничего не пишется). Обратную операцию — стирание стоящей над формулой-узлом дерева горизонтальной черты, над которой ничего не написано,— назовем раскрытием узла. Ясно, что (б) будет доказано, если мы установим справедливость следующих двух утверждений: ($\alpha$) если в дереве вывода в $L$ с множеством зеленых листьев $\Gamma \cup \Delta_1$, где $\Delta_1 \subset \Delta$, накрыть все листья, принадлежащие $\Delta_1 \backslash \Gamma$, то получится дерево вывода в $L'$ с множеством зеленых листьев $\Gamma$; ($\beta$) если в дереве вывода в $L'$ раскрыть все узлы, отвечающие применениям правил вида $\vdash \mathfrak{A}$, где $\mathfrak{A} \in \Delta$, то получится дерево вывода в $L$. ($\alpha$) легко доказывается возвратной индукцией по высоте исходного дерева, причем как базис, так и индукционный шаг распадаются на случаи, зависящие от того, какому правилу отвечает корень дерева, т. е. какое правило применяется на последнем шаге вывода (ср. доказательства теорем о семантической пригодности $G_0$ и $G_1$). Например, если корень дерева $\delta$ отвечает правилу ВИ, то $\delta$ имеет вид $\dfrac{\varepsilon}{\mathfrak{A} \supset \mathfrak{B}}$, где $\varepsilon$ — дерево с корнем $\mathfrak{B}$ и множеством зеленых листьев, содержащим $\mathfrak{A}$. Если при этом $\Delta_1$ — некоторое подмножество множества зеленых листьев дерева $\delta$, состоящее из элементов $\Delta$, то (поскольку все элементы $\Delta_1$ являются зелеными листьями также и для $\varepsilon$) по предположению индукции дерево $\varepsilon'$, получаемое из $\varepsilon$ накрытием всех листьев, принадлежащих $\Delta_1 \backslash \Gamma$, есть дерево вывода в $L'$; а т. к. формула $\mathfrak{A}$, не будучи зеленым листом $\delta$, не входит в $\Delta_1$, она остается зеленым листом для $\varepsilon'$, и, следовательно, дерево $\dfrac{\varepsilon'}{\mathfrak{A} \supset \mathfrak{B}}$ есть дерево вывода в $L'$. Особого внимания требуют случаи, отвечающие правилам В$\forall$ и У$\exists$, потому что их можно применять лишь при условии, что зеленые листья поддерева, «растущего» из узла, отвечающего формуле, к которой применяется правило, не содержат свободных вхождений связываемой переменной; но т. к. при накрытии узлов не возникает

новых зеленых листьев, выполнение этого условия для нового дерева всякий раз вытекает из выполнения его для старого. Точно так же доказывается и (β), но с той разницей, что теперь при преобразовании дерева добавляются новые зеленые листья, принадлежащие Δ; однако все они являются замкнутыми формулами, что и обеспечивает выполнение условия применимости правил В∀ и У∃.

Задача. Показать, подобрав соответствующий пример, что утверждение (б) леммы 1 может оказаться неверным, если хотя бы одна формула из Δ не замкнута.

Введем теперь понятие *исчисления на основе* $G_1$. Так мы будем называть всякое логическое исчисление, являющееся простым расширением какого-либо тривиального ограничения $G_1$. (В частности, само $G_1$ тоже есть исчисление на основе $G_1$).

Лемма 2. Если исчисление на основе $G_1$ противоречиво, то любая его формула является в нем теоремой.

Доказательство. Из $\mathfrak{A}$ и $\neg\mathfrak{A}$ по УО выводима константа $Л$, а из нее по ДС — любая формула.

Лемма 3. Пусть $G$ — исчисление на основе $G_1$ и $\mathfrak{C}$ — замкнутая формула в алфавите $G$, такая, что ее отрицание не является в $G$ теоремой. Тогда простое расширение $G$ с помощью $\mathfrak{C}$ непротиворечиво.

Доказательство. Допустим, что лемма неверна, т. е. существует такая формула $\mathfrak{D}$, что и она сама, и ее отрицание — теоремы нашего расширения. Тогда по лемме 1б $\mathfrak{C} \vdash_G \mathfrak{D}$, $\mathfrak{C} \vdash_G \neg\mathfrak{D}$, откуда по лемме 2 из § 5.3 $\neg\mathfrak{D} \vdash_G \neg\mathfrak{C}$, $\neg\neg\mathfrak{D} \vdash_G \neg\mathfrak{C}$ и далее по лемме 3 из § 5.3 $\vdash_G \neg\mathfrak{C}$, что противоречит условию.

Будем называть логическое исчисление *дедуктивно полным*, если, какова бы ни была его замкнутая формула, или она сама, или ее отрицание является в нем теоремой. Имеет место

Лемма 4 (лемма Линденбаума)[7]. Всякое непротиворечивое исчисление на основе $G_1$ имеет непротиворечивое дедуктивно полное простое расширение.

Доказательство. Обозначим наше исчисление через $P$. Поскольку множество $\Phi$ всех замкнутых формул $P$ есть бесконечное подмножество множества всех слов в алфавите $P$, а этот алфавит счетен, множество $\Phi$ также счетно (см. Приложение II, пример на с. 445). Пусть $\mathfrak{C}_1, \mathfrak{C}_2 \ldots$ — некоторый пересчет $\Phi$. Определим последовательность множеств формул $\Delta_0, \Delta_1, \Delta_2, \ldots$ и последовательность исчислений $L_0, L_1, L_2, \ldots$ следующим образом: $(i)\Delta_0 = \varnothing$; $L_0 = P$; $(ii)$ если $\Delta_n$ и

[7] А. Линденбаум (Adolf Lindenbaum) — польский математик и логик (род. в 1904 г., пропал без вести в вильнюсском гетто, где находился с осени 1941 г.).

$L_n$ определены, то в случае, когда формула $\neg\mathfrak{C}_{n+1}$ не является в $L_n$ теоремой, $\Delta_{n+1} = \Delta_n \cup \{\mathfrak{C}_{n+1}\}$ и $L_{n+1}$ есть простое расширение $L_n$ с помощью $\mathfrak{C}_{n+1}$; в противном случае $\Delta_{n+1} = \Delta_n$, $L_{n+1} = L_n$. Положим $\Delta = \bigcup_{n=1}^{\infty} \Delta_n$; простое расширение $P$ с помощью $\Delta$ обозначим $L$. Для каждого $n = 1, 2, \ldots$ одна из формул $\mathfrak{C}_n$, $\neg\mathfrak{C}_n$ является теоремой в $L_n$, а следовательно и в $L$ (по лемме 1а, поскольку $L$ — простое расширение $L_n$ с помощью $\Delta \backslash \Delta_n$); таким образом, $L$ дедуктивно полно. В то же время $L$ непротиворечиво. В самом деле, если бы две формулы вида $\mathfrak{D}$ и $\neg\mathfrak{D}$ были теоремами в $L$, они были бы по лемме 1б выводимы в $P$ из каких-то конечных подмножеств $\Delta$. Но всякое конечное подмножество $\Delta$ содержится в некотором $\Delta_n$, так что $\mathfrak{D}$ и $\neg\mathfrak{D}$ оказались бы выводимыми в $P$ из какого-то $\Delta_n$ и, значит, были бы теоремами в $L_n$ (по лемме 1б, т. к. $L_n$ — простое расширение $P$ с помощью $\Delta_n$). Однако все $L_n$ непротиворечивы: для $L_0$ это верно по условию, а непротиворечивость $L_{n+1}$ следует из непротиворечивости $L_n$ (тривиальным образом, если $\not\vdash_{L_n} \neg\mathfrak{C}_n$, и по лемме 3 в противном случае).

3. Назовем *моделью логического исчисления* такую интерпретацию множества его формул, в которой истинны все его теоремы (иначе говоря — которая является моделью множества его теорем). Для исчисления $G_1$ ввиду следствия 1 из теоремы о семантической пригодности всякая интерпретация множества его формул является моделью. Из этого же следствия мы вывели непротиворечивость $G_1$; но на самом деле для непротиворечивости исчисления на основе $G_1$ достаточно, чтобы у него была хотя бы одна модель — ведь формулы $\mathfrak{A}$ и $\neg\mathfrak{A}$ не могут быть истинны в одной и той же интерпретации. Естественно возникает вопрос: верно ли обратное? Следует ли из непротиворечивости логического исчисления, что у него есть модель? Для рассматриваемых нами исчислений на основе $G_1$ ответ оказывается положительным: справедлива

**Теорема 2.** Всякое непротиворечивое исчисление на основе $G_1$ имеет модель.

Именно из этой теоремы мы выведем потом теорему о полноте $G_1$, и даже без особого труда. Вся трудность сосредоточена в доказательстве теоремы 2, к которому мы теперь переходим.

Пусть $P$ — непротиворечивое исчисление на основе $G_1$. Обозначим через $L_0$ исчисление, получаемое из $P$ добавлением счетного множества новых символов предметных констант $\{c_1, c_2, \ldots\}$ с соответствующим изменением множества формул, но без изменения

правил вывода. $L_0$ фактически является, как и $P$, исчислением на основе $G_1$. (В самом деле, если в $G_1$ обозначать символы предметных констант не $a_1$, $a_2$, ..., а $a_1$, $c_1$, $a_2$, $c_2$, ..., то полученное исчисление будет обладать всеми свойствами $P$, кроме тех, в формулировках которых участвуют конкретные символы предметных констант, названные «по именам».) Всякое дерево вывода в исчислении $L_0$ превратится, очевидно, в дерево вывода в $P$, если для каждого символа $c_i$, встречающегося в формулах этого дерева, заменить все вхождения этого символа во все формулы дерева вхождениями некоторой переменной, не встречающейся в формулах данного дерева (причем разные $c_i$ должны заменяться разными переменными). Отсюда следует, в частности, что $L_0$ непротиворечиво, т. к. вывод противоречия в $L_0$ можно было бы преобразовать указанным способом в вывод противоречия в $P$.

Пусть $\mathfrak{A}_1$, $\mathfrak{A}_2$, ... — некоторый пересчет множества всех формул исчисления $L_0$, содержащих не более одной свободной переменной (счетность этого множества очевидна). Из множества $\{c_1, c_2, \ldots\}$ выберем последовательность $c_{i_1}$, $c_{i_2}$, ..., состоящую из попарно различных членов и такую, чтобы для любого $n = 1, 2, \ldots$ символ $c_{i_n}$ не входил ни в одну из формул $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$. Будем обозначать через $\mathfrak{B}_n$ формулу

$$\mathfrak{A}_n\left|\begin{matrix} x_{i_n} \\ c_{i_n} \end{matrix}\right. \supset \forall x_{i_n} \mathfrak{A}_n \quad \text{(в менее педантичной записи} — \mathfrak{A}_n(c_{i_n}) \supset$$

$\supset \forall x_{i_n} \mathfrak{A}_n(x_{i_n}))$, где $x_{i_n}$ есть (единственная) свободная переменная, входящая в $\mathfrak{A}_n$, если $\mathfrak{A}_n$ не замкнута, и $x_1$, если $\mathfrak{A}_n$ замкнута. Простое расширение $L_0$ с помощью формул $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$ обозначим через $L_n$, простое расширение $L_0$ с помощью множества $\{\mathfrak{B}_1, \mathfrak{B}_2, \ldots\}$ — через $L$.

Докажем, что $L$ непротиворечиво. Для этого достаточно доказать непротиворечивость всех $L_n$, $n = 0, 1, \ldots$ (ср. доказательство леммы 4), что мы сделаем индукцией по $n$. Непротиворечивость $L_0$ уже доказана. Допустим, что $L_n$ непротиворечиво. Если при этом $L_{n+1}$ противоречиво, то по лемме 2 в нем доказуема любая формула, в частности $\neg\mathfrak{B}_{n+1}$, и по лемме 1б $\mathfrak{B}_{n+1} \vdash_{L_n} \neg\mathfrak{B}_{n+1}$. Отсюда, поскольку $\neg\mathfrak{B}_{n+1} \vdash_{L_n} \neg\mathfrak{B}_{n+1}$, по лемме 3 из § 5.3 получаем $\vdash_{L_n} \neg\mathfrak{B}_{n+1}$. А т. к. для любых $\mathfrak{C}$ и $\mathfrak{D}$ из формулы $\neg(\mathfrak{C} \supset \mathfrak{D})$ выводима конъюнкция $\mathfrak{C} \& \neg\mathfrak{D}$ (см. в § 5.3 выводимость (30), лемму 2 и выводимость (23)), формулы

$\mathfrak{A}_{n+1}\begin{vmatrix} x_{i_{n+1}} \\ c_{i_{n+1}} \end{vmatrix}$ и $\forall x_{i_{n+1}}\ \mathfrak{A}_{n+1}$ оказываются теоремами в $L_n$. Заменяя всюду в доказательстве $\mathfrak{A}_{n+1}\begin{vmatrix} x_{i_{n+1}} \\ c_{i_{n+1}} \end{vmatrix}$ символ $c_{i_{n+1}}$ на переменную $x_t$, не входящую ни в одну из участвующих в этом доказательстве формул, получим доказательство формулы $\mathfrak{A}_{n+1}\begin{vmatrix} x_{i_{n+1}} \\ x_t \end{vmatrix}$; а вместе с этой последней по правилу B$\forall$ будет теоремой и формула $\forall x_t \mathfrak{A}_{n+1}\begin{vmatrix} x_{i_{n+1}} \\ x_t \end{vmatrix}$, из которой в силу (15) из § 6.1 выводима формула $\forall x_{i_{n+1}}\ \mathfrak{A}_{n+1}(x_{i_{n+1}})$, так что $L_n$ оказывается противоречивым вопреки предположению индукции.

Пусть теперь $T$ — непротиворечивое дедуктивно полное простое расширение $L$, существование которого следует из непротиворечивости $L$ по лемме 4. Определим интерпретацию $I$ множества всех формул исчисления $T$, которая, как мы потом докажем, будет моделью для $T$ и тем более для $P$, следующим образом:

Основным множеством интерпретации $I$ будет множество всех *замкнутых термов* — т. е. термов, не содержащих переменных — исчисления $T$ (или, что то же самое, исчисления $L_0$).

Каждому символу предметной константы будет отвечать в $I$ он сам.

Каждому $k$-местному функциональному символу $f_n^k$ будет отвечать в $I$ функция $k$ переменных $\overline{f}_n^k$, значение которой для любых $k$ замкнутых термов $t_1, \ldots, t_k$ есть терм $f_n^k(t_1, \ldots, t_k)$.

Каждому $k$-местному предикатному символу $F_n^k$ будет отвечать в $I$ $k$-местный предикат $\overline{F}_n^k$, значение которого для любых $k$ замкнутых термов $t_1, \ldots, t_k$ есть предложение «Формула $F(t_1, \ldots, t_k)$ доказуема в $T$».

Предложение или предикат, отвечающее ($n$-ий) формуле $\mathfrak{A}$ в интерпретации $I$, мы будем обозначать $\mathfrak{A}'$.

Теперь для завершения доказательства теоремы достаточно показать, что в интерпретации $I$ истинны все теоремы исчисления $T$. Нам будет удобнее установить более сильный факт: что формула $\mathfrak{A}$ в алфавите исчисления $T$ тогда и только тогда доказуема в $T$, когда она истинна в $I$. Достаточно доказать это утверждение для замкнутых формул, поскольку произвольная формула $\mathfrak{A}(z_1, \ldots, z_m)$ со свободными переменными $z_1, \ldots, z_m$, очевидно, тогда и только тогда доказуема в $T$, когда доказуема формула $\forall z_1 \ldots \forall z_m \mathfrak{A}(z_1, \ldots, z_m)$, и тогда и только

тогда истинна в $I$, когда истинна та же самая формула. Мы докажем наше утверждение (для замкнутых формул) возвратной индукцией по сложности $s(\mathfrak{A})$ формулы $\mathfrak{A}$.

Базис. Если $s(\mathfrak{A}) = 0$, то $\mathfrak{A}$ либо имеет вид $F^k_n(u_1, \ldots, u_k)$, где $u_1, \ldots, u_k$ — замкнутые термы, либо есть константа $Л$. В первом случае истинность формулы $\mathfrak{A}$ в интерпретации $I$ означает — по определению этой интерпретации,— что истинно предложение $\overline{F}^k_n(u_1, \ldots, u_k)$, т. е. что формула $F^k_n(u_1, \ldots, u_k) = \mathfrak{A}$ доказуема в $T$. Во втором случае формула $\mathfrak{A} = Л$ не доказуема в $T$ [8], и соответствующее предложение $\mathfrak{A}'$ = «формула $\mathfrak{A}$ доказуема в $T$» ложно.

Индукционный шаг. Пусть $s > 0$ и для всех замкнутых формул, сложность которых меньше $s$, наше утверждение справедливо. Рассмотрим произвольную замкнутую формулу $\mathfrak{A}$ сложности $s$ и покажем, что утверждение справедливо также и для нее. При этом, как всегда в доказательстве индукцией по сложности, нам придется рассмотреть несколько случаев, зависящих от вида формулы.

(а) $\mathfrak{A} = \mathfrak{B}\&\mathfrak{C}$. Формулы $\mathfrak{B}$ и $\mathfrak{C}$, очевидно, замкнуты. Пусть формула $\mathfrak{A}$ истинна в $I$ — иначе говоря, соответствующее предложение $\mathfrak{A}'$ истинно. Но $\mathfrak{A}'$ есть конъюнкция предложений $\mathfrak{B}'$ и $\mathfrak{C}'$: поэтому они тоже истинны, что по предположению индукции влечет $\vdash_T \mathfrak{B}$ и $\vdash_T \mathfrak{C}$, откуда по ВК $\vdash_T \mathfrak{B}\&\mathfrak{C}$. Обратно, если $\vdash_T \mathfrak{B}\&\mathfrak{C}$, то по УК $\vdash_T \mathfrak{B}$ и $\vdash_T \mathfrak{C}$; отсюда по предположению индукции следует, что предложения $\mathfrak{B}'$ и $\mathfrak{C}'$ истинны, а вместе с ними истинно и $(\mathfrak{B}\&\mathfrak{C})'$.

(б) $\mathfrak{A} = \mathfrak{B} \vee \mathfrak{C}$. Формулы $\mathfrak{B}$ и $\mathfrak{C}$ замкнуты. Если $\mathfrak{A}'$ истинно, то истинно хотя бы одно из предложений $\mathfrak{B}'$ и $\mathfrak{C}'$, откуда по предположению индукции следует, что хотя бы одна из формул $\mathfrak{B}$ и $\mathfrak{C}$ доказуема в $T$, и далее по ВД получается $\vdash_T \mathfrak{B} \vee \mathfrak{C}$. Обратно, если $\vdash_T \mathfrak{B} \vee \mathfrak{C}$, то хотя бы одна из формул $\mathfrak{B}$ и $\mathfrak{C}$ доказуема в $T$: в противном случае ввиду дедуктивной полноты $T$ были бы доказуемы формулы $\neg\mathfrak{B}$ и $\neg\mathfrak{C}$ и, следовательно, также их конъюнкция, из которой (по (24) из § 5.3) выводима формула $\neg(\mathfrak{B} \vee \mathfrak{C})$, а она не может быть теоремой ввиду непротиворечивости $T$. Отсюда по предположению индукции следует, что хотя бы одно из предложений $\mathfrak{B}'$ и $\mathfrak{C}'$ истинно, а поэтому истинна и их дизъюнкция $\mathfrak{B}' \vee \mathfrak{C}' = (\mathfrak{B} \vee \mathfrak{C})'$.

(в) $\mathfrak{A} = \mathfrak{B} \supset \mathfrak{C}$. Формулы $\mathfrak{B}$ и $\mathfrak{C}$ замкнуты. Если $\mathfrak{A}'$ истинно, то $\mathfrak{B}'$ ложно или $\mathfrak{C}'$ истинно. В первом случае по предположению индукции формула $\mathfrak{B}$ не доказуема в $T$ и, следовательно, доказуема формула $\neg\mathfrak{B}$, из которой с помощью (9) из § 5.3 можно вывести $\mathfrak{B} \supset \mathfrak{C}$. Во втором

[8] Это следует из непротиворечивости $T$, поскольку из $Л$ по правилу ДС выводится противоречие.

случае доказуема формула $\mathfrak{C}$, из которой с помощью (8) из § 5.3 опять-таки выводится $\mathfrak{B} \supset \mathfrak{C}$. Обратно, если $\vdash_T \mathfrak{B} \supset \mathfrak{C}$, то доказуема хотя бы одна из формул $\neg\mathfrak{B}$ и $\mathfrak{C}$ (в противном случае были бы доказуемы $\mathfrak{B}$ и $\neg\mathfrak{C}$, и из их конъюнкции ввиду (31) из § 5.3, закона контрапозиции и правила постановки двойного отрицания выводится $\neg(\mathfrak{B} \supset \mathfrak{C})$). Отсюда по предположению индукции следует, что $\mathfrak{B}'$ ложно или $\mathfrak{C}'$ истинно; но и то, и другое влечет истинность предложения $\mathfrak{B}' \supset \mathfrak{C}' = \mathfrak{A}'$.

(г) $\mathfrak{A} = \neg\mathfrak{B}$. Формула $\mathfrak{B}$ замкнута. Если $\mathfrak{A}'$ истинно, то $\mathfrak{B}'$ ложно, и по предположению индукции формула $\mathfrak{B}$ не доказуема в $T$, а, значит, доказуемо ее отрицание $\neg\mathfrak{B} = \mathfrak{A}$. Обратно, если $\vdash_T \neg\mathfrak{B}$, то $\mathfrak{B}$ не доказуема, и по предположению индукции $\mathfrak{B}'$ ложно и, стало быть, $\mathfrak{A}'$ истинно.

(д) $\mathfrak{A} = \forall y\mathfrak{B}(y)$. Из замкнутости $\mathfrak{A}$ следует, что формула $\mathfrak{B}$ либо содержит единственную свободную переменную $y$, либо также замкнута. Во втором случае формулы $\mathfrak{A}$ и $\mathfrak{B}$ дедуктивно эквивалентны ($\forall y\mathfrak{B} \vdash \mathfrak{B}$ по У$\forall$, а поскольку $\mathfrak{B}$ не содержит свободных вхождений $y$, из выводимости $\mathfrak{B} \vdash \mathfrak{B}$ по В$\forall$ получается $\mathfrak{B} \vdash \forall y\mathfrak{B}$); кроме того, они, очевидно, равносильны. Поэтому в данном случае справедливость нашего утверждения для $\mathfrak{A}$ тривиальным образом следует из справедливости его для $\mathfrak{B}$. Рассмотрим теперь первый случай. Пусть $\mathfrak{A}'$ истинно. Это значит, что предикат $\mathfrak{B}'(y)$ тождественно истинен, т. е. что для любого замкнутого терма $v$ истинно предложение $|\mathfrak{B}(v)|'$. Формула $\mathfrak{B}(v)$ замкнута, и по предположению индукции из истинности $|\mathfrak{B}(v)|'$ следует $\vdash_T \mathfrak{B}(v)$. Но формула $\mathfrak{B}$ входит в наш перечень формул, содержащих не более одной свободной переменной, т. е. совпадает с одной из формул $\mathfrak{A}_n$, а переменная $y$ совпадает с $x_{i_n}$. Имеем, таким образом, $\vdash_T \mathfrak{A}_n(v)$ для любого замкнутого терма $v$; в частности, $\vdash_T \mathfrak{A}_n(c_{i_n})$. Но одной из аксиом исчисления $T$ является формула $\mathfrak{B}_n = \mathfrak{A}_n(c_{i_n}) \supset \forall x_{i_n}\mathfrak{A}_n(x_{i_n})$; поэтому (ввиду УИ) в $T$ доказуема формула $\forall x_{i_n}\mathfrak{A}_n(x_{i_n}) = \forall y\mathfrak{B}(y)$. Обратно, если $\vdash_T \forall y\mathfrak{B}(y)$, то по У$\forall$ будет $\vdash_T \mathfrak{B}(v)$ для любого замкнутого терма $v$; отсюда по предположению индукции следует, что для любого замкнутого терма $v$ предложение $|\mathfrak{B}(v)|'$ истинно, а это и означает истинность предложения $|\forall y\mathfrak{B}(y)|'$.

(е) $\mathfrak{A} = \exists y\mathfrak{B}(y)$. Формула $\mathfrak{B}$ либо содержит единственную свободную переменную $y$, либо замкнута. Во втором случае $\mathfrak{A}$ и $\mathfrak{B}$ равносильны и дедуктивно эквивалентны ($\mathfrak{B}(y) \vdash \exists y\mathfrak{B}(y)$ по В$\exists$; из $\mathfrak{B} \vdash \mathfrak{B}$, поскольку $y$ не входит свободно в $\mathfrak{B}$, по У$\exists$ получается $\exists y\mathfrak{B}(y) \vdash \mathfrak{B}(y)$), и утверждение тривиально. В первом случае, если

$\mathfrak{A}'$ истинно, т. е. если существует замкнутый терм $v$, для которого истинно $[\mathfrak{A}(v)]'$, то по предположению индукции формула $\mathfrak{B}(v)$ доказуема в $T$ — а из нее по $B\exists$ выводится $\exists y\mathfrak{B}(y)$. Обратно, пусть $\vdash_T \exists y\mathfrak{B}(y)$. Допустим, что предложение $[\exists y\mathfrak{B}(y)]'$ ложно. Тогда для любого замкнутого терма $v$ предложение $\mathfrak{B}(v)$ также ложно и, следовательно, $\neg\mathfrak{B}(v)$ истинно. Отсюда ввиду предположения индукции и уже проведенного индукционного шага для отрицания вытекает, что для любого замкнутого терма $v$ доказуема формула $\neg\mathfrak{B}(v)$. Но из этого следует, что $\vdash_T \forall y\neg\mathfrak{B}(y)$ (рассуждение аналогично случаю (д), поскольку $\neg\mathfrak{B}$ совпадает с одной из формул $\mathfrak{A}_n$ и $y$ совпадает с $x_n$) и далее $\vdash_T \neg\exists y\mathfrak{B}(y)$ (по (3) из § 6.1), что невозможно ввиду непротиворечивости $T$.

Доказательство теоремы 2 окончено.

4. Теперь уже легко получается

**Теорема 3 (теорема Гёделя о полноте).** Всякая всюду истинная формула в алфавите исчисления $G_1$ является в $G_1$ теоремой.

Доказательство достаточно провести для случая замкнутой формулы (см. обоснование аналогичного соображения на с. 225). Допустим, что существует всюду истинная замкнутая формула $\mathfrak{A}$ в алфавите $G_1$, не доказуемая в $G_1$. Тогда не доказуема также и формула $\neg\neg\mathfrak{A}$, и по лемме 3 простое расширение $G_1$ с помощью $\neg\mathfrak{A}$ непротиворечиво. В силу теоремы 2 оно должно иметь модель. Таким образом, существует интерпретация формулы $\mathfrak{A}$, в которой $\neg\mathfrak{A}$ истинна и, стало быть, сама $\mathfrak{A}$ невыполнима, вопреки условию.

Следствие. Если формула $\mathfrak{A}$ в алфавите исчисления $G_1$ семантически следует из множества $\Gamma$ формул в том же алфавите, то $\mathfrak{A}$ выводима в $G_1$ из $\Gamma$.

Это можно доказать аналогично тому, как мы доказали в § 5.4, пункт 3, следствие из теоремы о полноте исчисления $G_0$. Подробности читатель восстановит сам.

Итак, для исчисления $G_1$ не только понятие теоремы совпадает по объему с понятием всюду истинной формулы, но и понятие выводимости с понятием семантического следования, аналогично тому, как было для $G_0$.

Теорему 3 можно обобщить следующим образом:

**Теорема 3′.** Если $L$ — исчисление на основе $G_1$, то формула в алфавите $L$ доказуема в $L$ тогда и только тогда, когда она истинна во всякой модели $L$.

Доказательство. Тот факт, что формула, доказуемая в $L$, истинна во всякой модели $L$, непосредственно следует из определения модели логического исчисления. Докажем обратное. Пусть формула

$\mathfrak{A}$ истинна во всякой модели $L$. Мы можем считать эту формулу замкнутой (ср. доказательство теоремы 3). Тогда, если $\mathfrak{A}$ не доказуема в $L$, то не доказуема также и $\neg\mathfrak{A}$; поэтому простое расширение $L$ с помощью $\neg\mathfrak{A}$ непротиворечиво и, следовательно, имеет модель, которая, очевидно, является моделью и для $L$; но в этой модели формула $\mathfrak{A}$, вопреки условию, невыполнима.

Из доказательства теоремы 2 легко получить еще один очень важный результат:

Теорема 4 (теорема Лёвенгейма — Сколема)[9]. Всякое исчисление на основе $G_1$, имеющее какую-либо модель, имеет также счетную модель (т. е. модель со счетным основным множеством).

Доказательство. Как было замечено в начале предыдущего пункта, если исчисление на основе $G_1$ имеет модель, оно непротиворечиво. Поэтому мы можем построить для него другую модель с помощью конструкции, использованной в доказательстве теоремы 2. Но основное множество этой модели содержится в множестве всех слов в счетном алфавите и содержит счетное множество $\{c_1, c_2, \ldots\}$; поэтому оно и само счетно (см. Приложение II, теорема 7).

Теорема Лёвенгейма — Сколема показывает, что исчисления на основе $G_1$ не могут служить для формализации таких математических теорий, которые предназначены для описания исключительно конечных или исключительно несчетных множеств — например, теории действительных чисел или теории конечных полей. Для формализации теории действительных чисел, равно как и для описания конечных множеств, нужно существенно расширить запас выразительных средств языка, а именно, ввести кванторы по предикатам[10]. Такое расширение связано, однако, с определенными

[9] Л. Лёвенгейм (Leopold Löwenheim, 1878—?) — немецкий математик (был учителем гимназии в Берлине). Т. Сколем (Thoralf Skolem, 1887—1963) — норвежский математик (был профессором университетов в Осло и Бергене), внесший существенный вклад в математическую логику.

[10] Кванторы по предикатам нужны для формулировки того свойства, которым система действительных чисел отличается от системы рациональных чисел — свойства непрерывности. Например, в теории Дедекинда это свойство формулируется так: «Каково бы ни было множество действительных чисел $D$, такое, что и оно само, и его дополнение не пусты и каждый элемент $D$ больше каждого элемента дополнения $D$, существует либо наименьший элемент в $D$, либо наибольший в дополнении $D$». Но вместо множества $D$ можно рассматривать его характеристический предикат, так что фактически мы имеем здесь квантор общности по одноместным предикатам. По поводу описания конечных множеств с помощью кванторов по предикатам см. задачу 11 в конце главы.

трудностями[11]. Исчисление предикатов рассматриваемого нами типа — без кванторов по предикатам, а также без предикатов от предикатов — часто называют *узким исчислением предикатов* или *исчислением предикатов 1-й ступени*.

Заметим еще, что для любого исчисления на основе $G_1$, имеющего хоть одну модель, существуют даже модели произвольной бесконечной мощности (строящиеся довольно тривиальным образом по счетной модели — см. задачу 12 в конце главы).

**5.** В заключение параграфа отметим еще один факт, устанавливаемый тривиально, но важный для приложений:

**Теорема 5.** Если $L_0$ — тривиальное ограничение $G_1$ и $L$ — простое расширение $L_0$ с помощью множества замкнутых формул $\Delta$ (иначе говоря — $L$ есть исчисление на основе $G_1$, заданное системой аксиом $\Delta$), то всякая интерпретация множества формул исчисления $L$, в которой истинны все формулы из $\Delta$, является моделью для $L$.

**Доказательство.** Всякая теорема исчисления $L$ выводима в $L_0$ из $\Delta$ (по лемме 1) и поэтому семантически следует из $\Delta$ (по теореме 1). А это и значит, что в любой интерпретации, в которой истинны все формулы из $\Delta$, истинны и все теоремы $L$.

## § 6.3. ИСЧИСЛЕНИЯ НА ОСНОВЕ $G_1$ С РАВЕНСТВОМ. НЕКОТОРЫЕ ПРИКЛАДНЫЕ ИСЧИСЛЕНИЯ

**1.** Едва ли не во всякой достаточно богатой содержанием математической теории так или иначе присутствует отношение равенства: «$x$ и $y$ — один и тот же предмет», символически обозначаемое обычно знаком $=$. Если мы хотим описать такую теорию с помощью логического исчисления, мы должны одному из его двуместных предикатных символов — скажем, символу $F_1^2$ — отвести роль предиката равенства. Это значит, что в исчислении должны быть теоремы (в частном случае они могут быть аксиомами), выражающие тот факт, что обозначенное данным символом отношение ведет

[11] Эти трудности возникают из-за того, что, вводя кванторы по предикатам, т. е. разрешая себе рассматривать всевозможные предикаты, например, от натуральных чисел как «заранее имеющиеся в наличии», мы можем столкнуться с парадоксами (ср. парадокс Ришара (см. Введение), связанный с рассмотрением как «наличных» всех функций натурального аргумента с натуральными значениями).

себя как равенство. Говоря неформально, эти теоремы должны утверждать, что, во-первых, всякий предмет находится в отношении $F_1^2$ с самим собой и, во-вторых, отношение $F_1^2$ может связывать предмет только с самим собой. Первое из этих двух утверждений выражается, очевидно, формулой $\forall x F_1^2(x, x)$. Со вторым дело обстоит сложнее — его не удается выразить на нашем языке вполне адекватно. Это утверждение означает, в сущности, что предметы, связанные отношением $F_1^2$, неразличимы, т. е. всякое свойство, которым обладает один из них, есть и у другого. Но у нас нет средств, позволяющих выразить л ю б о е мыслимое свойство предметов, и поэтому придется ограничиться более слабым утверждением: если два предмета связаны отношением $F_1^2$ и один из них обладает каким-либо свойством, п р е д с т а в и м ы м с п о м о щ ь ю н е к о т о р о й ф о р м у л ы н а ш е г о и с ч и с л е н и я, то и второй обладает этим свойством. Это можно записать в виде схемы формул

$$\forall x \forall y (F_1^2(x, y) \supset (\mathfrak{A}(x, x) \supset \mathfrak{A}(x, y))),$$

где $x$, $y$ — переменные, $\mathfrak{A}(x, x)$ — произвольная формула и $\mathfrak{A}(x, y)$ — формула, получаемая из $\mathfrak{A}(x, x)$ заменой некоторых свободных вхождений $x$ (не обязательно всех) вхождениями $y$, причем ни одно из заменяемых вхождений $x$ не должно содержаться в области действия квантора по $y$. В конкретных исчислениях, описывающих содержательные теории, такое ослабленное утверждение все же, как правило, удовлетворительно характеризует предикат равенства — в той же мере, в какой само исчисление можно считать удовлетворительным для описания соответствующей содержательной теории (подробности см. ниже).

Изложенные соображения приводят нас к следующему определению:

Исчисление $L$ на основе $G_1$ называется *исчислением на основе $G_1$ с равенством*, если его алфавит содержит предикатный символ $F_1^2$ — который мы в дальнейшем будем заменять символом $=$ и вместо $=(t_1, t_2)$ писать $t_1 = t_2$ — и в $G_1$ доказуемы следующие формулы:

$(r)$ $x = x$;

$(i)$ $x = y \supset (\mathfrak{A}(x, x) \supset \mathfrak{A}(x, y))$,

где $x$, $y$, $\mathfrak{A}(x, x)$, $\mathfrak{A}(x, y)$ удовлетворяют только что сформулированным условиям[12].

[12] Выше мы писали $(r)$ и $(i)$ с кванторами, которые здесь опущены ради технического удобства. (Их можно восстановить с помощью B∀.)

2. Установим теперь некоторые общие свойства исчислений на основе $G_1$ с равенством.

Теорема 1. Во всяком исчислении на основе $G_1$ с равенством:

$(\alpha) \vdash \forall x(x = x)$;

$(\beta) \vdash \forall x \forall y(x = y \supset y = x)$;

$(\gamma) \vdash \forall x \forall y \forall z(x = y \& y = z \supset x = z)$.

Доказательство. $(\alpha)$ получается из $(r)$ по правилу $B\forall$. Чтобы доказать $(\beta)$, достаточно установить $\vdash x = y \supset y = x$, откуда требуемое получится также по $B\forall$. Для этого возьмем в $(i)$ в качестве $\mathfrak{A}(x, x)$ формулу $x = x$ и в качестве $\mathfrak{A}(x, y)$ — $y = x$. Получим $\vdash x = y \supset (x = x \supset y = x)$, откуда по правилу перестановки посылок ((34) из § 5.3) $\vdash x = x \supset (x = y \supset y = x)$. Остается применить $(r)$ и УИ. Аналогично, для доказательства $(\gamma)$ достаточно установить $\vdash x = y \& y = z \supset x = z$, для чего, записав $(i)$ в виде $y = z \supset (\mathfrak{A}(y, y) \supset \mathfrak{A}(y, z))$, возьмем в качестве $\mathfrak{A}(y, y)$ формулу $x = y$ и в качестве $\mathfrak{A}(y, z)$ — $x = z$; получим $\vdash y = z \supset (x = y \supset x = z)$ и далее $\vdash x = y \& y = z \supset x = z$.

Следствие 1. Во всяком исчислении на основе $G_1$ с равенством для любых термов $t$, $t'$, $t''$:

$(\alpha_1) \vdash t = t$;

$(\beta_1) \vdash t = t' \supset t' = t$;

$(\gamma_1) \vdash t = t' \& t' = t'' \supset t = t''$.

Это получается из $(\alpha)$, $(\beta)$, $(\gamma)$ по $У\forall$.

Следствие 2. Во всякой модели исчисления на основе $G_1$ с равенством предикат, отвечающий символу $=$, есть отношение эквивалентности.

Доказательство. Пусть $R$ — этот предикат. Тогда в силу $(\alpha)$, $(\beta)$, $(\gamma)$ истинны предложения, выражающие рефлексивность, симметричность и транзитивность $R$.

Если в модели исчисления на основе $G_1$ с равенством символу $=$ отвечает предикат равенства, такую модель называют *нормальной*.

Теорема 2. Во всяком исчислении на основе $G_1$ с равенством:

$$(a) \vdash y_1 = z_1 \& \cdots \& y_k = z_k \supset$$

$$\supset (\mathfrak{A}(y_1, y_1, \ldots, y_k, y_k) \supset \mathfrak{A}(y_1, z_1, \ldots, y_k, z_k)),$$

где $y_1, \ldots, y_k, z_1, \ldots, z_k$ — переменные, $\mathfrak{A}(y_1, y_1, \ldots, y_k, y_k)$ — произвольная формула и $\mathfrak{A}(y_1, z_1, \ldots, y_k, z_k)$ — формула, получаемая из предыдущей путем замены некоторых (не обязательно всех) вхождений каж-

дой $y_i$ вхождениями $z_i$, причем ни одно из заменяемых вхождений $y_i$ не должно содержаться в области действия квантора по $z_i$;

(б) $\vdash y_1 = z_1 \,\&\cdots\&\, y_k = z_k \supset$

$\supset t(y_1, y_1, \ldots, y_k, y_k) = t(y_1, z_1, \ldots, y_k, z_k)$,

где $y_1, \ldots, y_k, z_1, \ldots, z_k$ — переменные, $t(y_1, y_1, \ldots, y_k, y_k)$ — произвольный терм и $t(y_1, z_1, \ldots, y_k, z_k)$ — терм, полученный из предыдущего заменой некоторых (не обязательно всех) вхождений каждой $y_i$ вхождениями $z_i$.

Доказательство. При $k = 1$ (а) совпадает с (*i*). При $k = 2$ по (*i*) имеем

$$\vdash y_1 = z_1 \supset (\mathfrak{A}(y_1, y_1, y_2, y_2) \supset \mathfrak{A}(y_1, z_1, y_2, y_2))$$

и

$$\vdash y_2 = z_2 \supset (\mathfrak{A}(y_1, z_1, y_2, y_2) \supset \mathfrak{A}(y_1, z_1, y_2, z_2)),$$

а из этих двух выводимостей, пользуясь правилом соединения импликаций и законом транзитивности импликации ((38) и (37) из § 5.3) и правилами УИ, УК и ВИ, легко получить

$$\vdash y_1 = z_1 \,\&\, y_2 = z_2 \supset \mathfrak{A}(y_1, y_1, y_2, y_2) \supset \mathfrak{A}(y_1, z_1, y_2, z_2)).$$

Аналогично доказывается (а) для произвольного $k > 1$.

Чтобы получить (б), достаточно взять в (а) формулу

$$t(y_1, y_1, \ldots, y_k, y_k) = t(y_1, y_1, \ldots, y_k, y_k)$$

в качестве $\mathfrak{A}(y_1, y_1, \ldots, y_k, y_k)$ и $t(y_1, y_1, \ldots, y_k, y_k) = t(y_1, z_1, \ldots, y_k, z_k)$ в качестве $\mathfrak{A}(y_1, z_1, \ldots, y_k, z_k)$ и затем воспользоваться правилом перестановки посылок, пунктом ($\alpha_1$) следствия 1 из теоремы 1 и правилом УИ.

Теорема 3. Если исчисление на основе $G_1$ с равенством имеет модель, то оно имеет и нормальную модель.

Доказательство. Пусть $L$ — наше исчисление, $M$ — основное множество данной модели, $R$ — предикат, отвечающий в ней символу $=$, $\Phi_n^k$ — предикат, отвечающий символу $F_n^k$, $\varphi_n^k$ — функция, отвечающая символу $f_n^k$, $\alpha_n$ — элемент $M$, отвечающий символу $a_n$. По следствию 2 из теоремы 1 $R$ есть отношение эквивалентности. Для произвольного $\alpha \in M$ мы будем обозначать через $|\alpha|$ тот класс эквивалентности, которому принадлежит $\alpha$.

Построим теперь новую интерпретацию исчисления $L$ следующим образом:

(а) Ее основным множеством будет фактор-множество $M/R$.

(б) Каждому предикатному символу $F_n^k$ будет отвечать предикат $\overline{\Phi}_n^k$, сопоставляющий всякому упорядоченному набору $k$ классов эквивалентности $B_1, \ldots, B_k$ предложение «Существуют такие $\beta_1, \ldots, \beta_k$, что $\beta_i \in B_i$ и предложение $\Phi_n^k(\beta_1, \ldots, \beta_k)$ истинно». Легко видеть, что это предложение равносильно следующему: «Для любых $\beta_1, \ldots, \beta_k$, таких, что $\beta_i \in B_i$, предложение $\Phi_n^k(\beta_1, \ldots, \beta_k)$ истинно». В самом деле, по теореме 2а в $L$ доказуема формула

$$y_1 = z_1 \& \cdots \& y_k = z_k \supset (F_n^k(y_1, \ldots, y_k) \supset F_n^k(z_1, \ldots, z_k)),$$

и потому отвечающий ей предикат

$$y_1 R z_1 \& \ldots \& y_k R z_k \supset (\Phi_n^k(y_1, \ldots, y_k) \supset \Phi_n^k(z_1, \ldots, z_k))$$

тождественно истинен, а это значит, что если $\beta_1 R \beta_1', \ldots, \beta_k R \beta_k'$, то истинностные значения предложений $\Phi_n^k(\beta_1, \ldots, \beta_k)$ и $\Phi_n^k(\beta_1', \ldots, \beta_k')$ совпадают.

(в) Каждому функциональному символу $f_n^k$ будет отвечать функция $\overline{\varphi}_n^k$, сопоставляющая всякому упорядоченному набору $k$ классов $[\beta_1], \ldots, [\beta_k] \in M/R$ класс $[\varphi_n^k(\beta_1, \ldots, \beta_k)]$. Это определение не зависит от выбора элементов в классах («представителей»), поскольку по теореме 2б в $L$ доказуема формула $y = z_1 \& \cdots \& y_k = z_k \supset f_n^k(y_1, \ldots, y_k) = f_n^k(z_1, \ldots, z_k)$, так что отвечающий ей предикат $y_1 R z_1 \& \cdots \& y_k R z_k \supset \supset \varphi_n^k(y_1, \ldots, y_k) R \varphi_n^k(z_1, \ldots, z_k)$ тождественно истинен — иначе говоря, если $\beta_1 R \beta_1', \ldots, \beta_k R \beta_k'$, то $\varphi_n^k(\beta_1, \ldots, \beta_k)$ и $\varphi_n^k(\beta_1', \ldots, \beta_k')$ принадлежат одному и тому же классу.

(г) Каждому символу предметной константы $a_n$ будет отвечать класс $[\alpha_n]$.

Очевидной возвратной индукцией по сложности терма (т. е. по числу вхождений в него функциональных символов) легко доказать, что для произвольного терма $t(y_1, \ldots, y_k)$, содержащего переменные $y_1, \ldots, y_k$ и не содержащего других переменных, и для любых $\beta_1, \ldots, \beta_k \in M$ имеет место равенство $\overline{\tau}([\beta_1], \ldots, [\beta_k]) = [\tau(\beta_1, \ldots, \beta_k)]$, где $\tau$ и $\overline{\tau}$ — функции, отвечающие терму $t$ соответственно в старой модели и в новой интерпретации. (В частности, при $k = 0$, если $\tau$ и $\overline{\tau}$ — образы $t$ в старой и новой интерпретациях, то $\overline{\tau} = [\tau]$.)

Теперь уже нетрудно доказать, что если $\mathfrak{A} = \mathfrak{A}(y_1, \ldots, y_k)$ — произвольная формула исчисления $L$, содержащая свободные переменные $y_1, \ldots, y_k$ и не содержащая других свободных переменных, и $A(y_1, \ldots, y_k)$, $\overline{A}(y_1, \ldots, y_k)$ — предикаты, отвечающие формуле $\mathfrak{A}$ в ста-

рой и новой интерпретациях соответственно, то предложения $A(\beta_1, \ldots, \beta_k)$ и $\bar{A}(|\beta_1|, \ldots, |\beta_k|)$ равносильны, каковы бы ни были $\beta_1, \ldots, \beta_k \in M$. (Это доказывается возвратной индукцией по сложности формулы; базис основывается на пункте (б) определения новой интерпретации и только что сформулированном утверждении о термах; индукционный шаг, как обычно, распадается на случаи, соответствующие пунктам индуктивного определения формулы; подробности предоставляются читателю.) А отсюда немедленно следует, что формула исчисления $L$ истинна в новой интерпретации тогда и только тогда, когда она истинна в старой; поэтому, поскольку старая интерпретация является моделью исчисления $L$, новая также будет его моделью. Кроме того, если $\bar{R}$ — предикат, отвечающий в новой модели символу $=$, то по пункту (б) ее определения $B\bar{R}B'$ истинно тогда и только тогда, когда найдутся такие $\beta \in B$ и $\beta' \in B'$, что $\beta R \beta'$ — иначе говоря, когда $B$ совпадает с $B'$. Таким образом, новая модель нормальна.

Описанный в доказательстве теоремы 3 способ построения нормальной модели по произвольной модели исчисления $L$ мы будем называть *нормализацией* исходной модели. Так же будет называться и сама новая модель. Примеры будут приведены ниже, после того, как мы научимся задавать многие важные исчисления с равенством с помощью легко обозримых множеств дополнительных аксиом.

Замечание. Из доказательства теоремы 3 непосредственно следует, что если формула в алфавите исчисления на основе $G_1$ с равенством истинна в некоторой модели $M$ этого исчисления, то она истинна и в модели, полученной из $M$ нормализацией, и обратно. Поэтому формула, истинная во всех нормальных моделях такого исчисления, истинна и во всех вообще его моделях. Отсюда вытекает, в частности — ввиду теоремы 3′ предыдущего параграфа — что формула в алфавите исчисления на основе $G_1$ с равенством доказуема в этом исчислении тогда и только тогда, когда она истинна во всех его нормальных моделях.

Из доказательства теоремы 3 легко получить также следующее дополнение к теореме Лёвенгейма — Сколема:

**Теорема 4.** Всякое исчисление на основе $G_1$ с равенством, имеющее какую-либо модель, имеет конечную или счетную нормальную модель.

В самом деле, по теореме Левенгейма — Сколема исчисление на основе $G_1$ с равенством имеет счетную модель; но мощность фактор-множества $M/R$ не превосходит мощности $M$.

3. Как же обеспечить для конкретного исчисления выполнение условий (*r*) и (*i*)? Напрашивается очевидный способ: взять их в каче-

стве схем аксиом. Однако схема (*i*) сложна и плохо обозрима. Поэтому будет полезна следующая теорема, которая даст нам возможность заменить эту схему другим условием, гораздо легче поддающимся проверке:

Теорема 5. Пусть для исчисления $L$ на основе $G_1$: (а) выполняется условие (*r*); (б) условие (*i*) выполняется для случая, когда $\mathfrak{A}(x, x)$ — атомная формула, не содержащая термов, отличных от переменных, и $\mathfrak{A}(x, y)$ получается из $\mathfrak{A}(x, x)$ заменой одного вхождения $x$ вхождением $y$; (в) для любого функционального символа $f_n^k$, принадлежащего алфавиту $L$, доказуемы формулы

$$y_i = z \supset f_n^k(y_1, \ldots, y_i, \ldots, y_k) = f_n^k(y_1, \ldots, z, \ldots, y_k),$$

где $y_1, \ldots, y_k, z$ — переменные, $i = 1, \ldots, k$. Тогда $L$ есть исчисление на основе $G_1$ с равенством.

Доказательство. Покажем сначала, что $\vdash_L x = y \supset t = t\|_y^x$, где $x$, $y$ — переменные, $t$ — произвольный терм, содержащий вхождения $x$, и $t\|_y^x$ — терм, полученный из $t$ заменой одного вхождения $x$ вхождением $y$. Доказательство проводится возвратной индукцией по сложности $s(t)$ терма $t$. Базис тривиален, поскольку при $s(t) = 0$ имеем $t = x$. Пусть $s > 0$ и утверждение справедливо для всех термов, сложности которых меньше $s$. Тогда, если $s(t) = s$ и $t$ содержит вхождения $x$, термы $t$ и $t\|_y^x$ можно представить в виде

$$t = f_n^k(t_1, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_k)$$

и

$$t\|_y^x = f_n^k(t_1, \ldots, t_{i-1}, t_i\|_y^x, t_{i+1}, \ldots, t_k),$$

где $t_1, \ldots, t_k$ — некоторые термы и $t_i$ содержит вхождения $x$. По предположению индукции $\vdash x = y \supset t_i = t_i\|_y^x$; из нашего условия (в) с помощью B∀ и У∀ получается $\vdash t_i = t_i\|_y^x \supset t = t\|_y^x$. Остается воспользоваться транзитивностью импликации.

Очевидно, для доказательства (*i*) достаточно установить, что $\vdash x = y \supset (\mathfrak{A} \supset \mathfrak{A}\|_y^x)$, где $\mathfrak{A}$ — произвольная формула, содержащая свободные вхождения $x$, и $\mathfrak{A}\|_y^x$ получается из $\mathfrak{A}$ заменой на $y$ одного свободного вхождения $x$, не содержащегося в области действия квантора по $y$. Чтобы это доказать, заметим сначала, что наших условий (а) и (б) достаточно для справедливости теоремы 1, так как в ее доказательстве (*i*) использовалось только для атомных формул, не содержащих термов, отличных от переменных. Далее проведем возвратную индукцию по сложности $s(\mathfrak{A})$ формулы $\mathfrak{A}$.

Базис. Если $s(\mathfrak{A}) = 0$, то $\mathfrak{A}$ и $\mathfrak{A}\|_y^x$ можно представить в виде $\mathfrak{A} = F_s^k(t_1, ..., t_s, ..., t_k)$, $\mathfrak{A}\|_y^x = F_s^k(t_1, ..., t_s\|_y^x, ..., t_k)$, и из условия (б) по $\mathrm{B}\forall$ и $\forall\forall$ получаем $\vdash t_s = t_s\|_y^x \supset (\mathfrak{A} \supset \mathfrak{A}\|_y^x)$, но по доказанному выше $\vdash x = y \supset t_s = t_s\|_y^x$. Остается воспользоваться транзитивностью импликации.

Индукционный шаг распадается на обычные случаи. (а) $\mathfrak{A} = \neg\mathfrak{B}$. Поскольку, очевидно, $\mathfrak{B} = (\mathfrak{B}\|_y^x)\|_x^y$, имеем по предположению индукции $\vdash y = x \supset (\mathfrak{B}\|_y^x \supset \mathfrak{B})$, откуда по правилу контрапозиции и закону транзитивности импликации $\vdash y = x \supset (\mathfrak{A} \supset \mathfrak{A}\|_y^x)$. Далее пользуемся пунктом (β) теоремы 1. (б) $\mathfrak{A} = \mathfrak{B}\&\mathfrak{C}$. Здесь возможны два подслучая:

$$(б1)\ \mathfrak{A}\|_y^x = \mathfrak{B}\|_y^x \& \mathfrak{C},\quad (б2)\ \mathfrak{A}\|_y^x = \mathfrak{B}\&\mathfrak{C}\|_y^x.$$

В первом из них по предположению индукции $\vdash x = y \supset (\mathfrak{B} \supset \mathfrak{B}\|_y^x)$, откуда требуемое получается ввиду легко проверяемого соотношения $\mathfrak{D} \supset \mathfrak{E} \vdash_{\sigma_0} \mathfrak{D}\&\tilde{\mathcal{F}} \supset \mathfrak{E}\&\tilde{\mathcal{F}}$ ($\mathfrak{D}$, $\mathfrak{E}$, $\tilde{\mathcal{F}}$ — произвольные формулы); так же рассуждаем и во втором. Случаи (в) $\mathfrak{A} = \mathfrak{B} \vee \mathfrak{C}$ и (г2) $\mathfrak{A} = \mathfrak{B} \supset \mathfrak{C}$, $\mathfrak{A}\|_y^x = \mathfrak{B} \supset \mathfrak{C}\|_y^x$ рассматриваются аналогично. В случае (г1) $\mathfrak{A} = \mathfrak{B} \supset \mathfrak{C}$, $\mathfrak{A}\|_y^x = \mathfrak{B}\|_y^x \supset \mathfrak{C}$ пользуемся выводимостью $\mathfrak{D} \supset \mathfrak{E} \vdash_{\sigma_0} (\mathfrak{E} \supset \tilde{\mathcal{F}}) \supset (\mathfrak{D} \supset \tilde{\mathcal{F}})$ и теоремой 1 (как в случае (а)). (д) $\mathfrak{A} = \forall z\mathfrak{B}$. Тогда $\mathfrak{A}\|_y^x = \forall z(\mathfrak{B}\|_y^x)$: поскольку $x$ — свободная переменная в $\mathfrak{A}$ и заменяемое вхождение $x$ не содержится в области действия квантора по $y$, обе переменные $x$ и $y$ отличны от $z$. По предположению индукции $\vdash x = y \supset (\mathfrak{B} \supset \mathfrak{B}\|_y^x)$; отсюда легко получить выводимость $x = y, \forall z\mathfrak{B} \vdash \mathfrak{B}\|_y^x$, после чего остается применить $\mathrm{B}\forall$ и дважды $\mathrm{B}\mathrm{И}$. Аналогично рассматривается случай (е) $\mathfrak{A} = \exists z\mathfrak{B}$.

Доказанной сейчас теоремой особенно удобно пользоваться тогда, когда алфавит содержит конечное число предикатных и функциональных символов (а в прикладных исчислениях чаще всего бывает именно так). В этом случае условие (*l*) можно заменить конечным числом схем аксиом, каждая из которых содержит о д и н конкретный предикатный или функциональный символ и символы, обозначающие п р о и з в о л ь н ы е переменные (в качестве таких «метапеременных для переменных» мы используем буквы $y$, $z$, $w$ с индексами или без них, а также $x$ без индекса). Такие схемы аксиом — не содержащие метапеременных для формул и термов, а только для переменных — мы будем называть *простей-*

*шими*[13]. В частности, среди простейших схем аксиом, возникающих из условия (б) теоремы 5, всегда должны присутствовать схемы

$$(\varepsilon_1)x = y \supset (x = z \supset y = z),\ (\varepsilon_2)x = y \supset (z = x \supset z = y).$$

Но они равносильны условиям $(s) \vdash x = y \supset y = x$; $(t) \vdash x = y \& y = z \supset x = z$. В самом деле, $(t)$ равносильно выводимости $x = y,\ y = z \vdash x = z$, которую можно записать также в виде $z = x,\ x = y \vdash z = y$, что равносильно доказуемости схемы $(\varepsilon_2)$, а из $(\varepsilon_2)$ с помощью $(s)$ легко вывести и $(\varepsilon_1)$. С другой стороны, при доказательстве теоремы 1 мы фактически вывели $(s)$ и $(t)$ из допущения, что доказуемы $(\varepsilon_1)$ и $(\varepsilon_2)$.

При описании конкретных исчислений с равенством обычно предпочитают пользоваться не схемами $(\varepsilon_1)$ и $(\varepsilon_2)$, а условиями $(s)$ и $(t)$ — *законами симметричности* и *транзитивности равенства*, — которые естественно объединяются с условием $(r)$ — *законом рефлексивности равенства* — в группу условий, характеризующих равенство как отношение эквивалентности. Так будем поступать и мы в нижеследующих примерах. Прежде чем переходить к их рассмотрению, условимся об одном полезном сокращении: будем обозначать через $\exists! x \mathfrak{A}(x)$ формулу

$$\exists x(\mathfrak{A}(x) \& \forall y(\mathfrak{A}(y) \supset y = x)),$$

где $y$ — произвольная переменная, свободная для подстановки вместо $x$ в $\mathfrak{A}(x)$. Выражение $\exists! x \mathfrak{A}(x)$ читается «Существует (или «найдется») единственное $x$, такое, что $\mathfrak{A}(x)$».

**4.** Перейдем к примерам исчислений на основе $G_1$ с равенством.

Пример 1. *Узкое исчисление предикатов с равенством* (обозначение $G_1^=$). Так мы будем называть простое расширение $G_1$ с помощью множества формул видов, описанных в условиях (а), (б), (в) теоремы 5 (причем в условии (б) берутся всевозможные предикатные символы, в условии (в) — всевозможные функциональные символы $G_1$).

Все следующие примеры будут представлять собой так называемые элементарные теории. Под *элементарной теорией* некоторого класса математических систем принято понимать логическое исчисление, множество теорем которого совпадает с множеством истинных в системах этого класса *элементарных предложений*, т. е. пред-

[13] Без простейших схем аксиом можно было бы обойтись, заменив их конкретными аксиомами. Например, схема $x = x$ равносильна аксиоме $x_1 = x_1$, поскольку из последней по правилам $\forall\vdash$ и $\vdash\forall$ получается $\vdash x_i = x_i$ для любой переменной $x_i$. Мы не делаем этого ради технического упрощения, пусть и небольшого. В дальнейшем мы часто будем называть простейшие схемы аксиом просто аксиомами.

ложений, формулируемых на языке узкого исчисления предикатов (и, значит, без использования кванторов по предикатам). Например, в теории упорядоченных множеств (см. о них в Приложении I) предложение «Если для любых двух элементов упорядоченного множества существует элемент, меньший их обоих, то и для любых трех элементов найдется элемент, меньший их всех» элементарно, а предложение «Если упорядоченное множество вполне упорядочено (т. е. в любом его непустом подмножестве имеется наименьший элемент), то оно линейно упорядочено» не элементарно[14]. Если класс состоит из одной системы, говорят просто об *элементарной теории этой системы*. Вообще говоря, элементарная теория не обязательно должна задаваться конечным или вообще легко обозримым множеством аксиом; можно, в частности, просто принять в качестве аксиом все предложения, истинные в системах данного класса. Мы, впрочем, подобные тривиальные способы задания рассматривать не будем.

Во всех дальнейших примерах подразумевается, что алфавит исчисления содержит символ = и что $(r)$, $(s)$, $(t)$ являются его аксиомами; поэтому задание исчисления будет состоять в перечислении остальных символов и остальных аксиом, которые мы будем называть *собственными аксиомами* данного исчисления.

Пример 2. *Элементарная теория полугрупп* (обозначение $\Pi$). Исчисление на основе $G_1$ с одним функциональным символом $f^2_1$, который мы будем заменять знаком + и вместо $+(t_1, t_2)$ писать $t_1 + t_2$, и собственными аксиомами

$(\pi_1)\ x = y \supset x + z = y + z;$

$(\pi_2)\ x = y \supset z + x = z + y;$

$(\pi_3)\ (x + y) + z = x + (y + z).$

Пример 3. *Элементарная теория групп* (обозначение $G$). Получается из $\Pi$ добавлением символа предметной константы $a_1$, который мы будем заменять знаком 0, и аксиом

$(\pi_4)\ x + 0 = x;$

$(\pi_5)\ \forall x \exists y (x + y) = 0.$

Пример 4. *Элементарная теория абелевых групп* (обозначение $AG$). Простое расширение $G$ с помощью формулы

$(\pi_6)\ x + y = y + x.$

[14] Часто говорят также *об элементарных свойствах* математических систем. Например, свойство упорядоченного множества быть линейно упорядоченным элементарно, а свойство быть вполне упорядоченным не элементарно.

Пример 5. *Элементарная теория колец* (обозначение $R$). Получается из $AG$ добавлением функционального символа $f^2_2$, который мы будем заменять знаком $\cdot$ и вместо $\cdot(t_1, t_2)$ писать $t_1 \cdot t_2$, и аксиом

$(\pi_7)\ x = y \supset x \cdot z = y \cdot z;$

$(\pi_8)\ x = y \supset z \cdot x = z \cdot y;$

$(\pi_9)\ (x \cdot y) \cdot z = x \cdot (y \cdot z);$

$(\pi_{10})\ (x + y) \cdot z = x \cdot z + y \cdot z;$

$(\pi_{11})\ x \cdot (y + z) = x \cdot y + x \cdot z.$

Пример 6. *Элементарная теория коммутативных колец* (обозначение $KR$). *Простое расширение* $R$ с помощью формулы

$(\pi_{12})\ x \cdot y = y \cdot x$

(одна из аксиом $(\pi_{10})$ или $(\pi_{11})$ становится здесь избыточной).

Пример 7. *Элементарная теория полей* (обозначение $C$). Получается из $KR$ добавлением символа предметной константы $a_2$, который мы будем заменять знаком 1, и аксиом

$(\pi_{13})\ x \cdot 1 = x;$

$(\pi_{14})\ \forall x(\neg(x = 0) \supset \exists y(x \cdot y = 1)).$

Пример 8. *Элементарная теория упорядоченных множеств* (обозначение $Or$). Исчисление на основе $G_1$ с предикатным символом $F^2_2$, который мы будем заменять знаком $<$ и вместо $<(t_1, t_2)$ писать $t_1 < t_2$, и собственными аксиомами

$(o_1)\ x = y \supset (x < z \supset y < z);$

$(o_2)\ x = y \supset (z < x \supset z < y);$

$(o_3)\ \neg(x < x);$

$(o_4)\ x < y \& y < z \supset x < z.$

Пример 9. *Элементарная теория линейно упорядоченных множеств* (обозначение $LOr$). Простое расширение $Or$ с помощью формулы

$(o_5)\ x = y \vee x < y \vee y < x.$

Все описанные исчисления являются исчислениями на основе $G_1$ с равенством. Ввиду теоремы 5 это следует из наличия в них аксиом $(r)$, $(s)$, $(t)$, а также аксиом $(\pi_1)$, $(\pi_2)$ (для примеров 2—7), $(\pi_7)$, $(\pi_8)$ (для примеров 5—7), $(o_1)$, $(o_2)$ (для примеров 8, 9).

Что представляют собой нормальные модели этих исчислений? Нормальные модели исчисления $G_1^=$ — это все те и только те интерпретации множества всех формул $G_1$, в которых символу = (т. е. $F_1^2$) отвечает предикат равенства. В самом деле, во всякой такой интерпретации аксиомы исчисления $G_1^=$ истины, так что по теореме 5 предыдущего параграфа она является моделью $G_1^=$. Точно так же видим, что нормальными моделями исчислений $\Pi$, $G$, $AG$ и т. д. служат в точности все полугруппы[15], все группы, все абелевы группы и т. д.

Поучительны также и примеры ненормальных моделей; три таких примера мы сейчас приведем. Это тоже широко употребительные алгебраические конструкции, и они позволят нам почувствовать природу описанного в доказательстве теоремы 3 метода нормализации.

Пример I. Рассмотрим следующую интерпретацию множества формул исчисления $C$: основным множеством будет множество целых чисел, символу = отвечает предикат сравнимости по некоторому фиксированному модулю $m$, символы $+$, $\cdot$, 0, 1 имеют обычный смысл. Нетрудно показать, что в этой интерпретации истинны формулы $(s)$, $(r)$, $(t)$ и $(\pi_1)$ — $(\pi_3)$, а при простом $m$ также и $(\pi_4)$. (Доказательства можно найти в любом курсе теории чисел.) Следовательно, эта интерпретация является моделью для $R$ и $KR$, а при простом $m$ и для $C$. При $m > 1$ эта модель ненормальна; ее нормализация приводит к кольцу (при простом $m$ — полю) классов вычетов по модулю $m$.

Пример II. Чтобы получить представление о наиболее интересном классе ненормальных моделей исчисления $\Pi$, введем предварительно некоторые алгебраические понятия. При этом мы будем обозначать полугрупповую операцию не знаком +, как выше, а знаком $\cdot$ (который часто будет опускаться) и называть ее *умножением*. Так же мы будем поступать и дальше (в частности, говоря о группах); соответственно вместо 0 будем писать 1.

Пусть $A$ — произвольный алфавит. Множество $A^*$ всех слов в этом алфавите образует полугруппу относительно операции «умножения слов», состоящей просто в том, что множитель записывается вслед за множимым, так что произведение слова $x$ на слово $y$ есть слово $xy$. (Например, если $x = рок$, $y = око$, то $xy = рококо$, $yx = окорок$.) Такая полугруппа называется *свободной*.

*Ассоциативным исчислением* называется упорядоченная пара $\mathcal{A} = (A, R)$, где $A$ — конечный алфавит и $R$ — конечное множество *правил* вида $x \Leftrightarrow y$, где $x$, $y$ — слова в алфавите $A$. *Применить* к слову

[15] *Полугруппой* называется, как известно, множество с определенной на нем ассоциативной бинарной операцией.

$z$ правило $x \Leftrightarrow y$ значит заменить в $z$ некоторое вхождение $x$ вхождением $y$ или наоборот (например, каждое из слов *неотлучный* и *неразлучный* получается из другого применением правила *от* $\Leftrightarrow$ *раз*). Слова $u$ и $v$ в алфавите ассоциативного исчисления эквивалентны в этом исчислении (обозначение: $u \underset{R}{\sim} v$), если $v$ можно получить из $u$ (или, что то же самое, $u$ можно получить из $v$) последовательным применением правил. Ясно, что это отношение действительно является отношением эквивалентности и вдобавок обладает тем свойством, что из $x_1 \underset{R}{\sim} x_2$ и $y_1 \underset{R}{\sim} y_2$ следует $x_1y_1 \underset{R}{\sim} x_2y_2$. Поэтому на фактор-множестве $A^*/R$ можно определить операцию умножения «по представителям», положив для любых классов эквивалентности $X$ и $Y$: $XY = \{xy \mid x \in X,\ y \in Y\}$. Эта операция ассоциативна, так что $A^*/R$ будет полугруппой (это так называемая фактор-полугруппа полугруппы $A^*$ по отношению $R$). Обычно в теории полугрупп алфавит ассоциативного исчисления называют *системой образующих полугруппы* $A^*/R$ (его элементы называются ее *образующими*), а правила — ее *определяющими соотношениями* (записывают их обычно не в виде $x \Leftrightarrow y$, а в виде $x = y$). Полугруппа, заданная конечной системой образующих и конечным множеством определяющих соотношений, называется *конечно определенной*.

Пусть теперь $M$ — конечно определенная полугруппа, заданная системой образующих $A$ и множеством определяющих соотношений $R$. Рассмотрим следующую интерпретацию множества формул исчисления $\Pi$: основным множеством будет множество $A^*$ всех слов в алфавите $A$, символу $=$ отвечает предикат $x \underset{R}{\sim} y$, символу $+$ отвечает функция $xy$. Из отмеченных выше свойств отношения $\underset{R}{\sim}$ и операции умножения слов немедленно следует, что в этой интерпретации истинны формулы $(r)$, $(s)$, $(t)$, $(л_1)$, $(л_2)$, $(л_3)$, так что данная интерпретация есть модель исчисления $\Pi$. Если отношение $R$ нетривиально (т. е. существуют хотя бы два различных слова, эквивалентных в смысле $R$), то эта модель ненормальна. Ее нормализация дает как раз полугруппу $A^*/R = M$.

Пример III. Ассоциативное исчисление $(A, R)$ называется *групповым*, если $A$ есть объединение двух непересекающихся равномощных алфавитов $A^+ = \{a_1, \ldots, a_n\}$ и $A^- = \{a_1^{-1}, \ldots, a_n^{-1}\}$, причем фиксировано взаимно однозначное соответствие между $A^+$ и $A^-$ (элементу $a_i$ соответствует $a_i^{-1}$) и $R$ содержит для каждого $i = 1, \ldots, n$ «правила сокращения» $aa_i^{-1} \Leftrightarrow \Lambda$, $a_i^{-1}a_i \Leftrightarrow \Lambda$ ($\Lambda$ — пустое слово). Нетрудно доказать, что для группового ассоциативного исчисления фактор-полугруппа $A^*/R$ является группой; единицей в ней будет класс, содержащий $\Lambda$, обратным элементом для класса $X$ — класс, содержащий для каждого слова $x \in X$ *обратное слово* $x^{-1}$, определяемое так:

если $x = a_{i_1}' \ldots a_{i_k}'$, где $a_i'$ есть $a_i$ или $a_i^{-1}$, то $x^{-1} = \bar{a}_{i_k}' \ldots \bar{a}_{i_1}'$, где $\bar{a}_i = a_i^{-1}$ и $\bar{a}_i^{-1} = a_i$; $\Lambda^{-1} = \Lambda$.. (Все слова, обратные словам из класса $X$, входят в один класс, поскольку из $x \underset{R}{\sim} y$ следует $x^{-1} = x^{-1}\Lambda \underset{R}{\sim} x^{-1}yy^{-1} \underset{R}{\sim} x^{-1}xy^{-1} \underset{R}{\sim} \Lambda y^{-1} = y^{-1}$.) Группы, задаваемые таким образом, называются *конечно определенными группами*. Чтобы задать конечно определенную группу, достаточно указать алфавит $A'$ (его называют *системой образующих группы*) и «собственные» определяющие соотношения (т. е. отличные от всегда имеющихся соотношений $a_i a_i^{-1} = 1$ и $a_i^{-1}a_i = 1$; символ 1 используется обычно вместо $\Lambda$). Говоря об определяющих соотношениях группы, подразумевают, как правило, «собственные» определяющие соотношения. Например, группа, заданная образующими $a$, $b$ и определяющими соотношениями $a^2 = 1$, $b^3 = 1$, $bab = a$, изоморфна, как легко проверить, группе подстановок 3-й степени[16].

Пусть теперь в интерпретации предыдущего примера исчисление $A^*/R$ — групповое. Если в этой интерпретации дополнительно сопоставить символу 0 пустое слово, она станет интерпретацией множества формул исчисления $G$, которая, очевидно, будет моделью этого исчисления, всегда ненормальной (т. к. теперь отношение $R$ не может быть тривиальным). Нормализация даст ту группу, которая задается данным ассоциативным исчислением.

Задачи. 1) Охарактеризовать класс групповых исчислений, являющихся моделями исчисления $AG$.

2) Указать примеры ненормальных моделей исчислений $Or$ и $LOr$.

3) Привести примеры выводов в исчислениях примеров 2—9 или хотя бы в некоторых из них. (Желательно показать, в частности, что в $G$ доказуемы формулы

$$0 + x = x,\ \forall x \exists! y(x + y = 0),$$

$$x + y = 0 \supset y + x = 0,$$

$$\forall x(x + z = x) \supset z = 0,$$

$$x + y = 0 \& x + z = 0 \supset y = z,$$

$$\forall x \forall y \exists! z(x + z = y),$$

в $R$ — формула $x \cdot 0 = 0$, в $C$ — формула $x \cdot y = 0 \supset x = 0 \vee y = 0$, в $Or$ — формула $x < y \supset \neg(y < x)$.)

Что можно сказать о семантической пригодности и семантической полноте рассмотренных исчислений? В § 5.4 мы определили

[16] Изоморфное соответствие получится, например, если сопоставить образующей $a$ транспозицию (12), а образующей $b$ — подстановку $\begin{pmatrix} 123 \\ 231 \end{pmatrix}$.

семантическую пригодность исчисления как истинность всякой доказуемой в нем формулы и семантическую полноту — как доказуемость всякой истинной. При этом истинность для каждого исчисления понимается по-своему — в зависимости от того, для каких целей оно построено. Когда речь идет об исчислениях на основе $G_1$, под истинностью естественно понимать истинность в интерпретациях определенного класса — тех, для описания которых это исчисление предназначается (тогда семантическая пригодность исчисления означает, что все эти интерпретации служат для него моделями). Для самого $G_1$, призванного обслуживать нужды любых математических теорий, этот класс состоит из всех вообще интерпретаций, для узкого исчисления предикатов с равенством — из всех тех интерпретаций, в которых символу $F_1^2$ отвечает предикат равенства, для элементарной теории групп — из всех групп, и т. д. И легко видеть, что при таком понимании истинности все эти исчисления семантически пригодны и семантически полны. Например, для элементарной теории групп в силу теоремы 5 предыдущего параграфа всякая группа является моделью[17], а в силу замечания после теоремы 3 настоящего параграфа всякая формула, истинная во всех группах, доказуема в элементарной теории групп. Аналогично для остальных исчислений. (Этим, собственно, и оправдываются термины «элементарная теория групп» и т. п.)

5. В § 1.2 (пункт 3) мы определили функцию как отношение, связывающее каждый элемент своей области определения с одним-единственным элементом множества значений. Для таких отношений в математике используются особые «функциональные» обозначения, очень упрощающие работу с ними. Эти обозначения фигурируют и в логических исчислениях в виде функциональных символов и строящихся с их помощью термов. Кажется правдоподобным, что ничего принципиально нового такие обозначения не дают и нужны только для удобства. Следующие рассуждения показывают, что эта догадка верна.

Пусть $L$ — непротиворечивое исчисление на основе $G_1$ с равенством и $\mathfrak{C}(y_1, \ldots, y_n, z)$ — формула в его алфавите, не содержащая свободных переменных, отличных от $y_1, \ldots, y_n, z$, и такая, что $\vdash_L \forall y_1 \ldots \forall y_n \exists! z \mathfrak{C}(y_1, \ldots, y_n, z)$. Добавим к алфавиту $L$ новый $n$-местный функциональный символ $g$ и к множеству аксиом $L$ — аксиому (точнее — простейшую схему аксиом) $\mathfrak{C}(y_1, \ldots, y_n, g(y_1, \ldots, y_n))$ и все новые аксиомы, возникающие после добавления $g$ из схемы аксиом

[17] В этой теореме шла речь о расширении с помощью замкнутых формул, но аксиомы любой из наших элементарных теорий можно «замкнуть», связав все свободные переменные кванторами общности.

(1) (или, если исчисление задано способом, основанным на теореме 5 — из условия (в) этой теоремы). Полученное исчисление — которое можно также считать исчислением на основе $G$ с равенством (ср. с. 224) — обозначим $L'$. Покажем теперь, что по любой формуле $\mathfrak{A}$ исчисления $L'$ можно эффективно построить дедуктивно эквивалентную ей (в исчислении $L'$) формулу $\mathfrak{A}'$ исчисления $L$ таким образом, что $\vdash_{L'} \mathfrak{A}$ тогда и только тогда, когда $\vdash_L \mathfrak{A}'$, и если $\mathfrak{A}$ не содержит $g$, то $\mathfrak{A}' = \mathfrak{A}$.

Пусть сначала $\mathfrak{A}$ — произвольная атомная формула в алфавите $L'$, содержащая вхождения $g$. Обозначим через $\mathfrak{A}^-$ формулу, полученную из $\mathfrak{A}$ заменой одного вхождения терма $g(t_1, \ldots, t_n)$, где $t_1, \ldots, t_n$ — термы, не содержащие $g$, вхождением некоторой переменной $x$, не содержащейся в $\mathfrak{A}$. (Для определенности будем считать, что заменяется самое левое вхождение терма такого вида и что $x$ — первая не входящая в $\mathfrak{A}$ переменная.) Положим $\mathfrak{A}^* = \exists x(\mathfrak{A}^- \& \mathfrak{S}(t_1, \ldots, t_n, x))$. Пользуясь аксиомой $\mathfrak{S}(y_1, \ldots, y_n, g(y_1, \ldots, y_n))$ и условием $\vdash_L \forall y_1 \ldots \forall y_n \exists! z \mathfrak{S}(y_1, \ldots, y_n, z)$, легко доказать (подробности предоставляются читателю), что формулы $\mathfrak{A}$ и $\mathfrak{A}^*$ дедуктивно эквивалентны. Поскольку $\mathfrak{A}^*$ содержит на одно вхождение $g$ меньше, чем $\mathfrak{A}$, последовательным повторением описанного преобразования мы получим в конце концов формулу $\mathfrak{A}'$, не содержащую $g$ и дедуктивно эквивалентную $\mathfrak{A}$. Теперь мы определим $\mathfrak{A}'$ для всех остальных формул в алфавите $L'$, полагая $\mathfrak{A}' = \mathfrak{A}$, если $\mathfrak{A}$ — атомная формула, не содержащая $g$, а для неатомных формул пользуясь индуктивным определением:

$$((\mathfrak{A})\mathfrak{o}(\mathfrak{B}))' = (\mathfrak{A}')\mathfrak{o}(\mathfrak{B}') \quad (\mathfrak{o} = \&, \vee, \supset);$$

$$(\mathfrak{p}(\mathfrak{A}))' = \mathfrak{p}(\mathfrak{A}') \quad (\mathfrak{p} = \neg, \forall x, \exists x).$$

Дедуктивная эквивалентность $\mathfrak{A}$ и $\mathfrak{A}'$ для общего случая следует из теоремы о замене дедуктивно эквивалентных формул. Далее, если $\vdash_L \mathfrak{A}'$, то тем более $\vdash_{L'} \mathfrak{A}'$, откуда ввиду дедуктивной эквивалентности $\mathfrak{A}$ и $\mathfrak{A}'$ следует $\vdash_{L'} \mathfrak{A}$. Остается доказать, что $\vdash_{L'} \mathfrak{A}$ влечет $\vdash_L \mathfrak{A}'$. Поскольку из $\vdash_{L'} \mathfrak{A}$ следует $\vdash_{L'} \mathfrak{A}'$, достаточно убедиться, что если $\mathfrak{A}$ — формула в алфавите $L$, то из $\vdash_{L'} \mathfrak{A}$ следует $\vdash_L \mathfrak{A}$. Это мы сделаем так. Пусть $M$ — какая-либо нормальная модель исчисления $L$ (существующая по теореме 2 предыдущего параграфа и теореме 3 настоящего). Ввиду условия $\vdash_L \forall y_1 \ldots \forall y_n \exists! z \mathfrak{S}(y_1, \ldots, y_n, z)$ для любых $n$ элементов $\alpha_1, \ldots, \alpha_n$ основного множества модели $M$ в этом множестве найдется единственный элемент $\beta$, для которого истинно предложение $C(\alpha_1, \ldots, \alpha_n, \beta)$,

где $C'$ — предикат, отвечающий в модели $M$ формуле $\mathfrak{C}$. Пусть $\psi$ — функция $n$ переменных, сопоставляющая любым $x_1, \ldots, x_n$ соответствующее $\beta$. Дополним $M$ до интерпретации $M'$ множества формул $L'$, сопоставив символу $g$ функцию $\psi$. Легко видеть, что $M'$ будет моделью исчисления $L'$. Действительно, все правила $G_i$ справедливы в любой интерпретации (см. доказательство теоремы о семантической пригодности $G_i$); справедливым в $M'$ и аксиомы равенства (в том числе и для формул, содержащих $g$), потому что символу $=$ отвечает в $M$ — а, стало быть, и в $M'$ — предикат равенства; собственные аксиомы исчисления $L$ не содержат $g$ и поэтому, будучи истинными в $M$, истинны и в $M'$: аксиома $\mathfrak{C}(y_1, \ldots, y_n, g(y_1, \ldots, y_n))$ истинна в силу определения функции $\psi$. Пусть теперь $\mathfrak{A}$ — формула в алфавите $L$, доказуемая в $L'$. Тогда для любой нормальной модели $M$ исчисления $L$ формула $\mathfrak{A}$ истинна в соответствующей модели $M'$, а поскольку $\mathfrak{A}$ не содержит $g$, она истинна и в $M$. Таким образом, $\mathfrak{A}$ истинна в любой нормальной модели исчисления $L$; но, как мы видели при доказательстве теоремы 3, для произвольной модели $L$ существует нормальная модель того же исчисления, в которой всякая формула истинна тогда и только тогда, когда она истинна в исходной модели; поэтому формула $\mathfrak{A}$ истинна в л ю б о й модели $L$ и, следовательно, по теореме 3 предыдущего параграфа она доказуема в $L$.

Замечание. Это утверждение можно доказать и чисто синтаксически, не обращаясь к моделям (см., например, [Клини 1957], § 74), но такое доказательство очень сложно.

Доказанное утверждение допускает следующую очевидную модификацию: вместо формулы $\mathfrak{C}(y_1, \ldots, y_n, z)$ можно взять формулу $\mathfrak{C}(z)$ с единственной свободной переменной $z$, удовлетворяющую условию $\vdash \exists!z\mathfrak{C}(z)$. Тогда вместо функционального символа вводится новый символ предметной константы, но все конструкции и доказательства остаются, в сущности, прежними.

Последовательно применяя описанную процедуру, можно, разумеется, ввести и несколько новых функциональных символов и/или символов предметных констант.

**Примеры.** 1) Поскольку в элементарной теории групп доказуема формула $\forall x\exists!y(x + y = 0)$ (см. задачу в конце пункта 4), мы можем добавить к ней новый одноместный функциональный символ $g$ и аксиомы $x = y \supset g(x) = g(y)$ и $x + g(x) = 0$. (Обычно вместо $g(x)$ пишут $-x$.) Однако ввиду доказанного нами утверждения при таком расширении исчисления будут доказуемы только те формулы в прежнем алфавите, которые были доказуемы ранее.

2) К элементарной теории полей мы можем тем же способом добавить два новых одноместных функциональных символа $g$ («про-

тивоположный элемент») и $h$ («обратный элемент»)[18], но никаких новых теорем при этом опять-таки не получится.

Наше утверждение дает возможность не только добавлять, но и устранять функциональные символы и символы предметных констант. Можно, например, в элементарной теории групп $G$ заменить символы + и 0 предикатными символами $F^3_1$ и $F^1_1$, добавив аксиомы $\forall y_1 \forall y_2 \exists! z F^3_1(y_1, y_2, z)$ и $\exists! z F^1_1(z)$ и заменив все аксиомы, содержащие + и 0, их «переводами», построенными в соответствии с описанной выше процедурой [например, $(\tau_1)$ заменится аксиомой

$$\exists z_2(\exists z_1((x = y \supset z_1 = z_2) \& F^1_1(x, z, z_1)) \& F^3_1(y, z, z_2)),$$

$(\tau_4)$ — аксиомой $\exists z_2(\exists z_1(z_2 = x \& F^1_1(z_1)) \& F^3_1(x, z_1, z_2))$].

В построенном таким образом исчислении — обозначим его $G^*$ — будут доказуемы «переводы» всех теорем исчисления $G$, и наше утверждение показывает, что если снова добавить к $G^*$ символы + и 0 вместе с аксиомами $F^3_1(x, y, x + y)$ и $F^1_1(0)$, то никаких новых теорем в алфавите $G^*$, кроме «переводов» теорем из $G$, мы не получим. Таким же способом можно и в любом исчислении на основе $G_1$ с равенством устранить все функциональные символы и символы предметных констант. Однако использование этих символов делает язык логики предикатов (как и содержательный математический язык) несравненно более обозримым и наглядным, и поэтому ими пользуются весьма широко.

6. В заключение параграфа сделаем еще одно замечание, которое понадобится нам позже. Для произвольного логического исчисления $L$, алфавит которого содержит символы предметных констант, и произвольной его интерпретации $I$ естественным образом определяется отображение множества замкнутых термов исчисления $L$ в основное множество интерпретации $I$: образом символа предметной константы служит тот элемент основного множества, который отвечает ему в интерпретации $I$, и если $\sigma_1, \ldots, \sigma_k$ — образы термов $t_1, \ldots, t_k$, $f^k_n$ — $k$-местный функциональный символ и $\varphi$ — функция, отвечающая ему в $I$, то образом терма $f^k_n(t_1, \ldots, t_k)$ служит $\varphi(\sigma_1, \ldots, \sigma_k)$. Образ замкнутого терма в этом отображении мы будем в дальнейшем называть просто *элементом, отвечающим* данному *терму* в данной *интерпретации*. Если $L$ — исчисление на основе $G$ с равенством и $I$ — его нормальная модель, то, очевидно, формула $t_1 = t_2$, где $t_1, t_2$ — замкнутые термы исчисления $L$, превращается в модели $I$ в предложение «$\tau_1$ совпадает с $\tau_2$», где $\tau_1$ и $\tau_2$ — элементы основного множества

[18] При этом $h(0)$ можно формально положить, например, равным 0.

$I$, отвечающие термам $t_1$ и $t_2$, а формула $\neg(t_1 = t_2)$ — в предложение «$\tau_1$ не совпадает с $\tau_2$». Поэтому из доказуемости в $L$ формулы $t_1 = t_2$ следует, что термам $t_1$ и $t_2$ отвечает в $I$ один и тот же элемент, а из доказуемости $\neg(t_1 = t_2)$ — что им отвечают разные элементы. (Обратное неверно: например, если добавить к алфавиту элементарной теории групп два новых символа предметных констант $a$ и $b$, то термам $ab$ и $ba$ в некоторых нормальных моделях полученного исчисления будет отвечать один и тот же элемент, а в некоторых — разные, и как раз поэтому ни одна из формул $ab = ba$ и $\neg(ab = ba)$ не может быть доказуема в этом исчислении.)

## § 6.4. ДРУГИЕ ВАРИАНТЫ УЗКОГО ИСЧИСЛЕНИЯ ПРЕДИКАТОВ

1. Рассмотрим исчисление гильбертовского типа $H_1$, определяемое следующим образом:

Алфавит $H_1$ состоит из тех же символов, что и алфавит $G_1$, кроме $\Lambda$.

Правила образования термов — те же, что в $G_1$.

Правила образования формул — те же, что в $G_1$, кроме правила (б).

Множество правил вывода $H_1$ состоит из двух правил:

*Modus ponens* (сокращенно MP): $\mathfrak{A}$, $\mathfrak{A} \supset \mathfrak{B} \vdash \mathfrak{B}$.

*Правило обобщения* (сокращенно Об): $\mathfrak{A} \vdash \forall x \mathfrak{A}$, где $x$ — любая переменная.

Аксиомы $H_1$ задаются с помощью схем, которые делятся на 5 групп, нумеруемых римскими цифрами. Группы I — IV — такие же, как в исчислении $H_0$ (см. § 5.5). Группа V состоит из четырех схем аксиом:

1. $\forall x \mathfrak{A}(x) \supset \mathfrak{A}(t)$;

2. $\mathfrak{A}(t) \supset \exists x \mathfrak{A}(x)$;

3. $\forall x(\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \forall x \mathfrak{B})$;

4. $\forall x(\mathfrak{A} \supset \mathfrak{B}) \supset (\exists x \mathfrak{A} \supset \mathfrak{B})$,

причем в первых двух схемах $t$ означает терм, свободный для подстановки вместо переменной $x$ в $\mathfrak{A}$, в схеме 3 переменная $x$ не должна входить свободно в $\mathfrak{A}$, а в схеме 4 — в $\mathfrak{B}$.

Задание. Для каждой схемы группы V найти аналог (или аналоги) в группе II или III.

Поскольку в $H_1$ входят все схемы аксиом и единственное правило вывода исчисления $H_0$, всякая схема вывода в $H_0$ будет также и схемой вывода в $H_1$. Приведем пример вывода в $H_1$ с использованием новых аксиом и правила **Об**: докажем, что $\mathfrak{A}, \exists x\mathfrak{A} \supset \mathfrak{B} \vdash \forall x\mathfrak{B}$.

1. $\exists x\mathfrak{A}(x) \supset \mathfrak{B}(x)$ (исходная формула)
2. $\forall x(\exists x\mathfrak{A}(x) \supset \mathfrak{B}(x))$ (по **Об** из 1)
3. $\forall x(\exists x\mathfrak{A}(x) \supset \mathfrak{B}(x)) \supset (\exists x\mathfrak{A}(x) \supset \forall x\mathfrak{B}(x))$ (аксиома по схеме V3)
4. $\exists x\mathfrak{A}(x) \supset \forall x\mathfrak{B}(x)$ (по MP из 2 и 3)
5. $\mathfrak{A}(x)$ (исходная формула)
6. $\mathfrak{A}(x) \supset \exists x\mathfrak{A}(x)$ (аксиома по схеме V2)
7. $\exists x\mathfrak{A}(x)$ (по MP из 5 и 6)
8. $\forall x\mathfrak{B}(x)$ (по MP из 7 и 4).

Других примеров «прямых» выводов в $H_1$ мы приводить не будем, потому что в интересных случаях такие выводы громоздки, и притом за счет не столько «новой», сколько «старой» («пропозициональной») части исчисления. Для упрощения доказательств выводимости в $H_1$ используются, как и в $H_0$, производные правила, среди которых центральное место занимает, как и там, теорема о дедукции. Однако дословно перенести эту теорему на случай $H_1$ нельзя. В самом деле, по правилу **Об** $F_1^1(x) \vdash \forall x F_1^1(x)$, и если бы теорема о дедукции в прежней формулировке была верна для $H_1$, мы имели бы $\vdash_{H_1} F_1^1(x) \supset \forall x F_1^1(x)$. Но естественно ожидать, что всякая теорема $H_1$ всюду истинна (и это действительно так ввиду равносильности $H_1$ и $G_1$, которая будет доказана ниже, и семантической пригодности $G_1$), между тем как формула $F_1^1(x) \supset \forall x F_1^1(x)$ не истинна ни в какой интерпретации, в которой символу $F_1^1$ отвечает предикат, не являющийся ни тождественно истинным, ни тождественно ложным (в такой интерпретации она перейдет в ложное предложение для всякого $x_0$, для которого предложение, отвечающее $F_1^1(x_0)$, истинно). Чтобы сформулировать теорему о дедукции для $H_1$, нам понадобится понятие *зависимости формул в выводе*, определяемое индуктивно следующим образом.

Пусть $\mathfrak{E}_1, \ldots, \mathfrak{E}_n$ — вывод в логическом исчислении гильбертовского типа. Тогда: (*i*) всякая формула $\mathfrak{E}_i$ зависит в данном выводе от самой себя; (*ii*) если $\mathfrak{E}_j$ зависит в данном выводе от $\mathfrak{E}_i$ и формула $\mathfrak{E}_k$ включена в вывод как результат применения некоторого правила к каким-либо входящим в вывод формулам, одна из которых есть $\mathfrak{E}_j$, то $\mathfrak{E}_k$ зависит в данном выводе от $\mathfrak{E}_i$; (*iii*) формула может зависеть от формулы в данном выводе только в силу пункта (*i*) или (*ii*).

Например, в приведенном выше выводе от формулы 1 зависят формулы 1, 2, 4 и 8, от формулы 2 — 2, 4, и 8, и т. д.

Теперь может быть сформулирована и доказана

Теорема о дедукции. Если $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$ и существует такой вывод формулы $\mathfrak{B}$ из множества $\Gamma, \mathfrak{A}$, в котором ни при каком применении правила Об к формуле, зависящей от $\mathfrak{A}$, не связывается квантором общности никакая переменная, входящая свободно в $\mathfrak{A}$, то $\Gamma \vdash \mathfrak{A} \supset \mathfrak{B}$.

В частности, если формула $\mathfrak{A}$ замкнута, то из $\Gamma, \mathfrak{A} \vdash \mathfrak{B}$ всегда следует $\Gamma \vdash \mathfrak{A} \supset \mathfrak{B}$.

Доказательство проводится по той же схеме, что и для $H_0$. Базис можно повторить слово в слово. В индукционном шаге к четырем разобранным для $H_0$ случаям, которые и здесь разбираются точно так же, добавляется еще один: когда формула $\mathfrak{C}_l = \mathfrak{B}$ получается из некоторой формулы $\mathfrak{C}_i$, $i < l$, по правилу Об, т. е. $\mathfrak{B} = \forall x \mathfrak{C}_i$. При этом по условию теоремы либо $x$ не входит свободно в $\mathfrak{A}$, либо $\mathfrak{C}_i$ не зависит в данном выводе от $\mathfrak{A}$. По предположению индукции $\Gamma \vdash \mathfrak{A} \supset \mathfrak{C}_i$, а это дает возможность, если $x$ не входит свободно в $\mathfrak{A}$, построить вывод формулы $\mathfrak{A} \supset \mathfrak{B}$ из $\Gamma$ следующим образом: к выводу $\mathfrak{A} \supset \mathfrak{C}_i$ из $\Gamma$ приписываем формулу $\forall x(\mathfrak{A} \supset \mathfrak{C}_i)$, получаемую по правилу Об, аксиому (по схеме $\forall 3$) $\forall x(\mathfrak{A} \supset \mathfrak{C}_i) \supset (\mathfrak{A} \supset \forall x \mathfrak{C}_i)$ и, наконец, формулу $\mathfrak{A} \supset \forall x \mathfrak{C}_i$, получаемую из MP из двух предыдущих. Если же $\mathfrak{C}_i$ не зависит от $\mathfrak{A}$, то, как сразу следует по определению зависимости, существует вывод $\mathfrak{C}_i$ из $\Gamma$; к нему достаточно дописать формулы $\forall x \mathfrak{C}_i$ (по Об из предыдущей), $\forall x \mathfrak{C}_i \supset (\mathfrak{A} \supset \forall x \mathfrak{C}_i)$ (аксиома по схеме $\Pi$), $\mathfrak{A} \supset \forall x \mathfrak{C}_i$ (по MP из двух предыдущих).

Замечание. Просмотрев доказательство теоремы, легко убедиться, что в строящемся в нем выводе формулы $\mathfrak{A} \supset \mathfrak{B}$ из $\Gamma$ правило Об применяется только к тем переменным, к которым оно применялось в исходном выводе $\mathfrak{B}$ из $\Gamma, \mathfrak{A}$.

Из доказанной теоремы можно заключить, что все производные правила и все выводимости, полученные нами для $H_0$ с применением теоремы о дедукции, верны и в $H$. В самом деле, при их доказательстве теоремой о дедукции приходится пользоваться только для таких выводов, в которых правило Об вообще не применяется. (Остается справедливым, очевидно, и правило устранения теоремы.)

Задача. Доказать для $H$ некоторые (или все) выводимости из § 6.1 (пункт 4).

Посмотрим теперь, как связаны между собой исчисления $H_1$ и $G_1$. В § 5.5 мы установили, что их «пропозициональные части» $H_0$ и $G_0$ равносильны в смысле совпадения по объему отношении выводимости (если в $G_0$ рассматривать только формулы, не содержащие кон-

станты $\mathcal{J}$). В этом смысле $H_1$ и $G_1$ не равносильны. В самом деле, в $H_1$ из формулы $F_1^1(x)$ выводима формула $\forall x F_1^1(x)$, но если бы это было верно в $G_1$, то по правилу ВИ получилось бы $\vdash_{G_1} F_1^1(x) \supset \forall x F_1^1(x)$, а этого не может быть, поскольку импликация $F_1^1(x) \supset \forall x F_1^1(x)$, как было уже замечено, не является всюду истинной. Однако в некотором более слабом и тоже естественном смысле исчисления $H_1$ и $G_1$ все же равносильны. Именно, формула $\mathfrak{A}$, не содержащая $\mathcal{J}$, выводима в $G_1$ из множества $\Gamma$ формул, не содержащих $\mathcal{J}$, тогда и только тогда, когда существует вывод $\mathfrak{A}$ из $\Gamma$ в $H_1$, в котором ни к одной переменной, входящей свободно в какую-либо формулу из $\Gamma$, не применяется правило обобщения. Отсюда следует, в частности, что формула в алфавите $H_1$ тогда и только тогда является в $H_1$ теоремой, когда она является теоремой в $G_1$.

Чтобы доказать это утверждение, предварительно устраним из $G_1$ символ $\mathcal{J}$ тем же способом, которым мы пользовались в § 5.5 для $G_0$: перейдем к исчислению $G_1'$, отличающемуся от $G_1$ тем, что в алфавите нет символа $\mathcal{J}$, среди правил образования формул — правила (б), а правила вывода УО, ВО и ДС заменены правилами ВО′ и ДС′ (их формулировки см. в § 5.5). Точно так же, как это делалось для $G_0$ и $G_0'$, можно доказать, что для любой формулы $\mathfrak{A}$ в алфавите $G_1'$ и любого конечного множества $\Gamma$ формул в том же алфавите $\Gamma \vdash_{G_1} \mathfrak{A}$ тогда и только тогда, когда $\Gamma \vdash_{G_1'} \mathfrak{A}$. (Вместо пропозициональной переменной $X$ здесь можно взять, например, формулу $\forall x F_1^1(x)$.) Покажем теперь, что $\Gamma \vdash_{H_1} \mathfrak{A}$ в том и только том случае, когда существует вывод $\mathfrak{A}$ из $\Gamma$ в $H_1$, в котором к переменным, входящим свободно в формулы из $\Gamma$, если такие есть, не применяется правило обобщения.

(а) Чтобы показать, что из существования удовлетворяющего указанному условию вывода $\mathfrak{A}$ из $\Gamma$ в $H_1$ следует $\Gamma \vdash_{G_1'} \mathfrak{A}$, достаточно убедиться, что всякая теорема $H_1$ есть теорема и в $G_1'$. Действительно, тогда при непустом $\Gamma = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_k\}$ мы сможем, ввиду наложенного на вывод условия, воспользоваться теоремой о дедукции; применяя ее $k$ раз, получим $\vdash_{H_1} \mathfrak{B}_1 \supset \cdots \supset (\mathfrak{B}_k \supset \mathfrak{A}) \cdots)$, откуда $\vdash_{G_1'} \mathfrak{B}_1 \supset \cdots \supset (\mathfrak{B}_k \supset \mathfrak{A}) \cdots)$ и далее по УИ $\mathfrak{B}_1, \ldots, \mathfrak{B}_k \vdash_{G_1'} \mathfrak{A}$. Теперь достаточно проверить, что все аксиомы $H_1$ доказуемы в $G_1'$ — или в $G_1$, так как они не содержат $\mathcal{J}$, — и что применение правил $H_1$ к теоремам $G_1'$ дает снова теоремы $G_1'$. Утверждение о правилах очевидно, поскольку МР действует и в $G_1'$ (под именем УИ) и из $\vdash_{G_1'} \mathfrak{A}$ ввиду ВА следует $\vdash_{G_1'} \forall x \mathfrak{A}$. Что касается аксиом, то для групп I—IV можно рассуждать слово в слово так же, как в § 5.5, а проверка доказуемости в $G_1'$ аксиом

группы V — несложное упражнение, выполнение которого предоставляется читателю.

(б) Чтобы доказать обратное утверждение, достаточно установить, что (а) для всякого безусловного правила исчисления $G'$ существует вывод в $H_1$ его заключения из его посылок без применения правила Об и (б) каково бы ни было условное правило $G'_1$, если в $H_1$ имеют место выводимости, фигурирующие в его условии, и соответствующие выводы можно провести без применения правила Об к переменным, входящим свободно в исходные формулы этих выводов, то выводимость, фигурирующая в заключении правила, также имеет место в $H_1$, причем соответствующий вывод можно провести с соблюдением того же ограничения (например, для правила ВА это означает следующее: если существует вывод $\mathfrak{A}$ из $\Gamma$ в $H_1$, в котором к переменным, входящим свободно в формулы из $\Gamma$ (если такие есть), не применяется правило Об, и переменная $x$ не входит свободно ни в одну формулу из $\Gamma$, то существует вывод формулы $\forall x\mathfrak{A}$ из $\Gamma$ в $H_1$, удовлетворяющий тому же ограничению). Утверждение (а) для «пропозициональных» правил $G'_1$, имеющихся также и в $G'_0$, фактически уже доказано в § 5.5 при доказательстве равносильности $G_0$ и $H_0$; для правила УА достаточно воспользоваться схемой аксиом V1 и правилом MP, для ВЕ — схемой V2 и тем же MP. Утверждение (б) нужно доказать для правил Т, УД, ВИ, ВО′, ВА, УЕ. Для правила Т оно тривиально (ср. сноску к доказательству теоремы о дедукции для $H_0$). Докажем его справедливость для УД. Пусть существуют выводы в $H_1$ формулы $\mathfrak{C}$ из $\Gamma$, $\mathfrak{A}$ и из $\Gamma$, $\mathfrak{B}$, в которых ни к каким переменным, входящим свободно в первом случае в формулы из $\Gamma$ и в $\mathfrak{A}$, а во втором — в формулы из $\Gamma$ и в $\mathfrak{B}$, не применяется правило Об. Ввиду этого ограничения мы можем воспользоваться теоремой о дедукции и заключить, что из $\Gamma$ выводимы в $H_1$ формулы $\mathfrak{A}\supset\mathfrak{C}$ и $\mathfrak{B}\supset\mathfrak{C}$; более того, их можно вывести так, чтобы к переменным, входящим свободно в $\Gamma$, не применялось правило Об (см. замечание к теореме о дедукции для $H_1$). Остается воспользоваться схемой аксиом П3 и (трижды) правилом MP. Аналогично доказывается утверждение для ВИ и ВО′ (в последнем случае нужно убедиться, что рассуждения, использованные при доказательстве ВО′ для $H_0$, пригодны и для $H_1$ и сохраняют ограничение, налагаемое нами теперь на вывод). Для правила ВА точная формулировка утверждения (б) приведена выше, а само оно очевидно, т. к. переменная $x$, к которой применяется Об при переходе от $\mathfrak{A}$ к $\forall x\mathfrak{A}$, по условию не входит свободно в формулы из $\Gamma$. Остается правило УЕ. Но если существует вывод $\mathfrak{C}$ из $\Gamma$, $\mathfrak{A}$, в

котором Об не применяется к переменным, входящим свободно в формулы из $\Gamma$ и в $\mathfrak{A}$, и переменная $x$ не входит свободно ни в одну формулу из $\Gamma$ и в $\mathfrak{C}$, то в силу теоремы о дедукции и замечания к ней существует вывод в $H_1$ импликации $\mathfrak{A}\supset\mathfrak{C}$ из $\Gamma$, в котором правило Об не применяется к переменным, входящим свободно в формулы из $\Gamma$, и отсюда $\Gamma\vdash_{H_1}\forall x(\mathfrak{A}\supset\mathfrak{C})$ с сохранением того же ограничения на вывод; но если к выводу формулы $\forall x(\mathfrak{A}\supset\mathfrak{C})$ из $\Gamma$ приписать формулу $\exists x\mathfrak{A}$ и аксиому (по схеме V4) $\forall x(\mathfrak{A}\supset\mathfrak{C})\supset(\exists x\mathfrak{A}\supset\mathfrak{C})$, а затем дважды применить MP, получится вывод $\mathfrak{C}$ из $\Gamma$, $\exists x\mathfrak{A}$, удовлетворяющий нашему ограничению.

**2.** Рассмотрим теперь секвенциальный вариант исчисления предикатов, который мы будем обозначать $S_1$. Алфавит и правила образования термов и формул исчисления $S_1$ будут те же, что в $H_1$. Схемами фигур заключения $S_1$ будут все схемы фигур заключения исчисления $S_0$ (см. § 5.5) и еще четыре схемы логических фигур:

9) *Введение общности в антецедент* (В∀А):

$$\frac{\mathfrak{A}(t),\ \Gamma\to\Delta}{\forall x\mathfrak{A}(x),\ \Gamma\to\Delta}$$

10) *Введение общности в сукцедент* (В∀С):

$$\frac{\Gamma\to\Delta,\ \mathfrak{A}(x)}{\Gamma\to\Delta,\ \forall x\mathfrak{A}(x)}$$

11) *Введение существования в антецедент* (В∃А):

$$\frac{\mathfrak{A}(x),\ \Gamma\to\Delta}{\exists x\mathfrak{A}(x),\ \Gamma\to\Delta}$$

12) *Введение существования в сукцедент (В∃С):*

$$\frac{\Gamma\to\Delta,\ \mathfrak{A}(t)}{\Gamma\to\Delta,\ \exists x\mathfrak{A}(x)}$$

В этих схемах на $x$ и $t$ накладываются следующие ограничения: в В∀А и В∃С $t$ должен быть термом, свободным для подстановки вместо переменной $x$ в $\mathfrak{A}$; в В∀С и В∃А переменная $x$ не должна входить свободно ни в одну формулу из $\Gamma\cup\Delta$.

*Дерево вывода* и *выводимая секвенция* определяются для $S_1$ так же, как для $S_0$.

Очевидно, всякая «схема деревьев вывода» в $S_0$ годится и для $S_1$; поэтому всякая «схема выводимых секвенций» исчисления $S_0$ будет «схемой выводимых секвенций» и в $S_1$.

Приведем два примера выводов в $S_1$ с использованием новых фигур заключения.

1) Вывод секвенции $\neg\exists x\mathfrak{A}(x) \to \forall x\neg\mathfrak{A}(x)$:

$$\dfrac{\dfrac{\dfrac{\mathfrak{A}(x)\to\mathfrak{A}(x)}{\mathfrak{A}(x)\to\exists x\mathfrak{A}(x)}\,\text{В}\exists\text{С} \qquad \dfrac{\dfrac{\exists x\mathfrak{A}(x)\to\exists x\mathfrak{A}(x)}{\neg\exists x\mathfrak{A}(x),\ \exists x\mathfrak{A}(x)\to}\,\text{ВОА}}{\exists x\mathfrak{A}(x),\ \neg\exists x\mathfrak{A}(x)\to}\,\text{ПА}}{\dfrac{\mathfrak{A}(x),\ \neg\exists x\mathfrak{A}(x)\to}{\neg\exists x\mathfrak{A}(x)\to\neg\mathfrak{A}(x)}\,\text{ВОС}}\ \text{сечение}$$
$$\dfrac{\neg\exists x\mathfrak{A}(x)\to\neg\mathfrak{A}(x)}{\neg\exists x\mathfrak{A}(x)\to\forall x\neg\mathfrak{A}(x)}\,\text{В}\forall\text{С}$$

2) Вывод секвенции $\forall x\mathfrak{A}\vee\mathfrak{B}\to\forall x(\mathfrak{A}\vee\mathfrak{B})$ (при условии, что $x$ не входит свободно в $\mathfrak{B}$):

$$\dfrac{\dfrac{\dfrac{\mathfrak{A}(x)\to\mathfrak{A}(x)}{\mathfrak{A}(x)\to\mathfrak{A}(x)\vee\mathfrak{B}}\,\text{ВДС}}{\forall x\mathfrak{A}(x)\to\mathfrak{A}(x)\vee\mathfrak{B}}\,\text{В}\forall\text{А} \qquad \dfrac{\mathfrak{B}\to\mathfrak{B}}{\mathfrak{B}\to\mathfrak{A}(x)\vee\mathfrak{B}}\,\text{ВДС}}{\forall x\mathfrak{A}(x)\vee\mathfrak{B}\to\mathfrak{A}(x)\vee\mathfrak{B}}\,\text{ВДА}$$
$$\dfrac{\forall x\mathfrak{A}(x)\vee\mathfrak{B}\to\mathfrak{A}(x)\vee\mathfrak{B}}{\forall x\mathfrak{A}(x)\vee\mathfrak{B}\to\forall x(\mathfrak{A}(x)\vee\mathfrak{B})}\,\text{В}\forall\text{С}$$

Отмеченное на с. 197 свойство фигур заключения исчисления $S_0$, отличных от сечения, имеет место и для новых логических фигур 9—12. Поэтому всякое дерево вывода в $S_1$, не содержащее сечений, обладает, и в $S_0$, свойством подформульности[19]. В то же время для $S_1$ справедлива *основная теорема Генцена*: для любой секвенции, выводимой в $S_1$, существует дерево вывода без сечений, и такое дерево можно эффективно построить по произвольному дереву вывода данной секвенции. Комментарии по поводу этой теоремы (которую мы не будем доказывать) и библиографические ссылки см. выше, в § 5.5.

Задачи. 1) Построить деревья вывода для секвенций, соответствующих некоторым (или всем) выводимостям из § 6.1 (пункт 4).

2) Вывести секвенцию примера 1) без сечения.

Можно показать, что исчисление $S_1$ равносильно исчислению $G_1$ в том смысле, что секвенция $\Gamma\to\Delta$ выводима в $S_1$ тогда и только тогда, когда $\Gamma'\to\widetilde{\delta}^{\wedge}$, где $\Gamma'$ — множество формул, входящих в $\Gamma$, и $\widetilde{\delta}^{\wedge}$ есть формула $\mathfrak{B}_1\vee\dots\vee\mathfrak{B}_k$, если $\Delta=\mathfrak{B}_1,\dots,\mathfrak{B}_k$, а если $\Delta$ — пустая последовательность, то $\widetilde{\delta}^{\wedge}=F_1^1(a_1)\,\&\,\neg F_1^1(a_1)$. Вместо этого, очевидно, достаточно доказать, что $S_1$ равносильно в том же смысле исчислению $G_1'$, построенному в пункте 1 настоящего параграфа. Доказательство

[19] Правда, здесь это свойство имеет место лишь при более общем понимании подформулы, при котором формула, получаемая из подформулы формулы $\mathfrak{A}$ заменой некоторых переменных произвольными свободными для подстановки вместо них термами, также считается подформулой формулы $\mathfrak{A}$.

аналогично намеченному в § 5.5 доказательству равносильности исчислений $S_0$ и $G_0'$; как и там, мы приведем сейчас только общую схему, по которой читатель сможет восстановить подробности.

а) Тот факт, что из выводимости в $S_1$ секвенции $\Gamma \to \Delta$ следует $\Gamma \vdash_{G_1} \widetilde{\forall}\Delta$, доказывается, как и для исчислений $S_0$ и $G_0'$ возвратной индукцией по высоте дерева вывода секвенции. Базис и случаи индукционного шага, отвечающие старым фигурам заключения, не отличаются от соответствующих частей рассуждения из § 5.5. Аналогично проводится и индукционный шаг для новых случаев: для BVC и B∃C при непустом $\Delta$ применяется тот же прием, который был использован для сечения при непустом $\Theta$.

б) Обратное утверждение также доказывается совершенно аналогично соответствующему утверждению для $S_0$ и $G_0'$; добавляются четыре новых случая, отвечающие правилам введения и удаления общности и существования. В качестве примера приведем стандартное секвенциальное дерево для правила B∃:

$$\dfrac{\Gamma \to \mathfrak{A}(t) \qquad \dfrac{\mathfrak{A}(t) \to \mathfrak{A}(t)}{\mathfrak{A}(t) \to \exists x \mathfrak{A}(x)}\ \text{B}\exists\text{C}}{\Gamma \to \exists x \mathfrak{A}(x)}\ \text{сечение}$$

Замечание. Проведя все рассуждения для новых случаев, читатель убедится, что в первой части доказательства закон исключенного третьего применяется, как и в старых случаях, лишь тогда, когда сукцедент содержит больше одной формулы, а во второй части ни в одном из стандартных деревьев, отвечающих новым случаям, нет секвенций более чем с одной формулой в сукцеденте. Отсюда и из замечания в конце пункта 4 § 5.5 следует, что конструктивный вариант $G_1$ (т. е. $G$ без закона исключенного третьего) равносилен исчислению $S_1$ с дополнительным условием, что сукцедент каждой секвенции содержит не более одной формулы.

## § 6.5. ИСЧИСЛЕНИЕ ПРЕДИКАТОВ И АРИСТОТЕЛЕВСКАЯ СИЛЛОГИСТИКА

1. В традиционной формальной логике, идущей от Аристотеля (см. Введение) было подробно разработано учение о *категорических суждениях* — предложениях, описывающих простейшие взаимоотношения между свойствами предметов. Рассматриваемые в традиционной логике категорические суждения разделяются,

с одной стороны, на *утвердительные* и *отрицательные*, с другой — на *частные* и *общие*. Это дает четыре типа суждений:

1. *Общеутвердительные*: «Все предметы, обладающие свойством $S$, обладают свойством $P$».

2. *Частноутвердительные*: «Некоторые предметы, обладающие свойством $S$, обладают свойством $P$».

3. *Общеотрицательные*: «Никакой предмет, обладающий свойством $S$, не обладает свойством $P$».

4. *Частноотрицательные*: «Некоторые предметы, обладающие свойством $S$, не обладают свойством $P$».

По давней традиции общеутвердительные и частноутвердительные суждения обозначают соответственно прописными латинскими буквами $A$ и $I$ (первой и второй гласными латинского слова *affirmo* — «утверждаю»), общеотрицательные и частноотрицательные — буквами $E$ и $O$ (первой и второй гласными латинского слова *nego* — «отрицаю»).

В литературе по традиционной логике суждения чаще представляются с помощью *терминов* — слов или словосочетаний (обычно существительных или именных групп), которые служат общими именами предметов, обладающих данными свойствами. Например, для свойства «быть человеком» соответствующий термин — «человек», для свойства «быть простым числом» — «простое число», для свойства «делиться на 5» — «число, делящееся на 5». Предложения, получающиеся при таком способе представления, обычно короче и лучше стилистически. Они имеют следующий вид ($T_s$ и $T_p$ — термины, отвечающие свойствам $S$ и $P$ соответственно):

$A$: «Все $T_s$ суть $T_p$» («Все существа, способные к абстрактному мышлению — люди»; «Все птицы — животные», «Все ромбы — параллелограммы».

$I$: «Некоторые $T_s$ суть $T_p$» («Некоторые люди — китайцы», «Некоторые морские животные — млекопитающие», «Некоторые ромбы — прямоугольники»).

$E$: «Ни одно $T_s$ не есть $T_p$» («Ни один великий поэт — не декадент», «Ни одно млекопитающее, обитающее в Европе,— не сумчатое»; «Ни один квадрат — не треугольник»).

$O$: «Некоторые $T_s$ не суть $T_p$» («Некоторые математики — не преподаватели»; «Некоторые лесные растения — не деревья»; «Некоторые делители числа 6 — не простые числа»).

Часто используется также «комбинированный» способ, при котором первый член суждения представляется термином, а второй — названием свойства: «Все $T_s$ обладают свойством $P$» и т. п. («Все люди смертны», «Некоторые бельгийцы говорят по-фламандски»

ски»; «Ни одно простое число не делится на 10»; «Некоторые птицы не умеют летать»).

Заметим, что при обоих способах представления суждения с помощью терминов его первый член — подлежащее (точнее, группа подлежащего), а второй — сказуемое (группа сказуемого). Их и называют соответственно *субъектом* и *предикатом* суждения[20].

Посмотрим, как выражаются суждения типов *A*, *I*, *E*, *O* на символическом языке современной математической логики. На первый взгляд их перевод на этот язык представляется совершенно очевидным: если обозначить, как мы делали в гл. 2, соответствующие свойствам $S$ и $P$ предикаты теми же буквами $S$ и $P$, то наши четыре типа суждений будут представляться так:

$$(1)\quad \begin{cases} A\colon \forall x(S(x)\supset P(x)); \\ I\colon \exists x(S(x)\&P(x)); \\ E\colon \forall x(S(x)\supset \neg P(x)); \\ O\colon \exists x(S(x)\&\neg P(x)); \end{cases}$$

Это простое представление нуждается, однако, в уточнении. Дело в том, что в отличие от математической логики, в основе которой лежит язык современной математики, традиционная формальная логика возникла и развивалась на базе естественного языка; а в естественном языке предложение, в котором идет речь о том или ином предмете, осмыслено лишь тогда, когда этот предмет существует; при произнесении такого предложения существование данного предмета подразумевается. Например, предложение «Жена Ивана работает на почте» подразумевает (независимо от того, истинно оно или ложно) истинность предложения «У Ивана есть жена»[21]. В частности, в предложениях, в которых идет речь обо всех или некоторых предметах, обладающих тем или иным свойством, подразумевается, что предметы с данным свойством существуют; как говорят лингвисты, такие предложения содержат *презумпцию*[22] существования предметов с данным свойством. Поэтому и в традиционной формальной логике при рассмотрении категорических суждений подразумевается, что свойства $S$ и $P$ для каких-то предметов имеют место, и предложения вроде «Все действительные корни уравнения

[20] Об истории этих терминов см. следующий параграф.

[21] Более точно это означает следующее: когда такое предложение произносится в условиях нормального речевого акта, говорящий уверен, что истинность предложения «У Ивана есть жена» не противоречит сведениям, имеющимся у слушающего.

[22] От лат. *praesumptio* — «предположение, ожидание». В том же значении употребляется также термин *пресуппозиция* (от латинского *praesuppositio*, имеющего тот же смысл).

$x^2 + 1 = 0$ — целые числа» или «Некоторые единороги живут в Гренландии» в этой логике не рассматриваются, в то время как математическая логика свободно оперирует и такими предложениями и присваивает им истинностные значения (первое из двух приведенных сейчас предложений она считает истинным, второе — ложным). Эта особенность языка математической логики связана с тем, что современная математика широко пользуется понятием пустого множества, введение которого позволило существенно упростить многие математические построения и придать им более законченный характер[23].

Впрочем, традиционная логика в своем понимании суждений также отошла от естественного языка, хотя и не так сильно, как математическая. В естественном языке предложения с кванторными словами «все», «некоторые», «ни один» и т. п. содержат более сильную презумпцию, чем существование предметов с соответствующими свойствами: в них подразумевается, что предметов с этими свойствами имеется «достаточно много» и уж во всяком случае больше одного. Эта презумпция была отброшена уже традиционной логикой: она признает законными (и истинными) такие необычные для обиходной речи суждения, как «Все делители единицы равны единице», «Некоторые тверские князья были братьями Александра Невского»[24], «Ни один русский царь по имени Михаил не отличался крепким здоровьем», «Некоторые острова, на которых родился Наполеон, не находятся в Тихом океане». Это, разумеется, подготовило почву для следующего шага — введения в рассмотрение предложений с кванторными словами, относящимися к «пустым» свойствам. С другой стороны, в естественном языке презумпция существования относится только к теме предложения (см. выше, с. 79), которая в предложениях нейтрального стиля, выражающих простые категорические суждения, обычно совпадает с подлежащим (ср. старое школьное определение подлежащего как «того, о чем говорится в предложении»). В самом деле, предложения вроде «Карл Великий был гренландским императором» или «Некоторые киевские княгини были ведьмами» воспринимаются не как неправильные (противоречащие языковым нормам), а только как ложные, подобно предложениям «Карл Великий был китайским императором» или «Некоторые киевские княгини были уроженками острова Пасхи». Однако традицион-

[23] Это можно сравнить с той ролью, которую в свое время сыграло введение числа нуль. Кстати, абстракции нуля и пустого множества тесно связаны между собой: ведь нуль — это не что иное, как мощность пустого множества. Введение нуля и введение пустого множества — два этапа одного процесса.

[24] На самом деле братом Александра Невского был только первый тверской князь Ярослав Ярославич.

ная логика не делает в этом отношении различия между субъектом и предикатом и предполагает (хотя и неявно), что существуют как предметы, обладающие свойством $S$, так и обладающие свойством $P$.

Возвращаясь к представлению категорических суждений традиционной логики на современном символическом языке, мы можем теперь сказать, что все они содержат следующую презумпцию: ни один из предикатов $S$ и $P$ не должен быть тождественно ложным. Иначе говоря, должно быть истинно предложение $\exists y S(y) \& \exists z P(z)$. Присоединив это предложение конъюнктивно к каждому из выражений (1), мы и получим точное представление традиционных типов категорических суждений на символическом языке:

$$(2)\quad \begin{cases} A\text{: } (\exists y S(y) \& \exists z P(z))(\& \forall x(S(x) \supset P(x)); \\ I\text{: } (\exists y S(y) \& \exists z P(z)) \& \exists x(S(x) \& P(x)); \\ E\text{: } (\exists y S(y) \& \exists z P(z))(\& \forall x(S(x) \supset \neg P(x)); \\ O\text{: } (\exists y S(y) \& \exists z P(z)) \& \exists x(S(x) \& \neg P(x)). \end{cases}$$

Общий для всех этих формул конъюнктивный член $\exists y S(y) \& \exists z P(z)$ мы будем называть *презумпцией* или *подразумеваемой частью* суждения, а второй конъюнктивный член — его *основой* или *утверждаемой частью*.

Формулы (2) для частных суждений можно очевидным образом упростить: представление $O$ равносильно $\exists z P(z) \& \exists x(S(x) \& \neg P(x))$, представление $I$ — $\exists x(S(x) \& P(x))$. Однако полные представления удобнее тем, что в них явно выделяются подразумеваемая и утверждаемая части.

В традиционной логике был установлен ряд свойств категорических суждений, важнейшие из которых следующие:

I. Суждения типов $A$ и $O$ находятся между собой в отношении противоречия, и то же верно для $I$ и $E$. Это значит, что суждение типа $A$ с членами $S$ и $P$ истинно тогда и только тогда, когда суждение типа $O$ с теми же членами ложно, и аналогично для $I$ и $E$.

II. Суждения типов $I$ и $E$ допускают обращение, т. е. сохраняют истинность при перестановке членов[25].

[25] В традиционной логике перестановка членов суждения называется *простым* или *чистым обращением* (*conversio simplex*) в отличие от *обращения посредством ограничения* (*conversio per limitationem* или *per accidens*) — операции, состоящей в перестановке членов общего суждения с одновременным превращением его в частное. Последняя операция применима и к суждениям типа $A$ (например, из истинности суждения «Все металлы — химические элементы» следует истинность суждения «Некоторые химические элементы — металлы»); это тривиальным образом выпекает из их представления в виде (2) (но не в виде (1)!).

Свойство II тривиальным образом следует из представлений (2), поскольку формула $S(x)\&P(x)$ равносильна (а в исчислении предикатов дедуктивно эквивалентна) формуле $P(x)\&S(x)$, и то же верно для формул $S(x)\supset\neg P(x)$ и $P(x)\supset\neg S(x)$. Сложнее обстоит дело со свойством I. Легко убедиться, что, например, отрицание представления (2) для $A$ не равносильно соответствующему представлению для $O$ (и вообще никакому из представлений (2)). Возникает эта неравносильность из-за того, что с точки зрения математической логики предложение типа $A$ ложно не только тогда, когда истинно предложение типа $O$ с теми же членами, но и при нарушении презумпции. (Например, если $S$ — свойство быть натуральным числом, удовлетворяющим условию $0 < n < 1$, и $P$ — любое свойство, то все формулы (2) дают ложные предложения.) Чтобы передать на нашем языке точку зрения традиционной логики, мы должны понимать отрицание суждения иначе — так, чтобы оно не затрагивало презумпцию. Для этого введем следующее определение:

Пусть $C$ — предложение одного из видов (2)$A$, (2)$I$, (2)$E$, (2)$O$. Мы будем называть *внутренним отрицанием* предложения $C$ конъюнкцию его подразумеваемой части и отрицания его утверждаемой части.

Теперь непосредственно очевидно, что внутреннее отрицание предложения вида (2)$A$ равносильно (и дедуктивно эквивалентно) предложению вида (2)$O$ с теми же членами, и то же верно при перемене местами $A$ и $O$; аналогично для $E$ и $I$. Тем самым обосновано свойство I.

Например, из истинности суждения «Все птицы — животные» вытекает ложность суждения «Некоторые птицы — не животные», и обратно; из истинности суждения «Некоторые ромбы — прямоугольники» вытекает ложность суждения «Ни один ромб — не прямоугольник», и обратно.

Замечание. Можно также интерпретировать категорические суждения в терминах отношений между классами. Если для простоты обозначать классы предметов, обладающих свойствами $S$ и $P$, также через $S$ и $P$, то основная часть суждения типа $A$ будет означать, что $S$ содержится в $P$, типа $I$ — что $S$ пересекается с $P$, типа $E$ — что $S$ содержится в дополнении $P$, типа $O$ — что $S$ пересекается с дополнением $P$; презумпция суждения любого типа означает, что $S$ и $P$ не пусты.

**2.** Важнейшим разделом традиционной формальной логики является учение о *простых категорических силлогизмах*[26] — элементарных умозаключениях, с помощью которых из двух категориче-

[26] От греч. συλλογισμός «рассуждение, умозаключение».

ских суждений выводится третье. Основные понятия и главнейшие положения этого учения содержатся уже в трудах Аристотеля. В дальнейшем мы будем для краткости называть простые категорические силлогизмы просто *силлогизмами*.

В каждом силлогизме суждение с субъектом $S$ и предикатом $P$, называемое *заключением* данного силлогизма, выводится из двух суждений, называемых его *посылками*, одно из которых содержит $S$, а другое $P$. Кроме того, обе посылки содержат еще один член $M$ (один и тот же в обеих). $P$, $S$ и $M$ мы будем называть соответственно *бо́льшим*, *меньшим* и *средним членами силлогизма* (чаще говорят, впрочем, о *бо́льшем*, *меньшем* и *среднем терминах*). Посылка, содержащая больший член, называется *бо́льшей посылкой*, содержащая меньший — *меньшей посылкой*.

Пример силлогизма:

Во всяком прямоугольнике диагонали равны.
Всякий квадрат есть прямоугольник.
---
Следовательно, во всяком квадрате диагонали равны.

Бо́льшая посылка может либо иметь $M$ своим субъектом, а $P$ — предикатом, либо, наоборот, $P$ — субъектом и $M$ — предикатом. Аналогичные две возможности имеются для меньшей посылки. Комбинирование этих возможностей дает четыре типа силлогизмов, или, как обычно говорят, четыре *фигуры силлогизма*:

| I | II | III | IV |
|---|---|---|---|
| MP | PM | MP | PM |
| SM | SM | MS | MS |
| SP | SP | SP | SP |

Здесь в каждой схеме над чертой записаны посылки, под чертой — заключение; в схематической записи каждого суждения на первом месте стоит субъект, на втором — предикат.

A priori каждое из трех суждений, входящих в силлогизм, может принадлежать к одному из четырех типов $A$, $I$, $E$, $O$. Это дает для каждой фигуры $4^3 = 64$ комбинации: $AAA$, $AAI$, $AAE$, ..., $OOO$. Всего получается таким образом, $64 \cdot 4 = 256$ мыслимых видов, или, как принято говорить, *модусов*[27] силлогизма. Но из всех этих формально возможных модусов лишь немногие *правильны*, т. е. обладают тем свойством, что из истинности обеих посылок построенного по данному модусу силлогизма вытекает истинность его заключения. Правильные модусы силлогизма принято обозначать специально придуманными словами из букв латинского алфавита (не имеющими собственного смысла), каждое из которых содержит три гласных; первая

[27] От лат. *modus* — «способ».

из них обозначает тип большей посылки, вторая — тип меньшей, третья — тип заключения[28]. Вот списки рассматриваемых в традиционной логике правильных модусов по фигурам:

| I | II | III | IV |
|---|---|---|---|
| Barbara | Cesare | Darapti | Bramantip |
| Celarent | Camestres | Disamis | Camenes |
| Darii | Festino | Datisi | Dimaris |
| Ferio | Baroko | Felapton | Fesapo |
| | | Bokardo | Fresison |
| | | Ferison | |

Приведенный выше силлогизм был построен по модусу Barbara. Дадим еще два примера.

Модус Ferio:

Ни один малограмотный не годится в учителя.
Некоторые выпускники педагогических институтов малограмотны.
Следовательно, некоторые выпускники педагогических институтов не годятся в учителя.

Модус Darapti:

Все киты живут в воде.
Все киты — млекопитающие.
Следовательно, некоторые млекопитающие живут в воде.

(Заметим, что в последнем примере используется презумпция непустоты классов).

Кроме перечисленных девятнадцати модусов, правильными являются еще пять: *AAI* и *EAO* первой фигуры, *EAO* и *AEO* второй фигуры, *AEO* четвертой фигуры. Их правильность тривиальным образом вытекает из правильности модусов Barbara, Celaren, Cesare, Camestres, Camenes, поскольку из истинности суждения типа *A* следует истинность суждения типа *I* с теми же членами (если верно, что все $T_s$ суть $T_p$, то тем более верно, что некоторые $T_s$ суть $T_p$), и то же справедливо для *E* и *O*[29]. Но для реальных рассуждений эти модусы

[28] Согласные, хотя и не все, тоже имеют мнемоническое значение (см. задачу 23 в конце главы).

[29] В обиходной речи в условиях нормального речевого акта предложение вида «Некоторые $T_s$ суть $T_p$» не может употребляться, если говорящий уверен, что на самом деле в с е $T_s$ суть $T_p$. Но его можно употребить, в частности, тогда, когда говорящий, будучи уверен, что хотя бы некоторые $T_s$ суть $T_p$, не знает, верно ли это для всех $T_s$, и если потом будет установлено, что в действительности все $T_s$ суть $T_p$, утверждение «Некоторые $T_s$ суть $T_p$» все-таки не считается опровергнутым. (Ср. описание значения союза «или» в § 2.3.) Такого понимания частных суждений — как не противоречащих общим, но более слабых — придерживается и традиционная формальная логика (равно как и математическая).

никакого значения не имеют: незачем доказывать более слабое утверждение, если можно в точности так же доказать более сильное. Поэтому в традиционной логике указанные пять модусов не рассматриваются.

Остальные 232 модуса — неправильные.

Теперь наша задача — понять, как, пользуясь средствами математической логики, обосновать модусы, признаваемые в традиционной логике правильными, и опровергнуть те, которые она считает неправильными.

Чтобы опровергнуть тот или иной модус, достаточно указать интерпретацию, в которой посылки некоторого построенного по этому модусу силлогизма истинны, а заключение ложно. Рассмотрим, например, модус *AEE* первой фигуры. По этому модусу, если бы он был правильным, из суждений «Все $T_M$ суть $T_P$» и «Ни одно $T_S$ не есть $T_M$» выводилось бы суждение «Ни одно $T_S$ не есть $T_P$». Но если взять в качестве $S$, $P$ и $M$ соответственно свойства «быть числом, дающим при делении на 3 остаток 1», «быть четным числом» и «быть числом, делящимся на 6», мы увидим, что хотя суждения «Все числа, делящиеся на 6, четны» и «Ни одно число, дающее при делении на 3 остаток 1, не делится на 6» истинны, суждение «Ни одно число, дающее при делении на 3 остаток 1, не является четным» ложно. Не составляет труда записать для этих суждений представления в виде (2).

Само собой, подбор опровергающих интерпретаций для 232 модусов был бы крайне скучным и утомительным занятием и потребовал бы очень много времени. Но тот, кто захочет лично убедиться, что традиционная логика права, отвергая эти модусы, легко заметит, что перебор можно существенно сократить. Прежде всего, поскольку из правильности модуса *XYA* некоторой фигуры следует правильность модуса *XYI* той же фигуры (этим мы пользовались выше), мы можем, доказав неправильность модуса *XYI* какой-либо фигуры, сразу заключить, что модус *XYA* этой фигуры тоже неправилен; аналогично для *XYO* и *XYE*. Уже одно это тривиальное соображение сокращает перебор почти вдвое. Но точно так же неправильность одного из модусов *AYZ*, *EYZ*, *XAZ*, *XEZ* той или иной фигуры влечет соответственно неправильность модуса *IYZ*, *OYZ*, *XIZ* или *XOZ* этой фигуры. Кроме того, работа намного облегчится, если пользоваться теоретико-множественной моделью (см. замечание в конце пункта 1 этого параграфа) и соответствующими рисунками. (Так, доказанная только что неправильность модуса *AEE* первой фигуры означает, что из $M \subset P$ и $S \cap M \neq \varnothing$ даже при дополнительном условии непустоты всех трех классов $S$, $M$, $P$ не следует $S \cap P \neq \varnothing$.) Внимательное рассмотрение этой модели даст возможность заметить некоторые

закономерности (приводимые обычно в учебниках традиционной логики): обе посылки правильного модуса не могут быть частными; обе посылки правильного модуса не могут быть отрицательными; если одна из посылок частная, то и заключение должно быть частным; если одна из посылок отрицательная, то и заключение должно быть отрицательным, и обратно, если заключение отрицательное, то одна из посылок должна быть также отрицательной, и т. д. Использование этих закономерностей позволяет свести перебор к минимуму. В подробности мы вдаваться не будем: такого рода работу всегда проще и полезнее проделать самому, чем проследить, как ее выполнил другой.

Перейдем теперь к обоснованию правильных модусов. Это можно делать либо синтаксическим способом, доказывая, что формула, представляющая заключение силлогизма, выводима в исчислении предикатов из формул, представляющих посылки, либо семантическим, доказывая вместо выводимости семантическое следование. Ввиду полноты и семантической пригодности исчисления предикатов эти способы равносильны. Мы применим синтаксический способ, причем будем пользоваться исчислением $G_1$; говоря о выводимости, будем иметь в виду выводимость в этом исчислении. Кроме того, условимся еще об одном соглашении: в дальнейшем, говоря о большей посылке, меньшей посылке или заключении силлогизма, мы будем подразумевать представления этих суждений в виде (2).

Прежде всего ясно, что для любого мыслимого силлогизма из презумпций его посылок, т. е. формул $\exists y M(y)\&\exists z P(x)$ и $\exists y S(y)\&\exists z M(z)$ (так для первой фигуры; для остальных аналогично) выводима презумпция его заключения — $\exists y S(y)\&\exists z P(z)$. Поэтому для доказательства правильности силлогизма достаточно вывести из его посылок основную часть заключения.

Начнем с первой фигуры. Для каждого из ее правильных модусов можно вывести основную часть заключения даже из основных частей посылок, не пользуясь презумпциями, а именно:

Barbara: $\forall x(M \supset P), \forall x(S \supset M) \vdash \forall x(S \supset P)$ по У$\forall$, ТИ[10] и В$\forall$.
Celarent: $\forall x(M \supset \neg P), \forall x(S \supset M) \vdash \forall x(S \supset \neg P)$ точно так же.
Darii: $\forall x(M \supset P), \exists x(S\&M) \vdash \exists x(S\&P)$ по У$\forall$, УК, УИ, ВК, В$\exists$, У$\exists$.
Ferio: $\forall x(M \supset \neg P), \exists x(S\&M) \vdash \exists x(S\&\neg P)$

точно так же.

Для правильных модусов второй фигуры основные части заключений также выводятся из основных частей посылок. При этом соответствующие выводимости легко получить из выводимостей, дока-

[10] ТИ — закон транзитивности импликации ((37) из § 5.3).

занных только что для силлогизмов первой фигуры[51]. Например, для модуса Camestres нужная выводимость $\forall x(P \supset M)$, $\forall x(S \supset \neg M) \vdash \forall x(S \supset \neg P)$ получается из выводимости для силлогизма по модусу Celarent со средним членом $\neg M$, если воспользоваться дедуктивной эквивалентностью импликаций $P \supset M$ и $\neg M \supset \neg P$. Легко проверить, что тем же способом — контрапозицией в большей посылке — модус Cesare сводится также к Celarent, а Festino и Baroko — к Ferio.

В третьей фигуре для четырех из шести правильных модусов — Disamis, Datisi, Bokardo, Ferison — тоже можно вывести основные части заключений из основных частей посылок; соответствующие деревья вывода читатель легко построит сам. Для модусов Darapti и Felapton основные части заключений не выводимы из основных частей посылок. В самом деле, для Darapti соответствующая выводимость имела бы вид $\forall x(M \supset P)$, $\forall x(M \supset S) \vdash \exists x(S \& P)$; если бы она была верна, то третья формула также и семантически следовала бы из первых двух, но это опровергается любой интерпретацией, в которой предикат $M(x)$ тождественно ложен, а $P(x)$ и $S(x)$ несовместимы. Совершенно аналогично можно рассуждать для модуса Felapton. Таким образом, здесь для вывода основной части заключения из посылок нужно пользоваться также и презумпциями последних. Для модуса Darapti соответствующая выводимость имеет вид

$$\exists y M(y) \& \exists z P(z) \& \forall x(M(x) \supset P(x)),$$

$$\exists y M(y) \& \exists z S(z) \& \forall x(M(z) \supset S(x)) \vdash \exists x(S(x) \& P(x));$$

читатель без труда докажет ее сам. Совершенно аналогичный вид имеет выводимость для модуса Felapton.

Наконец, в четвертой фигуре для модусов Camenes, Dimaris, Fresison основные части заключений выводимы из основных частей посылок, а для Fesapo и Bramantip необходимо пользоваться презумпциями. При этом первые четыре модуса легко свести к предыдущим подобно тому, как это было сделано для модусов второй фигуры: Camenes контрапозицией в обеих посылках сводится к Celarent; Dimaris перестановкой членов в большей посылке — к Disamis; Fresison перестановкой членов в меньшей посылке — к Festino; Fesapo контрапозицией в большей посылке — к Felapton. Для Bramantip нужная выводимость есть

$$\exists y P(y) \& \exists z M(z) \& \forall x(P(x) \supset M(x)),$$

$$\exists y M(y) \& \exists z S(z) \& \forall x(M(x) \supset S(x)) \vdash \exists x(S(x) \& P(x)).$$

[51] Сходным образом поступают и в традиционной логике: модусы первой фигуры считаются в ней очевидными, и к ним сводятся все остальные. Однако наши способы сведения отличаются от традиционных (о них см. задачу 23 в конце главы).

Ее легко доказать, заметив, что $P(x)$, $P(x) \supset M(x)$, $M(x) \supset S(x) \vdash P(x) \& S(x)$. Чтобы доказать для Bramantip невыводимость основной части заключения из основных частей посылок, можно взять в качестве $P$ и $M$ тождественно ложный предикат, для Fesapo — тождественно истинный в качестве $P$ и тождественно ложный в качестве $M$.

Итак, мы показали, что все девятнадцать традиционных правильных модусов обосновываются выводами в исчислении предикатов. Во всех этих выводах участвуют только одноместные предикаты; поэтому при обосновании аристотелевской силлогистики можно обойтись ослабленным вариантом исчисления предикатов — без многоместных предикатных символов (а также без функциональных символов и символов предметных констант, которыми мы тоже не пользовались). Для пятнадцати модусов основные части заключений выводимы из основных частей посылок — иначе говоря, выводимы из посылок без использования «непустоты» свойств, о которых идет речь в силлогизме; следовательно, эти модусы остаются правильными и при допущении суждений с кванторными словами, относящимися к «пустым» свойствам. Остальные четыре модуса при таком расширении традиционного представления о суждении теряют силу[32].

Замечание. Поскольку в традиционной логике требование непустоты рассматриваемых свойств не формулировалось явно, а лишь подразумевалось, можно спорить о том, какое уточнение презумпции существования лучше отвечает ее (традиционной логики) духу: в виде конъюнкции $\exists y S(y) \& \exists z P(z)$ или в более простом и более адекватном с точки зрения естественного языка виде $\exists y S(y)$ (ср. выше, с. 258). Решающий довод в пользу нашего представления подразумеваемой части суждения в виде конъюнкции состоит в том, что представление в виде $\exists y S(y)$ не обеспечивает выводимости всех традиционных правильных модусов силлогизма. При таком представлении подразумеваемая часть заключения следует из подразумеваемых частей посылок только для тех фигур, где субъект заключения является в меньшей посылке также субъектом, т. е. для первой и второй; что же касается третьей и четвертой фигур, то там при усло-

[32] В современной логической литературе иногда встречаются утверждения вроде следующего: «...Математическая логика доказала, что модус Bramantip... не может считаться общезначимым» (К о н д а к о в Н. И., Логический словарь. М., «Наука», 1971. С. 61). Это, разумеется, не так. Традиционная логика понимает суждение иначе, чем математическая, и при этом свойственном ей понимании все 19 модусов одинаково правильны. Математическая логика не «отменяет» традиционную (точно так же, как, скажем, теория относительности не «отменяет» классическую физику); нужно только ясно представлять себе, в каких границах справедливы традиционные логические законы.

вии, что меньшая посылка — утвердительное суждение, из этой посылки с использованием ее основной части можно вывести подразумеваемую часть заключения (действительно, в этом случае меньшая посылка представляется в виде $\exists y M(y) \& \forall x(M(x) \supset S(x))$ или $\exists y M(y) \& \& \exists x(M(x) \& S(x))$; из той и другой формулы очевидным образом следует $\exists y S(y)$). Этому условию удовлетворяют все модусы третьей фигуры, а в четвертой все, кроме одного — Camenes. В нем подразумеваемая часть заключения не следует из посылок, и по этому модусу из суждений с «непустыми» субъектами можно вывести суждение с «пустым» субъектом, например:

Все тигры — хищные животные
Ни одно хищное животное — не единорог
Ни один единорог — не тигр

По-видимому, в логике, которая стремилась бы в наибольшей возможной степени остаться верной духу естественного языка, модус Camenes не должен был бы считаться правильным[33].

На этом мы заканчиваем наш краткий очерк аристотелевской силлогистики и ее взаимоотношения с математической логикой[34]. В наши дни эта силлогистика может показаться частным и нетрудным вопросом, не идущим ни в какое сравнение с современными достижениями науки. Действительно, логика ушла далеко вперед с тех пор, как взяла на вооружение математические методы. Но фундаментом здания математической логики послужило именно это старое учение о суждении и силлогизме. В этом учении отражены самые существенные черты дедуктивного мышления; ему обязана математическая логика и самой идеей логического вывода, и главнейшим из своих понятий — понятием предиката, и теми представлениями, которые привели впоследствии к введению логических операций (см. следующий параграф).

Традиционная формальная логика — это замечательное достижение человеческого гения, потребовавшее огромной силы мысли (вспомним хотя бы о том, что Аристотелю и его последователям приходилось все, что мы сейчас записываем символически, выражать словами) и сильно повлиявшее на развитие не только науки, но и культуры в целом. И подобно всем таким достижениям она заслуживает не только почтительного взгляда, как некая реликвия, но и живого интереса и изучения.

[33] Нельзя не вспомнить в этой связи, что многие логики считают все вообще силлогизмы четвертой фигуры искусственными и бесполезными.

[34] Вопрос о взаимоотношении между аристотелевской силлогистикой и современной формальной логикой подробно рассмотрен в книге [Лукасевич 1959].

## § 6.6. ИСТОРИЧЕСКИЙ КОММЕНТАРИЙ К ГЛАВАМ 2—6

Как мы уже говорили, основы формальной логики были заложены Аристотелем. Ее основные понятия введены им в книгах «Категории» и «Об истолковании». Во второй из этих книг он определяет предмет своего исследования как «высказывающую речь», т. е. такую речь (λόγος), «в которой содержится истинность или ложность». В высказывающей речи он выделяет две части, соответствующие тому, что сейчас называют субъектом и предикатом, или подлежащим и сказуемым[35]. В качестве двух основных типов «высказывающих речей» он рассматривает утверждение и отрицание. В следующих книгах — «Первая аналитика» и «Вторая аналитика» — он строит теорию силлогизмов. (При этом первые три фигуры изложены систематически, по существу так же, как принято делать и сейчас; что касается четвертой, то все ее модусы упоминаются Аристотелем, но он не дает ее систематического изложения.)

После Аристотеля формальную логику развивали философы, принадлежавшие к различным школам. В частности, школа стоиков интересовалась в логике прежде всего способами составления сложных предложений из простых: именно стоики положили начало тому, что теперь называется логикой предложений или логикой высказываний. Одним из основных правил их логики был modus ponens. (Это правило еще до них использовали ученики Аристотеля Феофраст (Θεόφραστος, ок. 372—287 до н. э.) и Эвдем (Εὔδημος).) Тонкость и глубина логических построений стоиков были оценены по достоинству только в наше время[36].

Из ученых, занимавшихся логикой в последующие столетия[37],

---

[35] Аристотель не отделял учение о формах мышления (т.е. логику — сам он еще не пользовался этим термином) от учения о языке (см. об этом, например, [Steinthal 1863]), для которого его труды также сыграли основополагающую роль. И после Аристотеля в течение многих веков лингвистика развивалась под сильнейшим влиянием логики и нередко не отделялась от нее (см. [Steinthal 1863], [Pinborg 1967], [Ashworth 1974]). Правда, уже древнегреческие грамматики разработали учение о частях речи, склонении, спряжении и т. д. (см., например, [Античные теории ... 1936]; школьная грамматика до сих пор во всем существенном следует этому учению), но ни в античное время, ни в средние века не было учения о членах предложения. Грамматические понятия подлежащего и сказуемого, отдельные от логических понятий субъекта и предиката, появились, видимо, не ранее XVII в.

[36] В книгах по истории логики, написанных в XIX в., можно прочесть, что вклад стоиков в развитие логики был крайне незначительным, а многие их рассуждения попросту бессмысленны. (См., например, [Prantl 1855].) Авторы этих книг не знали математической логики.

[37] Логические исследования стоиков относятся в основном к III веку до н.э.

можно отметить Галена (Γαληνός ок. 130—200 н.э.); это тот самый Гален, который считается одним из величайших врачей древности. Он первый выдвинул требование строгой аксиоматизации логики. (Прежде ему приписывали также изобретение четвертой фигуры силлогизма, но многие современные исследователи вслед за Я. Лукасевичем считают это ошибкой.)

В средние века логика развивалась в рамках так называемой схоластической (т. е. «школьной») философии. Для ознакомления средневековых западноевропейских ученых с наследием античной логики огромное значение имела деятельность последнего значительного римского философа Боэция (Anicius Manlius Torquatus Severinus Boethius, ок. 480—525): переводы с греческого на латинский, комментарии к трудам древних авторов, а также его собственные логические сочинения. Именно Боэций ввел в употребление термины *subiectum* (в более позднем написании *subjectum*) и *praedicatum* (*subjectum* — от пассивного причастия глагола *subjicio* — «бросать, подкладывать, подставлять»; *praedicatum* — от пассивного причастия глагола *praedico* — «объявлять, заявлять, говорить»; русские термины «подлежащее» и «сказуемое» — переводы этих слов.) Схоластическая философия, подчиненная богословию и занимавшаяся чрезвычайно абстрактными вопросами, сделалась потом объектом насмешек, и слово «схоластика» стало употребляться для обозначения любых бесплодных, пустопорожних умствований. В действительности же средневековая философия внесла свой вклад в развитие человеческого мышления; в частности, были сделаны успехи в развитии логики, чему как раз способствовала изощренность схоластов в отвлеченных умозрительных построениях. Мы уже упоминали о правиле Дунса Скота: «Из противоречия можно вывести все, что угодно». Средневековым философам фактически были известны законы Де Моргана (разумеется, в словесной форме). В XIII в. испанский философ и богослов Раймунд Луллий (Raimundus Lullius, 1235—1315) предпринял попытку разработать способ механического моделирования логических операций, т. е., выражаясь современным языком, построить логическое исчисление. Выработанные схоластической философией представления о бесконечности содержали в себе зачатки идей, которые привели впоследствии к возникновению теории множеств. (Ее создатель Г. Кантор (см. сноску на с. 432) был глубоким знатоком философии, в том числе средневековой, и это обстоятельство, несомненно, имело существенное влияние на направление его исследований. Предшественник Кантора, предвосхитивший некоторые его идеи — чешский богослов, философ и математик Б. Больцано (Bernhard Bolzano, 1781—1848), в своих исследованиях о бесконечности непосредственно отправлялся от схоластики.) Однако качественный сдвиг в развитии формальной логики мог про-

изойти только благодаря ее символизации и математизации. Это стало возможно лишь после того, как символические обозначения вошли в обиход математики, т. е. уже в новое время[38]. Идея математизации логики впервые была выдвинута великим философом и математиком Г.В. Лейбницем (Gottfried Wilhelm Leibniz, 1646—1716). Он представлял себе математизированную логику как систему знаков, находящихся во взаимно однозначном соответствии с мыслями, и правил оперирования с этими знаками, построенных таким образом, что всякий раз, когда некоторая мысль является следствием другой, «образ» первой получается из «образа» второй по этим правилам[39]; эту систему Лейбниц называл «Всеобщей характеристикой» (Characteristica universalis). Он мечтал о времени, когда философы вместо того, чтобы спорить, будут говорить: «Посчитаем!»[40].

Лейбниц не построил развернутой формально-логической системы (сохранились только наброски), но под его влиянием в XVIII в. предпринимались попытки построения математизированных логических систем, продолжавшиеся и в первой половине XIX в. Первыми серьезными успехами в этом направлении были работы английских математиков А. Де Моргана[41] (Augustus De Morgan, 1806—1871) и Дж. Буля (George Boole, 1815—1864), с которых и начинается история математической логики как таковой — все предыдущее было предысторией (без которой, однако, математическая логика не могла бы возникнуть). А. Де Морган опубликовал в 1847 г. работу «Formal logic or the calculus of inference, necessary and probable» («Формальная логика или исчисление выводов, необходимых и вероятных»), в которой, поставив себе целью усовершенствовать теорию силлогизма, пользовался в неявном виде алгеброй классов (т. е. фактически алгеброй множеств, подчиняющейся тем же законам, что и алгебра предложений — см. § 1.1, пункт 9, и § 2.1, пункт 3; алгебраическую систему, подчиняющуюся этим законам, называют теперь *булевой алгеброй*). Законы, носящие теперь его имя, Де Морган сформулировал также на языке классов. В более поздних работах он заложил основы теории отношений.

В том же 1847 г. была опубликована работа Дж. Буля «The mathematical analysis of logic» («Математический анализ логики»). В

---

[38] Символические обозначения арифметических действий, знаки =, >, < и скобки вошли в употребление в течение XV—XVII веков. Тогда же появились буквенные обозначения для чисел.

[39] См. [Scholz 1931], с. 52—53.

[40] Развитие математической логики не оправдало этих надежд Лейбница. Более того, оно позволило установить (см. следующие две главы), что даже математическое рассуждение не всегда можно заменить вычислением.

[41] Встречающееся иногда написание «де Морган» неправильно.

которой также фактически вводится алгебра классов. Буль использует в этой работе символы двух видов: $X$, $Y$, $Z$, ..., и $x$, $y$, $z$, ... . Первые служат для обозначения предметов, входящих в определенные классы — $X$ для членов одного класса, $Y$ для членов другого и т. д.,— а вторые представляют собой «операторы выбора»: например, символ $x$, действуя на какой-либо класс, «выбирает» из него все $X$-ы, которые в нем содержатся. Но так как «универсум» (класс, содержащий все мыслимые предметы) естественно обозначать через 1, и так же естественно результат действия $x$ на 1 обозначать той же буквой $x$, то $x$ становится фактически также и обозначением класса всех $X$-ов, а $xy$ — обозначением класса, состоящего из всех тех $X$-ов, которые одновременно являются $Y$-ами (т. е., выражаясь современным языком, пересечения $x \cap y$). Далее Буль говорит, что если разделить какую-либо «группу объектов» на две части и из каждой части выбрать все $X$-ы, то результат будет тот же, как если бы мы выбирали все $X$-ы из этой группы как целого; этот факт он записывает символически в виде $x(u + v) = xu + xv$. (Таким образом, знак + фактически служит для обозначения объединения классов, но лишь в случае, когда они не пересекаются). К полученному таким образом дистрибутивному закону присоединяются еще два закона, обосновываемые аналогичным образом: $xy = yx$ и $x^n = x$. Затем вводится обозначение $1-x$ для класса «всех не-$X$-ов» (т. е. для дополнения класса $x$). Далее Буль показывает, как можно интерпретировать на этом языке традиционные типы суждений $A$, $E$, $I$, $O$ (см. предыдущий параграф). Например, суждение типа $A$: «Все $X$-ы суть $Y$-и» — представляется равенством $xy = x$, которое переписывается также в виде $x(1-y) = 0$. так что 0 оказывается фактически обозначением пустого класса. (В явном виде это не объясняется; нет и обоснования перехода от равенства $xy = x$ к равенству $x(1 - y) = 0$.) Потом дается интерпретация на том же языке категорических и гипотетических силлогизмов и рассматриваются еще некоторые свойства введенных в начале работы операций[42]. В дальнейшем Буль написал еще несколько работ, в которых развивались эти идеи. В частности, он занимался (начиная уже с первой работы, о которой говорилось выше) решением «уравнений в классах» («булевых уравнений»); эти уравнения и в последующие несколько десятилетий неизменно привлекали внимание ученых, занимавшихся математической логикой.

[42] Мы подробно остановились на содержании этой работы не только ввиду ее важности для истории математической логики, но и с целью показать, как далеки старые работы по математической логике от современного стиля ее изложения. К сожалению, в книгах по истории логики рассуждения старых авторов часто излагаются в модернизированном виде.

Идеи Буля были развиты во второй половине XIX в. английским логиком, философом и экономистом У. С. Джевонсом (William Stanley Jevons, 1835—1882) и немецким математиком Э. Шрёдером (Ernst Schröder, 1841—1902). В их работах алгебра классов приобрела уже отчетливый характер. Джевонс разработал технику вывода следствий из посылок, основанную фактически на совершенных дизъюнктивных нормальных формах (на языке классов). (Он построил также «логическую машину» для механического осуществления таких выводов.) Шрёдер в трехтомном сочинении «Vorlesungen über die Algebra der Logic» («Лекции по алгебре логики») дал подробное изложение алгебры логики (все еще на языке классов); он ввел для представления булевых функций нормальные формы (фактически — дизъюнктивные).

Настоящая логика предложений, не зависящая от логики классов, впервые появилась в опубликованной в 1877 г. работе английского математика Х. Мак-Колла (Hugh MacColl, 1837—?) «The calculus of equivalent statements and integration limits» («Исчисление эквивалентных предложений и пределы интегрирования»).

Истинностные таблицы впервые были применены в 1879 г. для некоторых частных случаев немецким математиком и философом Г. Фреге (Gottlob Frege, 1848—1925), а шесть лет спустя уже в общем виде — американским логиком Ч. Пирсом (Charles Sanders Peirce, 1839—1914). Кванторы также вел в употребление Фреге; несколько позже независимо от Фреге их использовал Пирс, ссылаясь как на автора идеи на своего соотечественника Митчелла (O. H. Mitchell). (Пирс ввел также префиксную нормальную форму.) Но самая глубокая идея Фреге состояла в построении математической логики в виде логического исчисления; таким образом, он был основоположником современной теории доказательств. Эту идею он осуществил в работе «Begriffschrift», опубликованной в 1879 г.[43]. Однако эта работа не была тогда оценена по достоинству; ее значение было понято специалистами только через три десятилетия[44]. В течение этих десятиле-

[43] Идеи теории доказательства в известной степени предвосхитил еще в первой половине XIX в. Б. Больцано (см. выше).

[44] Фреге был также автором очень глубоких исследований по теории смысла, которые дают право считать его основоположником современной логической семантики, а также ею направления в современном позитивизме, которое известно под именем «логического анализа языка». Эти исследования полностью сохраняют свое значение и сейчас. Три его важнейшие работы по семантике опубликованы в русском переводе: [Фреге 1977], [Фреге 1978], [Фреге 1980]. Изложение основ теории смысла Фреге имеется во введении к книге [Чёрч 1960].) Первое прикладное логическое исчисление также построил Фреге (в работе «Die Grundgesetze der Arithmetik» («Основные законы арифметики»)). Заметим еще, что именно он заменил неясное выражение «переменное количество» принятым сейчас представлением о переменной как символе.

тий появились работы по математической логике итальянского математика Дж. Пеано (Giuseppe Peano, 1858—1932) и его учеников и последователей, содержавшие подходы к логическим исчислениям, не уступавшие в этом отношении более ранней работе Фреге. Под влиянием сначала этих работ, а затем и работы Фреге в начале XX в. двое английских ученых: математик и философ А. Уайтхед (Alfred North Whitehead, 1861—1947) и философ Б. Рассел (Bertrand Russell, 1872—1970) — предприняли капитальное исследование, результатом которого был трехтомный труд «Principia Mathematica» («Основания математики»), опубликованный в 1910—1913 гг. Эта книга оказала большое влияние на последующее развитие математической логики и исследований по основаниям математики. Однако в книге Уайтхеда и Рассела еще не было явной формулировки исчисления предикатов как отдельного логического исчисления; впервые такая формулировка была приведена, видимо, в книге [Гильберт — Аккерман 1947] (ее первое немецкое издание вышло в 1928 г.). Там же впервые было использовано в качестве термина математической логики слово «предикат». Этот термин, получивший потом широкое распространение, следует признать очень удачным, так как обычно в предложении, выражающем тот факт, что какой-то предмет обладает тем или иным свойством (см. § 2.1) именем свойства является сказуемое. Тем не менее его приняли не все авторы (например, в книге [Чёрч 1960] вместо него употребляется термин «пропозициональная функция»). Используемое в нашей книге определение предиката как функции, значениями которой служат предложения, заимствовано у С.К. Клини (см. [Клини 1957], [Клини 1973]).

Что касается обозначений, то символы $\vee$ для дизъюнкции и $\supset$ для импликации введены Уайтхедом и Расселом (точнее, Уайтхед и Рассел видоизменили обозначения $\cup$ и $\supset$, которые применял Пеано; Гильберт и Аккерман обозначали импликацию знаком $\rightarrow$); символ $\&$ как обозначение конъюнкции впервые использован, вероятно, Гильбертом и Аккерманом (Пеано обозначал конъюнкцию знаком $\cap$, Уайтхед и Рассел — точкой); знак $\exists$ для квантора существования ввел Пеано; символ $\neg$ для отрицания предложен Гейтингом, символ $\forall$ для квантора общности — Генценом (у Уайтхеда и Рассела отрицание обозначается знаком $\sim$, у Гильберта и Аккермана — чертой над отрицаемым выражением; квантор общности по $x$ в обеих этих книгах обозначается $(x)$).

Более подробные сведения по истории формальной логики можно найти в специальных книгах, например, [Bocheński 1970], [Scholz 1931]. На русском языке есть книга [Стяжкин 1967] (содержащая обширную библиографию). В статье [Кузичева 1978] дан очерк развития математической логики в XIX в. (к сожалению, неполный: не затрагиваются работы Фреге, Пирса, Мак-Колла). Очень ценные

исторические сведения имеются в книге [Чёрч 1960]. Существует хрестоматия по истории математической логики с комментариями и обширной библиографией [Berka-Kreiser 1971]. Логические работы Аристотеля помещены во 2-м томе собрания его сочинений на русском языке [Аристотель 1978].

## Задачи и упражнения

1) Изменить правила образования формул исчисления $G_1$ аналогично задачам 1 а, б, в в конце гл. 5.

2) Изменить алфавит и правила образования термов и формул исчисления $G_1$ применительно к бескобочной записи термов и формул (см. задачу 2 в конце гл. 5). (В бескобочной записи вместо $F^k_n(t_1, \ldots, t_k)$ пишется $F^k_n t_1 \ldots t_k$; аналогично для функциональных символов.)

3) Показать, что правила У$\forall$ и В$\exists$ можно заменить условными правилами по образцу задачи 3 в конце гл. 5.

4) Убедиться, что правило У$\exists$ равносильно следующему правилу: Если $\Gamma, \mathfrak{A} \vdash \mathfrak{C}$ и $\Gamma \vdash \exists x \mathfrak{A}$, причем $x$ не входит свободно ни в одну формулу из $\Gamma$ и в $\mathfrak{C}$, то $\Gamma, \Gamma \vdash \mathfrak{C}$ (ср. задачу 4 в конце гл. 5).

5) Показать, что если в исчислении $G_1$ заменить правило В$\forall$ правилом $\mathfrak{A} \vdash \forall x \mathfrak{A}$, то теоремами полученного исчисления будут те и только те формулы, которые истинны во всевозможных интерпретациях с одноэлементными основными множествами.

6) а) Показать, что правила В$\exists$ и У$\exists$ можно заменить правилами $\neg\forall x \neg\mathfrak{A} \vdash \exists x \mathfrak{A}$ и $\exists x \mathfrak{A} \vdash \neg\forall x \neg\mathfrak{A}$.

б) Показать, что правила В$\forall$ и У$\forall$ можно заменить правилами $\neg\exists x \neg\mathfrak{A} \vdash \forall x \mathfrak{A}$ и $\forall x \mathfrak{A} \vdash \neg\exists x \neg\mathfrak{A}$.

7) Показать, что если $\mathfrak{A}$ — формула в алфавите $G_1$, такая, что $\exists x \mathfrak{A} \vdash_{\overline{G}_1} \forall x \mathfrak{A}$, то можно указать формулу, дедуктивно эквивалентную $\mathfrak{A}$ и не содержащую свободных вхождений $x$.

8) Доказать непротиворечивость $G_1$, не пользуясь теоремой о семантической пригодности. [Указание. Если в формуле исчисления $G_1$ вычеркнуть все кванторы, а от каждой атомной подформулы оставить только предикатный символ, получится формула исчисления предложений $\tilde{G}_0$, в котором роль пропозициональных символов играют символы $F^k_n$. Установить связь между выводимостью в $G_1$ и в $\tilde{G}_0$ и воспользоваться непротиворечивостью $\tilde{G}_0$. (Этот способ, в сущности, равносилен доказательству того, что всякая теорема $G_1$ истинна в любой интерпретации с одноэлементным основным множеством.)]

9) Доказать, что если $\Gamma \vdash_{\overline{G}_1} \mathfrak{A}$ и все формулы, входящие в $\Gamma$, равно как и формулы $\mathfrak{A}$, — бескванторные, то $\mathfrak{A}$ можно вывести из $\Gamma$ без использования правил введения и удаления общности и существования (и, значит, с использованием только бескванторных промежуточных формул). [Указание. Можно воспользоваться теоремой о семантической пригодности $G_1$.]

10) Показать, что теорема о полноте остается справедливой для исчисления, полученного из $G_1$ изъятием знака существования (или существования и импликации, или существования, конъюнкции и дизъ-

юнкции) и отвечающих этому знаку (или знакам) правил с соответствующим изменением определения формулы. (Ср. задачу 14 в конце гл. 5.)

11) Показать, что формула с кванторами по предикатам

$$\neg\exists F_1^2(\neg\exists x_1 F_1^2(x_1, x_1)\&\forall x_1\forall x_2\forall x_3(F_1^2(x_1, x_2)\ \&$$
$$\&\ F_1^2(x_2, x_3) \supset F_1^2(x_1, x_3))\ \&\ \forall x_1\exists x_2 F_1^2(x_1, x_2))$$

истинна на всех конечных множествах и ложна на всех бесконечных.

12) Доказать, что всякое исчисление на основе $G_1$, имеющее хоть одну модель, имеет модели любой бесконечной мощности. [Указание. Ввиду теоремы Лёвенгейма — Сколема достаточно показать, что если $A \subset B$ и $L$ — исчисление на основе $G_1$, то всякую модель $L$ с основным множеством $A$ можно расширить до модели с основным множеством $B$.]

13) Пусть $\bar{G}_1$ — исчисление, полученное из $G_1$ изъятием знаков конъюнкции, дизъюнкции и существования и отвечающих им правил (с соответствующим изменением правил образования формул). Можно определить понятие исчисления на основе $\bar{G}_1$ аналогично тому, как было сделано для $G_1$. Убедиться, что для $\bar{G}_1$ и исчислений на основе $\bar{G}_1$ сохраняют силу все теоремы из § 6.2.

14) а) Доказать, что если исчисление на основе $G_1$ с равенством имеет бесконечную нормальную модель, то оно имеет и счетную нормальную модель.

б) То же для исчисления на основе $G_1$ с равенством, имеющего конечные нормальные модели с основными множествами, содержащими сколь угодно много элементов.

[Указание. Добавить к данному исчислению $L$ новые символы предметных констант $b_1$, $b_2$, ..., и аксиомы $\neg(b_i = b_j)$ $(i \neq j)$. Доказать непротиворечивость этого расширения (от противного, интерпретируя участвующие в выводе противоречия символы $b_i$ элементами подходящей нормальной модели $L$). Воспользоваться тем, что всякая модель такого расширения бесконечна.]

15) а) Добавим к исчислению $G_1^-$ (§ 6.3, пункт 4, пример 1) аксиому $\exists x\exists y(\neg(x = y)\ \&\ \forall z(z = x \vee z = y))$. Что можно сказать о мощности основного множества нормальной модели такого исчисления?

б) Показать, что для любого целого положительного $n$ найдется исчисление на основе $G_1$ с равенством, для которого мощность основного множества всякой нормальной модели равна $n$.

16) а) Указать пример модели исчисления $C$ (§ 6.3, пункт 4, пример 7), основным множеством которой служило бы множество всевозможных многочленов с рациональными (или действительными, или комплексными) коэффициентами.

б) Указать примеры моделей исчисления $G$ (там же, пример 3), основным множеством одной из которых служило бы множество комплексных чисел, другой — множество отличных от нуля комплексных чисел, а нормализациями — аддитивная группа действительных чисел и мультипликативная группа положительных действительных чисел соответственно.

17) Пусть $I_1$ и $I_2$ — следующие интерпретации множества формул исчисления $R$ (§ 6.3, пункт 4, пример 5): их основными множе-

ствами служат множества всевозможных упорядоченных пар натуральных чисел для $I_1$ и множество всевозможных упорядоченных пар целых чисел, вторые элементы которых отличны от нуля — для $I_2$, выражения $(a, b) = (c, d)$, $(a, b) + (c, d)$, $(a, b) \cdot (c, d)$, 0 и 1 означают для $I_1$ соответственно $a + d = b + c$, $(a + c, b + d)$,

$$\left(\frac{(a-b)(c-d)+|(a-b)(c-d)|}{2}, \frac{|(a-b)(c-d)|-(a-b)(c-d)}{2}\right)^{45}, (0,0),$$

(1,0), для $I_2$ — $ad = bc$, $(ad + bc, bd)$, $(ac, bd)$, (0,1), (1,1).

Показать, что:

а) $I_1$ есть модель исчисления $KR$, и ее нормализация дает кольцо целых чисел;

б) $I_2$ есть модель исчисления $C$, и ее нормализация дает поле рациональных чисел.

18) а) Показать, что если из исчисления $Or$ (§ 6.3, пункт 4, пример 8) изъять символ $=$ и все содержащие его аксиомы и в полученном исчислении пользоваться записью $t_1 = t_2$ как сокращением для формулы

$$\forall z(t_1 < z \supset t_2 < z \& t_2 < z \supset t_1 < z \& z < t_1 \supset z < t_2 \& z < t_2 \supset z < t_1),$$

где $z$ — переменная, не входящая в $t_1$ и $t_2$, то в таком исчислении будут доказуемы все опущенные аксиомы.

б) Верно ли то же самое для исчисления $LOr$?

в) Указать модели исчисления $Or$, в которых «восстановленное» в соответствии с пунктом а) отношение «равенства» не совпадает с исходным. (В частности, нормальная модель может стать ненормальной.)

19) Охарактеризовать множество теорем исчисления, полученного добавлением к $H_1$ правила введения импликации.

20) Пусть $H_1^*$ — исчисление, полученное из $H_1$ заменой схем аксиом V3,4 и правила Об двумя правилами: если $\Gamma \vdash \mathfrak{A} \supset \mathfrak{B}$ и переменная $x$ не входит свободно в $\mathfrak{A}$ и ни в одну формулу из $\Gamma$, то $\Gamma \vdash \mathfrak{A} \supset \forall x \mathfrak{B}$, если $\Gamma \vdash \mathfrak{A} \supset \mathfrak{B}$ и переменная $x$ не входит свободно в $\mathfrak{B}$ и ни в одну формулу из $\Gamma$, то $\Gamma \vdash \exists x \mathfrak{A} \supset \mathfrak{B}$[46].

а) Сформулировать индуктивное определение выводимости для $H_1^*$.

б) Показать, что $H_1^*$ равносильно исчислению $G_1'$ в смысле совпадения по объему отношений выводимости. Указание. Доказать для $H_1^*$ «сильную» теорему о дедукции (без каких-либо ограничений на вывод $\mathfrak{B}$ из $\Gamma$, 20.).

21) Дать обоснование правильных модусов силлогизма с помощью теоретико-множественной интерпретации.

---

[45] Смысл этого выражения станет понятен, если заметить, что $\frac{x+|x|}{2} = \begin{cases} |x| & \text{при } x \geq 0 \\ 0 & \text{при } x < 0, \end{cases} \quad \frac{|x|-x}{2} = \begin{cases} 0 & \text{при } x \geq 0 \\ |x| & \text{при } x < 0 \end{cases}$

[46] В основных чертах $H^*$ совпадает с исчислением, рассмотренным в книге [Новиков 1959].

22) Показать, что правильность модусов Darapti и Felapton можно непосредственно вывести из правильности двух других модусов третьей фигуры (каких?), а модусов Bramantip и Fesapo — из правильности двух других модусов четвертой фигуры (каких?).

23) Названия правильных модусов второй, третьей и четвертой фигур силлогизма содержат в себе указания на способы их сведения к модусам первой фигуры (см. сноску на с. 262): первая буква показывает, к какому модусу нужно сводить, буква *s* или *p* означает, что суждение, обозначенное предшествующей гласной, следует подвергнуть обращению — соответственно простому (simplex) или посредством ограничения (per limitationem); при наличии буквы *m* нужно поменять местами посылки (metathesis — перестановка), при наличии буквы *k* — применить reductio ad absurdum. Процедура сведения состоит в следующем, а) если в названии нет буквы *k*, то сначала производится обращение посылок, обозначенных гласными, за которыми следует *s* или *p*; затем, если название содержит букву *m*, посылки меняются местами, далее производится вывод по модусу первой фигуры, название которого начинается той же буквой, что и название сводимого модуса, и, наконец, производится обращение заключения, если за обозначающей его гласной следует *s* или *p*; б) если в названии есть буква *k*, то посылка, за обозначением которой она следует, заменяется суждением, противоположным заключению[47], и производится вывод по соответствующему модусу первой фигуры, в результате чего получается суждение, противоположное замененной посылке. Например, силлогизм по модусу Disamis «Некоторые травы ядовиты; все травы — растения; следовательно, некоторые растения ядовиты» обосновывается так: из большей посылки простым обращением получается равносильное суждение «Некоторые ядовитые предметы — травы», из этого суждения как из меньшей посылки и из суждения «все травы — растения» как из большей выводится по модусу Darii суждение «Некоторые ядовитые предметы — растения», из которого еще одним простым обращением получается нужное заключение.

а) Привести примеры обоснования модусов, в названиях которых есть буквы *p* и *k*.

б) Хотя бы для некоторых модусов второй — четвертой фигур указать выводы в исчислении $G_1$, воспроизводящие описанный способ обоснования. (Особенно желательно сделать это для модусов, в сведении которых участвует обращение посредством ограничения; это как раз те модусы, для которых основные части заключений не выводимы из основных частей посылок.)

[47] Суждением, *противоположным* для суждения типа *A*, *I*, *E* или *O*, называется соответственно суждение типа *O*, *E*, *I* или *A* с теми же членами. (Ср. с понятием внутреннего отрицания; в чем различие?)

ГЛАВА

7

# ЭЛЕМЕНТЫ ТЕОРИИ АЛГОРИТМОВ

## § 7.1. ПРЕДВАРИТЕЛЬНЫЕ СООБРАЖЕНИЯ

1. Одним из главнейших понятий математики является, как известно, понятие функции (см. выше, § 1.2, пункт 3). Содержательно функция представляет собой «закон соответствия», по которому каждому элементу области определения — значению аргумента — сопоставляется какой-то элемент области прибытия — значение функции. При этом, вообще говоря, не требуется, чтобы значение функции можно было каким-либо способом «в самом деле найти» («построить», «вычислить» и т. п.) по соответствующему значению аргумента; однако ясно, что для математики и в особенности для ее приложений все же должны быть наиболее интересны те функции, для которых способы нахождения (иначе — «построения» или «вычисления») их значений существуют.

В трудах Ньютона и Лейбница, в которых впервые появилось понятие функции, равно как и в работах математиков многих следующих поколений, неявно предполагалось, что значение функции всегда можно так или иначе «найти», производя над значением аргумента некоторые «действия», предписываемые связанным с этой функцией «аналитическим выражением»[1]. Правда, тогда рассматривались только функции действительной и комплексной переменной; но потом, в XIX столетии, было замечено, что даже если ограничиться только такими функциями, их общие свойства никак не связаны с возможностью «вычислять» их значения (более того, с ней не связаны и те специальные свойства, которые играют основную роль в анализе — непрерывность, дифференцируемость и т. п.). Тогда понятие функции было освобождено от связи с аналитическим выражением и приобрело ту общность, в которой мы пользуемся им теперь

[1] Откуда и самый термин «функция» (см. сноску на с. 37).

Но осознание того факта, что не для всех функций можно «вычислять» их значения, не могло, разумеется, уменьшить практического интереса к изучению тех функций, для которых такое вычисление возможно; с теоретической же стороны естественно было теперь поставить вопрос о том, чем отличаются «вычислимые» функции от «невычислимых», т. е. о выработке *точного понятия* «способа вычисления функции».

2. *Интуитивное* представление о «вычислительной процедуре» существовало у математиков уже давно, и за этими процедурами был закреплен специальный термин, не отвечавший еще никакому точному понятию: *алгоритмы*[2]. Примерами могут служить, скажем, изучаемые в школе процедуры выполнения арифметических действий над натуральными числами в десятичной записи, или над обыкновенными дробями, или над десятичными дробями; все эти процедуры обычно называют алгоритмами. Несколько более сложные примеры — алгоритм Евклида для нахождения наибольшего общего делителя двух натуральных чисел, правило Крамера для решения систем линейных уравнений, правила дифференцирования элементарных функций и т. п. Кроме алгоритмов для вычисления функций, говорят еще об алгоритмах *для распознавания свойств и отношений*, подразумевая под этим строго определенные «правила» или «процедуры», позволяющие отвечать на вопросы вроде «Является ли данное натуральное число простым?», «Являются ли два данных натуральных числа взаимно простыми?» и т. п. Однако задача распознавания свойства или отношения всегда может быть представлена как задача нахождения, или «вычисления», истинностного значения некоторого предиката (одноместного или многоместного); поэтому под алгоритмом всегда можно понимать процедуру, позволяющую «находить» или «вычислять» значения некоторой функции.

---

[2] Слово «алгоритм» происходит от имени работавшего в IX в. в Багдаде (и писавшего, как все тогдашние мусульманские ученые, по-арабски) математика ал-Хорезми (это имя указывает на происхождение из Хорезма). В латинских переводах его сочинений, получивших распространение в Европе с XII века, имя автора писалось в искаженной форме, чаще всего Algorithmus или Algorismus. По арифметическому трактату ал-Хорезми европейцы впервые познакомились с созданной в Индии позиционной системой счисления, которой мы пользуемся и сейчас. Со временем слово Algorithmus превратилось в название основанной на этой системе арифметики, излагавшейся тогда в виде собрания правил действий над числами, а потом так стали называть любые правила, допускающие «механическое» выполнение.

В русском языке существуют два варианта этого термина: «алгоритм» и «алгорифм». В одной из двух главных имеющихся в нашей стране школ математической логики, созданной П. С. Новиковым, говорят и пишут «алгоритм», в другой, созданной А. А. Марковым — «алгорифм». Автор, являясь учеником П. С. Новикова, придерживается первого варианта.

Анализ только что приведенных и любых других примеров алгоритмов (много таких примеров читатель без труда укажет сам по аналогии) показывает, что все они обладают следующими двумя характерными особенностями:

1) Наличие четкого описания: алгоритм всегда описывается настолько четко, что на основе этого описания можно действовать чисто механически, не вникая в смысл (выражаясь «на современный лад», можно сказать, что эти действия можно поручить машине).

2) Детерминированность. Это значит, что если процедура является алгоритмом, то ни в какой момент ее выполнения не должно возникать сомнения, что делать дальше: каждый следующий шаг должен однозначно определяться исходными данными (т. е. значением аргумента) и результатами уже выполненных шагов.

Сказанное сейчас ни в коей мере не может еще претендовать на статус математического определения; мы хотели только подытожить, хотя бы частично, давно существующие в математике интуитивные представления об алгоритме, или «вычислительной процедуре». Этими интуитивными представлениями математики могли обходиться до тех пор, пока речь шла только об отыскании алгоритмов для решения конкретных «вычислительных» задач и при этом всякий раз нужный алгоритм удавалось найти — потому что когда алгоритм найден, ни у кого из математиков не возникает сомнения, что это действительно алгоритм, т. е. вычислительная процедура. Но со временем возникли некоторые задачи несомненно «вычислительного» характера, для которых все попытки нахождения алгоритмов заводили в тупик, и появилась гипотеза, что по крайней мере для части этих задач вообще никаких алгоритмов не существует. Проверка этой гипотезы в каждом случае требует уже строгого определения алгоритма: ведь если мы хотим математически доказать, что чего-то не существует, это «что-то» должно быть определено так, как полагается определять математические понятия[3].

Именно в связи с проблемой доказательства несуществования алгоритма в 30-е годы нынешнего столетия одновременно несколькими исследователями — К. Гёделем, Э. Постом, А. Тьюрингом[4], А. Чёрчем[5] — были предприняты усилия дать точное определение соответствующего понятия.

---

[3] В то же время доказать существование некоторого объекта нередко удается и при отсутствии строгого определения: для этого достаточно построить пример.

[4] А. Тьюринг (Alan M. Turing, 1912—1954) — английский математик.

[5] А. Чёрч (Alonzo Church, 1903—1995) — американский математик.

В результате этих усилий было предложено несколько вариантов определения, которые оказались равносильными между собой, и на их основе удалось доказать, что для многих «вычислительных» задач алгоритмы действительно невозможны. Вместе с тем благодаря наличию строгого определения математики смогли заняться изучением общих свойств алгоритмов (или, что, по существу, то же самое — «вычислимых» функций), их классификацией и т. п. Возникла, таким образом, новая математическая дисциплина — *теория алгоритмов*, с самого начала осознавшая себя частью математической логики, ибо алгоритм есть один из видов математического рассуждения, изучение структуры которого математическая логика имеет своим предметом. Изложением основных понятий и фактов теории алгоритмов мы сейчас и займемся.

## § 7.2. МАШИНЫ ТЬЮРИНГА

1. Нашей ближайшей задачей будет теперь сформулировать точное определение алгоритма. В настоящее время существует много вариантов этого определения. Все они представляют собой довольно сложные, развернутые конструкции и по форме нередко различаются весьма существенно. Поэтому они обычно трактуются как самостоятельные математические понятия, и каждое из них имеет свое название; доказательство равносильности двух таких конструкций (а все они между собой равносильны) иногда оказывается не слишком простым. Две из этих конструкций получили особенно широкое распространение ввиду их наглядности и удобства. Сейчас мы опишем одну из них, названную в честь ее автора «машиной Тьюринга»; уместность слова «машина» будет ясна из дальнейшего. Другая конструкция будет изложена в §§ 7.8 и 7.9[6].

Прежде чем переходить к точной формулировке, необходимо сделать следующее замечание. Отмеченное в § 1 условие наличия четкого описания алгоритма предполагает, очевидно, что все объекты, с которыми алгоритм имеет дело — значения аргумента вычисляемой функции, значения самой функции, возникающие в процессе вычисления «промежуточные данные» — также должны быть описаны настолько четко, чтобы с ними можно было оперировать механически.

[6] Из остальных конструкций наиболее распространенная (и также очень естественная и наглядная) — нормальный алгорифм А. А. Маркова. Основные понятия теории нормальных алгорифмов можно найти в книге [Мендельсон 1971], ее подробное изложение — в книгах [Марков 1954] и [Марков — Нагорный 1984].

Но любые «четко описываемые» математические объекты допускают представление в виде слов в алфавитах; поэтому можно потребовать, чтобы именно слова в алфавитах были теми объектами, с которыми работает алгоритм. Для машин Тьюринга, к определению которых мы теперь приступим, дело обстоит именно так[7].

Машина Тьюринга по определению представляет собой совокупность нескольких компонент, которые мы опишем сейчас по отдельности. При этом мы будем, следуя установившейся традиции, пользоваться наглядными образами, так что по форме наше определение может показаться не вполне строгим. Однако без использования этих образов изложение проиграло бы в ясности и простоте и фактически ничего не выиграло бы в строгости, т. к. перевод на «абсолютно строгий» язык не представляет никаких принципиальных трудностей.

Итак, *машина Тьюринга* есть совокупность следующих пяти компонент:

1) *Лента*, разделенная на конечное число *ячеек* ($\geq 1$). На ленте выбрано направление, называемое *направлением слева направо*. Соответственно этому на ленте выделяются *крайняя слева* и *крайняя справа ячейки* (в частном случае, когда лента состоит из одной ячейки, они совпадают); каждая ячейка, кроме крайней слева, имеет единственную *соседнюю слева*, каждая, кроме крайней справа — единственную *соседнюю справа*. В процессе работы машины лента может изменяться, а именно, к ней могут подклеиваться новые ячейки справа (но не слева!).

2) *Головка*, которая в каждый момент работы машины находится в некоторой ячейке ленты — или, как чаще говорят, *обозревает* эту ячейку (рис. 10). («Устройство» головки и ленты нас не интересует — существенно лишь то, что было о них сказано.)

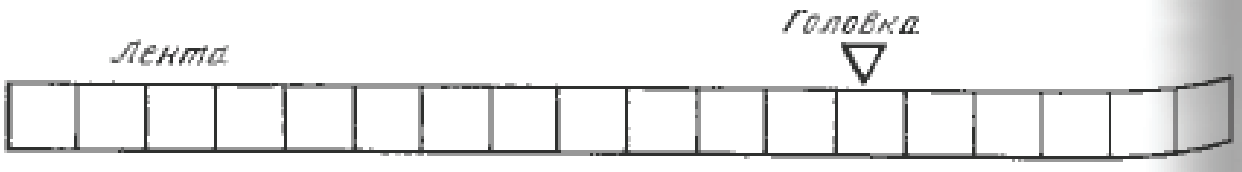



Рис. 10

[7] Имеются и другие универсальные способы представления «четко описанных» объектов; в частности, их можно представлять с помощью натуральных чисел, и некоторые варианты понятия алгоритма «работают» не со словами, а с натуральными числами — например, рассматриваемые ниже, в §§ 7.8 и 7.9, рекурсивные функции.

3) Два конечных *алфавита* — *внешний*

$$A = \{a_{-1}, a_0, \ldots, a_n\}\ (n \geq 1)$$

и *внутренний*

$$Q = \{q_0, q_1, \ldots, q_l\}\ (l \geq 1),$$

называемый также *множеством состояний*. Элементы $A$ называются *внешними символами* машины, элементы $Q$ — *внутренними состояниями* или просто *состояниями*. В каждый момент работы машина *находится в некотором состоянии* (т. е. ей сопоставлен некоторый элемент алфавита $Q$) и в каждой ячейке ленты *записан* некоторый (единственный) внешний символ. (Таким образом, внешние символы «видны» на ленте, являющейся «внешним устройством» машины, в то время как состояние «не видно» и является в каждый момент чем-то «внутренне присущим» машине в целом.)

Символы $a_{-1}$, $a_0$, $q_0$, $q_1$ играют особую роль и носят особые названия: $a_{-1}$ называется *граничным маркером*, $a_0$ — *пустым символом*, $q_0$ — *заключительным состоянием*, $q_1$ — *начальным состоянием*. Особенности употребления этих символов будут точно указаны ниже, предварительно же можно сделать следующие пояснения:

Граничный маркер записывается в крайней слева ячейке и остается в ней в течение всего процесса вычисления, чтобы головка не могла «свалиться» с ленты влево[8]. Вместо $a_{-1}$ мы часто будем писать #.

Пустой символ служит для того, чтобы можно было рассматривать ленту, у которой в некоторых ячейках ничего не записано (это удобно из содержательных соображений) и в то же время формально считать, что в каждой ячейке всегда записан какой-то символ (что упрощает формулировки и рассуждения). Таким образом, если в некоторой ячейке записан символ $a_0$, содержательно это означает, что ячейка пуста.

Начальное и заключительное состояния указывают соответственно начало и конец процесса вычисления.

4) *Программа* машины — конечное множество слов специального вида, называемых *командами*. Именно, каждая команда имеет вид

$$q_i a_j \to a_k C q_l,$$

где:

(а) $\to$ («стрелка») — некоторый специальный символ, не входящий ни в $A$, ни в $Q$ [9];

---

[8] «Сваливание» вправо предотвращается другим способом — подклеиванием ячейки (см. ниже).

[9] Стрелка используется только ради наглядности — если ее опустить, никакая информация не потеряется.

(б) $a_j$ и $a_k$ — внешние символы; при этом либо ни один из них не есть граничный маркер, либо оба совпадают с граничным маркером;

(в) $q_i$ и $q_l$ — внутренние состояния; при этом состояние $q_i$ — не заключительное.

(г) $C$ («эс» русское прописное[10], не «це» латинское) — одна из трех русских букв $Л$, $Н$, $П$; если при этом команда содержит граничный маркер, то $C \neq Л$.

Кроме того, программа в целом должна удовлетворять условию, которое мы, назвав части команды, стоящие слева и справа от стрелки, ее *левой частью* и *правой частью* соответственно, сформулируем так:

(д) если левые части двух входящих в программу команд совпадают, то совпадают и правые; иначе — программа не может содержать двух (или более) различных команд с одинаковыми левыми частями[11].

Содержательно команда представляет собой предписание, в соответствии с которым выполняется очередной шаг вычисления. Именно, если программа машины содержит команду $q_i a_j \to a_k C q_l$, то всякий раз, когда машина находится в состоянии $q_i$ и головка обозревает ячейку, в которой записан символ $a_j$, очередной шаг состоит в том, что: (*i*) в обозреваемой ячейке символ $a_j$ стирается и вместо него записывается $a_k$[12]; (*ii*) головка сдвигается на одну ячейку влево, если $C = Л$, на одну ячейку вправо, если $C = П$, и остается на месте, если $C = Н$; (*iii*) машина переходит в состояние $q_l$[13].

Поскольку программа может содержать только одну команду с левой частью $q_i a_j$, очередной шаг определяется однозначно. Таким образом, условие (д) обеспечивает выполнение сформулированного в § 1 принципа детерминированности.

Может случиться, конечно, что машина окажется в таком состоянии $q_i$ и головка — в ячейке, где записан такой символ $a_j$, что программа не содержит команды с левой частью $q_i a_j$; тогда очередной шаг невозможен, и вычисление прекращается.

Смысл оговорок в условиях (б), (в) и (г) теперь достаточно ясен: первая из них означает, что граничный маркер в процессе вычисления не может быть ни стерт, ни записан заново ни в какой ячейке;

---

[10] От слова «сдвиг».

[11] Таким образом, программа определяет функцию, отображающую некоторое подмножество декартова произведения $(Q \setminus \{q_0\}) \times A$ в декартово произведение $A \times \{Л, Н, П\} \times Q$.

[12] В частности, если $j = k$, содержимое ячейки не меняется.

[13] В частности, если $i = l$, состояние не меняется.

вторая — что, оказавшись в заключительном состоянии, машина не может продолжать работу; третья — что из ячейки, в которой записан граничный маркер, головка не может сдвинуться влево.

2. Определение машины Тьюринга закончено. Из сопровождавших его содержательных пояснений понятно, что представляет собой «работа машины», или «*вычисление*». Но среди вычислений нам удобно будет выделить некоторые «правильные», которых для всех наших целей будет достаточно. Именно, *правильными* мы будем считать такие вычисления, при которых: (1) в крайней слева ячейке ленты записан граничный маркер, и ни в какой другой ячейке его нет; (2) в начальный и заключительный моменты головка обозревает крайнюю слева ячейку; (3) в начальный момент машина находится в начальном состоянии, а в заключительный — в заключительном; (4) в заключительный момент все пустые ячейки (если они есть) расположены правее всех непустых.

Теперь мы определим правильное вычисление формально. Для этого введем сначала понятие *ситуации* машины Тьюринга: так мы будем называть всякое слово вида $xq_iy$, где $x \in A^*$, $y \in A^+$ ($A^*$ означает множество всех слов в алфавите $A$, $A^+$ — множество всех непустых слов в алфавите $A$), $q_i \in Q$ и $xy$ представимо в виде $\#z$, где $z$ не содержит $\#$. Содержательно ситуация — это «моментальная фотография» машины в процессе правильного вычисления: $xy$ есть содержимое ленты в данный момент, $q_i$ — состояние, в котором в этот момент находится машина, а первая буква слова $y$ (т. е. то место в слове $xy = \#z$, перед которым вставляется $q_i$) отвечает обозреваемой ячейке.

Ситуацию вида $q_1\#t$ мы будем называть *начальной*, ситуацию вида $q_0ua_0^m$ $(m \geq 0)$, где $u$ не содержит $a_0$ — *заключительной*[14]. Начальная ситуация будет называться *n-местной* $(n = 1, 2, \ldots)$, если она содержит точно $n - 1$ вхождение $a_0$. $n$-местную начальную ситуацию $q_1\#x_1\,a_0\,x_2\,a_0 \cdots a_0x_n$ мы будем интерпретировать как запись упорядоченной $n$-ки слов $x_1, \ldots, x_n$. (Например, $q_1\#\,a_1\,a_2$ — запись слова $a_1a_2$; $q_1\#\,a_2\,a_1\,a_0\,a_2\,a_2$ — запись пары слов $a_2a_1$, $a_2a_2$; $q_1\#\,a_0\,a_0\,a_1\,a_2\,a_0$ — запись четверки $\Lambda$, $\Lambda$, $a_1\,a_2$, $\Lambda$, где $\Lambda$ — пустое слово).

Мы будем, далее, говорить, что *ситуация $s'$ получается из ситуации $s$ выполнением команды $K$*, если имеет место одно из следующих условий:

($\alpha$) $K = q_i\,a_j \to a_kHq_l$, $s = vq_i\,a_jw$, $s' = vq_l\,a_kw$;

[14] $a^m$ — сокращенная запись слова $\underbrace{a \ldots a}_{m \text{ раз}}$.

($\beta$) $K = q_i a_j \to a_k \Lambda q_l$, $s = v_1 a_r q_i a_j w$, $s' = v_1 q_l a_r a_k w$, где $a_r \in A$;

($\gamma 1$) $K = q_i a_j \to a_k \Pi q_l$, $s = v q_i a_j a_r w_1$, $s' = v a_k q_l a_r w_1$, где $a_r \in A$;

($\gamma 2$) $K = q_i a_j \to a_k \Pi q_l$, $s = v q_i a_j$, $s' = v a_k q_l a_0$.

Смысл этого определения ясен; в пояснении нуждается только пункт ($\gamma 2$), отвечающий случаю, когда головка обозревает крайнюю справа ячейку, а команда требует сдвига головки вправо. Тогда справа подклеивается новая ячейка и в нее передвигается головка; при этом в подклеенной ячейке ничего не пишется (формально — записывается пустой символ).

Теперь мы можем дать формальное определение правильного вычисления:

*Правильным вычислением* машины Тьюринга $M$ мы будем называть последовательность $(s_0, s_1, \ldots, s_p)$ ситуаций этой машины, такую, что:

(а) для каждого $i = 0, \ldots, p-1$ ситуация $s_{i+1}$ получается из $s_i$ выполнением некоторой команды машины $M$;

(б) $s_0$ — начальная ситуация;

(в) $s_p$ — заключительная ситуация.

Если существует правильное вычисление машины $M$, начинающееся $n$-местной начальной ситуацией $q_1 \# t_1 a_0 \cdots a_0 t_n$ и заканчивающееся ситуацией $q_0 \# u a_0^m (m \geq 0)$, где $u$ не содержит $a_0$, мы будем говорить, что машина $M$ *перерабатывает* упорядоченный набор слов $t_1, \ldots, t_n$ (при $n = 1$ — просто слово $t_1$) в слово $u$, и писать $u = M|t_1, \ldots, t_n|$. Если $M|t_1, \ldots, t_n|$ существует, мы говорим, что машина $M$ *применима* к набору $t_1, \ldots, t_n$ (при $n = 1$ — к слову $t_1$).

Остается определить понятие функции, вычисляемой машиной Тьюринга. При этом будет удобно дополнить определение машины, выделив во внешнем алфавите — точнее, во множестве $A \setminus \{a_{-1}, a_0\}$ — два подалфавита $A_{вх}$ и $A_{вых}$, которые мы назовем *входным* и *выходным* алфавитами соответственно. (В частном случае они могут совпадать.) Если теперь $M$ — машина Тьюринга с входным и выходным алфавитами, мы скажем, что $M$ *вычисляет функцию* $f$ вместимости $n$, если $f$ удовлетворяет следующим условиям:

(1) область определения $f$ содержится в $A_{вх}^{*n}$ ($n$-й декартовой степени множества слов в алфавите $A_{вх}$), а множество значений — в $A_{вых}^*$;

(2) для произвольного набора $(x_1, \ldots, x_n) \in A_{вх}^{*n}$ тогда и только тогда $y = f(x_1, \ldots, x_n)$, когда $y = M|x_1, \ldots, x_n|$ и $y \in A_{вых}^*$.

Из определения ясно, что каждая машина Тьюринга $M$ с входным

и выходным алфавитами для всякого $n = 1, 2, \ldots$ вычисляет некоторую функцию вместимости $n$, и притом единственную. Правда, при этом может оказаться, что область определения этой функции пуста (т. е. не существует такого набора $(x_1, \ldots, x_n) \in A_{вх}^*$, что машина $M$ к нему применима и при этом $M(x_1, \ldots, x_n) \in A_{вых}^*$), так что иногда приходится рассматривать нигде не определенную функцию; такая функция представляет собой, впрочем, не менее «законный» объект, чем пустое множество.

Теперь мы можем, наконец, дать определение *вычислимой функции* — или, более подробно, *функции, вычислимой по Тьюрингу*: так мы будем называть всякую функцию, вычисляемую некоторой машиной Тьюринга с входным и выходным алфавитами.

В дальнейшем нам понадобится также понятие *вычислимого предиката*. Его нельзя ввести просто как частный случай вычислимой функции, т. к. значения предиката — предложения — не являются конструктивными объектами. Поэтому мы примем следующее естественное определение:

Предикат $F(x_1, \ldots, x_n)$, определенный на некотором подмножестве $n$-й декартовой степени множества всех слов в некотором конечном алфавите, называется *вычислимым (по Тьюрингу)*, если вычислима функция, сопоставляющая каждому набору $x_1^0, \ldots, x_n^0$ значений переменных $x_1, \ldots, x_n$ истинностное значение предложения $F(x_1^0, \ldots, x_n^0)$.

## § 7.3. ПРИМЕРЫ МАШИН

Чтобы освоиться с понятием машины Тьюринга, необходимо разобрать достаточное число примеров и, главное, поупражняться в самостоятельном построении машин. Сейчас мы приведем ряд примеров; при этом каждый раз будет выписываться только программа машины. Иногда мы будем отступать от стандартных обозначений внешних символов и состояний, введенных в предыдущем параграфе: для обозначения состояний будет в некоторых случаях использоваться буква $q$ с двойными индексами, а в качестве внешних символов будут допускаться любые знаки (отличные от $q$ с индексами). Начальное и заключительное состояния, пустой символ и граничный маркер всегда будут обозначаться стандартным способом. Внешний алфавит машины, из которого исключены граничный маркер и пустой символ, мы часто будем обозначать через $A_1$.

Пример 1. Построим машину, которая к каждому слову $x$ в алфавите $A_1$ будет приписывать справа символ $a_1$, т. е. будет перерабатывать $x$ в $xa_1$.

(1) $q_1a_i \to a_iHq_1$ $(i = -1, 1, ..., n)$

(2) $q_1a_0 \to a_1Hq_2$

(3) $q_2a_i \to a_iHq_2$ $(i = 1, ..., n)$

(4) $q_2\# \to \#Hq_0$

Программа содержит, таким образом, $2n + 3$ команды. Нумерация строк команд введена только для того, чтобы сделать более наглядной запись вычислений (см. ниже).

Приведем два правильных вычисления этой машины, начинающихся словами $a_2a_1a_2$ и $\Lambda$ соответственно:

1) $q_1\#a_2a_1a_2$
(1)
$\#q_1a_2a_1a_2$
(1)
$\#a_2q_1a_1a_2$
(1)
$\#a_2a_1q_1a_2$
(1)
$\#a_2a_1a_2q_1a_0$
(2)
$\#a_2a_1a_2q_2a_1$
(3)
$\#a_2a_2q_2a_1a_1$
(3)
$\#a_2a_2a_1q_2a_1$
(3)
$q_2\#a_2a_2a_1a_1$
(4)
$q_0\#a_2a_2a_1a_1$

2) $q_1\#$
(1)
$\#q_1a_0$
(2)
$q_2\#a_1$
(4)
$q_0\#a_1$

Цифра между ситуациями обозначает здесь номер той строки программы, выполнением команд которой нижняя ситуация получается из верхней.

Таким образом, правильное вычисление этой машины состоит в следующем: сначала, находясь в состоянии $q_1$, машина двигает

головку вправо, ничего при этом не изменяя на ленте, пока головка не дойдет до конца исходной цепочки; затем она справа от исходной цепочки пишет $a_1$, переходя при этом в состояние $q_2$, в котором головка движется влево (ничего не изменяя), пока не дойдет до граничного маркера; тогда состояние заменяется на $q_0$, и вычисление заканчивается.

Дальнейшие примеры мы не будем разбирать так подробно; в частности, образцы вычислений приводиться не будут. Однако читателю рекомендуется самому строить такие образцы.

Пример 2. Построим теперь машину, приписывающую к каждому слову в алфавите $A_1$ символ $a_1$ слева.

(1) $q_1\# \to \#\Pi q_1$

(2) $q_1a_i \to a_1\Pi q_1$, $(i = 1, \ldots, n)$

(3) $q_1a_j \to a_j\Pi q_1$, $(i, j = 1, \ldots, n)$

(4) $q_1a_0 \to a_1Hq_2$ $(i = 1, \ldots, n)$

(5) $q_2a_i \to a_iHq_2$ $(i = 1, \ldots, n)$

(6) $q_2\# \to Hq_0$

(7) $q_1a_0 \to a_1Hq_0$

Здесь символ $a_1$ приходится записывать в уже занятой ячейке; поэтому все символы, входящие в цепочку, нужно сдвинуть на одну ячейку вправо, для чего служат команды строк 2, 3, 4. Сдвигаемые символы «запоминаются» с помощью состояний. Команда 7 служит для обработки пустого слова.

Пример 3. Следующая машина у каждого слова длины $\geq 3$ в алфавите $A_1$ стирает три последних символа, а слова меньшей длины перерабатывает в пустое слово.

(1) $q_1a_i \to a_i\Pi q_1$ $(i = -1, 1, \ldots, n)$

(2) $q_1a_0 \to a_0Hq_2$

(3) $q_2a_i \to a_0Hq_3$ $(i = 1, \ldots, n)$

(4) $q_3a_i \to a_0Hq_4$ $(i = 1, \ldots, n)$

(5) $q_4a_i \to a_0Hq_5$ $(i = 1, \ldots, n)$

(6) $q_5a_i \to a_iHq_5$ $(i = 1, \ldots, n)$

(7) $q_h\# \to \#Hq_0$ $(h = (2, 3, 4, 5)$

Положив теперь в каждом из рассматриваемых примеров $A_{in} = A_{out} = A_1$, мы видим, что машины этих примеров вычисляют

соответственно функции $f_1$, $f_2$, $f_3$, определенные на всем множестве $A^*_{вх}$ и такие, что

$f_1(x) = xa_1$;

$f_2(x) = a_1x$;

$$f_3 = \begin{cases} y, \text{ если } |x| \geq 3, \ x = ya_{i_1}a_{i_2}a_{i_3}, \\ \Lambda, \text{ если } |x| < 3. \end{cases}$$

Здесь $|x|$ означает длину слова (см. с. 156), $\Lambda$ — пустое слово.

Задача. Построить машины Тьюринга, работающие следующим образом:

(а): Машину, приписывающую к каждому слову в алфавите $A_1$ слово $a_2a_1a_2$ справа;

(б) То же — слева;

(в) Машину, стирающую у каждого непустого слова первый символ, а пустое слово перерабатывающую в себя.

Во всех следующих примерах будут рассматриваться машины с входным и выходным алфавитами. Когда о входном алфавите ничего не говорится, подразумевается, что он есть $\{a_1, \ldots, a_s\}$. Если ничего не говорится о выходном алфавите, это означает, что он совпадает с входным. Нам будет удобно «помечать» внешние символы различными «метками», т. е. рассматривать символы вроде $\overline{a}_i$, $\overline{\overline{a}}_i$, $a'_i$, $\overline{b}$ и т. п. Все такие «помеченные символы» считаются принадлежащими разности $A_1 \setminus (A_{вх} \cup A_{вых})$.

Пример 4. Построим машину, удваивающую каждое слово в алфавите $A_{вх}$, т. е. вычисляющую функцию $f(x) = xx$.

(1) $q_1\# \to \Pi q_1$

(2) $q_1a_i \to \overline{a}_i\Pi q_{1i}$ $(i = 1, \ldots, s)$

(3) $q_{1i}a_j \to a_j\Pi q_{1i}$ $(i, j = 1, \ldots, s)$

(4) $q_{1i}\overline{a}_j \to \overline{a}_j\Pi q_{1i}$ $(i, j = 1, \ldots, s)$

(5) $q_{1i}a_0 \to \overline{\overline{a}}_i\Pi q_2$ $(i = 1, \ldots, s)$

(6) $q_2a_i \to a_i\Pi q_2$ $(i = 1, \ldots, s)$

(7) $q_2\overline{a}_i \to \overline{\overline{a}}_i\Pi q_2$ $(i = 1, \ldots, s)$

(8) $q_2\overline{\overline{a}}_i \to \overline{a}_i\Pi q_1$ $(i = 1, \ldots, s)$

(9) $q_1\overline{a}_i \to \overline{\overline{a}}_i\Pi q_3$ $(i = 1, \ldots, s)$

(10) $q_3\overline{a}_i \to \overline{\overline{a}}_i\Pi q_3$ $(i = 1, \ldots, s)$

(11) $q_3a_0 \to a_0Hq_4\ (i = 1, \ldots, s)$

(12) $q_3\overline{a}_i \to a_iHq_4\ (i = 1, \ldots, s)$

(13) $q_4\overline{a}_i \to a_iHq_4\ (i = 1, \ldots, s)$

(14) $q_4\# \to \#Hq_0$

(15) $q_1a_0 \to a_0Hq_0$

Работа машины состоит в том, что каждый символ входного слова копируется справа. Копируемый символ помечается (одной чертой), чтобы избежать его повторного копирования, и запоминается с помощью состояния (строка 2). Затем головка идет вправо (строки 3 и 4) до первой пустой ячейки, где записывается копия (строка 5), которая также помечается (двумя чертами), чтобы избежать в дальнейшем копирования копии. Потом головка идет влево (строки 7 и 6) до первого помеченного символа, встреча с которым в состоянии $q_2$ служит сигналом к началу нового цикла (строка 8). Если в состоянии $q_1$, с которого должен начинаться цикл, головка попала не на $a_i$, а на $\overline{\overline{a}}_i$, это значит, что копирование окончено; тогда остается снять метки (строки 9—14). Команда 15 служит для обработки пустого слова.

Пример 5. Следующая машина будет «разбавлять» каждое непустое слово в алфавите $A_{вх}$, записывая перед каждым его символом букву $c \notin A_{вх}$ (например, $a_2a_1a_3$ перерабатывается в $ca_2ca_1ca_3$). При этом мы полагаем $A_{внут} = A_{вх} \cup \{c\}$. Пустое слово эта машина будет перерабатывать в себя.

(1) $q_1\# \to \#\Pi q_1$

(2) $q_1a_i \to \overline{a}_i\Pi q_2\ (i = 1, \ldots, s)$

(3) $q_2a_i \to a_iHq_2\ (i = 1, \ldots, s)$

(4) $q_2b \to bHq_2$

(5) $q_2a_0 \to bHq_3$

(6) $q_3b \to bHq_3$

(7) $q_3a_i \to a_iHq_3\ (i = 1, \ldots, s)$

(8) $q_3\overline{a}_i \to \overline{a}_i\Pi q_1\ (i = 1, \ldots, s)$

(9) $q_1b \to bHq_4$

(10) $q_4b \to bHq_4$

(11) $q_4\overline{a}_i \to bH\overline{a}_iq_4\ i = (1, \ldots, s)$

(12) $q_4b \to bHbq_4\ (i = 1, \ldots, s)$

(13) $q_i a_0 \to a_0 \Pi q_2$ $(i = 1, \ldots, s)$

(14) $q_i c \to c \Pi q_2$ $(i = 1, \ldots, s)$

(15) $q_2 b \to a_i \Pi q_5$ $(i = 1, \ldots, s)$

(16) $q_5 b \to c \Pi q_4$

(17) $q_2 \# \to \# H q_0$

(18) $q_1 a_0 \to a_0 \Pi q_0$

Здесь команды строк 2—8 служат для того, чтобы «отмерить» справа от входного слова кусок ленты, равный ему по длине. С помощью команд строк 9—16 каждый символ входного слова (начиная с крайнего справа) переносится вправо и перед ним вставляется $c$. Встреча с граничным маркером в состоянии $q_4$ (команда 17) сигнализирует об окончании работы. Команда 18 служит для обработки пустого слова.

Задача. Построить машины Тьюринга, вычисляющие следующие функции:

(а) $f(x) = c^{|x|}$;

(б) $f(x) = c^{s(|x|)}$;

(в) $f(x) = x\,\widehat{x}$, где $\widehat{x}$ — обращение слова $x$ [15];

(г) $f(x) = \widehat{x}$.

Машины следующих четырех примеров предназначаются для распознания свойств слов и бинарных отношений между словами — иначе говоря, для вычисления одноместных и двуместных предикатов. Выходным алфавитом каждой из этих машин будет $\{и, л\}$; слова, обладающие нужным свойством (соответственно пары, находящиеся в нужном отношении), будут перерабатываться в $и$, не обладающие (не находящиеся) — в $л$.

Пример 6. Следующая машина распознает четность длины слова.

(1) $q_1 \# \to \# \Pi q_1$

(2) $q_1 a_i \to a_i \Pi q_2$ $(i = 1, \ldots, s)$

(3) $q_2 a_i \to a_i \Pi q_1$ $(i = 1, \ldots, s)$

(4) $q_1 a_0 \to a_0 H q_4$

(5) $q_2 a_0 \to a_0 H q_4$

(6) $q_3 a_i \to a_i \Pi q_3$ $(i = 1, \ldots, s)$

[15] Например, обращение слова «рыба» есть «абыр». По определению полагают $\widehat{\Lambda} = \Lambda$.

(7) $q_4 a_i \to a_i \Pi q_4$ $(i = 1, \ldots, s)$

(8) $q_4 \# \to \# \Pi q_5$

(9) $q_4 \# \to \# \Pi q_6$

(10) $q_5 a_0 \to a_0 \Pi q_0$

(11) $q_6 a_0 \to a_0 \Pi q_0$

Пример 7. Следующая машина распознает, является ли слово симметричным[16].

(1) $q_1 \# \to \# \Pi q_5$

(2) $q_1 a_i \to \overline{a}_i \Pi q_{1i}$ $(i = 1, \ldots, s)$

(3) $q_{1i} a_j \to a_j \Pi q_{1i}$ $(i, j = 1, \ldots, s)$

(4) $q_{1i} a_0 \to a_0 \Pi q_{2i}$ $(i = 1, \ldots, s)$

(5) $q_{2i} \overline{\overline{a}}_j \to \overline{\overline{a}}_j \Pi q_{2i}$ $(i, j = 1, \ldots, s)$

(6) $q_{2i} a_i \to \overline{\overline{a}}_i \Pi q_2$ $(i = 1, \ldots, s)$

(7) $q_{2i} a_j \to \overline{\overline{a}}_j \Pi q_3$ $(i, j = 1, \ldots, s, i \neq j)$

(8) $q_3 a_i \to a_i \Pi q_2$ $(i = 1, \ldots, s)$

(9) $q_2 \overline{a}_i \to a_i \Pi q_1$ $(i = 1, \ldots, s)$

(10) $q_1 \overline{\overline{a}}_i \to \overline{\overline{a}}_i \Pi q_4$ $(i = 1, \ldots, s)$

(11) $q_{2i} \overline{a}_j \to \overline{a}_j \Pi q_4$ $(i, j = 1, \ldots, s)$

(12) $q_4 \overline{\overline{a}}_i \to \overline{\overline{a}}_i \Pi q_3$ $(i = 1, \ldots, s)$

(13) $q_4 a_0 \to a_0 \Pi q_5$

(14) $q_5 \overline{\overline{a}}_i \to a_0 \Pi q_5$ $(i = 1, \ldots, s)$

(15) $q_5 \overline{a}_i \to a_0 \Pi q_5$ $(i = 1, \ldots, s)$

(16) $q_5 \# \to \# \Pi q_6$

(17) $q_6 a_0 \to a_0 \Pi q_0$

(18) $q_3 \overline{\overline{a}}_i \to \overline{\overline{a}}_i \Pi q_4$ $(i = 1, \ldots, s)$

(19) $q_3 a_0 \to a_0 \Pi q_0$

[16] Слово *симметрично*, если оно совпадает со своим обращением — иначе говоря, если оно представимо в виде $x\tilde{x}$ (как «Анна») или $x c \tilde{x}$, где $c$ — буква (как «слово»).

(20) $q_7\overline{\overline{a}}_i \to a_0 \Pi q_7$ $(i = 1, \ldots, s)$

(21) $q_7 a_i \to a_0 \Pi q_7$ $(i = 1, \ldots, s)$

(22) $q_7\overline{a}_i \to a_0 \Pi q_7$ $(i = 1, \ldots, s)$

(23) $q_7\# \to \# \Pi q_8$

(24) $q_8 a_0 \to \Lambda \Pi q_0$

(25) $q_1 a_0 \to \text{и} \Pi q_0$

При работе машины сравниваются между собой сначала первый и последний символы, затем второй и предпоследний и т. д. (строки 2—9). Если оказалось, что какие-либо два сравниваемых символа различны (строка 7), то все стирается и записывается $л$ (строки 18—24). Об успешном окончании сравнения сигнализирует в случае слова четной длины встреча в состоянии $q_1$ с символом, помеченным двумя чертами, т. е. первым символом правой половины слова (строка 10), в случае слова нечетной длины — встреча в состоянии $q_2$ с символом, помеченным одной чертой — этот символ стоит тогда в середине слова (строка 11). В обоих случаях все стирается и записывается $и$ (строки 12—17). Команда 25 служит для обработки пустого слова.

**Пример 8.** Аналогично машине примера 7 будет работать машина, распознающая, является ли слово $x$ началом слова $y$. Эта машина начинает работу с двуместной начальной ситуации $q_1\#xa_0y$ ($x$, $y$ — слова в алфавите $\{a_1, \ldots, a_s\}$). Она сравнивает сначала первые (слева) символы слов $x$ и $y$, затем вторые и т. д.; сравниваемые символы помечаются. Если при этом окажется, что каждый символ слова $x$ совпадает с занимающим такое же место символом слова $y$, то все стирается и записывается $и$. Если же на каком-либо месте обнаружится несовпадение или в слове $y$ не хватит букв для сравнения — также все стирается, но записывается $л$. Программу машины читатель построит сам. Во всех следующих примерах мы также будем предоставлять выписывание программ читателю.

**Пример 9.** Небольшим усложнением машины примера 8 можно получить машину, распознающую, является ли слово $x$ подсловом слова $y$. Она работает сначала так же, как предыдущая, но если окажется, что $x$ не есть начало $y$, машина не торопится закончить работу: вместо этого она зачеркивает первую букву слова $y$ (т. е. помечает ее особой меткой) и проверяет, является ли $x$ началом оставшегося слова; при отрицательном ответе зачеркивается вторая буква слова $y$, и т. д. Работа заканчивается, когда либо $x$ оказалось началом одного из «укороченных $y$-ов» (или самого $y$) — тогда все

стирается и пишется $a$,— либо очередной «укороченный $y$» оказался короче $x$-а — тогда все стирается и пишется $\Lambda$.

Замечание. В программах машин примеров 8 и 9 должны быть команды, обеспечивающие получение $a$ при пустом $x$.

Задача. Построить машины Тьюринга, распознающие:

(а) Дает ли длина слова при делении на 3 остаток 2.

(б) Содержит ли слово заданную букву.

(в) Имеет ли слово вид $xx$.

(г) Выполняется ли неравенство $|x| > |y|$.

(д) Является ли $x$ концом $y$.

(е) Совпадают ли $x$ и $y$.

Пример 10. Как построить машину Тьюринга, вычисляющую функцию Subst $(x, y, z)$, значение которой равно результату замены в $z$ первого (считая слева) вхождения слова $x$ словом $y$, если такое вхождение существует, и равно $z$ в противном случае?[17]

Удобно начать с построения вспомогательной машины, перерабатывающей $xa_0ya_0z$ в $xa_0ya_0$ Subst $(x, y, z)$. Прежде всего эта машина будет, работая аналогично машине предыдущего примера, распознавать, является ли слово $x$ подсловом слова $z$. Однако теперь содержимое ленты не стирается; вместо этого в случае, когда $x$ не содержится в $z$, стираются все метки и записи возвращается ее первоначальный вид; если же удалось найти вхождение $x$ в $z$ (ясно, что способом, описанным в примере 9, отыскивается именно первое вхождение, считая слева), то оно, буква за буквой, заменяется вхождением слова $y$, причем если длина $y$ не равна длине $x$, то «хвост» слова $z$ придется сдвинуть влево или вправо. Разумеется, программа этой машины будет громоздкой, но никаких принципиальных трудностей ее построение не представляет. Нужная машина получится теперь из вспомогательной добавлением блока команд, стирающего $x$ и $y$ и сдвигающего оставшуюся часть записи в начало ленты.

Задача. Построить машину Тьюринга, вычисляющую наибольшее общее начало слов $x$ и $y$.

В заключение параграфа остановимся на использовании машин Тьюринга для вычисления числовых функций (точнее — функций, определенных на подмножествах натурального ряда или его декартовых степеней и принимающих в качестве значений натуральные числа), а также предикатов от натуральных чисел. Для этого нужно условиться о некотором способе записи натуральных чисел. Проще всего пользоваться одноэлементным входным алфавитом $\{1\}$ и изображать число $n$ словом, состоящим из $n$ палочек. Пользуясь такой записью натуральных чисел (мы будем называть ее *простейшей*),

[17] Subst от лат. *substitutio* — «подстановка».

читатель без труда построит, например, машины, вычисляющие функции $f(n) = n$, $f(n) = n + 1$ (ср. пример 1), $f(n) = 2n$ (ср. пример 4), $f(n) = 3n$, машину, распознающую четность числа (ср. пример 6) и т. п. Рассмотрим, кроме того, два примера машин, вычисляющих числовые функции двух переменных.

**Пример 11.** Очень легко построить машину, вычисляющую сумму двух натуральных чисел, т. е. перерабатывающую $ma_0n$ в $m + n$. В самом деле, эта машина должна только поставить в первой пустой ячейке палочку и стереть последнюю палочку полученного слова.

**Пример 12.** Значительно сложнее будет машина, вычисляющая произведение. Впрочем, принципиальных трудностей ее построение также не представляет, так как идея ее работы достаточно ясна. Проще всего организовать работу такой машины следующим образом. Имея на ленте перед началом работы ситуацию $q_1\#ma_0n$, она прежде всего проверяет, есть ли слева от первой пустой ячейки хоть одна палочка. Если нет (это значит, что $m = 0$), то все содержимое ленты стирается. В противном случае стирается первая слева палочка слова $m$ и затем, если стертая палочка не была в $m$ единственной, слово $n$ копируется, т. е. справа от него $n$ раз записывается некоторый вспомогательный символ — скажем, $d$. Потом стирается вторая палочка слова $m$, после чего $n$ копируется еще раз, и т. д.— до тех пор, пока не будет стерта последняя палочка слова $m$. Тогда $n$ уже не копируется; вместо этого все $d$ превращаются в палочки и все палочки придвигаются вплотную к граничному маркеру.

Описанная машина умножает, собственно, $n$ на $m$.

**Задача.** Построить машины Тьюринга, вычисляющие (в простейшей записи):

(а) Разность $m - n$;

(б) неполное частное от деления $m$ на $n$;

(в) остаток от деления $m$ на $n$.

(Машина пункта (а) должна быть неприменима к парам $(m, n)$, у которых $m < n$, машины пунктов (б) и (в) — к парам вида $(m, 0)$.)

**Замечания.** 1) Вместо простейшей записи натуральных чисел можно, разумеется, использовать любую другую — например, обычную позиционную или позиционную без нуля (о ней см. ниже, в начале § 7.7). Но программы машин будут тогда сложнее.

2) Мы не можем касаться здесь вычисления функций действительной (и тем более комплексной) переменной, так как рассматриваемые в классическом анализе действительные числа не допускают необходимого для наших целей четкого описания (см. начало предыдущего параграфа), т. е. изображения в виде слов в каком-либо конечном алфавите. С помощью точного понятия алгоритма — например, в форме машины Тьюринга — можно ввести понятие вы-

числимого действительного числа, объем которого охватывает все числа, реально встречающиеся в вычислительной практике; такие числа допускают изображение в виде слов в конечном алфавите, и для них можно естественным образом ввести понятие вычислимой функции. Но рассмотрение этих вопросов выходит за рамки нашей книги[18].

## § 7.4. ТЕЗИС ЧЕРЧА — ТЬЮРИНГА

Рассмотрим теперь доводы в пользу того, что понятие машины Тьюринга действительно может служить уточнением интуитивного понятия алгоритма — иначе говоря, в пользу следующего утверждения:

Для всякой функции, которую можно каким-либо способом вычислить, можно построить вычисляющую ее машину Тьюринга.

Это утверждение, называемое обычно тезисом Чёрча — Тьюринга, впервые было высказано А. Тьюрингом в 1936 г. применительно к конструкции машины, от которой описанная выше отличается лишь несущественными деталями[19]; аналогичное утверждение применительно к некоторому совсем другому уточнению того же интуитивного понятия было несколько раньше высказано А. Чёрчем.

Разумеется, тезис Чёрча — Тьюринга не может быть математической теоремой или аксиомой, потому что участвующее в его формулировке понятие «каким-либо способом вычислить» не есть точное математическое понятие. По своему статусу этот тезис похож скорее на законы физики, представляющие собой обычно утверждения о том, что то или иное явление природы описывается некоторой математической конструкцией (например, дифференциальным уравнением) — с той разницей, что речь идет не о явлении природы, а об одном из видов человеческой деятельности — вычислении. В справедливости физических законов мы убеждаемся путем анализа опытных данных; аналогичным образом, к убеждению в справедли-

[18] О вычислимых действительных числах и вычислимых функциях действительной переменной см. [Кушнер 1973], [Мартин-Лёф 1975] или [Марков — Нагорный 1984].

[19] Сходная конструкция была предложена тогда же Э. Постом (который является также автором еще одной конструкции, предназначенной для той же цели — сейчас она известна под именем продукции Поста).

вости тезиса Чёрча — Тьюринга приводит нас анализ фактов, относящихся к вычислительной практике и смежным с ней областям.

Обратимся прежде всего к вычислению, выполняемому человеком без использования вспомогательных средств. Слово «вычисление» мы будем понимать в широком смысле — не обязательно как оперирование с числами. Примерами «нечисловых вычислений» могут служить тождественные преобразования в элементарной алгебре или в логике предложений, нахождение производных от элементарных функций и т. п. Каждое вычисление состоит в последовательном преобразовании некоторого комплекса символов, записанных на бумаге или на доске. (Вычисления «в уме» можно не рассматривать особо, т. к. их всегда можно заменить письменными вычислениями, имеющими ту же структуру.) Принципиально ничего не изменится, если мы будем представлять себе, что всякое вычисление производится на одной достаточно большой доске (доска отличается от бумаги тем, что написанное на ней можно стирать и на освободившемся месте писать снова) и что доска разграфлена на клетки, причем в каждой клетке можно записать только один символ. Вычисление можно теперь рассматривать как последовательность шагов, на каждом из которых изменяется содержимое одной клетки; в общем случае это означает, что записанный в клетке символ стирается и на его месте записывается другой. Но от чего зависит, в какой клетке производится очередной шаг и что в ней на этом шаге записывается? Разумеется, не только от того, что было раньше записано в ней самой, но и от содержимого других клеток; например, при сложении «столбиком» записываемая в клетке цифра определяется цифрами, стоящими над ней. Следовательно, прежде чем изменить содержимое какой-либо клетки, нужно, вообще говоря, просмотреть некоторые другие клетки и запомнить какие-то сведения о том, что в них находится. Кроме того, следующий шаг может зависеть от предыдущих; поэтому после выполнения очередного шага бывает нужно что-то о нем запомнить. Мы можем сказать теперь, что кроме «явных» шагов, на которых изменяется содержимое клеток, имеются еще «неявные», состоящие в просмотре клеток без изменения их содержимого. Но между этими двумя типами шагов нет принципиальной разницы, так как просмотр клетки можно представлять себе как «нулевое изменение»: записываемый в клетке символ совпадает с находившимся там ранее. Таким образом, вычисление состоит из «элементарных шагов», на каждом из которых изменяется содержимое какой-то клетки, и обо всяком шаге вычислитель должен, вообще говоря, что-то запомнить. В любой момент он держит в памяти какие-то сведения об уже выполненной части вычисления. После очередного шага к этим сведениям что-то добавляется и вместе с тем что-то из имевшихся ранее сведений может быть на данном шаге

«использовано до конца» и за ненужностью забыто; естественно сказать, что при каждом шаге «состояние памяти изменяется». Это «состояние памяти» можно представлять себе как набор сведений о некоторых уже выполненных шагах, причем для каждого шага указываются, скажем, координаты клетки, где он выполняется, характер изменения содержимого и «давность» этого шага по отношению к настоящему моменту. Все эти или любые другие сведения о выполненных шагах можно записать в виде некоторого слова в конечном алфавите (для данного вычисления фиксированном). Но объем памяти человека ограничен: существует константа (сейчас нам неважно, какая), ограничивающая сверху длины запоминаемых слов. Поэтому число возможных «состояний памяти» конечно.

Заметим теперь, что в отличие от «явных шагов», с которых мы начинали анализ процесса вычисления, каждый «элементарный шаг» зависит только от состояния памяти и от содержимого той клетки, где этот шаг выполняется (результаты просмотра других клеток учитываются в состоянии памяти). На каждом «элементарном шаге» изменяются содержимое одной клетки и состояние памяти[20]. Кроме того, каждый предыдущий «элементарный шаг» должен включать в себя указание «адреса» клетки, где нужно произвести следующий. Не будет существенным ограничением считать, что эта новая клетка, если она не совпадает со старой, расположена рядом с ней — ведь до любой клетки можно дойти «мелкими шажками», сдвигаясь каждый раз на одну клетку (вправо, влево, вверх или вниз).

Итак, мы расчленили процесс вычисления на «элементарные шаги», каждый из которых состоит в том, что вычислитель, обозревая некоторую клетку и учитывая, (а) каково состояние его памяти и (б) что записано в обозреваемой клетке, производит три операции: (*i*) заменяет символ, записанный в обозреваемой клетке, другим символом; (*ii*) переходит к обозрению одной из четырех соседних клеток или продолжает обозревать ту же клетку; (*iii*) изменяет состояние памяти. Ясно, что такой шаг может быть выполнен часто механически, без понимания его смысла, если имеется инструкция — при таком-то состоянии памяти и таком-то символе в обозреваемой клетке заменить этот символ на такой-то, сдвинуться в такую-то сторону (или не сдвигаться) и заменить состояние памяти на такое-то. Эта инструкция может быть, очевидно, записана в точно такой же форме, как мы записываем команды машины Тьюринга: $qa \to a'Cq'$, где $q$ и $q'$ — состояния памяти, $a$ и $a'$ — символы, используемые при вычислении, и $C$ принимает одно из значений «вправо», «влево», «вверх», «вниз», «на месте». Таким образом, анализ процесса вычисления привел нас к «двумерной машине Тьюринга»,

[20] Разумеется, изменение состояния памяти также может быть нулевым.

отличающейся от рассматривавшейся одномерной только тем, что лента заменена разграфленной на клетки доской и головка движется не в двух, а в четырех направлениях. Такая двумерная машина вполне могла бы использоваться в качестве уточнения понятия алгоритма. Но одномерная машина «технически проще» и поэтому удобнее для формальной трактовки (т. е. для доказательства теорем и т. п.), хотя принципиальной разницы между одномерным и двумерным вариантами нет: нетрудно понять, что клетки, на которые разграфлена доска, можно тем или иным регулярным способом расположить на одномерной ленте; при этом клетки, соседние на доске, не обязательно будут соседними на ленте, но всегда можно «найти» на ленте клетку, которая на доске была рядом с обозреваемой, с помощью некоторой «стандартной подпрограммы».

Таким образом, анализ того, как вычисляет человек, подтверждает тезис Чёрча — Тьюринга. Применение вспомогательных средств (например, таблиц) или механических приспособлений (счеты, арифмометр) не даст ничего принципиально нового: использование таблиц всего лишь увеличивает объем памяти вычислителя (что может быть очень важно практически, но теоретического значения не имеет), а вычисления с помощью простых механизмов можно «моделировать» последовательными изменениями их (механизмов) схем, выполненных с помощью символов на клетчатой доске.

Что касается вычислений с помощью современных вычислительных машин с программным управлением[21], то и их принципиальные возможности, как известно, не превышают возможностей человека-вычислителя (единственное их преимущество — быстродействие). Кроме того, читатель, хотя бы немного знакомый с этими машинами, наверняка сразу заметил, что машины Тьюринга очень на них похожи, и построение машин Тьюринга для вычисления конкретных функций — это, в сущности, программирование[22]. Главное отличие машин Тьюринга от реальных ЭВМ (если отвлечься от ограниченности объема памяти и времени работы последних) — крайняя простота элементарных шагов; эта простота позволяет легко строить «трансляторы» с языков реальных машин на язык машины Тьюринга. Можно сказать даже, что машина Тьюринга — это общая абстрактная схема вычислительной машины с программным управлением. (Но стоит подчеркнуть, что Тьюринг придумал свои машины

[21] В русском языке эти машины обычно обозначаются не слишком удачным термином «электронная вычислительная машина (ЭВМ)», подчеркивающим не принцип работы, а способ технической реализации, или совсем уж неудачным словечком «компьютер» (транслитерация английского computer), пущенным в ход малообразованными журналистами, лишенными чувства родного языка.

[22] В отличие от программы для ЭВМ программа машины Тьюринга считается частью самой машины, но это вопрос терминологии.

за несколько лет до появления первых ЭВМ; это лишний раз опровергает расхожее мнение, что «теория должна следовать за практикой».)

Подытоживая все изложенное, мы можем сказать, что анализ строения реальных вычислительных процедур убеждает нас в возможности указать для каждой такой процедуры осуществляющую ее машину Тьюринга. Это и есть главный довод в пользу тезиса Чёрча — Тьюринга; к нему мы добавим еще два косвенных довода:

1) Для уточнения понятия алгоритма предложено довольно много конструкций, основанных на различных соображениях и весьма разнообразных по форме; нередко в двух таких конструкциях трудно на первый взгляд усмотреть что-либо общее. Однако все эти конструкции равносильны между собой в том смысле, что всякая функция, вычислимая с помощью какой-либо одной из них, вычислима и с помощью любой другой. (При этом для каждой пары конструкций их равносильность удается строго доказать.) Никто еще не смог предложить конструкцию, приводящую к более широкому классу вычислимых функций.

2) До сих пор во всех случаях, когда для какой-либо конкретной функции, вычислимость которой в интуитивном смысле не вызывает сомнений, исследовался вопрос, вычислима ли она также и в смысле какого-либо уточнения понятия алгоритма (а значит, и всех известных уточнений), на этот вопрос удавалось получить положительный ответ.

Тезисом Чёрча — Тьюринга часто пользуются для сокращения доказательств теорем теории алгоритмов: если по ходу рассуждения нужно установить, что некоторая функция вычислима по Тьюрингу, довольствуются указанием «неформальной» вычислительной процедуры и построение машины Тьюринга опускают. (Впрочем, в тех случаях, когда мы будем им пользоваться в этой книге, способы построения машин будут довольно очевидны.)

## § 7.5. УНИВЕРСАЛЬНАЯ МАШИНА ТЬЮРИНГА

**1.** В дальнейшем нам понадобится машина Тьюринга, обладающая следующим свойством: если записать на ее ленте программу произвольной машины Тьюринга $M$ и произвольное слово во внешнем алфавите этой машины, она переработает это слово так же, как переработала бы его машина $M$. Иначе говоря, нам нужна машина, которая могла бы работать за любую машину Тьюринга; такую машину естественно назвать универсальной.

Чтобы выразить понятие универсальной машины Тьюринга в точных терминах, нужно прежде всего уточнить, что значит «записать на ленте программу машины $M$ и слово в ее внешнем алфавите». Проще всего было бы понимать это так, что на ленте пишется слово $p\square x$, где $p$ состоит из записанных подряд команд машины $M$, $x$ — слово во внешнем алфавите $M$ и $\square$ — разделительный знак. Но тогда все символы, входящие в $p$ и в $x$, должны принадлежать внешнему алфавиту универсальной машины; следовательно, этот алфавит должен содержать все внешние и внутренние символы машины $M$. Однако внешний алфавит универсальной машины — как и всякой другой — конечен и поэтому не может содержать все внешние и внутренние символы л ю б о й машины.

Выход из затруднения состоит в том, чтобы научиться к о д и р о в а т ь программы произвольных машин и слова в их внешних алфавитах словами в каком-либо одном конечном алфавите. Посмотрим, как это можно сделать.

Заметим сначала, что, раз навсегда фиксировав два произвольных счетных множества символов

$$\mathfrak{A} = \{a_{-1}, a_0, a_1, \cdots\}$$

и

$$\mathfrak{Q} = \{q_0, q_1, q_2, \cdots\},$$

мы можем ограничиться рассмотрением только тех машин Тьюринга, у которых внешние и внутренние алфавиты содержатся в $\mathfrak{A}$ и в $\mathfrak{Q}$ соответственно, поскольку всякую другую машину можно получить из некоторой машины этого класса простым переименованием символов; более того, в этом классе можно рассматривать только такие машины, у которых граничным маркером, пустым символом, начальным и заключительным состоянием служат $a_{-1}$, $a_0$, $q_1$ и $q_0$ соответственно. Так мы и будем теперь поступать, при этом множества $\mathfrak{A}$ и $\mathfrak{Q}$ выберем так, чтобы они не имели общих элементов.

Определим *коды символов*, участвующих в наших записях, следующим образом: кодом символа $a_n$ $(n = -1, 0, 1, \cdots)$ будет слово $a_2\, a_1^{n+2}\, a_2$, кодом символа $q_m$ $(m = 0, 1, \cdots)$ — слово $a_1\, a_1^{m+2}\, a_1$, кодами символов $Л$, $Н$, $П$, $\rightarrow$, $*$, $\square$ — символы $a_4$, $a_5$, $a_6$, $a_7$, $a_8$, $a_9$ соответственно. (Роль символа $*$ выяснится позже.) Код символа $b$ будет обозначаться $\varkappa(b)$.

*Кодом слова* $b_1 \ldots b_k$ в алфавите $\mathfrak{A} \cup \mathfrak{Q} \cup \{Л, Н, П, \rightarrow, *, \square\}$, где $b_1, \ldots, b_k$ — символы, мы будем называть теперь слово $\varkappa(b_1) \ldots \varkappa(b_k)$. *Кодом пустого слова* будет служить оно само. Код слова $x$ будет обозначаться $\varkappa(x)$.

В частности, код команды машины Тьюринга всегда имеет вид

$a_3a_1^g a_1a_2a_1^h a_2a_1a_2a_1^m a_2a_1a_3a_1^l a_3$, где: $g = 3,4, \ldots$; $n = 2, 3, \ldots$; $h, m = 1, 2, \ldots$; $l = 4, 5, 6$.

Если теперь $M$ — некоторая машина Тьюринга, то *кодом* ее *программы* мы будем называть слово $a_8\varkappa(K_1)a_8 \cdots a_8\varkappa(K_r)a_8$, где $K_1, \ldots, K_r$ — составляющие программу команды, расположенные в лексикографическом порядке кодов. Если считать, что внешний и внутренний алфавиты машины содержат только символы, встречающиеся в командах[23], то — поскольку граничный маркер, пустой символ и начальное состояние мы договорились всегда обозначать одинаково — машина будет полностью определяться своей программой. Поэтому вместо «код программы машины $M$» мы будем говорить просто «*код машины* $M$». Код машины $M$ будет обозначаться $\varkappa(M)$.

Задача. Построить машины Тьюринга, распознающие для каждого слова в алфавите $\{a_1, \ldots, a_9\}$, является ли оно: кодом какого-либо символа; кодом какой-либо команды; кодом какой-либо машины Тьюринга. Убедиться, что первые две машины можно построить так, чтобы, какое бы слово в алфавите $\{a_1, \ldots, a_9\}$ ни было записано на ленте к началу вычисления, головка сначала проходила бы его слева направо, ничего не изменяя на ленте, а затем двигалась бы влево, стирая при этом все[24].

Теперь мы можем сформулировать следующее определение: машина Тьюринга $U$ называется *универсальной*, если, какова бы ни была машина Тьюринга $M$ и каково бы ни было слово $x$ во внешнем алфавите $M$, машина $U$ применима к цепочке $\varkappa(M)a_9\varkappa(x)$ тогда и только тогда, когда $M$ применима к $x$, и в случае применимости

$$U|\varkappa(M)a_9\varkappa(x)| = \varkappa(M|x|).$$

Иначе говоря, универсальная машина перерабатывает код слова $p\square x$, где $p$ — программа $M$, в код того слова, в которое $M$ перерабатывает $x$.

Замечание. Можно было бы рассматривать машину, универсальную не для всех машин, а только для машин с фиксированным внешним алфавитом. Тогда в определении универсальной машины можно было бы заменить $\varkappa(M)a_9\varkappa(x)$ на $\varkappa(M)a_9x$ и $\varkappa(M|x|)$ на $M|x|$; код машины также можно было бы упростить — кодировать только состояния, а внешние символы в кодах команд записывать без изменения.

---

[23] На это мы имеем право, т. к. нас интересует только то, как машина работает, а на работу машины «лишние» символы никак не влияют.

[24] Такие машины называются *конечными автоматами*. Конечным автоматом является также машина примера 6 из § 7.3.

2. Теорема. Универсальная машина Тьюринга существует.

Доказательство этой теоремы должно было бы состоять, строго говоря, попросту в выписывании программы нужной машины. Однако мы этого делать не будем, потому что такая программа была бы чрезвычайно громоздкой и трудно обозримой. Вместо этого мы опишем «общую стратегию» работы машины, причем постараемся сделать это так, чтобы из описания был ясен способ построения программы.

В самых общих чертах работу нашей машины можно охарактеризовать так: справа от разделительного знака $a_0$ она имитирует вычисление машины $M$, пользуясь при этом «инструкциями», полученными слева от разделительного знака, т. е. там, где записан код программы $M$; перед тем, как имитировать очередной шаг вычисления, машина должна «заглянуть в программу» и «выяснить», что на этом шаге делать. Более подробно это выглядит следующим образом. В начале вычисления между $a_0$ и $\varkappa(x)$ вставляется $\varkappa(q_1\#)$; тем самым справа от $a_0$ оказывается код начальной ситуации машины $M$. Затем машина имитирует начинающееся с этой ситуации вычисление $M$, последовательно выполняя «макрошаги», отвечающие шагам вычисления $M$. Каждый шаг вычисления $M$ состоит в переходе от некоторой ситуации $s$ машины $M$ к другой ситуации $s'$, получающейся из $s$ выполнением одной из команд $M$. Перед началом соответствующего «макрошага» на ленте универсальной машины — в дальнейшем мы обозначаем ее через $U$ — должна быть записана цепочка $\varkappa(M)a_0\varkappa(s)$. Всякий раз, когда на ленте машины $U$ записана цепочка такого вида, она будет работать следующим образом. Пусть $s = vq_ia_jw$. Тогда прежде всего слева от $a_0$ — т. е. в слове $\varkappa(M)$ — ищется подслово $\varkappa(q_ia_j)$. Поскольку такое подслово имеется справа от $a_0$ (и притом только одно), искать его слева от $\square$ можно с помощью подпрограммы, аналогичной программе примера 9 из § 7.3. Если в $\varkappa(M)$ такого подслова не нашлось, это значит, что в программе $M$ нет команды с левой частью $q_ia_j$, т. е. что $M$, оказавшись в ситуации $s$, не может продолжать работу. Тогда и машина $U$ прекратит вычисление («сломается»). Если же подслово $\varkappa(q_ia_j)$ в $\varkappa(M)$ имеется (очевидно, там может быть только одно такое подслово), то за ним должно непосредственно следовать подслово $a_j\varkappa(a_kCq_l)$, где $a_kCq_l$ — правая часть содержащейся в программе $M$ команды с левой частью $q_ia_j$. Тогда машина $U$ должна будет преобразовать $\varkappa(s)$ в $\varkappa(s')$, где $s'$ — ситуация машины $M$, получающаяся из $s$ выполнением команды $q_ia_j \to a_kCq_l$. Для этого она заменит некоторое подслово слова $\varkappa(s)$ другим подсловом; характер этой замены зависит от вида команды в соответствии с определением отношения «ситуация $s'$ получается из ситуации $s$

выполнением команды $K$» (§ 7.2, п. 2). Именно: если имеет место условие $(\alpha)$ из этого определения, то происходит замена $\varkappa(q_i a_j)$ на $\varkappa(q_r a_s)$; если имеет место $(\beta)$, то заменяется $\varkappa(a_i q_i a_j)$ на $\varkappa(q_r a_i a_s)$; в случае $(\gamma 1)$ заменяется $\varkappa(q_i a_i a_s)$ на $\varkappa(a_s q_r a_s)$, и в случае $(\gamma 2)$ — $\varkappa(q_i a_i)$ на $\varkappa(a_s q_r a_0)$. Прежде чем производить замену, машина должна выяснить, что представляет собой $C$ (т. е. какой из трех символов $a_4$, $a_5$, $a_6$ содержится в подслове $\varkappa(q_i a_i \to a_k C q_r)$ слова $\varkappa(M)$), а если $C = \Pi$, то проверить еще, пусто или непусто слово $w$ (для этого нужно справа от второго вхождения $a_1$ в $\varkappa(s)$ отсчитать два вхождения $a_2$ и проверить, что стоит непосредственно за вторым из этих вхождений — $a_2$ или $a_0$). Саму замену можно произвести с помощью подпрограммы, аналогичной программе примера 10 из § 7.3. На этом «макрошаг» заканчивается; слово, записанное на ленте после его окончания, есть $\varkappa(M) a_0 \varkappa(s')$. Затем, если состояние, входящее в $s'$, — не заключительное, начинается следующий «макрошаг». В противном случае, если ситуация $s'$ не заключительная (т. е. если непосредственно справа от $a_0$ не стоит $a_3 a_1^2 a_3$[25] или непосредственно справа от $a_0$ стоит $a_3 a_1^2 a_3$, но $\varkappa(s')$ содержит вхождение слова $a_2 a_1^2 a_2$, правее которого есть $a_2 a_1^p a_2$), где $p > 2^{26}$), то вычисление прекращается безрезультатно («машина ломается»); если же ситуация $s'$ — заключительная, то машина переходит к последнему этапу работы, на котором стирается слово $\varkappa(M) a_0 \varkappa(q_0 \#)$ и оставшееся слово сдвигается влево вплотную к граничному маркеру, после чего машина переходит в заключительное состояние.

Теперь ясно, что если перед началом работы на ленте машины $U$ записано слово $\varkappa(M) a_0 \varkappa(x)$, то в случае, когда $M$ перерабатывает $x$ в $y$, машина $U$ завершит работу в заключительном состоянии с записанным на ленте словом $\varkappa(y)$; если же $M$ неприменима к $x$, то $U$ «сломается» или будет работать вечно. Таким образом, $U$ действительно есть универсальная машина.

---

[25] Это значит, что головка обозревает не крайнюю слева ячейку или состояние машины отлично от $q_0$.

[26] Это значит, что содержимое ленты не имеет вида $a a_0^l$, где $a$ не содержит $a_0$.

## § 7.6. НЕРАЗРЕШИМЫЕ АЛГОРИТМИЧЕСКИЕ ПРОБЛЕМЫ

1. Сейчас мы познакомимся с примерами невычислимых предикатов, или, иначе, нераспознаваемых свойств и отношений — т. е. таких свойств и отношений, для которых не существует распознающих их алгоритмов (см. § 7.1). Задачи о нахождении алгоритмов для вычисления функций (в частности, предикатов) называют обычно *алгоритмическими проблемами*; если алгоритма для вычисления той или иной функции не существует, говорят, что соответствующая алгоритмическая проблема *неразрешима*.

Утверждения о неразрешимости проблем распознавания свойств имеют следующий вид: «не существует алгоритма, позволяющего по любому конструктивному объекту из заданного класса $A$ узнать, обладает ли этот объект данным свойством». Тезис Чёрча — Тьюринга позволяет уточнить эту формулировку так: «Не существует машины Тьюринга, распознающей данное свойство объектов класса $A$». При этом предполагается, что класс $A$ состоит из слов в некотором конечном алфавите; но в действительности очень часто речь идет о классах иной природы, элементы которых кодируются словами (примеры см. ниже). Что касается выражения «машина Тьюринга распознает свойство», то это понимается, как в § 7.3: машина перерабатывает каждый элемент класса $A$ в $u$, если он обладает данным свойством, и в $л$ — если не обладает[27]. Аналогичным образом уточняются утверждения о нераспознаваемости отношений.

Проще всего доказывается неразрешимость некоторых алгоритмических проблем, относящихся к самой теории алгоритмов — именно, проблем распознавания определенных свойств машин Тьюринга. Из них самая простая — проблема распознавания самоприменимости, с которой мы и начнем.

Будем называть машину Тьюринга *самоприменимой*, если она применима к своему собственному коду. В противном случае машина называется *несамоприменимой*.

**Теорема 1.** Не существует алгоритма, позволяющего для любой машины Тьюринга узнать, является ли она самоприменимой.

В соответствии со сказанным выше точный смысл этого утверждения таков: не существует машины Тьюринга, перерабатывающей

[27] Вместо $u$ и $л$ можно, само собой, использовать любые другие символы. Можно также пользоваться вместо машины Тьюринга каким-либо другим точным определением алгоритма.

код любой самоприменимой машины Тьюринга в $a$ и код любой несамоприменимой в $я$.

Доказательство. Допустим, что такая машина существует; обозначим ее $M_0$. По этой машине легко построить другую машину $M_1$, работающую на кодах несамоприменимых машин так же, как $M_0$, а на кодах самоприменимых машин работающую вечно. (Например, если $q_0$ — заключительное состояние машины $M_0$, то $M_1$ можно получить из $M_0$ добавлением двух новых состояний $q'$ и $q''$, причем заключительным состоянием $M_1$ будет уже не $q_0$, а $q''$, и трех новых команд: $q_0\# \to \#Пq'$; $q'и \to иНq'$, $q'я \to яЛq''$.)

Какова бы ни была машина Тьюринга $M$, машина $M_1$, очевидно, применима к ее коду тогда и только тогда, когда $M$ несамоприменима. Но отсюда следует, что: во-первых, $M_1$ не может быть самоприменимой, так как тогда она была бы неприменима к своему коду, т. е. была бы несамоприменима; во-вторых, $M_1$ не может быть несамоприменимой, так как в этом случае она была бы применима к своему коду, т. е. была бы самоприменима. Имеем противоречие[28].

Следствие. Существует машина Тьюринга, для которой неразрешима проблема распознавания применимости, т. е. нет алгоритма, позволяющего по любому слову в ее внешнем алфавите, не содержащему граничного маркера и пустого символа, узнать, применима ли она к этому слову.

Доказательство. Нужным свойством обладает универсальная машина Тьюринга $U$. В самом деле, она применима к слову вида $ж(M)a_0ж(M)$, где $ж(M)$ — код произвольной машины Тьюринга $M$, тогда и только тогда, когда $M$ самоприменима; поэтому, если бы для $U$ существовал алгоритм, распознающий применимость, мы могли бы для произвольной машины $M$, применяя этот алгоритм к слову $ж(M)a_0ж(M)$, узнать, является ли $M$ самоприменимой.

В дальнейшем нам не раз придется строить по заданным машинам Тьюринга другие, определенным образом от них зависящие. Мы всегда будем делать это неформально, ограничиваясь описанием «стратегии работы» новой машины (ср. построение универсальной машины в предыдущем параграфе). Однако при некотором навыке обращения с машинами Тьюринга читатель всегда сможет извлечь из такого описания способ фактически преобразовать программу данной машины (или программы данных машин, если их несколько) в программу новой машины.

---

[28] Стоит обратить внимание, что здесь использован диагональный метод Кантора — тот самый, с помощью которого доказываются теоремы о несчетности континуума и о мощности множества подмножеств (теоремы 12 и 18 из Приложения II).

**2.** Для формулировки следующей теоремы нам понадобятся некоторые новые понятия.

Две машины Тьюринга, имеющие один и тот же внешний алфавит, мы будем называть *эквивалентными*, если, каково бы ни было слово в их общем внешнем алфавите, не содержащее граничного маркера и пустого символа, они либо перерабатывают его в одно и то же слово, либо обе к нему неприменимы. Свойство машин Тьюринга называется *инвариантным*, если любые две эквивалентные машины либо обе обладают этим свойством, либо обе не обладают. Свойство машин Тьюринга называется *нетривиальным*, если существуют как машины, обладающие этим свойством, так и не обладающие.

Задачи. 1) Привести примеры инвариантных и неинвариантных свойств машин Тьюринга.

2) Является ли самоприменимость: а) инвариантным свойством; б) нетривиальным свойством?

**Теорема 2 (теорема Райса [Rice 1953]).** Ни для какого нетривиального инвариантного свойства машин Тьюринга не существует алгоритма, позволяющего для любой машины Тьюринга узнать, обладает ли она этим свойством.

Доказательство. Пусть $\alpha$ — произвольное нетривиальное инвариантное свойство машин Тьюринга. Рассмотрим машины, не применимые ни к какому слову; все они, очевидно, эквивалентны между собой, и ввиду инвариантности свойства $\alpha$ оно либо выполняется для всех таких машин, либо не выполняется ни для одной из них. Пусть для определенности имеет место второе (в противном случае вместо $\alpha$ возьмем его отрицание). Пусть, кроме того, $M_1$ — некоторая машина, обладающая свойством $\alpha$ (она существует ввиду нетривиальности $\alpha$). Рассмотрим теперь произвольную машину Тьюринга $M$. По ней без труда можно построить другую машину $M'$, работающую следующим образом: если в начальной ситуации на ее ленте записано слово $x$, она ставит справа от него разделительный знак, за ним записывает слово $y = \varkappa(M)$, и далее, «не трогая» $x$, перерабатывает $y$ по программе машины $M$. Очевидно, этот этап вычисления в том и только в том случае успешно закончится (т. е. приведет к заключительной ситуации машины $M$), когда $M$ самоприменима. В этом случае вычисление продолжается так: все, что правее разделительного знака, а также он сам, стирается, а затем оставшееся слово $x$ перерабатывается по программе машины $M_1$. (В случае же несамоприменимости $M$ машина $M'$, очевидно, «ломается» или работает вечно.) Таким образом, если $M$ самоприменима, то $M'$ эквивалентна $M_1$, а если $M$ несамоприменима, то $M'$ не применима ни к какому слову. Следовательно, $M'$ обладает свойством $\alpha$ тогда и только тогда, когда $M$ самоприменима. Но программу $M'$ — а значит, и ее код — можно без труда построить по программе или коду $M$. Поэтому, если бы

существовал алгоритм, распознающий $\alpha$, из него можно было бы получить алгоритм, распознающий самоприменимость произвольной машины $M$ (он состоял бы в том, чтобы построить по $M$ соответствующую машину $M'$ и применить к этой последней алгоритм, распознающий $\alpha$),— а такой алгоритм невозможен по предыдущей теореме.

Замечания. 1) Чтобы доказать неразрешимость проблемы распознавания свойства $\alpha$, мы установили, что из разрешимости этой проблемы следовала бы разрешимость проблемы распознавания самоприменимости — иначе говоря, *свели* проблему распознавания самоприменимости к проблеме распознавания $\alpha$. Так поступают очень часто — чтобы доказать неразрешимость некоторой алгоритмической проблемы, *сводят к ней* (а не наоборот!) другую проблему, заведомо неразрешимую. Прием, как видим, совсем простой — но осуществить сведение может оказаться не просто и даже очень не просто.

2) В конце рассуждения мы оперировали интуитивным понятием алгоритма и, следовательно, фактически воспользовались тезисом Чёрча — Тьюринга. Полное доказательство, не использующее этот тезис, должно было бы включать в себя построение машины Тьюринга — скажем, $M_0$,— строящей по коду произвольной машины $M$ код соответствующей машины $M'$. Тогда по машине $\overline{M}$, распознающей $\alpha$, легко строилась бы машина $\overline{\overline{M}}$, распознающая самоприменимость: $\overline{\overline{M}}$ перерабатывала бы код произвольной машины так же, как $M_0$, а результат перерабатывала бы, как $\overline{M}$. Фактическое построение машины $M_0$ было бы довольно-таки трудоемкой технической работой, которую мы позволяем себе не проводить, ссылаясь на то, что провести ее в принципе нетрудно (см. § 7.4). Так всегда поступают при доказательстве неразрешимости алгоритмических проблем методом сведения.

Выведем теперь из теоремы 2 три следствия.

**Следствие 1.** Ни для какого нетривиального свойства одноместных числовых функций[29] не существует алгоритма, позволяющего для любой машины Тьюринга, внешний алфавит которой содержит символ 1, узнать, обладает ли данным свойством функция, вычисляемая этой машиной (в простейшей записи).

**Доказательство.** Пусть $\alpha$ — произвольное нетривиальное свойство одноместных числовых функций. Мы скажем, что машина Тью-

[29] Свойство числовых функций (т. е. функций, определенных на подмножествах натурального ряда — см. с. 295) *нетривиально*, если существуют как функция, обладающая этим свойством, так и не обладающая.

рина $M$ обладает свойством $\beta_1$, если при отождествлении символа $a_1$ с 1 и выборе в качестве входного и выходного алфавитов одного и того же одноэлементного множества $\{a_1\}$ эта машина будет вычислять одноместную функцию, обладающую свойством $\alpha$. Свойство $\beta_{a_1}$ очевидно, нетривиально и инвариантно. Но если бы существовал алгоритм, распознающий по любой машине с внешним алфавитом, содержащим палочку, обладает ли вычисляемая ею функция свойством $\alpha$, то для распознавания по любой машине, обладает ли она свойством $\beta_{a_1}$, достаточно было бы воспользоваться этим алгоритмом, отождествив палочку с $a_1$.

Замечания. 1) Следствие 1 справедливо и для любых других эффективных способов записи натуральных чисел (например, для обычной десятичной записи: достаточно было бы отождествить $a_1, \ldots, a_9, a_{10}$ с цифрами 1, ..., 9, 0).

2) Легко распространить следствие 1 и на многоместные функции.

А теперь пусть читатель немного задумается над только что доказанным утверждением. Казалось бы, что может быть естественнее такой задачи: дано некоторое свойство вычислимых функций; требуется найти алгоритм, позволяющий по любой вычислительной процедуре узнать, обладает ли вычисляемая с помощью этой процедуры функция данным свойством. И вот оказывается, что ни для одного нетривиального свойства такого алгоритма быть не может! Это кажется чрезвычайно удивительным — но это так.

Следствие 2. (а) Не существует алгоритма, позволяющего для любых двух машин Тьюринга узнать, эквивалентны ли они.

б) Не существует алгоритма, позволяющего для любых двух машин Тьюринга, внешние алфавиты которых содержат символ 1, узнать, совпадают ли вычисляемые ими числовые функции.

Доказательство. (а) Фиксируем произвольную машину Тьюринга $M$ и обозначим через $\alpha_M$ свойство машины Тьюринга быть эквивалентной машине $M$. Это свойство, очевидно, инвариантно и нетривиально. Но алгоритм, распознающий эквивалентность двух произвольных машин, позволял бы распознавать для любой машины, обладает ли она свойством $\alpha_M$.

б) Получается аналогично с использованием следствия 1.

Следствие 3. Существует машина Тьюринга, для которой неразрешима проблема распознавания переработки слов, т. е. нет алгоритма, позволяющего для любых слов $x$, $y$ в ее внешнем алфавите, не содержащих пустого символа и граничного маркера, узнать, перерабатывает ли она $x$ в $y$.

Доказательство. Этим свойством обладает универсальная машина Тьюринга. В самом деле, если бы это было не так, мы могли бы для произвольной машины Тьюринга $M$ узнать, например, перерабатыв

вает ли универсальная машина слово $\varkappa(M)a_0\varkappa(a_1)$ в $\varkappa(a_1)$ — иначе говоря, перерабатывает ли $M$ однобуквенное слово $a_1$ в себя. Но свойство перерабатывать $a_1$ в себя нетривиально и инвариантно.

Задача. Доказать, что не существует алгоритмов, позволяющих по любым двум машинам Тьюринга, внешние алфавиты которых содержат символ 1, узнать, вычисляют ли они функции:

(а) с одной и той же областью определения;

(б) с одним и тем же множеством значений;

(в) с непересекающимися областями определения;

(г) с непересекающимися множествами значений;

(д) взаимно обратные.

**3.** Неразрешимые алгоритмические проблемы встречаются не только в теории алгоритмов и не только в математической логике[30], но и в других областях математики. Наиболее важные и интересные из них относятся к алгебре и теории чисел. Ради примера мы рассмотрим сейчас первую алгебраическую проблему, для которой была доказана неразрешимость — проблему тождества для полугрупп. Именно, для каждой полугруппы, заданной конечной системой образующих и конечным числом определяющих соотношений (см. выше, § 6.3, пример 11) естественно возникает следующая проблема: найти алгоритм, позволяющий для любых двух слов, составленных из образующих данной полугруппы, узнать, представляют ли они один и тот же ее элемент. Это и есть **проблема тождества для конечно определенной полугруппы**. Если вместо полугруппы рассматривать соответствующее ассоциативное исчисление, речь будет идти об алгоритме для распознавания эквивалентности слов, и саму проблему называют тогда **проблемой эквивалентности**[31]. Например, для исчисления с алфавитом $\{a, b\}$ и единственным правилом $ab \leftrightarrow ba$ проблема эквивалентности разрешима, и алгоритм сводится к подсчету числа вхождений $a$ и $b$ в обоих словах — поскольку, как легко убедиться, два слова $u$ и $v$ эквивалентны в этом исчислении тогда и только тогда, когда для каждой из букв $a$, $b$ число ее вхождений в $u$ равно числу вхождений в $v$. Однако не для любого ассоциативного исчисления такой алгоритм существует: в 1947 г. А. А. Марковым и Э. Постом были независимо построены примеры ассоциативных исчислений с неразрешимой проблемой эквивалентности. Один подобный пример мы сейчас опишем.

Пусть $M$ — произвольная машина Тьюринга с внешним алфавитом $\{a_{-1}, a_0, \ldots, a_n\}$ и внутренним алфавитом $\{q_0, q_1, \ldots, q_l\}$, причем

---

[30] Одна очень важная неразрешимая проблема, относящаяся к логике предикатов, будет рассмотрена в § 8.5.

[31] Проблему эквивалентности слов поставил в 1914 г. норвежский математик А. Туэ (Axel Thue, 1863—1922).

$a_{-1}$, $a_0$, $q_0$, $q_1$ имеют стандартный смысл. Построим по этой машине ассоциативное исчисление $И_M$ следующим образом:

Алфавит исчисления $И_M$ есть $\{a_{-1}, \ldots, a_n, q_0, \ldots, q_n, d\}$.

Множество правил исчисления $И_M$ состоит из *основных правил*, сопоставленных командам машины $M$, и одного *дополнительного правила*. Основные правила таковы:

а) Каждой команде вида $q_i a_j \to a_k H q_l$ сопоставляется правило $q_i a_j \leftrightarrow q_l a_k$;

б) Каждой команде вида $q_i a_j \to a_k Л q_l$ сопоставляется совокупность всевозможных правил $a_r q_i a_j \leftrightarrow q_l a_r a_k$, где $r = -1, 0, \ldots, n$;

в) Каждой команде вида $q_i a_j \to a_k П q_l$ сопоставляется совокупность всевозможных правил $q_i a_j a_r \leftrightarrow a_k q_l a_r$, где $r = 0, \ldots, n$.

Дополнительное правило есть $a_0 d \leftrightarrow d$.

Ясно, что если $x$ и $x'$ — ситуации машины $M$, такие, что $x'$ получается из $x$ выполнением некоторой команды, то, применяя к слову $xd$ или к слову $xa_0d$, получаемому из $xd$ применением дополнительного правила, одно из правил, сопоставленных этой команде, мы сможем получить слово $x'd$[42]. Поэтому, если $M$ перерабатывает слово $x$ в слово $y$, то из слова $q_1 a_{-1} xd$ применением наших правил можно получить некоторое слово вида $q_0 a_{-1} y a_0^m d$ $(m = 0, 1, \ldots)$, из которого при $m \neq 0$ с помощью дополнительного правила можно получить $q_0 a_{-1} yd$. Следовательно, если $M$ перерабатывает $x$ в $y$, то слово $q_1 a_{-1} xd$ эквивалентно в $И_M$ слову $q_0 a_{-1} yd$.

Покажем теперь, что верно и обратное: если $x$, $y$ — слова в алфавите $\{a_1, \ldots, a_n\}$, и слово $q_1 a_{-1} xd$ эквивалентно в $И_M$ слову $q_0 a_{-1} yd$, то $M$ перерабатывает $x$ в $y$.

Для произвольной ситуации $x$ машины $M$ будем обозначать через $\bar{x}$ всякое слово, получающееся из $x$ приписыванием или вычеркиванием на правом конце некоторого числа вхождений $a_0$ (в частности, и сама $x$ может быть обозначена через $\bar{x}$). Слово вида $\bar{x}d$ с помощью дополнительного правила может быть преобразовано, очевидно, только в слово такого же вида (с тем же $x$).

Пусть $u$ и $v$ — произвольные слова, эквивалентные в $И_M$. Тогда существует последовательность слов $u = z_0, z_1, \ldots, z_m = v$, в которой каждый следующий член получается из предыдущего применением некоторого правила. Такую последовательность мы будем называть *путем* из $u$ в $v$. Слово вида $\bar{x}d$, где $x$ — ситуация машины $M$, будем называть *нормальным*: все правила исчисления $И_M$ переводят нор-

[42] Применять дополнительное правило необходимо в случае (2) (см. § 7.2).

мальные слова в нормальные, так что если путь начинается с нормального слова, то он весь состоит из нормальных слов; такой путь мы также будем называть *нормальным*.

Если $u = z_0, \ldots, z_m = v$ — нормальный путь из $u$ в $v$, мы скажем, что слова $z_i$ и $z_j$, где $0 \leq i$ и $i + 1 < j \leq m$, *образуют вилку*, если при переходе от $z_i$ к $z_{i+1}$ применяется основное правило справа налево, при переходе от $z_{j-1}$ к $z_j$ — основное правило слева направо, а при переходе от $z_{i+1}$ к $z_{j-1}$, если $i + 1 < j - 1$, применяется только дополнительное правило. Очевидно, в этом случае $z_i$, $z_{i+1}$ и $z_j$ имеют соответственно вид $\widetilde{s'}d$, $\widetilde{sd}$ и $\widetilde{s''}d$, где ситуации $s'$ и $s''$ получаются из ситуации $s$ выполнением некоторых команд; но ввиду детерминированности машины Тьюринга к каждой ситуации применима только одна команда, так что $s' = s''$. Следовательно, слова $z_i$ и $z_j$ могут отличаться друг от друга разве только числом вхождений $a_0$ перед $d$, и $z_j$ можно получить из $z_i$ с помощью дополнительного правила. Заменяя отрезок пути $z_i, \ldots, z_j$ отрезком с теми же первым и последним словами, на котором применяется только дополнительное правило (или, если $z_i = z_j$, просто вычеркивая отрезок $z_{i+1}, \ldots, z_j$), мы получим путь из $u$ в $v$, содержащий двумя применениями основных правил меньше; произведя это преобразование достаточное число раз, можно получить путь, к которому оно уже неприменимо и который, следовательно, не содержит вилок.

Пусть теперь $x$ и $y$ — слова в алфавите $\{a_1, \ldots, a_n\}$, такие, что $q_i a_{-1} x d$ и $q_0 a_{-1} y d$ эквивалентны в $H_M$. По только что доказанному существует нормальный путь без вилок $z_0, \ldots, z_r$ из $q_i a_{-1} x d$ в $q_0 a_{-1} y d$. Пусть $z_k$ — последнее на этом пути слово, такое, что при переходе от $z_{k-1}$ к $z_k$ применяется основное правило. Очевидно, $z_k$ имеет вид $q_0 a_{-1} y a_0^p d$ $(p = 0, 1, \ldots)$. Поэтому правило, применяемое при переходе от $z_{k-1}$ к $z_k$, отвечает команде, содержащей $q_0$; а поскольку $q_0$ может содержаться только в правой части команды, это правило применяется слева направо. Но отсюда немедленно вытекает, что все основные правила на данном пути применяются слева направо — иначе он содержал бы вилку. Следовательно, если $z_i, \ldots, z_j$ — отрезок нашего пути, на первом шаге которого применяется основное правило, а на всех остальных — дополнительное, то $z_i$ и $z_j$ имеют вид соответственно $\widetilde{sd}$ и $\widetilde{s'}d$, где ситуация $s'$ получается из $s$ выполнением некоторой команды. Поэтому, если $i_0, i_1, \ldots, i_l$ $(0 \leq i_0 < i_1 < \ldots < i_l = k - 1 \leq n)$ — последовательность, состоящая из всех номеров $i_h$, для которых при переходе от $z_{i_h}$ к $z_{i_h+1}$ применяются основные правила, то слова

$z_{i_0}, z_{i_1}, \ldots, z_{i_l}$ имеют вид $\widetilde{s}_0 d, \widetilde{s}_1 d, \ldots, \widetilde{s}_l d$, где для каждого $h = 0, 1, \ldots, l-1$ ситуация $s_{h+1}$ получается из $s_h$ выполнением некоторой команды; при этом можно считать, что $s_0 = q_1 a_{-1} x$; а так как из $s_l$ выполнением некоторой команды получается заключительная ситуация $s_{l+1}$, последовательность $s_0, s_1, \ldots, s_l, s_{l+1}$ есть правильное вычисление машины $M$, начинающееся словом $x$ и заканчивающееся словом $y$.

Итак, мы доказали, что если $x$ и $y$ — слова в алфавите $\{a_1, \ldots, a_s\}$, то слово $q_1 a_{-1} x d$ эквивалентно в $И_M$ слову $q_0 a_{-1} y d$ тогда и только тогда, когда машина $M$ перерабатывает $x$ в $y$. Поэтому, если существует алгоритм, позволяющий для любых двух слов в алфавите исчисления $И_M$ узнать, эквивалентны ли они в $И_M$, то этот же алгоритм позволит нам для любых двух слов $x$, $y$ в алфавите $\{a_1, \ldots, a_s\}$ узнать, перерабатывает ли машина $M$ $x$ в $y$. Следовательно, если взять в качестве $M$ машину с неразрешимой проблемой распознавания переработки слов (см. следствие 3 из теоремы 2), то для исчисления $И_M$ алгоритм, распознающий эквивалентность слов, будет невозможен.

Замечание. Ассоциативное исчисление с неразрешимой проблемой эквивалентности, строящееся описанным только что способом, очень громоздко: даже при самом экономном программировании оно будет содержать сотни, если не тысячи правил. Но существуют и совсем простые примеры полугрупп с неразрешимой проблемой тождества[33], указанные Г. С. Цейтиным и Ю. В. Матиясевичем (ссылки см. в книге [Мальцев 1965], 2-е изд.) Так, полугруппа Г. С. Цейтина имеет пять образующих $a, b, c, d, e$ и семь определяющих соотношений: $ac = ca$, $ad = da$, $bc = cb$, $bd = db$, $eca = ce$, $edb = de$, $cca = ccae$. Полугруппа Ю. В. Матиясевича имеет всего три определяющих соотношения.

4. В заключение параграфа приведем без доказательства два самых знаменитых результата о неразрешимости алгоритмических проблем.

1) **Проблема тождества для конечно определенных групп.** Эту проблему, формулируемую точно так же, как соответствующая проблема для более общего класса конечно определенных полугрупп[34], поставил в 1912 г. немецкий математик М. Дэн (Max Dehn, 1878—1952). Долгое время она считалась одной из главных нерешенных задач теории групп. Для довольно широких частных классов групп удалось найти решающие ее алгоритмы, и еще в 40-е годы многие

[33] Просты в этих примерах, впрочем, только описания полугрупп, а не доказательства неразрешимости для них проблемы тождества.

[34] Очевидно, из неразрешимости более частной проблемы всегда следует неразрешимость более общей, но не наоборот.

специалисты надеялись на положительное решение для общего случая. Однако в 1949 г. П. С. Новиков (1901—1975) построил пример конечно определенной группы, для которой проблема тождества неразрешима [Новиков 1955]. (Этот пример очень сложен; впоследствии были найдены более простые доказательства существования таких групп — см., например, [Шенфилд 1975], Приложение I.)

2) Десятая проблема Гильберта. С давних времен математики интересуются поиском целочисленных решений алгебраических уравнений с целыми коэффициентами — так называемых диофантовых уравнений (по имени греческого математика Диофанта (Διόφαντος), жившего, по-видимому, в III в. н. э., чьи работы сыграли большую роль в их изучении). Для многих частных типов диофантовых уравнений были найдены алгоритмы, позволяющие их решать. В 1900 г. Д. Гильберт поставил задачу решения диофантовых уравнений в общем виде; на современном языке она может быть сформулирована так: найти алгоритм, позволяющий для любого уравнения вида $f(x_1, \ldots, x_n) = 0$, где $f(x_1, \ldots, x_n)$ — многочлен с целыми коэффициентами от неизвестных $x_1, \ldots, x_n$ ($n$ — произвольное целое положительное число[35]), узнать, имеет ли оно целочисленные решения. Эта задача находится под номером 10 в списке важнейших проблем математики, содержащемся в докладе, с которым Гильберт выступил на II Международном конгрессе математиков в августе 1900 г. В течение десятилетий попытки найти нужный алгоритм ни к чему не приводили; после появления результатов об алгоритмической неразрешимости возникла гипотеза, что и эта проблема неразрешима. Но только в 1970 г. Ю. В. Матиясевичу (и несколько позже независимо Г. В. Чудновскому) удалось доказать, что это действительно так — алгоритма для решения произвольных диофантовых уравнений не существует. (См., например, приложение (написанное Д. А. Захаровым) ко 2-му изданию книги [Мальцев 1965].)

## § 7.7. РАЗРЕШИМЫЕ И ПЕРЕЧИСЛИМЫЕ МНОЖЕСТВА

1. Точное понятие алгоритма позволило нам выделить среди всевозможных функций вычислимые, т. е. такие, значения которых можно «в самом деле находить». Под таким же углом зрения

[35] Для уравнений с одним неизвестным такой алгоритм существует; его описание можно найти в любом учебнике высшей алгебры.

можно рассмотреть и понятие множества: весьма естественно попытаться среди всевозможных способов задания множеств выделить «эффективные», т. е. такие, которые позволяли бы «в самом деле работать» с множествами — указывать их конкретные элементы и производить над ними вычислительные операции, отвечать для конкретных объектов на вопрос, входят ли эти объекты в данное множество, и т. п. При этом, разумеется, нам придется ограничиться множествами, состоящими из конструктивных объектов; как и прежде, моделью конструктивного объекта будет служить для нас слово в конечном алфавите. Однако во многих случаях удобно вместо слов рассматривать натуральные числа, пользуясь тем, что между словами в заданном конечном алфавите и натуральными числами можно установить очень простое взаимно однозначное соответствие. Именно, если фиксировать произвольное целое $P > 1$, то любое целое положительное $n$ может быть единственным образом представлено в виде

$$(*)\quad n = \alpha_1 \cdot P^{k-1} + \alpha_2 \cdot P^{k-2} + \cdots + \alpha_{k-1} \cdot P + \alpha_k,$$

где $\alpha_i$ принимают значения $1, \ldots, P$. (Доказать это можно индукцией; читателю рекомендуется восстановить доказательство[46]). Поэтому, если выбрать конечный алфавит $V = \{a_1, \ldots, a_P\}$ мощности $P$ и сопоставить числу $n$, представленному в виде (*), слово $a_{\alpha_1} a_{\alpha_2} \cdots a_{\alpha_k}$, то каждому целому положительному $n$ будет отвечать единственное слово; обратно, для каждого непустого слова $a_{\alpha_1} \cdots a_{\alpha_k}$ в алфавите $V$ по формуле (*) вычисляется единственное целое положительное число, которому отвечает это слово. Если, кроме того, числу 0 сопоставить пустое слово, мы получим взаимно однозначное соответствие между натуральным рядом и множеством всех слов в алфавите $V$. Число, соответствующее слову $x$, мы будем обозначать $\nu x$ и называть *стандартным номером* этого слова, а само отображение $\nu$ — *стандартной нумерацией* слов в алфавите $V$.

От обычной записи натуральных чисел в системе счисления с основанием $P$ представление с помощью отображения $\nu$ отличается тем, что «цифры» $a_1, \ldots, a_P$ имеют значения $1, \ldots, P$, а не $0, \ldots, P-1$. Для наших целей обычная запись непригодна из-за того, что при ней используются не все слова, составленные из цифр, а только те, которые не начинаются с нуля[47]. Читателю рекомендуется поупраж-

[46] Для доказательства существования представления (*) воспользоваться теоремой о делении с остатком (см. пример на с. 459); единственность доказать от противного.

[47] Можно, конечно, пользоваться также записями вроде 02 или 002, но тогда исчезает взаимная однозначность.

няться в записи чисел в «десятичной системе счисления без нуля» (обозначая цифры хотя бы 1, ..., 9, X), а также решить задачи 16—19 в конце главы.

В настоящем параграфе мы будем все время, говоря о множествах, подразумевать множества натуральных чисел (и говоря о дополнении множества — дополнение до натурального ряда). Кроме того, мы будем считать, что фиксирован некоторый конечный алфавит $V = \{a_1, ..., a_p\}$, $P > 1$, и во всех вычислениях на машинах Тьюринга числа представляются словами в этом алфавите описанным только что способом [38]. Сплошь и рядом мы ради упрощения речи не будем различать число и представляющее его слово (здесь это не может привести к путанице).

Вернемся к нашей основной задаче. Существуют, как известно, два основных способа задания множества — путем указания характеристического свойства его элементов и путем их перечисления (см. § 1.1, пункт 4). Владея точным понятием алгоритма, мы можем теперь указать для каждого из этих двух способов «алгоритмический вариант». Для первого способа такой вариант получается наложением условия, чтобы характеристическое свойство было р а с п о з н а в а е м ы м (или, как часто говорят, р а з р е ш и м ы м), т. е. чтобы существовал алгоритм, позволяющий по любому слову узнать, обладает ли оно этим свойством. В алгоритмическом варианте второго способа перечисление должно быть «в самом деле перечислением», т. е. происходить с помощью некоторого п е р е ч и с л я ю щ е г о а л г о р и т м а. Эти соображения нетрудно уточнить следующим образом. В первом варианте не вполне четкое понятие «характеристического свойства» можно заменить понятием характеристического предиката (см. выше, § 3.1, пункт 3). Во втором варианте перечисляющий алгоритм можно понимать как машину Тьюринга, которая «выдает» в заключительных ситуациях всевозможные элементы множества, если «подавать» на ее ленту в начальных ситуациях всевозможные натуральные числа: иначе говоря, перечисляемое множество должно быть множеством значений (одноместной) функции, которую вычисляет некоторая машина Тьюринга с входным и выходным алфавитами, совпадающими с нашим алфавитом $V$. Это приводит нас к следующим двум определениям:

1. Множество называется *разрешимым* (или *рекурсивным*) [39], если его характеристический предикат является вычислимым.

---

[38] В примерах параграфа 7.3 мы пользовались другой записью (простейшей) только из-за того, что при ней программы машин намного проще.

[39] Термины «рекурсивное множество» и «рекурсивно перечислимое множество» связаны с тем, что при определении этих понятий часто используется другое уточнение понятия алгоритма — рекурсивные функции (см. ниже, §§ 7.8 и 7.9).

2. Множество называется *перечислимым*[40] (или *рекурсивно перечислимым*), если оно является множеством значений некоторой вычислимой функции.

Здесь и далее в этом параграфе, говоря о вычислимых функциях, мы подразумеваем одноместные вычислимые функции.

Задачи. 1) Доказать без использования тезиса Чёрча (т. е. построением соответствующих машин) разрешимость следующих множеств слов в алфавите $\{a_1, \ldots, a_s\}$ $(s \geq 1)$[41]:

(а) Множества слов чётной длины.

(б) Множества слов, длины которых дают при делении на 3 остаток 2.

(в) Множества симметричных слов.

(г) Множества слов, содержащих заданную букву.

(д) Множества слов вида $xx$.

(е) Множества слов, начинающихся заданным словом.

(ж) Множества слов, содержащих заданное подслово.

(з) Произвольного одноэлементного множества.

(и) Пустого множества.

Для пунктов (а) — (ж) воспользоваться примерами и задачами из § 7.3.

2) Доказать без использования тезиса Чёрча разрешимость следующих числовых множеств, понимаемых как множества слов в алфавите {1} (см. § 7.3):

а) Множества чётных чисел.

б) Множества чисел, делящихся на 5.

в) Множества полных квадратов.

3) Доказать с использованием тезиса Чёрча разрешимость следующих числовых множеств (способ записи чисел здесь несуществен):

а) Множества простых чисел.

б) Множества степеней двойки.

в) Множества чисел вида $C_n \cdot 10^n$, где $C_n$ — $n$-е десятичное приближение с недостатком числа $\sqrt{2}$.

г) То же для числа $\pi$.

4) Доказать без использования тезиса Чёрча перечислимость множеств из задач 1) и 2).

Размышляя над результатами задач 1, 2 и в особенности 3, читатель без труда поймет, что практически все множества натуральных

---

[40] Мы говорим просто «перечислимое», а не «алгоритмически перечислимое», так как в действительности перечислять что-либо (как и вычислять) можно только с помощью какого-то алгоритма.

[41] Алфавит $\{a_1, \ldots, a_s\}$ считается здесь содержащимся в нашем основном алфавите $\{a_1, \ldots, a_p\}$, но не обязан совпадать с ним; поэтому допускается и случай $s = 1$. Машина для $s = 1$ может строиться так же, как для общего случая.

чисел и слов в алфавитах, возникающие из задач вычислительного характера, разрешимы. (То же верно и для перечислимости — см. ниже теорему 4.)

2. Займемся теперь изучением свойств разрешимых и перечислимых множеств.

Теорема 1. Объединение и пересечение разрешимых множеств разрешимы; дополнение к разрешимому множеству разрешимо.

Ввиду известного соответствия между теоретико-множественными операциями и пропозициональными связками (см. выше, § 3.1, пункт 3) эта теорема немедленно вытекает из следующей:

Теорема 1′. Дизъюнкция и конъюнкция вычислимых предикатов вычислимы; отрицание вычислимого предиката вычислимо.

Теорема 1′ справедлива для предикатов любой вместимости; мы, однако, докажем ее только для одноместных предикатов — этого достаточно, чтобы получить теорему 1. Для общего случая теорема доказывается аналогично.

Доказательство теоремы 1′. 1) Пусть машины Тьюринга $M_1$ и $M_2$[42] вычисляют предикаты $F_1(x)$ и $F_2(x)$ соответственно. Тогда машина, вычисляющая предикат $F_1(x) \vee F_2(x)$ (с входным алфавитом, равным объединению входных алфавитов $M_1$ и $M_2$), будет работать следующим образом. Если на ее ленте в начальной ситуации записано слово (число) $x$, она это слово удваивает (см. пример 4 из § 7.3), вставляя между двумя его экземплярами разделительный знак (не принадлежащий объединению внешних алфавитов $M_1$ и $M_2$); затем она работает со вторым экземпляром $x$, как $M_1$ (обращаясь при этом с разделительным знаком, как с граничным маркером); если в результате получится $и$, то все содержимое ленты стирается и вслед за (настоящим) граничным маркером записывается $и$; если же в результате работы со вторым экземпляром $x$ получилось $л$, то машина стирает это $л$ и разделительный знак, а затем работает с первым экземпляром $x$, как $M_2$.

2) Если машина $M$ вычисляет предикат $F(x)$, то машина, вычисляющая $\neg F(x)$ (с тем же входным алфавитом), должна работать так же, как $M$, до самого конца, а затем, если получилось $и$, переработать его в $л$, а если $л$ — в $и$.

3) Утверждение для конъюнкции следует из утверждений для дизъюнкции и отрицания ввиду соотношения $F_1(x) \,\&\, F_2(x) \equiv \neg(\neg F_1(x) \vee \neg F_2(x))$.

Задачи

1) Доказать пункт 3) теоремы 1 непосредственно.

[42] Всюду в этом параграфе, говоря о машинах Тьюринга, мы подразумеваем машины с входными и выходными алфавитами.

2) Используя задачи 1) и 2) в конце предыдущего пункта и теорему 1, доказать разрешимость следующих множеств:

а) Произвольного конечного множества.

б) Множества всех натуральных чисел.

в) Множества нечетных чисел.

г) Множества чисел, делящихся на 10.

Теорема 2. Объединение и перечисление перечислимых множеств перечислимы.

Доказательство. Пусть машины $M_1$ и $M_2$ вычисляют функции $f_1(x)$ и $f_2(x)$ с множествами значений $E_1$ и $E_2$ соответственно. Тогда:

1) По машинам $M_1$ и $M_2$ легко построить машину, которая будет вычислять функцию $f$, определенную следующим образом:

$$f(2x)\begin{cases} = f_1(x), & \text{если } f_1(x) \text{ определена;} \\ \text{не определена}, & \text{если } f_1(x) \text{ не определена;} \end{cases}$$

$$f(2x+1)\begin{cases} = f_2(x), & \text{если } f_2(x) \text{ определена;} \\ \text{не определена}, & \text{если } f_2(x) \text{ не определена.} \end{cases}$$

Ясно, что значениями $f$ будут те и только те числа, которые служат значениями хотя бы одной из функций $f_1, f_2$, так что множество ее значений есть $E_1 \cup E_2$.

2) Нетрудно построить по $M_1$ и $M_2$ также машину, вычисляющую функцию $g$, такую, что: (а) для чисел вида $x = 2^{x_1} \cdot 3^{x_2}$ $g(x)$ определена тогда и только тогда, когда $f_1(x_1)$ и $f_2(x_2)$ определены и совпадают, и в этом случае значение $g(x)$ равно общему значению $f_1(x_1)$ и $f_2(x_2)$; (б) для остальных $x$ значение $g(x)$ не определено. Значениями $g$ будут, очевидно, те и только те числа, которые служат значениями как $f_1$, так и $f_2$, так что множество ее значений есть $E_1 \cap E_2$.

Теорема 3. Множество тогда и только тогда перечислимо, когда оно является областью определения некоторой вычислимой функции.

Доказательство. 1) Пусть машина $M$ вычисляет функцию $f(x)$ с множеством значений $E$. Рассмотрим машину, входной и выходной алфавиты которой совпадают с выходным алфавитом машины $M$, работающую следующим образом. Если в начальной ситуации на ее ленте записано число $x$, машина ставит справа от него разделительный знак («квадратик») и справа от этого знака проделывает два первых шага того вычисления машины $M$, которое начинается с числа 0. Затем головка идет вправо: в первой встретившейся ей при этом пустой ячейке ставится другой разделительный знак («звездочка»), справа от этого знака записывается число 1 и производится первый шаг вычисления машины $M$, начинающегося с этого числа. Затем головка идет влево до квадратика, и на том участке ленты, где были

проделаны два первых шага вычисления $M$, начинающегося с нуля, производится третий шаг этого вычисления. (Для этого нужно, разумеется, чтобы после первых двух шагов была помечена ячейка, в которой остановилась головка, и метка указывала, на каком состоянии вычисление было прервано.) Если на этом шаге головка машины $M$ сдвигалась вправо, то производится сдвиг вправо той части записи, которая расположена правее преобразуемого сейчас участка. Далее головка идет вправо, и на том участке ленты, где был выполнен первый шаг вычисления $M$, начинающегося с единицы, производится второй шаг (здесь нужно сделать те же оговорки, которые были сделаны относительно вычисления, начинающегося с нуля). После этого головка идет дальше вправо; в первой встретившейся ей пустой ячейке ставится еще одна звездочка, за ней записывается число 2 и производится первый шаг начинающегося с него вычисления $M$. Потом головка снова идет влево до квадратика, после чего производится четвертый шаг вычисления с нулем, третий с единицей, второй с двойкой, затем через звездочку записывается число 3 и над ним производится первый шаг вычисления, и т. д. Таким образом, наша машина параллельно вычисляет (вернее, пытается вычислять) значения функции $f$ для всевозможных значений аргумента $n$. Этот процесс продолжается до тех пор, пока на каком-то «$n$-участке» вычисление не остановится. Если эта остановка безрезультатная, так что $f(n)$ не определена, машина продолжает работу с той только разницей, что далее головка проходит этот «$n$-участок», не изменяя его. Если же вычислено значение $f(n)$, оно сравнивается с $x$. При $f(n) \neq x$ работа продолжается так же, как в случае безрезультатной остановки; при $f(n) = x$ все содержимое ленты стирается, и машина переходит в заключительное состояние.

Ясно, что функция, вычисляемая описанной машиной, определена для тех и только для тех $x$, которые служат значениями функции $f$, т. е. принадлежат $E$.

2) Пусть машина $M$ вычисляет функцию $f$ с областью определения $E$. Рассмотрим машину, входной и выходной алфавиты которой совпадают с входным алфавитом $M$, работающую так: если в начальной ситуации на ее ленте записано слово $x$, оно удваивается с постановкой разделительного знака между двумя экземплярами, затем со вторым экземпляром машина работает, как $M$, и если при этом будет получено какое-то значение $f(x)$, то справа от разделительного знака все стирается и он сам тоже, головка становится на граничный маркер и машина переходит в заключительное состояние; если же $f(x)$ не определено, то машина «ломается» или работает вечно. Вычисляемая этой машиной функция определена в точности для тех же $x$, что и $f$, и в случае, когда ее значение определено, оно совпадает со

значением аргумента; таким образом, множество значений этой функции есть $E$.

Теорема 4. Всякое разрешимое множество перечислимо.

Доказательство. По машине $M$, вычисляющей характеристический предикат множества $E$, легко построить другую машину, которая выдает $u$, если $M$ выдает $u$, и работает вечно, если $M$ выдает $л$ (ср. доказательство теоремы 1 предыдущего параграфа). Область определения вычисляемой этой машиной функции есть $E$. Остается воспользоваться теоремой 3.

Задача. Доказать теорему 4 без использования теоремы 3. [Указание. Начать с удвоения исходного слова.]

Теорема 5 (теорема Поста). Множество тогда и только тогда разрешимо, когда оно само и его дополнение перечислимы.

Доказательство. 1) Пусть множества $E$ и $CE$ (дополнение $E$) перечислимы. По теореме 3 существуют машины Тьюринга $M_1$ и $M_2$, вычисляющие функции $f_1$ и $f_2$ с областями определения $E$ и $CE$ соответственно. Построим по ним машину (входной алфавит которой будет совпадать с входным алфавитом $A'_{вх}$ машины $M_1$), работающую следующим образом. Если на ее ленте в начальной ситуации записано слово $x$ в алфавите $A'_{вх}$, оно удваивается (с постановкой разделительного знака между экземплярами), а затем оба экземпляра обрабатываются параллельно — первый по программе машины $M_1$, второй по программе $M_2$ (шаги вычислений с первым и вторым экземплярами производятся поочередно — ср. доказательство теоремы 2). Поскольку $x$ принадлежит одному и только одному из множеств $E$ и $CE$, один и только один из этих двух параллельных процессов закончится вычислением значения соответствующей функции. После этого все стирается и записывается $u$, если вычислено значение $f_1$, и $л$, если вычислено значение $f_2$. Таким образом, наша машина вычисляет характеристический предикат множества $E$.

2) Обратное утверждение непосредственно вытекает из теорем 4 и 1.

3. Обратимся теперь к вопросу о существовании неразрешимых и неперечислимых множеств, а также невычислимых функций. (Разумеется, речь идет о множествах натуральных чисел — или слов в конечных алфавитах — и о функциях, отображающих такие множества на такие же.) Ответить на этот вопрос очень просто, исходя из мощностных соображений. Действительно, мощность множества функций, вычисляемых всевозможными машинами Тьюринга, во всяком случае не превосходит мощности множества кодов всевозможных машин Тьюринга, т. е. слов специального вида в алфавите $\{a_1, \ldots, a_8\}$; но даже множество всех слов в конечном алфавите счетно, в то время как множество всех функций, отображающих подмноже-

ства натурального ряда на подмножества натурального ряда, имеет мощность континуума. Далее, мощность множества всех перечислимых множеств натуральных чисел не превосходит мощности множества вычислимых функций, значения которых пробегают эти множества; таким образом, множество перечислимых множеств натуральных чисел счетно, в то время как множество всех подмножеств натурального ряда имеет мощность континуума. Итак, невычислимые функции и неперечислимые (а значит, и неразрешимые) множества не только существуют, но их «больше», чем вычислимых функций, соответственно перечислимых множеств.

Это простое решение страдает, однако, существенным недостатком: оно не дает никакого конкретного примера неперечислимого множества или невычислимой функции. Кроме того, мощностные соображения не позволяют решить столь же естественный вопрос о существовании неразрешимых перечислимых множеств; как легко видеть, множество разрешимых множеств тоже счетно. Заметим, что если нам удастся указать пример неразрешимого перечислимого множества, то его дополнение в силу теоремы 5 даст нам пример неперечислимого множества, а его характеристический предикат (точнее — функция, сопоставляющая значениям аргумента истинностные значения значений предиката) — пример невычислимой функции. Сейчас мы укажем такой пример; но сначала нам будет удобно ввести следующее простое, но важное для дальнейшего определение:

Стандартный номер кода машины Тьюринга называется *гёделевским номером* — или просто *номером* — этой машины.

Это определение нуждается, впрочем, в уточнении: ведь стандартная нумерация слов зависит от выбора алфавита (а также от выбора его пересчета). Коды машин Тьюринга — это цепочки в алфавите $A' = \{a_1, ..., a_8\}$, и мы можем выбрать любой алфавит, содержащий $A'$. Мы остановимся на алфавите $\{a_1, ..., a_9\}$ — из соображений, которые выяснятся ниже, в § 7.9. А сейчас перейдем к обещанному примеру.

Теорема 6. Множество номеров самоприменимых машин Тьюринга перечислимо, но не разрешимо.

Поскольку мы обычно отождествляем слово с его номером, вместо множества номеров мы можем говорить здесь о множестве кодов.

Доказательство. Утверждение о неразрешимости этого множества есть просто другая формулировка теоремы 1 предыдущего параграфа. Чтобы доказать его перечислимость, рассмотрим машину Тьюринга с входным алфавитом $\{a_1, ..., a_9\}$, работающую следующим образом: если на ее ленте в начальной ситуации записано слово $x$, она прежде всего, не изменяя этого слова, распознает, является ли оно кодом какой-либо машины Тьюринга; если нет — машина «ломает-

ся», если да — удваивает слово $x$, вставляя между двумя его экземплярами $a_0$, и далее работает как универсальная машина, т. е. преобразовывает слово $x$ в соответствии с программой той машины, для которой это же слово служит кодом. Если при этом будет получен результат — т. е. если машина с кодом $x$ самоприменима,— то все содержимое ленты стирается, и машина переходит в заключительное состояние. (В противном случае она, очевидно, «ломается» или работает вечно.) Ясно, что вычисляемая этой машиной функция определена для тех и только для тех слов, которые являются кодами самоприменимых машин Тьюринга. Остается применить теорему 3.

Таким образом, два основных способа задания множеств при алгоритмизации оказываются неэквивалентными: перечисление — способ более сильный, чем (эффективное) указание характеристического свойства элементов.

Отметим еще

Следствие. Множество номеров несамоприменимых машин Тьюринга неперечислимо.

Доказательство. Пусть $A$, $B$ и $C$ — соответственно множество номеров несамоприменимых машин, дополнение к множеству номеров самоприменимых машин и множество чисел, не являющихся номерами никаких машин. Множество $C$ разрешимо и тем более перечислимо, и если бы $A$ также было перечислимо, то ввиду очевидного равенства $B = A \cup C$ по теореме 2 оказалось бы перечислимым и $B$, что невозможно в силу теорем 5 и 6.

С помощью конструкции, использованной в доказательстве теоремы 6, мы докажем сейчас еще одну важную теорему. Ее доказательство доставит нам еще два примера неразрешимых перечислимых множеств (а также способ получать такие примеры в любом числе).

Теорема 7. Существуют непересекающиеся перечислимые множества $E_1$ и $E_2$, такие, что никакое разрешимое множество не может содержать $E_1$, не имея при этом общих точек с $E_2$. (Как иногда говорят, $E_1$ и $E_2$ *не отделимы* разрешимыми множествами.)

Доказательство. Обозначим через $E_1$, соответственно через $E_2$, множество кодов тех машин Тьюринга, которые перерабатывают свой собственный код в пустое, соответственно в непустое слово. Для доказательства перечислимости этих множеств достаточно рассмотреть машину, использовавшуюся в доказательстве теоремы 6, изменив ее в случае $E_1$ так, чтобы она переходила в заключительное состояние лишь при условии, что результат, получаемый на этапе, когда машина работает как универсальная, есть пустое слово[41],

[41] Напомним, что пустое слово служит своим собственным кодом.

а в случае $E_2$ — при условии, что этот результат есть непустое слово. Допустим теперь, что существует разрешимое множество $E$, содержащее $E_1$ и не пересекающееся с $E_2$. По машине, вычисляющей характеристический предикат множества $E$, легко построить другую машину — обозначим ее $M$,— которая каждое число, т. е. каждое слово $x$ в алфавите $\{a_1, ..., a_9\}$, перерабатывает в непустое слово, если $x \in E$, и в пустое, если $x \notin E$. Но во что переработает машина $M$ свой собственный код $\varkappa(M)$? Если в пустое слово, то тем самым $\varkappa(M) \in E_1$, откуда $\varkappa(M) \in E$ — а тогда по построению машины она должна перерабатывать $\varkappa(M)$ в непустое слово. Если же $M$ перерабатывает $\varkappa(M)$ в непустое слово, то $\varkappa(M) \in E_2$, откуда $\varkappa(M) \notin E$ и, следовательно, $M$ должна перерабатывать $\varkappa(M)$ в пустое слово. Полученное противоречие завершает доказательство.

Замечания. 1) Очевидно, любая неразрешимая алгоритмическая проблема дает пример неразрешимого множества. Например, в силу теоремы Райса для любого нетривиального инвариантного свойства машин Тьюринга множество номеров (или кодов) машин, обладающих этим свойством, неразрешимо; для всякой полугруппы с неразрешимой проблемой тождества неразрешимо множество слов вида $x \square y$, где $x$ и $y$ — произвольные слова из образующих полугруппы, представляющие один и тот же ее элемент, и $\square$ — символ, отличный от всех ее образующих, и т. п.

2) Существуют и такие множества натуральных чисел, которые неперечислимы вместе со своими дополнениями (см. задачу 35 в конце главы).

Задачи. 1) Доказать, что множество номеров машин, применимых каждая хотя бы к одному слову, перечислимо.

2) Доказать, что множество номеров машин, не применимых ни к каким словам, неперечислимо. [Указание. Воспользоваться теоремой Райса, результатом предыдущей задачи и теоремами 5 и 2.]

3) Доказать, что для любого слова $y$ множество номеров машин, вычисляющих функции, принимающие хотя бы для одного слова значение $y$, перечислимо, а множество номеров машин, вычисляющих функции, не принимающие значения $y$, неперечислимо.

4) Теорема 7 допускает следующее обобщение: для любого $n = 2, 3, ...$ найдутся попарно непересекающиеся перечислимые множества $E_1, ..., E_n$, для которых не существует попарно непересекающихся разрешимых множеств $G_1, ..., G_n$, таких, что $E_i \subseteq G_i$. Доказать.

4. В заключение параграфа докажем еще две теоремы о способах перечисления множеств.

Прежде всего естественно спросить: нельзя ли использовать для перечисления множеств только всюду определенные вычислимые функции? Это лучше отвечало бы интуитивному представлению о

перечислении: «запуская» машину последовательно для чисел 0, 1, 2, ..., мы получили бы один за другим все элементы множества, никогда не рискуя, что вычисление окажется бесконечным или оборвется безрезультатно. Ответ на этот вопрос, за очевидным исключением пустого множества, оказывается положительным, как видно из следующей теоремы.

**Теорема 8.** Всякое непустое перечислимое множество является множеством значений некоторой всюду определенной вычислимой функции.

**Доказательство.** Пусть машина $M$ вычисляет функцию $f$ с непустым множеством значений $E$, и пусть $x_0$ — некоторый элемент $E$. Построим по машине $M$ новую машину $M_1$, которая будет работать так же, как машина, построенная в пункте 1 доказательства теоремы 3, с той только разницей, что зона ленты, где записано данное число $x$, используется теперь как «счетчик шагов»: после имитации каждого шага какого-либо вычисления машины $M$ головка машины $M_1$ идет в зону счетчика, и содержащееся в этой зоне число уменьшается на единицу. Когда содержимое зоны счетчика оказывается нулем (пустым словом), имитация вычислений машины $M$ прекращается и, если на имитировавшемся перед этим шаге работы машины $M$ как раз было вычислено какое-то значение $f(z)$ функции $f$, машина записывает это $f(z)$ на ленте (стирая все остальное) и переходит в заключительное состояние; в противном случае она все стирает, записывает на ленте слово $x_0$ и также переходит в заключительное состояние. Вычисляемая машиной $M_1$ функция $f_1$ всюду определена, и легко видеть, что множество ее значений совпадает с $E$.

Еще лучше отвечало бы интуитивному представлению о перечислении использование разнозначных всюду определенных функций (т. е. таких, значения которых для любых двух различных значений аргумента различны); тогда каждый элемент множества считался бы только один раз. Разумеется, для конечных множеств такими функциями обойтись нельзя; но для бесконечных множеств это возможно, как показывает

**Теорема 9.** Всякое бесконечное перечислимое множество является множеством значений некоторой разнозначной всюду определенной вычислимой функции.

**Доказательство.** Пусть машина $M$ вычисляет функцию $f$ с бесконечным множеством значений $E$. По машине $M$ мы построим новую машину $M_1$, вычисляющую функцию $f$; эта машина будет работать так же, как машина, построенная при доказательстве теоремы 8, но со следующими отличиями: 1) каждый раз, когда при имитации какого-либо шага работы машины $M$ вычисляется некоторое значение функции $f$, оно сравнивается со всеми ранее вычисленными ее значениями, и только в случае, когда оно отлично от всех этих значений,

происходит обращение к счетчику и уменьшение на единицу его содержимого; 2) после имитации тех шагов работы $M$, на которых не вычисляется никакое значение $f$, обращения к счетчику не происходит.

Пусть теперь $M'$ — машина, отличающаяся от $M_1$ тем, что она вообще никогда не обращается к счетчику. Эта машина работает вечно, вычисляя одно за другим значения функции $f$, так что каждое значение в какой-то момент оказывается вычисленным. Пусть $b_1, b_2, b_3, \ldots$ — последовательность, состоящая из значений $f$, расположенных в том порядке, в котором их «выдаст» машина $M'$, и $b_{i_1}, b_{i_2}, b_{i_3}, \ldots$ — подпоследовательность этой последовательности, определенная так: $b_{i_1} = b_1$; $b_{i_2}$ есть первый член последовательности, отличный от $b_{i_1}$; $b_{i_3}$ есть первый член, отличный от $b_{i_1}$ и от $b_{i_2}$, и т. д. Легко понять, что если на ленте машины $M_1$ в начальной ситуации записано число $k$, то в заключительной ситуации на ней будет $b_{i_{k+1}}$. А поскольку $b_{i_1}, b_{i_2}, b_{i_3}, \ldots$ — бесповторный пересчет множества $E$, машина $M_1$ вычисляет разнозначную функцию, для которой $E$ есть множество значений.

Замечания. 1) Эта конструкция годится и для конечного $E$, но тогда она даст функцию, определенную на некотором отрезке натурального ряда.

2) Потом мы усилим теорему 5 еще и в другом направлении (см. § 7.9, теорема 4).

Задачи. 1) Показать, что множество значений возрастающей всюду определенной вычислимой функции разрешимо, и обратно — всякое бесконечное разрешимое множество есть множество значений некоторой возрастающей всюду определенной вычислимой функции.

2) Показать, что всякое перечислимое множество есть множество значений некоторой возрастающей вычислимой функции. [Указание: см. пункт 2 доказательства теоремы 3.]

## § 7.8. ПРИМИТИВНО РЕКУРСИВНЫЕ ФУНКЦИИ

1. В этом и следующем параграфах мы познакомимся еще с одним уточнением понятия вычислимой функции, в основе которого лежит широко распространенный способ вычисления функ-

ций натурального аргумента, состоящий в том, что задается $f(0)$ и так называемая рекуррентная[44] формула $f(n+1) = h(f(n))$, позволяющая вычислить $f(n+1)$, если известно $f(n)$, и с помощью этой формулы последовательно вычисляются $f(1)$, $f(2)$ и т. д. Такой процесс последовательного вычисления значений функции называется *рекурсией*[45]. Метод рекурсии дает возможность сводить вычисление одной функции к вычислению другой: если мы умеем вычислять $h$, то мы сумеем вычислить и любое значение $f$. (Примером может служить функция $2^n$, которую можно задать равенствами $2^0 = 1$, $2^{n+1} = 2^n \cdot 2$, сводящими вычисление ее значений к вычислению значений функции $h(m) = m \cdot 2$.) Таким образом, если из вычислимой (в интуитивном смысле) функции получена с помощью рекурсии другая функция, то эта новая функция также вычислима (в том же смысле).

Разумеется, рекурсия — не единственный способ получать одни функции из других, при котором вычислимая функция переходит в вычислимую. Тем же свойством обладает, например, подстановка (суперпозиция): если мы умеем вычислять функции $f(x)$ и $g(x)$, то мы сумеем вычислить и функцию $g(f(x))$.

Если у нас есть некоторый запас «простейших» функций, вычисление которых тривиально, то все функции, которые можно из них получить, производя сколько угодно раз суперпозиции и рекурсии, с точки зрения любой разумной интуиции также будут вычислимыми. Естественно спросить: насколько широк класс вычислимых функций, которые можно так получить? Прежде чем выяснять этот вопрос, нужно, разумеется, уточнить, из какого запаса «простейших» функций мы исходим. Но целесообразно также обобщить понятие рекурсии — и даже в двух направлениях. Во-первых, $f(n+1)$ может зависеть не только от $f(n)$, но и от самого $n$: в этом случае рекуррентная формула имеет вид $f(n+1) = h(n, f(n))$, где $h$ — некоторая заведомо вычислимая функция двух переменных. Например, для функции $f(n) = n!$ будет $h(l, m) = m \cdot (l+1)$, что дает формулу $(n+1)! = n! \cdot (n+1)$[46]. (В рассмотренном выше частном случае, когда $h$ — одноместная функция и $f(n+1) = h(f(n))$, функцию $f$ часто называют *итерацией*[47] функции $h$.) Во-вторых, с помощью рекурсии можно вычислять также и функции нескольких переменных[48].

---

[44] От лат. *recurro* — «возвращаюсь».

[45] От лат. *recursio* — «возвращение, круговорот» (*recurso* — «возвращаюсь»).

[46] 0! можно формально положить равным 1.

[47] От лат. *iteratio* — «повторение» (*iterum* — «еще раз»).

[48] Которые мы теперь обязаны ввести в рассмотрение, поскольку рекурсивное вычисление функции одной переменной мы производим с помощью функции двух переменных.

При этом все переменные, кроме одной, служат «параметрами», и для каждого фиксированного набора их значений вычисление функции от оставшейся переменной производится точно так же, как мы это делали для одноместных функций. Это значит, что если мы вычисляем функцию $f(x_1, \ldots, x_k)$, $k > 1$, и рекурсия проводится по переменной $x_k$, то $f(x_1, \ldots, x_{k-1}, 0)$ вычисляется по формуле $f(x_1, \ldots, x_{k-1}, 0) = g(x_1, \ldots, x_{k-1})$, а $f(x_1, \ldots, x_{k-1}, x_k + 1)$ — по формуле $f(x_1, \ldots, x_{k-1}, x_k + 1) = h(x_1, \ldots, x_{k-1}, x_k, f(x_1, \ldots, x_{k-1}, x_k))$, где $g$ и $h$ — заведомо вычислимые функции вместимости $k - 1$ и $k + 1$ соответственно. Например, для $f(x_1, x_2) = x_1 \cdot x_2$ функция $g(x_1)$ тождественно равна нулю, а $h(x_1, x_2, x_3)$ есть $x_1 + x_1$, что дает формулы $x_1 \cdot 0 = 0$, $x_1 \cdot (x_2 + 1) = x_1 \cdot x_2 + x_1$.

Что касается исходного набора «простейших» функций, то в него естественно включить тривиальные функции вида $f(x_1, \ldots, x_k) = x_i$ $(i = 1, \ldots, k)$, а также функции-константы $f(x_1) = m$. Но одних этих функций недостаточно, чтобы получить сколько-нибудь интересный класс с помощью подстановки и рекурсии (см. задачу 36 в конце главы), и мы добавим к ним еще одну, также очень простую и вычислимую тривиальным образом: $S(x) = x + 1$. При этом, кстати, мы сможем вместо всевозможных функций-констант обойтись функцией, тождественно равной нулю: из нее и из $S(x)$ с помощью подстановки очевидным образом получаются все остальные функции-константы.

Функции, получаемые из описанного исходного набора с помощью подстановки и рекурсии, принято называть примитивно рекурсивными[49]. Фактически мы их уже определили, но ввиду важности этого понятия приведем строгие формулировки.

Всюду в этом параграфе, говоря о функциях, мы будем подразумевать функции, у которых область определения состоит из упорядоченных систем натуральных чисел (для одноместных функций — просто из натуральных чисел) и множество значений также есть подмножество натурального ряда.

---

[49] Этот термин — перевод английского *primitive recursive functions*. Правильнее было бы переводить «примитивные рекурсивные функции» или даже «простые рекурсивные функции»: в английском термине слово *primitive* — не наречие, а прилагательное, означающее «первоначальный, простой» (ср. *primitive number* — простое число), в противоположность «общим рекурсивным функциям» (*general recursive functions*, в общепринятом русском варианте — общерекурсивные функции), которые будут рассмотрены ниже. (Английское *primitive*, как и русское «примитивный», происходит от латинского *primitivus* — «первый».) Однако в русской литературе по теории алгоритмов сложилась уже традиция, которую не стоит нарушать.

Дальнейшие подробности см. в § 7.9, пункт 1.

Будем называть *исходными примитивно рекурсивными функциями* функции $e'_k(x_1, \ldots, x_k) = x_l$, $0(x) = 0$, $S(x) = x + 1$ (функции $e'_k$ называют *функциями выделения аргумента*, или *проектирующими функциями*).

Рассмотрим, далее, два оператора, действующие на функции: оператор подстановки и оператор рекурсии.

*Оператор подстановки* применяется к функциям $g_1, \ldots, g_l$ вместимости $k$ и функции $h$ вместимости $l$ ($k, l = 1, 2, \ldots$); результат его применения есть функция $f$ вместимости $k$, определяемая равенством

$$f(x_1, \ldots, x_k) = h(g_1(x_1, \ldots, x_k), \ldots, g_l(x_1, \ldots, x_k))^{50}.$$

*Оператор рекурсии* применяется либо к натуральному числу и функции $h$ вместимости 2, либо к функциям $g$ и $h$ вместимости $n - 1$ и $n + 1$ соответственно, где $n = 2, 3, \ldots$; результат его применения есть функция $f$ вместимости 1 в первом случае и $n$ во втором, удовлетворяющая *рекурсивным равенствам*: в первом случае это равенства

$$(R_1)\ \begin{cases} f(0) = c \\ f(x + 1) = h(x, f(x)), \end{cases}$$

во втором

$$(R_2)\ \begin{cases} f(x_1, \ldots, x_{n-1}, 0) = g(x_1, \ldots, x_{n-1}) \\ f(x_1, \ldots, x_{n-1}, x_n + 1) = h(x_1, \ldots, x_{n-1}, x_n, f(x_1, \ldots, x_{n-1}, x_n)). \end{cases}$$

Рекурсивные равенства вполне определяют функцию $f$: ее значение для $x = 0$ или для $x_n = 0$ однозначно находится из первого равенства, а из второго равенства по значению для очередного $x$ или $x_n$ также однозначно находится значение для $x + 1$, соответственно для $x_n + 1$.

Теперь мы можем, наконец, сформулировать основное определение: *примитивно рекурсивной функцией* (сокращенно *п. р. ф.*) называется функция, которая либо принадлежит к числу исходных примитивно рекурсивных функций, либо может быть получена из них с помощью операторов подстановки и рекурсии.

Задача. Описать класс функций, получаемых из исходных п. р. ф. с помощью одного лишь оператора подстановки.

---

[50] Вообще говоря, функции $g_1, \ldots, g_l, h$ не обязаны быть всюду определенными, однако в настоящем параграфе оператор подстановки будет применяться только к всюду определенным функциям (так что и результат его применения будет всюду определенной функцией).

Примеры п. р. ф.:

1) Функции произвольной вместимости $n$ $(n > 1)$, тождественно равные нулю: $0_n(x_1, \ldots, x_n) = 0(e^1_n(x_1, \cdots, x_n))$.

2) Функции-константы $k(x)(k = 1, 2, \ldots)$: $1(x) = S(0(x))$, $2(x) = S(1(x))$ и т. д. Аналогично, с использованием примера 1, получаются функции-константы $k_n(x_1, \ldots, x_n) = k$ вместимости $n > 1$.

3) Функции $S_k(x) = x + k$ $(k = 2, 3, \ldots)$: $S_2(x) = S(S1(x))$, $S_3(x) = S(S_2(x))$ и т.д.

4) Функция $x_1 + x_2$ получается с помощью оператора рекурсии из функции $e^1_1(x_1) = x_1$ (в качестве $g$) и $S(e^3_3(x_1, x_2, x_3)) = x_3 + 1$ (в качестве $h$), так что рекурсивные равенства для $x_1 + x_2$ имеют вид

$$\begin{cases} x_1 + 0 = e^1_1(x) \\ x_1 + (x_2 + 1) = S(e^3_3(x_1, x_2, x_1 + x_2)). \end{cases}$$

или, в менее педантичной записи,

$$\begin{cases} x_1 + 0 = x_1 \\ x_1 + (x_2 + 1) = (x_1 + x_2) + 1. \end{cases}$$

5) Функция $x_1 \cdot x_2$ получается с помощью оператора рекурсии из функций $0(x_1) = 0$ и $e^3_3(x_1, x_2, x_3) + e^1_3(x_1, x_2, x_3) = x_3 + x_1$. Рекурсивные равенства выписаны выше (с. 329).

6) Функция $x \dot{-} 1$ («усеченная разность между $x$ и единицей»), равная $x - 1$ при $x \geq 1$ и 0 при $x = 0$, получается с помощью оператора рекурсии из числа 0 и функции $e^1_1(x_1, x_2) = x_1$, так что рекурсивные равенства имеют вид

$$\begin{cases} 0 \dot{-} 1 = 0 \\ (x + 1) \dot{-} 1 = x. \end{cases}$$

В дальнейших примерах мы уже не указываем явно функции $g$ и $h$ (или число $c$ и функцию $h$) и ограничиваемся выписыванием рекурсивных равенств.

7) Функция $x \dot{-} y$ («*усеченная разность*»), равная $x - y$ при $x \geq y$ и 0 при $x < y$:

$$\begin{cases} x \dot{-} 0 = x \\ x \dot{-} (y + 1) = (x \dot{-} y) \dot{-} 1. \end{cases}$$

8) $|x - y| = (x \dot{-} y) + (y \dot{-} x)$.

9) Функция $sg\,x$ (читается «знак $x$»), равная 0 при $x = 0$ и 1 при $x > 0$:

$$\begin{cases} sg\ 0 = 0 \\ sg\ (x + 1) = 1. \end{cases}$$

10) Функция $\overline{sg}x$, равная 1 при $x = 0$ и 0 при $x > 0$:

$$\begin{cases} \overline{sg}\ 0 = 1 \\ \overline{sg}\ (x + 1) = 0. \end{cases}$$

11) $\min(x, y) = x \dot{-} (x \dot{-} y)$.

12) $\max(x, y) = y + (x \dot{-} y)$.

13) Функция $r(x,y)$, равная остатку от деления $y$ на $x$, если $x \neq 0$, и нулю, если $x = 0$:

$$\begin{cases} r(x, 0) = 0 \\ r(x, y + 1) = (r(x, y) + 1) \cdot sg(x \dot{-} (r(x, y) + 1)). \end{cases}$$

14) Функция $q(x, y)$, равная целой части частного от деления $y$ на $x$, если $x \neq 0$, и нулю, если $x = 0$:

$$\begin{cases} q(x, 0) = 0 \\ q(x, y + 1) = q(x, y) + \overline{sg}\,|x - (r(x, y) + 1)|. \end{cases}$$

15) $x!$ (см. с. 329).

16) $a^x$, где $a$ — константа (см. с. 328).

Задача. Доказать, что следующие функции примитивно рекурсивны:

а) $x^3$;

б) $[\sqrt{x}\,]$;

в) $[\log_2 x\,]$;

г) $\min_n(x_1, \ldots, x_n)$ — наименьшее из чисел $x_1, \ldots, x_n$ $(n = 3, 4, \cdots)$;

д) $\max_n(x_1, \ldots, x_n)$ — наибольшее из чисел $x_1, \ldots, x_n$ $(n = 3, 4, \cdots)$.

2. Наряду с примитивно рекурсивными функциями естественно ввести в рассмотрение примитивно рекурсивные предикаты. Мы будем называть предикат $F(x_1, \ldots, x_n)$, определенный на множестве натуральных чисел, *примитивно рекурсивным*, если примитивно рекурсивна функция $\varphi_F(x_1, \ldots, x_n)$, сопоставляющая каждому набору $x_1^0, \ldots, x_n^0$ значений переменных $x_1, \ldots, x_n$ число 1, если предложение $F(x_1^0, \ldots, x_n^0)$ истинно, и 0, если это предложение ложно.

Функция $\varphi_F$ называется *характеристической функцией* предиката $F$.

Замечание. Точно так же можно было бы определить и предикат, вычислимый по Тьюрингу — как предикат, для которого вычислима по Тьюрингу характеристическая функция (ср. конец § 7.2).

Примеры примитивно рекурсивных предикатов:

1) $x = c$, где $c$ — произвольная константа: его характеристической функцией служит $\overline{sg}\,|x - c|$.

2) $x > c$: характеристическая функция $sg(x \dot{-} c)$.

3) $x = y$: характеристическая функция $\overline{sg}\,|x - y|$.

4) $x > y$: характеристическая функция $sg(x \dot{-} y)$.

5) «$x$ четно»: характеристическая функция задается рекурсивными равенствами

$$\begin{cases} f(0) = 1 \\ f(x + 1) = \overline{sg} f(x). \end{cases}$$

6) $d(x, y) \equiv$ «$x$ делится на $y$»: характеристическая функция $\overline{sg}\, r(y, x) \cdot sgy + \overline{sg}x \cdot \overline{sg}y$ [51].

7) $y = \varphi(x_1, \ldots, x_n)$, где $\varphi$ — некоторая заданная п. р. ф.; характеристическая функция $\overline{sg}\,|y - \varphi(x_1, \ldots, x_n)|$.

3. Докажем теперь несколько простых теорем, облегчающих доказательство примитивной рекурсивности функций и предикатов.

Теорема 1. Если функция $f(x_1, \ldots, x_n)$ $(n = 1, 2, \ldots)$ примитивно рекурсивна, то таковы же и функции

$$g(x_1, \ldots, x_n) = \sum_{i=0}^{x_n} f(x_1, \ldots, x_{n-1}, i)$$

и

$$h(x_1, \ldots, x_n) = \prod_{i=0}^{x_n} f(x_1, \ldots, x_n, i).$$

Доказательство. Функция $g$ задается равенствами

$$\begin{cases} g(x_1, \ldots, x_{n-1}, 0) = f(x_1, \ldots, x_{n-1}, 0) \\ g(x_1, \ldots, x_{n-1}, x_n + 1) = g(x_1, \ldots, x_{n-1}, x_n) + f(x_1, \ldots, x_{n-1}, x_n + 1)). \end{cases}$$

Функция $h$ задается аналогично.

Замечание. Теорема 1 останется справедливой, если вместо $x_n$ верхней границей суммирования или перемножения будет произвольная п. р. ф. (Достаточно воспользоваться оператором подстановки.)

---

[51] Если функция $f(x_1, \ldots, x_n)$ примитивно рекурсивна и $i_1, \ldots, i_n$ — какая-либо перестановка из чисел $1, \ldots, n$, то функция $f(x_{i_1}, \ldots, x_{i_n})$ также примитивно рекурсивна, поскольку $f(x_{i_1}, \ldots, x_{i_n}) = f(e_1^n(x_1, \ldots, x_n), \ldots, e_n^n(x_1, \ldots, x_n))$.

Пример. Функции $\tau(x)$ и $\sigma(x)$ — число делителей и сумма делителей числа $x$ — примитивно рекурсивны, поскольку

$$\tau(x) = \sum_{t=0}^{x} \overline{sg}\, r(t, x) \dot{-} 1;$$

$$\sigma(x) = \sum_{t=0}^{x} t \cdot \overline{sg}\, r(t, x).$$

(Здесь условно считается $\tau(0) = \sigma(0) = 0$.)

Теорема 2. Если предикаты $F(x_1, \ldots, x_n)$ и $G(x_1, \ldots, x_n)$ примитивно рекурсивны, то таковы же и предикаты $\neg F(x_1, \ldots, x_n)$, $F(x_1, \ldots, x_n)\ \&\ G(x_1, \ldots, x_n)$, $F(x_1, \ldots, x_n) \vee G(x_1, \ldots, x_n)$, $F(x_1, \ldots, x_n) \supset G(x_1, \ldots, x_n)$.

Доказательство. Достаточно доказать утверждение теоремы для $\neg F$ и $F\&G$. Но если $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ — характеристические функции предикатов $F$ и $G$ соответственно, то для $\neg F$ и $F\&G$ характеристическими функциями будут $\overline{sg}\, f(x_1, \ldots, x_n)$ и $f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n)$.

Пример. Ввиду теоремы 2 из примеров в конце п. 2 вытекает, что примитивно рекурсивны предикаты $x \neq y$, $x \leq y$, $x < y$, $a < x < b$ ($a$, $b$ — константы) «$z$ есть общий делитель чисел $x$ и $y$» и т. п.

Впоследствии мы увидим, что утверждение теоремы 2 нельзя распространить на кванторы (§ 7.9, замечание 2 к теореме 5). Однако во многих случаях кванторы, участвующие в определениях арифметических предикатов, можно заменить ограниченными кванторами (см. с. 83), берущимися не по всем натуральным числам, а лишь по тем, которые не превосходят значений некоторой примитивно рекурсивной функции от свободных переменных. Такие кванторы сохраняют примитивную рекурсивность: имеет место

Теорема 3 (об ограниченных кванторах). Если предикат $F(x_1, \ldots, x_n, y)$ и функция $q(x_1, \ldots, x_n)$ примитивно рекурсивны, то таковы же и предикаты $\underset{y \leq q(x_1, \ldots, x_n)}{\forall y} F(x_1, \ldots, x_n, y)$ и $\underset{y \leq q(x_1, \ldots, x_n)}{\exists y} F(x_1, \ldots, x_n, y)$.

Доказательство. Если $f(x_1, \ldots, x_n, y)$ — характеристическая функция предиката $F$, то для предикатов $\underset{y \leq r}{\forall y} F$ и $\underset{y \leq r}{\exists y} F$ характеристическими функциями будут соответственно

$$\prod_{y=0}^{r(x_1, \ldots, x_n)} f(x_1, \ldots, x_n, y) \quad \text{и} \quad \overline{sg} \sum_{y=0}^{r(x_1, \ldots, x_n)} f(x_1, \ldots, x_n, y).$$

Примеры. Следующие предикаты примитивно рекурсивны ввиду теоремы 3:

1) $D(x, y, z)$ — «$z$ есть наибольший общий делитель чисел $x$ и $y$»:

$$D(x, y, z) \equiv d(x, z) \,\&\, d(y, z) \,\&\, \underset{t \le \min(x, y)}{\&\, \forall t} (d(x, t) \,\&\, d(y, t) \supset d(z, t)).$$

2) $P(x, y)$ — «$x$ и $y$ взаимно просты»:

$$P(x, y) \equiv \underset{z \le \min(x, y)}{\forall z} (d(x, z) \,\&\, d(y, z) \supset z = 1).$$

3) $p(x)$ — «$x$ — простое число»:

$$p(x) \equiv \neg(x = 1) \,\&\, \underset{y \le x}{\forall y} (d(x, y) \supset y = 1 \vee y = x).$$

Теперь мы рассмотрим еще один естественный оператор, применяемый к предикатам и переводящий их в функции — так называемый оператор минимизации. Результатом его применения к предикату $F(x_1, \ldots, x_n, y)$ является функция вместимости $n$, сопоставляющая каждому набору $x_1^0, \ldots, x_n^0$ значений переменных $x_1, \ldots, x_n$ наименьшее значение $y^0$ переменной $y$, при котором предложение $F(x_1^0, \ldots, x_n^0, y^0)$ истинно (если такое значение существует). Этот оператор не сохраняет примитивную рекурсивность (см. ниже, § 7.9, замечание 2 к теореме 3) не говоря уже о том, что результатом его применения может быть не всюду определенная функция. Но в ряде важных случаев его можно заменить *оператором ограниченной минимизации*, который применяется к предикату $F(x_1, \ldots, x_n, y)$ и функции $\varphi(x_1, \ldots, x_n)$ $(n = 1, 2, \ldots)$; результат его применения есть функция $f(x_1, \ldots, x_n)$, значение которой для каждого набора $x_1^0, \ldots, x_n^0$ значений переменных $x_1, \ldots, x_n$ определяется следующим образом: если хотя бы для одного числа $y$, не превосходящего $\varphi(x_1^0, \ldots, x_n^0)$, предложение $F(x_1^0, \ldots, x_n^0, y)$ истинно, то $f(x_1^0, \ldots, x_n^0)$ равно наименьшему из таких $y$; в противном случае $f(x_1^0, \ldots, x_n^0) = 0$. Эту функцию $f(x_1, \ldots, x_n)$ принято обозначать $\underset{y \le \varphi(x_1, \ldots, x_n)}{\mu y} F(x_1, \ldots, x_n, y)$. Оператор ограниченной минимизации сохраняет примитивную рекурсивность, как показывает

Теорема 4 (об ограниченной минимизации). Если предикат $F(x_1, \ldots, x_n, y)$ и функция $\varphi(x_1, \ldots, x_n)$ примитивно рекурсивны, то таков же и функция $\underset{y \le \varphi(x_1, \ldots, x_n)}{\mu y} F(x_1, \ldots, x_n, y)$.

Доказательство. Если $g(x_1, \ldots, x_n, y)$ — характеристическая функция предиката $F$, то

$$\mu y_{y \le \varphi(x_1, \ldots, x_n)} F(x_1, \ldots, x_n, y) =$$

$$= \left[ \sum_{k=0}^{\varphi(x_1, \ldots, x_n)} \prod_{t=0}^{k} \overline{sg}\, g(x_1, \ldots, x_n, t) \right] \cdot sg \sum_{t=0}^{\varphi(x_1, \ldots, x_n)} g(x_1, \ldots, x_n, t).$$

(В самом деле, $\prod_{t=0}^{k} \overline{sg}\, g(x_1, \ldots, x_n, t)$ есть 1 для всех $k$, меньших наименьшего $y$, для которого $F(x_1, \ldots, x_n, y)$ истинно, и 0 для всех $k$, бо́льших или равных этому $y$; второй сомножитель равен единице, если $F(x_1, \ldots, x_n, y)$ истинно хотя бы для одного $y \le \varphi(x_1, \ldots, x_n)$, и нулю в противном случае.)

Примеры. 1) Функция $(x, y)$ — наибольший общий делитель чисел $x$ и $y$:

$$(x, y) = \mu z_{z \le \max(x, y)} D(x, y, z).$$

2) Функция $p_x$ — простое число, имеющее номер $x$ в последовательности простых чисел, расположенных в порядке возрастания (причем считается $2 = p_0$):

$$\begin{cases} p_0 = 2 \\ p_{x+1} = \mu y_{y \le p_x! + 1} (y > p_x \& p(y)). \end{cases}$$

(Таким образом, здесь во втором рекурсивном равенстве $h(x_1, x_2) = \mu y_{y \le x_2! + 1} (y > x_2 \& p(y))$. При выборе ограничивающей функции использовано евклидово доказательство существования сколь угодно больших простых чисел: каково бы ни было $N = 2, 3, \ldots$, среди чисел $N + 1$, $N + 2, \ldots, N! + 1$ должно быть хоть одно простое, поскольку $N! + 1$ делится на какое-то простое число, но ни на одно из чисел $2, \ldots, N$ делиться не может.)

3) Функция $\exp_x x$ — показатель, с которым простое число $p_x$ входит в каноническое разложение $x$ (например, $\exp_0 54 = 1$, $\exp_1 54 = 3$, $\exp_2 54 = 0$):

$$\exp_x x = \mu z_{z \le x} \neg d(x, p_x^{z+1})^{52}.$$

---

[52] Здесь использована примитивная рекурсивность функции $x^y$ задачи в конце пункта 1).

Часто бывает полезна также

Теорема 5 (о кусочном задании функции). Если $f_1(x_1, \ldots, x_n)$, $\ldots, f_k(x_1, \ldots, x_n)$ — примитивно рекурсивные функции и $F_1(x_1, \ldots, x_n)$, $\ldots, F_k(x_1, \ldots, x_n)$ — примитивно рекурсивные предикаты, такие, что предикат $F_1 \vee \cdots \vee F_k$ тождественно истинен и все предикаты $F_i \& F_j$, где $i \neq j$, тождественно ложны, то функция

$$f(x_1, \ldots, x_n) = \begin{cases} f_1(x_1, \ldots, x_n), & \text{если } F_1(x_1, \ldots, x_n) \equiv И \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(x_1, \ldots, x_n), & \text{если } F_k(x_1, \ldots, x_n), \equiv И \end{cases}$$

примитивно рекурсивна.

Доказательство. Очевидно,

$$f(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n) \cdot g_1(x_1, \ldots, x_n) + \ldots$$

$$+ f_k(x_1, \ldots, x_n) \cdot g_k(x_1, \ldots, x_n),$$

где $g_i$ — характеристическая функция предиката $F_i$.

4. В начале параграфа мы уже заметили, что все примитивно рекурсивные функции вычислимы в интуитивном смысле; запас этих функций, как видно из теорем и примеров предыдущего пункта, весьма широк. Но все же не каждая вычислимая функция примитивно рекурсивна. Сейчас мы построим пример функции, допускающей вычисление с помощью довольно очевидной, хотя и громоздкой процедуры и в то же время не примитивно рекурсивной. Для этого нам придется провести некоторую подготовительную работу.

Будем сопоставлять примитивно рекурсивным функциям натуральные числа, которые будем называть их *гёделевскими номерами* или просто *номерами*, следующим образом:

а) Число 2 будет номером функции $0(x)$.

б) Число 3 будет номером функции $S(x)$.

в) Функции $c_k^l$ будут нумероваться последовательными простыми числами $p_2, p_3, \ldots$ таким образом, что с возрастанием $k$ номера возрастают, а при одинаковых $k$ функция с бо́льшим $l$ имеет бо́льший номер. Например, $c_1^1$ имеет номер 5, $c_2^1$ — 7, $c_2^2$ — 11 и т. д.

г) Если одноместная функция $f$ получается с помощью оператора рекурсии из числа $c$ и двуместной функции $h$, имеющей номер $j$, то число $2^{c+1} \cdot 5^j$ будет номером функции $f$.

д) Если $n > 1$ и $n$-местная функция $f$ получается с помощью оператора рекурсии из $(n-1)$-местной функции $g$ и $(n+1)$-местной функции $h$, имеющих номера $i$ и $j$ соответственно, то число $3^i \cdot 5^j$ будет номером функции $f$.

c) Если $f(x_1, \ldots, x_k) = h(g_1(x_1, \ldots, x_k), \ldots, g_l(x_1, \ldots, x_k))$ и функции $h, g_1, \ldots, g_l$ имеют номера $i, j_1, \ldots, j_l$ соответственно, то число $p_1^i p_2^{j_1} \cdots p_{l+1}^{j_l}$ будет номером функции $f$.

Заметим, что поскольку, как легко сообразить, каждую п. р. ф. можно получить из исходных бесконечно многими способами[53], всякая п. р. ф. имеет бесконечно много номеров.

Задача. Найти хотя бы по одному номеру функций $0_2(x_1, x_2)$, $2(x)$, $x + 2$, $x + 3$, $sgx$, $x \dot{-} 1$, $x + y$.

Нетрудно указать эффективную процедуру, позволяющую по любому натуральному числу распознать, является ли оно номером какой-либо п. р. ф., и в случае положительного ответа указать способ ее вычисления. Эту процедуру мы будем называть *расшифровкой* натурального числа; производится она шаг за шагом: сначала расшифровывается нуль, потом единица, потом 2 и т. д. Расшифровка нуля состоит просто в констатации, что нуль не является номером никакой п. р. ф. Пусть $n > 0$ и все числа $0, \ldots, n - 1$ уже расшифрованы. Тогда расшифровка числа $n$ состоит в следующем. Прежде всего проверяем, является ли $n$ простым числом. Если да — находим исходную п. р. ф. с номером $n$ (это не представляет труда, и способ вычисления такой функции очевиден), и на этом расшифровка заканчивается. Если нет — проверяем, имеет ли $n$ вид $2^{c+1} \cdot 5^i$, и если имеет — является ли $j$ номером какой-либо двуместной п. р. ф. (Число $j$, поскольку оно меньше $n$, уже расшифровано, а т. к. при расшифровке номера функции указывается способ ее вычисления, то должна быть, разумеется, указана и ее вместимость.) Если $j$ есть номер двуместной п. р. ф. $h$, то $n$, очевидно, является номером одноместной п. р. ф., получающейся из $c$ и $h$ с помощью оператора рекурсии, и из способа вычисления $h$ получается способ вычисления $f$, так что расшифровка на этом заканчивается. Если $j$ не есть номер двуместной п. р. ф., мы констатируем, что $n$ не есть номер п .р. ф., и расшифровка заканчивается. Если же $n$ не имеет вида $2^{c+1} \cdot 5^i$, мы проверяем, имеет ли $n$ вид $3^i \cdot 5^j$, и если да — являются ли $i$ и $j$ номерами каких-либо п. р. ф. $g$ и $h$ вместимости $k - 1$ и $k + 1$ соответственно для некоторого $k = 2, 3, \ldots$ . В случае положительного ответа $n$ есть номер $k$-местной п. р. ф. $f$, получающейся из $g$ и $h$ с помощью оператора рекурсии, и из способов вычисления $g$ и $h$ получается способ вычисления $f$. В противном случае проверяем, имеет ли $n$ вид $p_3^l p_4^{i} \cdots p_{s+3}^{j_s}$ для каких-либо целых положительных $l, i, j_1, \ldots, j_s$ и если да — верно ли, что $i$

[53] Не составляют исключения и сами исходные функции: например, $0(x) = S(0(x)) \dot{-} 1 = (S(S(0(x))) \dot{-} 1) \dot{-} 1$ и т. д.

является номером некоторой $l$-местной п. р. ф. $h$, а $j_1$, ..., $j_l$ — номерами некоторых п. р. ф. $g_1$, ..., $g_l$ одной и той же вместимости $k$. В случае положительного ответа $n$ есть номер п. р. ф. $h(g_1(x_1, ..., x_k), ..., g_l(x_1, ..., x_k))$, способ вычисления которой очевидным образом получается из способов вычисления $h, g_1, ..., g_l$; в противном случае остается констатировать, что $n$ не является номером никакой п. р. ф.

Задача. Расшифровать числа: 23; 75; 100; 5929; $7^2 \cdot 11^{13}$; $2 \cdot 5^{7^2} \cdot 11^{11}$.

Обозначим теперь через $\psi(x, y)$ двуместную функцию, определяемую следующим образом: если $x$ есть номер некоторой одноместной п. р. ф. $\varphi$, то $\forall y(\psi(x, y) = \varphi(y))$; в противном случае $\forall y(\psi(x, y) = 0)$. Поскольку мы располагаем эффективной процедурой, позволяющей для любого числа $x$ узнать, является ли оно номером одноместной п. р. ф., и в случае положительного ответа указать способ вычисления этой п. р. ф., функция $\psi$ должна быть признана в интуитивном смысле вычислимой. (Разумеется, она вычислима и по Тьюрингу.) В то же время легко показать, что она не примитивно рекурсивна. В самом деле, в противном случае вместе с ней была бы примитивно рекурсивна также и одноместная функция $\psi(x, x) + 1$ (поскольку $\psi(x, x) = \psi(e_1^1(x), e_1^1(x))$. Поэтому она имела бы в нашей нумерации некоторый номер $x_0$. (У нее было бы даже бесконечно много номеров, но нам достаточно одного.) А тогда по определению функции $\psi$ оказалось бы $\psi(x_0, y) = \psi(y, y) + 1$ для любого $y$, и, в частности, $\psi(x_0, x_0) = \psi(x_0, x_0) + 1$. Полученное противоречие доказывает, что $\psi$ не есть п. р. ф.[54]

Итак, мы убедились, что не все вычислимые функции примитивно рекурсивны. Тем не менее примитивная рекурсивность — понятие очень естественное и полезное. Примитивно рекурсивных функций более чем достаточно для всех практических вычислительных задач, да и в теоретических математических исследованиях вне математической логики и смежных с ней областей вряд ли можно столкнуться с конкретной числовой функцией, которая не была бы примитивно рекурсивной.

В то же время класс примитивно рекурсивных функций можно естественным образом расширить так, чтобы полученный класс совпал с классом всех вычислимых функций. Этим мы займемся в следующем параграфе.

[54] Еще один пример вычислимой, но не примитивно рекурсивной функции см. в задаче 46 в конце главы.

## § 7.9. ЧАСТИЧНО РЕКУРСИВНЫЕ И ОБЩЕРЕКУРСИВНЫЕ ФУНКЦИИ

1. Чтобы получить все вычислимые функции тем же способом, которым в предыдущем параграфе были получены п. р. ф., достаточно добавить к операторам подстановки и рекурсии упоминавшийся выше (с. 335) оператор минимизации. Однако нам придется применять этот оператор и к таким предикатам, которые определены не для всех, а только для некоторых наборов натуральных чисел. (Функции, которыми мы сейчас займемся, тоже не всегда будут всюду определенными. Но все функции и предикаты, рассматриваемые в настоящем параграфе, определены на множествах, состоящих из упорядоченных наборов натуральных чисел, и значения функций — также натуральные числа; в дальнейшем это специально оговариваться не будет.)

В применении к всюду определенным предикатам оператор минимизации в том виде, как он упоминался выше, сохраняет вычислимость (хотя и не сохраняет свойство быть всюду определенным). В самом деле, если $F(x_1, \ldots, x_n, y)$ — всюду определенный вычислимый предикат, то для всякого набора $x_1^0, \ldots, x_n^0$ значений $x_1, \ldots, x_n$ мы можем, последовательно вычисляя $F(x_1^0, \ldots, x_n^0, 0)$, $F(x_1^0, \ldots, x_n^0, 1)$ и т. д., найти наименьшее число $y^0$, для которого $F(x_1^0, \ldots, x_n^0, y^0) \equiv И$, если только оно существует (в противном случае этот процесс будет продолжаться вечно). Но для не всюду определенных предикатов такой способ не годится: если, например, $F(x_1^0, \ldots, x_n^0, 0)$ не определено, а $F(x_1^0, \ldots, x_n^0, 1) \equiv И$, то, пытаясь вычислить $F(x_1^0, \ldots, x_n^0, 0)$ (например, с помощью машины Тьюринга), мы, быть может, будем вынуждены работать вечно и так никогда и не узнаем, что это значение не существует, а следующее есть как раз то, которое нам нужно. Поэтому для общего случая *оператор минимизации* определяется так: он применяется к предикату $F$ вместимости $k+1$ ($k = 1, 2, \ldots$), и результат его применения есть функция $f$ вместимости $k$, такая, что для всякого упорядоченного набора $x_1^0, \ldots, x_k^0$, для которого существуют такие числа $y$, что $F(x_1^0, \ldots, x_k^0, y) \equiv И$ и при этом, если $y > 0$, для всех $t = 0, \ldots, y-1$ значения $F(x_1^0, \ldots, x_k^0, t)$ определены, значение $f(x_1^0, \ldots, x_k^0)$ равно наименьшему из таких $y$; если же таких $y$ не существует, то значение $f(x_1^0, \ldots, x_k^0)$ не определено.

Результат применения к предикату $F$ оператора минимизации принято обозначать $\mu y F(x_1, \ldots, x_k, y)$.

Мы будем теперь называть функцию *частично рекурсивной*[55] (сокращенно *ч. р. ф.*), если она либо принадлежит к числу исходных п. р. ф., либо может быть получена из них с помощью операторов подстановки, рекурсии и минимизации.

Всюду определенная частично рекурсивная функция называется *общерекурсивной*[56] (сокращенно *о. р. ф.*).

Исторический комментарий. Идея использования рекурсии для решения задач, связанных с основаниями математики, восходит к Т. Сколему и Д. Гильберту. Точное понятие примитивно рекурсивной функции было введено К. Гёделем [Gödel 1931]; он называл эти функции просто рекурсивными (*rekursive Funktionen*). Термин «примитивная рекурсия» (*primitive Rekursion*) предложила в 1934 г. Р. Петер[57] для обозначения рекурсии простейшего вида (описанной в начале предыдущего параграфа) в отличие от более сложных рекурсий, сводящихся к примитивной (как возвратная и одновременная рекурсии, описанные в задачах 39 и 41 в конце этой главы) или не сводящихся (как «рекурсия со вставками», используемая при определении функции Аккермана — см. задачу 46). Общерекурсивные и частично рекурсивные функции были введены Ж. Эрбраном[58] и К. Гёделем; наиболее распространенную сейчас форму их определения — с помощью оператора минимизации,— использованную и в нашей книге, предложил С. К. Клини[59]. Он же ввел термины *primitive recursive function*, *general recursive function*, *partial recursive function*. Более подробный исторический обзор см. в его статье [Клини 1982].

2. Главной задачей оставшейся части этого параграфа будет доказать, что понятие частично рекурсивной функции совпадает по объему с понятием функции, вычислимой по Тьюрингу. Точнее, мы докажем следующие две теоремы.

Теорема 1. Если $V$ — конечный алфавит мощности $> 1$ и $\nu$ — стандартная нумерация слов в этом алфавите, то для всякой ч. р. ф. $f(x_1, \ldots, x_n)$ можно построить машину Тьюринга с входным и выход-

---

[55] Этот закрепленный уже традицией термин — неправильный перевод английского *partial recursive function* (ср. сноску 49). Правильно должно бы было быть «частичная рекурсивная функция» («частичной функцией», по-английски *partial function*, иногда называют функцию, определенную на подмножестве натурального ряда).

[56] Перевод английского *general recursive function*. Правильнее было бы «общая рекурсивная функция» (ср. предыдущую сноску).

[57] Р. Петер (Péter Rózsa, 1905—1977) — венгерский математик. Ее работы имели большое значение для выяснения объема понятия примитивно рекурсивной функции.

[58] Ж. Эрбран (Jacques Herbrand) — французский математик, проживший всего 23 года (род. в 1908 г., погиб в горах в 1931 г.), но успевший внести значительный вклад в развитие математической логики.

[59] С.К. Клини (Stephen Cole Kleene, 1909—1994) — американский математик, один из создателей теории алгоритмов.

ным алфавитами, совпадающими с $V$, которая будет вычислять функцию $\nu^{-1}f(\nu v_1, \ldots, \nu v_n)$.

**Теорема 2.** Если $V$ — конечный алфавит мощности $> 1$, $\nu$ — стандартная нумерация слов в этом алфавите и $f(v_1, \ldots, v_n)$ — функция, вычисляемая некоторой машиной Тьюринга с входным и выходным алфавитами, совпадающими с $V$, то функция $\nu f(\nu^{-1}x_1, \ldots, \nu^{-1}x_n)$ частично рекурсивна.

При доказательстве этих теорем мы не будем, как правило, различать число и представляющее его слово (как не различали их в § 7.7); будем говорить, например: «машина вычисляет функцию $x + y$» (а не «функцию, сопоставляющую словам $\nu^{-1}x$ и $\nu^{-1}y$ слово $\nu^{-1}(x + y)$»), «число $x$ содержит вхождения символа $a_i$» и т. п.

Начнем с доказательства теоремы 1, идея которого очевидна: достаточно построить машины для вычисления исходных п. р. ф. и для каждого из трех операторов указать способ, позволяющий по машинам, вычисляющим функции, к которым этот оператор применяется, построить машину для вычисления функции, получающейся в результате его применения. Построение машин, вычисляющих исходные п. р. ф., равно как и построение машины, вычисляющей функцию $h(g_1(x_1, \ldots, x_k), \ldots, g_l(x_1, \ldots, x_k))$, по машинам, вычисляющим функции $h, g_1, \ldots, g_l$ — это простые упражнения, которые читатель легко выполнит сам. Если даны машины для вычисления функций $g(x_1, \ldots, x_{n-1})$ и $h(x_1, \ldots, x_{n+1})$, то машина, вычисляющая функцию, получаемую из $g$ и $h$ рекурсией, может работать следующим образом. Когда в начальной ситуации на ее ленте записано слово $x_1a_0 \cdots a_0x_n$, она записывает справа от него слово $\square x_n\square$, затем справа от второго квадратика вычисляет $g(x_1, \ldots, x_{n-1})$, и если между двумя квадратиками записан нуль, создает заключительную ситуацию с записанным на ленте словом (числом) $g(x_1, \ldots, x_{n-1})$; в противном случае она уменьшает число между двумя квадратиками на единицу и справа от второго квадратика вычисляет $h(x_1, \ldots, x_n, g(x_1, \ldots, x_{n-1}))$; после чего, если между двумя квадратиками оказался нуль, создает заключительную ситуацию с записанным на ленте числом $h(x_1, \ldots, x_n, g(x_1, \ldots, x_{n-1}))$, а в противном случае уменьшает число между квадратиками еще на единицу и справа от второго квадратика вычисляет $h(x_1, \ldots, x_n, h(x_1, \ldots, x_n, (g(x_1, \ldots, x_{n-1}))))$, и т. д. Аналогично для случая, когда оператор рекурсии применяется к константе и двуместной функции. Наконец, если дана машина, вычисляющая характеристическую функцию $f(x_1, \ldots, x_n, y)$ предиката $F(x_1, \ldots, x_n, y)$, то функция $\mu y F(x_1, \ldots, x_n, y)$ будет вычисляться машиной, которая, когда в начальной ситуации на ее ленте записано слово $x_1a_0 \cdots a_0x_n$, справа

от него вычисляет последовательно $f(x_1, \ldots, x_n, 0)$, $f(x_1, \ldots, x_n, 1)$ и т. д., пока для какого-то $y$ не окажется $f(x_1, \ldots, x_n, y) = 1$: тогда создается заключительная ситуация с записанным на ленте числом $y$.

3. Сложнее и интереснее доказывается теорема 2. Для ее доказательства мы воспользуемся методом арифметизации конструктивных процессов, который был уже использован выше, при построении примера в конце предыдущего параграфа. Арифметизация состоит в том, что конструктивные процедуры некоторого строго определенного класса нумеруются натуральными числами так, что всякую процедуру можно однозначно «расшифровать» по ее номеру. Свойства процедур превращаются тогда в свойства чисел, преобразования процедур — в числовые функции. Этот метод — изобретенный К. Гёделем и впервые примененный им в доказательстве знаменитой теоремы о неполноте арифметики (см. ниже, § 8.3) — настолько поразителен как по простоте и изяществу идеи, так и по силе получаемых с его помощью результатов, что напрашивается сравнение с другой арифметизацией, по праву причисляемой к величайшим достижениям математики — декартовой арифметизацией геометрии.

Для доказательства частичной рекурсивности вычислимых функций метод арифметизации применил С.К. Клини.

Одновременно с теоремой 2 будет доказана

Теорема 3 (теорема Клини о нормальной форме). Существуют такие примитивно рекурсивные предикаты $T_1$, $T_2$,... вместимости 3, 4, ... соответственно и такая одноместная п. р. ф. $F$, что для всякого $n = 1, 2, \ldots$ любая $n$-местная ч. р. ф. $f$ может быть представлена в виде

$$f(x_1, \ldots, x_n) = F(\mu z T_n(i_0, z, x_1, \ldots, x_n))$$

при некотором подходящем $i_0$.

Из этой теоремы следует, между прочим, что при получении произвольной частично рекурсивной функции из исходных всегда можно обойтись одним применением оператора минимизации.

Другое очевидное следствие из теоремы 3 — существование при любом $n = 1, 2, \ldots$ $(n + 1)$-местной ч. р. ф., универсальной для $n$-местных ч. р. ф., т. е. такой ч. р. ф. $\Theta(y_0, x_1, \ldots, x_n)$, что для всякой $n$-местной ч. р. ф. $\varphi$ при подходящем $y_0$ справедливо тождество $\varphi(x_1, \ldots, x_n) = \Theta(y_0, x_1, \ldots, x_n)$. Действительно, этим свойством обладает функция

$$F(\mu z T_n(y, z, x_1, \ldots, x_n)).$$

Замечания. 1) Построенная в конце предыдущего параграфа двуместная вычислимая функция $\psi$ является универсальной для одноместных п. р. ф. При доказательстве того, что сама $\psi$ не есть п. р. ф.,

мы пользовались только ее универсальностью; таким образом, фактически мы доказали, что никакая функция, универсальная для одноместных п. р. ф., не может сама быть примитивно рекурсивной. Легко обобщить это доказательство на случай функций любой вместимости. Точно так же функция, универсальная для $n$-местных о. р. ф., не может быть общерекурсивной — это можно доказать тем же самым рассуждением.

2) Еще одно очевидное следствие теоремы 3 — несохранение примитивной рекурсивности оператором минимизации.

При доказательстве теорем 2 и 3 мы будем пользоваться описанным в § 7.5 кодированием слов и машин Тьюринга, а также введенной в § 7.7 стандартной нумерацией слов в фиксированном конечном алфавите, причем этот алфавит будет теперь не произвольным, а конкретным — именно, это будет тот самый алфавит $\{a_1, \ldots, a_0\}$, который мы использовали в том же параграфе при определении номера машины Тьюринга. Номер машины $M$ мы будем теперь обозначать $\nu M$.

Наряду с машинами Тьюринга мы будем нумеровать также их правильные вычисления, которые мы будем в дальнейшем называть для краткости просто *вычислениями*. Именно, пусть $S = (s_0, s_1, \ldots, s_p)$ — вычисление некоторой машины Тьюринга. Тогда стандартный номер слова $\square\varkappa(s_0)\square\varkappa(s_1)\square\cdots\square\varkappa(s_p)\square$ (здесь, как всегда, $\varkappa(x)$ — код слова $x$) будет называться *номером вычисления* $S$ и обозначаться $\nu S$.

Очевидно, по номеру машины или вычисления можно однозначно восстановить программу этой машины, соответственно вычисление.

Будем в дальнейшем обозначать алфавит $\{a_1, \ldots, a_0\}$ через $W$. Вычисление машины Тьюринга, в начальной и заключительной ситуациях которого на ленте записаны слова в алфавите $W$, назовем $W$-вычислением.

Пусть теперь $T_n(t, z, x_1, \ldots, x_n)$ — предикат, заданный на $\mathbf{N}^{n+2}$ и означающий «$t$ есть номер некоторой машины Тьюринга и $z$ — номер некоторого $W$-вычисления этой машины с $n$-местной начальной ситуацией, в которой на ленте записаны числа[60] $x_1, \ldots, x_n$».

Введем в рассмотрение также следующую одноместную функцию $F$ с областью определения $\mathbf{N}$: если $x$ есть номер $W$-вычисления машины Тьюринга, то $F(x)$ — то число, которое записано на ленте в заключительной ситуации этого вычисления; в противном случае $F(x) = 0$.

[60] Напомним, что числа мы отождествляем с представляющими их словами в алфавите $W$.

*Основная лемма.* Предикаты $T_1$, $T_2$,... и функция $F$ примитивно рекурсивны.

Из основной леммы легко выводятся теоремы 2 и 3. В самом деле: пусть сначала $f(w_1, ..., w_n)$ — функция, вычисляемая машиной Тьюринга $M$ с входным и выходным алфавитом $W$, и пусть $x_1^0, ..., x_n^0$ — произвольный упорядоченный набор $n$ натуральных чисел. Тогда, если для этого набора функция $f$ определена и $f(x_1^0, ..., x_n^0) = y^0$, то существует $W$-вычисление машины $M$ с $n$-местной начальной ситуацией, в которой на ленте записаны числа $x_1^0, ..., x_n^0$ (или, если выражаться более педантично — слова $\nu^{-1}x_1^0, ..., \nu^{-1}x_n^0$) и в заключительной ситуации этого вычисления на ленте записано число $y^0$ (т. е. слово $\nu^{-1}y^0$). Если $z^0$ — номер этого вычисления и $i^0$ — номер машины $M$, то предложение $T_n(i^0, z^0, x_1^0, ..., x_n^0)$ истинно и $z^0 = \mu z T_n(i^0, z, x_1^0, ..., x_n^0)$ (в самом деле, существует только одно вычисление машины $M$ с $n$-местной начальной ситуацией, в которой на ленте записаны числа $x_1^0, ..., x_n^0$, и это вычисление — как и всякое — имеет только один номер; поэтому для каждого $z < z^0$ предложение $T_n(i_0, z, x_1^0, ..., x_n^0)$ ложно). В то же время ясно, что $y^0 = F(z^0)$. Если же $f$ не определена для $x_1^0, ..., x_n^0$, то предложение $T_n(i^0, z, x_1^0, ..., x_n^0)$ ложно при любом $z$, и поэтому выражение $\mu z T_n(i^0, z, x_1^0, ..., x_n^0)$, а вместе с ним и $F(\mu z T_n(i^0, z, x_1^0, ..., x_n^0))$, не определено. Итак, функция $f(x_1, ..., x_n)$ представима в виде $F(\mu z T_n(i^0, z, x_1, ..., x_n))$, и если мы докажем, что $T_n$ и $F$ примитивно рекурсивны, то $f$ окажется частично рекурсивной. Тем самым будет доказана теорема 2 для частного случая, когда $V = W$ и стандартная нумерация отвечает выбранному нами пересчету алфавита, а заодно и теорема 3, т. к. по теореме 1 всякая ч. р. ф. вычисляется некоторой машиной Тьюринга с входным и выходным алфавитами, совпадающими с $W$. Для общего случая теорема 2 будет теперь следовать из того, что для любого конечного алфавита $V$ и любой стандартной нумерации $\nu_1$ слов в этом алфавите по всякой машине Тьюринга с входным и выходным алфавитом $V$, вычисляющей функцию $f(v_1, ..., v_n)$, т. е. вычисляющей некоторую числовую функцию в системе счисления с множеством цифр $V$, можно построить машину, вычисляющую ту же числовую функцию в системе счисления с множеством цифр $W$, т. е. машину с входным и выходным алфавитом $W$, которая будет вычислять функцию $g(w_1, ..., w_n) = \nu^{-1}\nu_1 f(\nu_1^{-1}\nu w_1, ..., \nu_1^{-1}\nu w_n)$, где $\nu$ — стандартная нумерация слов в алфавите $W$, отвечающая выбранному нами пересчету этого алфавита, так что числовая функция $\nu g(\nu^{-1}x_1, ..., \nu^{-1}x_n)$ будет совпадать с функцией $\nu_1 f(\nu_1^{-1}x_1, ..., \nu_1^{-1}x_n)$. (Эта машина может, на-

пример, сначала переводить исходные данные из «новой» системы счисления в «старую», а затем работать как старая машина и переводить результат из «старой» системы в «новую». Построение машины для перехода от одной системы счисления к другой — хорошее упражнение, не представляющее, впрочем, принципиальных трудностей.)

4. Теперь нам остается доказать основную лемму, к чему мы и переходим. Для этого мы последовательно докажем примитивную рекурсивность ряда функций и предикатов, связанных с девятеричным представлением натуральных чисел (без нуля) и с машинами Тьюринга. При этом мы будем пользоваться теоремами пункта 3 предыдущего параграфа. В качестве обозначений для этих функций и предикатов будут использоваться русские буквы и их сочетания, представляющие собой понятные сокращения (обозначения функций будут состоять из строчных букв, обозначения предикатов — из прописных). Выражения «число» и «слово» (подразумевается слово в алфавите $\{a_1, \ldots, a_0\}$) будут употребляться как синонимы. «Цифры» $a_1, \ldots, a_0$ будут обозначаться просто $1, \ldots, 9$.

1) пц$(x)$ — последняя цифра числа $x$ (пц$(0) = 0$):

$$\text{пц}(x) = r(9, x) + 9\overline{sg}\, r(9, x) \cdot sgx.$$

2) бпц$(x)$ = число $x$ без последней цифры (бпц$(0) = 0$):

$$\text{бпц}(x) = q(9, x \dot{-} \text{пц}(x)).$$

3) бхв$(x, n)$ — число $x$ без «хвоста» длины $n$, т. е. без $n$ последних цифр (если $n$ больше длины записи $x$, то бхв $(x, n) = 0$):

$$\begin{cases} \text{бхв}(x, 0) = x \\ \text{бхв}(x, n+1) = (\text{бпц}(\text{бхв}(x, n)). \end{cases}$$

4) хв$(x, n)$ — «хвост» числа $x$ длины $n$ (если $n$ больше длины записи $x$, то хв$(x, n) = x$):

$$\text{хв}(x, n) = x \dot{-} \text{бхв}(x, n) \cdot 9^n.$$

5) НАЧ$(x, y)$ — «слово $y$ есть начало слова $x$»):

$$\text{НАЧ}(x, n) \equiv \exists_{n \le x} [y = \text{бхв}(x, n)].$$

6) КОН$(x, y)$ — «слово $y$ есть конец слова $x$»):

$$\text{КОН}(x, n) \equiv \exists_{n \le x} [y = \text{хв}(x, n)].$$

7) ВХОД$(x, y)$ — «слово $y$ входит в слово $x$»:

$$\text{ВХОД}(x, y) \equiv \exists_{z \le x} [\text{КОН}(x, z) \,\&\, \text{НАЧ}(z, y)].$$

8) произв$(x, y)$ — произведение $x$ на $y$ в смысле умножения слов,

т. е. слово, полученное из слова $x$ приписыванием к нему слова $y$ (справа):

$$\text{произв}(x, y) = \mu z_{z \le 9^{x+y+1}} \exists n_{n \le z} [x = \text{бхв}(z, n) \,\&\, y = \text{хв}(z, n)].$$

(Оценка для $z$ основана на том, что самое большое $n$-значное число в девятеричной системе без нуля есть $\underbrace{9\ldots9}_{n \text{ раз}} = \sum_{k=1}^{n} 9^k$; поэтому

$$\text{произв}(x, y) \le \sum_{k=1}^{|x|+|y|} 9^k < 9^{|x|+|y|+1} \le 9^{x+y+1}$$ [61].)

9) $\text{произв}_n(x_1, \ldots, x_n)$ — произведение слов $x_1, \ldots, x_n$ в смысле умножения слов ($n = 2, 3, \ldots$):

$$\text{произв}_2(x_1, x_2) = \text{произв}(x_1, x_2);$$

$$\text{произв}_{n+1}(x_1, \ldots, x_{n+1}) = \text{произв}(\text{произв}_n(x_1, \ldots, x_n), x_{n+1}).$$

10) Если функция $f(x_1, \ldots, x_n)$ примитивно рекурсивна, то такова же и фуикция

$$\prod_{i=0}^{x_n} f(x_1, \ldots, x_{n-1}, i) = \text{произв}_{x_n+1}(f(x_1, \ldots, x_{n-1}, x_n), \ldots, f(x_1, \ldots, x_{n-1}, 1),$$

$$f(x_1, \ldots, x_{n-1}, 0)).$$

Доказывается аналогично теореме 1 из § 7.8 (с той только разницей, что умножение производится справа налево).

11) $\text{ц}(x, n)$ — $n$-я справа цифра числа $x$ (если $n = 0$ или $n > |x|$, то $\text{ц}(x, n) = 0$):

$$\text{ц}(x, n) = \text{пц}(\text{бхв}(x, n \dot{-} 1)) \cdot \text{sg}\, n.$$

12) $\text{НОМ}_c(x)$ — «$x$ есть номер заданного символа $c$, принадлежащего одному из алфавитов $\mathfrak{A}$, $\Omega$, {Л, Н, П, →, *, □}» (см. начало § 7.5).

Этот предикат примитивно рекурсивен, как всякий предикат вида $x = a$, где $a$ — константа (см. пример 1 в пункте 2 §7.8).

13) $\text{НОМ}_{\mathfrak{A}}(x)$ — «$x$ есть номер некоторого символа из алфавита $\mathfrak{A}$»:

$$\text{НОМ}_{\mathfrak{A}}(x) \equiv \exists z_{z \le x} [x = \text{произв}_3(2, z, 2) \,\&\, (z \ne 0) \,\&$$

$$\&\, \forall t_{t \le z} (\text{ВХОД}(z, t) \,\&\, 1 \le t \le 9 \supset t = 1)].$$

---

[61] Напомним, что через $|x|$ обозначается длина слова $x$.

(Третий член конъюнкции означает, что $t$ состоит только из единиц.)

14) $\text{НОМ}_{\mathfrak{L}}(x)$ — «$x$ есть номер некоторого символа из алфавита $\mathfrak{L}$».

Аналогично предыдущему.

15) ном-однозн$(x)$ — функция, значение которой есть номер числа (слова) $x$, если $x$ однозначно (т. е. $x = 1, \ldots, 9$) и нуль в противном случае.

Примитивная рекурсивность этой функции следует из теоремы о кусочном задании (§ 7.8, теорема 5).

16) ном$(x)$ — номер числа $x$:

$$\text{ном}(x) = \sum_{n=0}^{x} \text{ном-однозн}\,(\text{ц}(x, n)).$$

17) КОМ$(x)$ — «$x$ есть номер команды (машины Тьюринга)».

Примитивная рекурсивность этого предиката следует из того, что номер (т. е. код) команды есть произведение шести слов, первое из которых является номером некоторого символа из $\mathfrak{L}$, отличного от $a_0$, второе — номером некоторого символа из $\mathfrak{A}$ и т. д. Представляющую формулу читатель выпишет сам[62].

Для следующих шести предикатов мы также ограничимся указанием идеи доказательства примитивной рекурсивности, предоставляя читателю выписать соответствующие формулы:

18) МАШ$(x)$ — «$x$ есть номер некоторой машины Тьюринга».

Доказательство основывается на том, что слово $x$ является номером машины Тьюринга, т. е. имеет вид $8v_18 \ldots 8v_r8$, где $v_1, \ldots, v_r$ — коды команд с попарно различными левыми частями, расположенные в лексикографическом порядке, тогда и только тогда, когда выполняются следующие пять условий: ($\alpha$) $x$ начинается и кончается цифрой 8; ($\beta$) $x$ не содержит двух восьмерок подряд; ($\gamma$) каждое слово $z$, не содержащее восьмерок и такое, что слово $8z8$ входит в $x$, является номером команды; ($\delta$) если слово $8y_17w8y_17$ входит в $x$ и слова $y_1$, $y_2$ не содержат восьмерок, то $y_1 \neq y_2$ (условие детерминированности); ($\varepsilon$) если слово $8z_18z_28$ входит в $z$ и слова $z_1$, $z_2$ не содержат восьмерок, то существуют такие слова $u$, $t_1$, $t_2$, $v_1$, $v_2$, что $z_1 = ut_1v_1$, $z_2 = ut_2v_2$ и $1 \leq t_1 < t_2 \leq 9$ (лексикографическая упорядоченность кодов команд). Формулы (с ограниченными кванторами), отвечающие условиям ($\alpha$) — ($\varepsilon$), строятся очевидным образом.

19) СИТ$(x)$ «$x$ есть номер ситуации машины Тьюринга».

---

[62] При этом нужно не забыть об ограничениях, содержащихся в пунктах (б) и (г) определения программы машины (§ 7.2).

Представляющую формулу легко записать, воспользовавшись определением ситуации (§ 7.2) и заметив, что слово $z$ тогда и только тогда является номером некоторого слова в алфавите $\mathfrak{A}$, когда оно удовлетворяет следующим условиям: ($\varkappa$) если слово $t$ не содержит двоек и слово $2t2$ входит в $z$, то $t$ состоит только из единиц; ($\beta$) $z$ либо пусто, либо начинается словом 21 и кончается словом 12; ($\gamma$) $z$ не содержит вхождений слов 121 и 222; ($\delta$) $z$ не содержит вхождений цифр 3, ..., 9.

20. 21) НАЧСИТ($x$), ЗАКСИТ($x$) — «$x$ есть номер начальной (заключительной) ситуации машины Тьюринга».

Соответствующие формулы получаются из формулы для СИТ добавлением конъюнктивного члена, означающего, что $x$ начинается словом $3113 = \varkappa(q_1)$ в случае НАЧСИТ и $3113 = \varkappa(q_0)$ в случае ЗАКСИТ, и во втором случае еще одного конъюнктивного члена, означающего, что $x$ есть номер слова вида $ya_0^m$ ($m = 0, 1, \ldots$), где $y$ не содержит $a_0$. (Свойство быть номером слова вида $a_0^m$ можно представить аналогично свойству быть номером слова в алфавите $\mathfrak{A}$, заменив условие ($\varkappa$) условием ($\varkappa'$) если слово $t$ не содержит двоек и $2t2$ входит в $z$, то $t = 11$.)

22) ВЫП($x$, $y$, $z$) — «$x$ и $y$ — номера ситуаций, $z$ — номер команды, и ситуация с номером $y$ получается из ситуации с номером $x$ выполнением команды с номером $z$».

Представляющая формула будет иметь вид

$$\text{СИТ}(x)\ \&\ \text{СИТ}(y)\ \&\ \text{КОМ}(z)\ \&\ \mathfrak{B},$$

где $\mathfrak{B}$ — дизъюнкция четырех формул, отвечающих условиям ($\alpha$), ($\beta$), ($\gamma 1$), ($\gamma 2$) из определения выполнения команды (§ 7.2.). Например, условию ($\varkappa$) отвечает формула

$$\exists t_1\ \exists t_2\ \exists t_3\ \exists t_4\ \exists v_1\ \exists v_2\ \underset{t_1 \le z}{\ } \underset{t_2 \le z}{\ } \underset{t_3 \le z}{\ } \underset{t_4 \le z}{\ } \underset{v_1 \le z}{\ } \underset{v_2 \le z}{\ } [z = \text{произв}_6(t_1, t_2, 7, t_3, 5, t_4)\ \&$$

$$\&\ \text{НОМ}_{\text{с}}(t_1)\ \&\ \text{НОМ}_{\text{а}}(t_2)\ \&\ \text{НОМ}_{\text{а}}(t_3)\ \&\ \text{НОМ}_{\text{с}}(t_4)\ \&$$

$$\&\ x = \text{ПРОИЗВ}_4(v_1, t_1, t_2, v_2)\ \&\ y = \text{ПРОИЗВ}_4(v_1, t_4, t_3, v_2)].$$

23) ВЫЧ ($x$, $y$) — «$x$ есть номер некоторого $W$-вычисления машины с номером $y$».

Представляющая формула будет конъюнкцией пяти членов, первый из которых есть МАШ($y$), второй означает, что $x$ имеет вид $9t_1 9 \ldots 9t_r 9$, где $t_1$, ..., $t_r$ — номера ситуаций, третий — что ситуация с номером $t_1$ начальная, а с номером $t_r$ — заключительная, четвертый — что для каждого слова $9t_i 9t_{i+1} 9$ ситуация с номером $t_{i+1}$ получается из ситуации с номером $t_i$ выполнением некоторой команды, номер которой входит в $y$, пятый — что в ситуациях с номерами $t_i$ и $t_r$

записаны слова в алфавите $W$. Второй член этой конъюнкции легко построить по аналогии с формулой для предиката МАШ, остальные члены строятся с использованием предикатов НАЧСИТ, ЗАКСИТ, ВЫП и функции ном-однозн очевидным образом.

Теперь уже легко записать представляющую формулу для предиката $T_n$:

$$T_n(i, z, x_1, \ldots, x_n) \equiv \text{ВЫЧ}(z, t) \,\&\, \exists t \underset{t \le z}{|} \text{НАЧ}(z, t) \,\&$$

$$\&\, \exists u_1 \underset{u_1 \le t}{\cdots} \exists u_n \underset{u_n \le t}{(u_1} = \text{ном}(x_1) \,\&\, \cdots \,\&\, u_n = \text{ном}(x_n) \,\&\, t =$$

$$= \text{произв}_{2n+1}(931113212, u_1, 2112, u_2, 2112, \ldots, 2112, u_n, 9)\,|.$$

Остается доказать примитивную рекурсивность функции $F$. Для этого рассмотрим вспомогательные предикаты $T'(i, z, y)$ — «$i$ есть номер некоторой машины Тьюринга и $z$ — номер некоторого $W$-вычисления этой машины, в заключительной ситуации которого на ленте записано число $y$», и $T''(z, y) \equiv \exists i T'(i, z, y)$. Предикат $T'$ примитивно рекурсивен, поскольку для него можно записать представляющую формулу, совершенно аналогичную записанной только что для $T_n$. Но вместе с $T'$ примитивно рекурсивен и $T''$. В самом деле, всякое вычисление машины Тьюринга $M$ будет также и вычислением машины $M'$, программа которой получается из программы $M$ изъятием всех команд, не участвующих в данном вычислении. Если это вычисление есть $(s_0, \cdots s_r)$ и $q_i a_j \to a_k C q_l$ — одна из команд машины $M'$, то в вычислении найдутся такие две соседние ситуации $s_m$ и $s_{m+1}$, что $s_m$ содержит $q_i$ и $a_j$, а $s_{m+1}$ — $q_l$ и $a_k$. Поэтому суммарная длина номеров символов из $\mathfrak{A}$ и $\mathfrak{Q}$, входящих в код машины $M'$, не превосходит удвоенной длины номера вычисления. Номера остальных символов, входящих в код $M'$, однозначны; общее число их не превосходит увеличенного на единицу утроенного числа команд $M'$ и поэтому меньше длины номера вычисления[63]. Следовательно, если $i$ — номер машины $M'$ и $z$ — номер вычисления, то длина $i$ меньше утроенной длины $z$, и поэтому $i < \sum_{k=1}^{3\cdot|z|} 9^k < 9^{3\cdot|z|+1} < 9^{3z+1}$. Таким образом, в формуле $\exists i T'(i, z, y)$ можно ограничить квантор примитивно рекурсивной функцией $9^{3z+1}$. Но из примитивной рекурсивности $T''$ немедленно следует, что и $F$ примитивно рекурсивна, т. к. $F(z) = \mu y \underset{y \le z}{} T''(z, y)$.

Тем самым доказательство основной леммы и вместе с ней теорем 2 и 3 завершено.

---

[63] Число команд $M'$ не больше числа ситуаций вычисления, а длина номера ситуации не меньше семи.

5. Из доказательства основной леммы нетрудно вывести еще одну теорему — усиление теоремы 8 из § 7.7;

**Теорема 4.** Всякое непустое перечислимое множество является множеством значений некоторой п.р.ф.

Доказательство. Пусть $i_0$ — номер машины Тьюринга $M$, вычисляющей (одноместную) функцию с множеством значений $E$, и $x_0$ — некоторый элемент $E$. Обозначим через $S(z)$ предикат $\underset{x\le z}{\exists} xT_1(i_0, z, x)$ и положим

$$\varphi(z) = \begin{cases} \underset{y\le z}{\mu y} T'(i_0, z, y), & \text{если } S(z) \equiv И \\ x_0, & \text{если } S(z) \equiv Л. \end{cases}$$

Очевидно, множество значений $\varphi$ есть $E$, и по теореме о кусочном задании функции $\varphi$ примитивно рекурсивна.

Замечание. Усилить аналогичным образом теорему 9 из § 7.7 нельзя (см. задачу 46д в конце главы).

Кроме того, легко получается

**Теорема 5.** Множество $E$ тогда и только тогда перечислимо, когда существует такой двуместный примитивно рекурсивный предикат $P$, что $E = \{x \mid \exists y P(x, y)\}$. (Этот факт иногда выражают так: «Множество перечислимо тогда и только тогда, когда оно является проекцией некоторого примитивно рекурсивного множества».)

Доказательство. а) Пусть $i_0$ — номер машины Тьюринга, вычисляющей (одноместную) функцию с множеством значений $E$. Тогда

$$E = \left\{y \mid \exists z \left[ \underset{x\le z}{\exists} xT_1(i_0, z, x) \;\&\; T'(i_0, z, y)\right]\right\}.$$

б) Для произвольного двуместного предиката $P$ множество $\{x \mid \exists y P(x, y)\}$ является множеством значений функции

$$f(z) = \begin{cases} \exp_0 z, & \text{если } \varphi_P(\exp_0 z, \exp_1 z) = 1 \\ \text{не определена, если } \varphi_P(\exp_0 z, \exp_1 z) = 0, \end{cases}$$

где $\varphi_P$ — характеристическая функция предиката $P$. Если $P$ примитивно рекурсивен, то $f$ вычислима.

Замечания. 1) Пункт б) доказательства теоремы 5 остается справедливым для любого вычислимого предиката. Таким образом, проекция разрешимого множества всегда есть перечислимое множество.

2) Взяв в теореме 5 в качестве $E$ неразрешимое перечислимое множество, мы видим, что операция связывания квантором существования не сохраняет ни вычислимость, ни примитивную рекурсивность предиката (ср. с теоремой 1 из § 7.7 и теоремой 2 из § 7.8). То же верно и для квантора общности, поскольку дополнение к любому

перечислимому множеству, в частности неразрешимому, можно теперь представить в виде $\{x \mid \forall y P(x, y)\}$ с примитивно рекурсивным $P$.

6. В этой главе мы изложили только основные понятия и факты теории алгоритмов. Более полное изложение можно найти в книгах [Роджерс 1972], [Мальцев 1965], [Марков — Нагорный 1984].

7. Наряду с алгоритмами в математике и за ее пределами широко используются родственные им *исчисления*, или *дедуктивные системы*. Исчисление «работает» так же, как алгоритм, с тем единственным отличием, что оно не обязано удовлетворять условию детерминированности: на каждом шаге возможно, вообще говоря, несколько вариантов продолжения работы. (Строго говоря, алгоритм есть частный случай исчисления — «детерминированное исчисление».) Так, если в определении программы машины Тьюринга (§ 7.2) отказаться от условия (д), то полученный объект (*недетерминированная машина Тьюринга*) будет реализовать уже не алгоритм, а исчисление. Если такая машина применима к какому-либо слову в том смысле, в котором мы определили применимость в § 7.2, то она перерабатывает его (вообще говоря) не в одно слово, а в некоторое множество слов. (Такую «недетерминированную переработку» называют обычно не «вычислением», а «порождением» или «выводом».) Другой пример — логические исчисления, которыми мы занимались в двух предыдущих главах и будем заниматься в следующей главе. Еще один важный класс исчислений — *формальные грамматики*, применяемые в лингвистике и теории программирования. Основы общей теории исчислений были заложены Э. Постом [Post 1943]. С основными понятиями и результатами общей теории исчислений, а также с некоторыми ее важнейшими приложениями, в том числе гуманитарными, можно познакомиться по книге [Маслов 1986], с теорией формальных грамматик — по книге [Гладкий 1973].

## Задачи и упражнения

1) Построить машины Тьюринга, осуществляющие сложение и умножение натуральных чисел в двоичной записи (с нулем).

2) Построить машины Тьюринга, преобразующие простейшую запись натурального числа в двоичную (с нулем и без нуля) и обратно.

3) Построить машины Тьюринга, вычисляющие следующие числовые функции в простейшей записи:

(а) $n!$

(б) $\lfloor \sqrt{n} \rfloor$,

(в) $\lfloor \log_2 n \rfloor$.

4) Построить машины Тьюринга, распознающие следующие свойства натуральных чисел в простейшей записи:

(а) быть степенью двойки;

(б) быть полным квадратом;

(в) быть простым числом.

5) Убедиться, что для пунктов (а) и (б) задачи после примера 9 в § 7.3 можно построить конечные автоматы. (См. сноску[24] на с. 303).

6) Построить конечный автомат, распознающий свойство слова в алфавите $\{a_1, \ldots, a_9\}$ быть кодом какого-либо слова в алфавите $\mathfrak{A} \cup \mathfrak{Q}$ (см. § 7.5).

7) Показать, что по конечным автоматам, распознающим какие-либо свойства $A$ и $B$ слов в некотором заданном алфавите, можно построить конечные автоматы, распознающие свойства $A\&B$, $A \vee B$, $A \supset B$.

8) (а) Назовем машину Тьюринга «нестирающей», если на каждом ее элементарном шаге либо записывается символ в пустой ячейке, либо над обозреваемым символом ставится метка, причем имеются метки только одного «сорта» (и в дальнейшем метку нельзя стереть), либо обозреваемый символ не меняется. Показать, что по всякой машине Тьюринга $M$ можно построить такую нестирающую машину $M'$, что $M[t_1, \ldots, t_n] = y$ тогда и только тогда, когда $M'$ перерабатывает набор слов $t_1, \ldots, t_n$ в слово вида $z*y$, где $*$ — фиксированный символ, не принадлежащий внешнему алфавиту $M$.

(б) Показать, что, добавив к машине Тьюринга еще одну головку (причем на каждом шаге работает одна головка и в каждой команде указывается, какая головка должна работать на следующем шаге), в пункте (а) можно обойтись без меток.

9) Для недетерминированной машины Тьюринга (н. м. Т.) (§ 7.9, пункт 7) можно определить правильное вычисление так же, как для обычной машины Тьюринга, но правильное вычисление, начинающееся данным словом, не обязательно единственно. Н. м. Т. *распознает* некоторое свойство слов в заданном алфавите, если для слова $x$ в этом алфавите тогда и только тогда существует правильное вычисление, начинающееся этим словом и заканчивающееся некоторым фиксированным символом (скажем, единицей), когда $x$ обладает данным свойством. Аналогично определяется распознавание отношений.

(а) Убедиться, что распознавание отношений «быть подсловом» (пример 9 из § 7.3) и «иметь вид $xx$» (задача после этого примера) можно производить на н. м. Т. проще, чем на детерминированной машине Тьюринга.

(б) Доказать, что по н. м. Т., распознающей некоторое свойство слов, можно построить детерминированную машину Тьюринга, распознающую то же свойство.

10) (а) Показать, что всякая вычислимая по Тьюрингу числовая функция может быть вычислена (в простейшей записи) с помощью машины Тьюринга с внешним алфавитом $\{a_{-1}, a_0, a_1\}$ ($a_1$ отождествляется с палочкой).

(б) Указать способ кодирования машин Тьюринга с использованием только символов $a_0$ и $a_1$.

(в) Доказать существование универсальной машины Тьюринга с внешним алфавитом $\{a_{-1}, a_0, a_1\}$. (Разделительный знак $\square$ заменяется в такой машине «пробелом» некоторой фиксированной длины.)

11) Показать, что не существует алгоритма, позволяющего для любой машины Тьюринга узнать, является ли она универсальной.

12) Показать, что не существует алгоритмов, позволяющих для любых двух машин Тьюринга узнать:

(а) применимы ли они обе к заданному слову;

(б) существует ли хоть одно слово, к которому они обе применимы;

(в) применима ли хоть одна из них к заданному слову;

(г) применима ли хоть одна из них хоть к одному слову.

13) Сформулировать (по образцу теоремы Райса) и доказать (с ее помощью) общую теорему о нераспознаваемости бинарных отношений для машин Тьюринга.

14) Доказать, что существует машина Тьюринга, для которой нельзя распознать по данному слову, является ли оно результатом переработки какого-либо слова этой машиной. [Указание. Построить машину, для которой результатами переработки слов служат все коды самоприменимых машин и только они.]

15) (а) Доказать, что существует машина Тьюринга, для которой нельзя распознать по данному слову, перерабатывает ли она его в $a_1$.

(б) Доказать, что существует ассоциативное исчисление, для которого нельзя распознать по данному слову, эквивалентно ли оно некоторому фиксированному однобуквенному слову.

16) Какие числа было бы удобно называть, если бы мы пользовались десятичной системой счисления без нуля, «десятнадцать», «двадцать десять — девяносто десять»?

17) Указать условие, необходимое и достаточное для совпадения записей числа в системе счисления с основанием $P$ с нулем и без нуля.

18) Указать алгоритмы для перевода из системы счисления с нулем в систему без нуля (с тем же основанием) и обратно.

19) Найти наименьшее и наибольшее $k$-значные числа в системе счисления с основанием $P$ без нуля.

20) Доказать, что функция, обратная к разнозначной вычислимой функции, также вычислима. [Указание. Использовать конструкцию, аналогичную пункту 1) доказательства теоремы 3 из § 7.7.]

21) (а) Доказать, что множество тогда и только тогда перечислимо, когда оно является «срезом» графика вычислимой функции (т. е. представимо в виде $\{x \mid f(x) = c\}$ для некоторой вычислимой функции $f$ и некоторого числа $c$).

(б) Доказать, что множество тогда и только тогда разрешимо, когда оно является «срезом» графика всюду определенной вычислимой функции.

22) Понятия разрешимости и перечислимости легко обобщить на многомерные множества, фиксировав какую-либо нумерацию упорядоченных систем натуральных чисел (например, считая номером системы

$(a_1, \ldots, a_n)$ число $2^{a_1} 3^{a_2} \ldots p_n^{a_n-1}$)[64]. Доказать, что:

(а) Функция тогда и только тогда вычислима, когда ее график есть перечислимое множество.

(б) Всюду определенная функция вычислима тогда и только тогда, когда ее график есть разрешимое множество.

23) Доказать, что если объединение $n$ попарно непересекающихся перечислимых множеств ($n = 1, 2, \ldots$) совпадает со всем натуральным рядом, то все эти множества разрешимы.

24) Доказать, что для любых бесконечных перечислимых множеств $E_1$ и $E_2$ найдется взаимно однозначная вычислимая функция с областью определения $E_1$ и множеством значений $E_2$.

25) Если всюду определенная взаимно однозначная вычислимая функция отображает множество $E_1$ на множество $E_2$, то из разрешимости $E_2$ следует разрешимость $E_1$[65], но обратное неверно. Доказать.

26) Доказать, что если $f$ — вычислимая функция с областью определения $E$ и множества $E_1$ и $E_2$ таковы, что $E_1 \subset E$ и $x \in E_1$ тогда и только тогда, когда $f(x) \in E_2$, то из перечислимости $E_2$ следует перечислимость $E_1$.

В задачах 27—35 будут использоваться следующие понятия. *Номером перечислимого множества* называется номер любой машины Тьюринга, вычисляющей одноместную функцию, для которой данное множество служит множеством значений. Класс перечислимых множеств называется *вполне разрешимым* (*вполне перечислимым*), если множество всех номеров всех множеств этого класса разрешимо, соответственно перечислимо. Класс $A$ конечных множеств натуральных чисел *вполне перечислим*, если перечислимо множество номеров упорядоченных систем (об этих номерах см. задачу 22), составленных из расположенных в порядке возрастания элементов множеств, принадлежащих $A$ (например, для множества {6, 3, 8, 2} берется упорядоченная четверка (2, 3, 6, 8)).

27) Указать хотя бы по одному номеру пустого множества, множеств {0} и {1}, множества всех чисел вида 11...1.

28) Доказать, что существуют только два вполне разрешимых класса перечислимых множеств: класс всех перечислимых множеств и пустой класс[66].

29) Доказать, что:

(а) Класс всех непустых перечислимых множеств вполне перечислим;

(б) Класс, единственным элементом которого служит пустое множество, не является вполне перечислимым.

---

[64] Единственное требование, предъявляемое к этой нумерации — наличие алгоритмов, позволяющих находить по системе ее номер и обратно.

[65] Более того, если всюду определенная вычислимая функция $f$ (не обязательно взаимно однозначная) такова, что $x \in E_1$ тогда и только тогда, когда $f(x) \in E_2$, то из разрешимости $E_2$ следует разрешимость $E_1$. В § 7.6 мы фактически пользовались этим (в сущности, очевидным) соображением, доказывая неразрешимость алгоритмических проблем методом сведения.

[66] Это утверждение — другая форма теоремы Райса (которая именно так была сформулирована им самим в статье [Rice 1953]).

30) Доказать, что для любого конечного множества натуральных чисел $E$ класс всех перечислимых множеств, содержащих $E$, вполне перечислим.

31) Доказать, что если $E$ и $E'$ — перечислимые множества и $E \subset E'$, то никакой класс перечислимых множеств, содержащий $E$ и не содержащий $E'$, не является вполне перечислимым. [Указание. Построить по произвольной машине $M$ машину $M'$ так, что если $M$ вычисляет функцию с пустым множеством значений, то множеством значений функции, вычисляемой машиной $M'$, будет $E$, а в противном случае — $E'$. Воспользоваться результатами задач 26 и 29б.]

32) Доказать, что если $E$ — бесконечное перечислимое множество, то никакой класс перечислимых множеств, содержащий $E$ и не содержащий ни одного конечного подмножества $E$, не является вполне перечислимым. [Указание. Действовать аналогично решению предыдущей задачи.]

33) Доказать, что для любого вполне перечислимого класса $K$ перечислимых множеств класс конечных множеств, принадлежащих $K$, внешне перечислим.

34) Пользуясь результатами предыдущих задач, доказать **вторую теорему Райса** [Rice 1953]. Класс $K$ перечислимых множеств тогда и только тогда вполне перечислим, когда существует такой внешне перечислимый класс $A$ конечных множеств, что

$$K = \{E \mid E \text{ перечислимо и } \exists E'(E' \in A \& E' \subset E)\}$$

35) (а) Пользуясь второй теоремой Райса (см. предыдущую задачу), показать, что для произвольного непустого перечислимого множества $E$ ни множество всех номеров $E$, ни дополнение к этому множеству не являются перечислимыми.

(б) Привести другие примеры множеств натуральных чисел, неперечислимых вместе с их дополнениями.

36) Доказать, что всякая функция $f(x_1, \ldots, x_n)$, которую можно получить из функций $e^k_i(x_1, \ldots, x_k) = x_i$ и функций-констант с помощью подстановки и рекурсии, обладает следующим свойством: существуют такие натуральные числа $c_1, \ldots, c_m$ $(m = 1, 2, \ldots)$ и такое $i = 1, \ldots, n$, что для любого набора $n$ натуральных чисел $x_1^0, \ldots, x_n^0$ значение $f(x_1^0, \ldots, x_n^0)$ либо не превосходит $x_i^0$, либо равно одному из чисел $c_1, \ldots, c_m$.

37) Доказать, что следующие функции примитивно рекурсивны:

(а) число простых делителей числа $x$;

(б) $\pi(x)$ — число простых чисел, не превосходящих $x$;

(в) $\varphi(x)$ — число чисел, не превосходящих $x$ и взаимно простых с $x$ (*функция Эйлера*);

(г) число степеней двойки, не превосходящих $x$.

38) Доказать, что предикат «Число $z$ есть наименьшее общее кратное чисел $x$ и $y$» и функция $z = [x, y]$ — наименьшее общее кратное чисел $x$ и $y$ — примитивно рекурсивны.

39) Доказать теорему о возвратной рекурсии: Если $(n-1)$-местная функция $g$, $(n+s)$-местная функция $h$ и одноместные

функции $\varphi_1, \ldots, \varphi_s$ примитивно рекурсивны и $\varphi_i(x+1) \leq x$ ($i = 1, \ldots, s$; $x = 0, 1, \ldots$), то $n$-местная функция $f$, определяемая равенствами

$$\begin{cases} f(x_1, \ldots, x_{n-1}, 0) = g(x_1, \ldots, x_{n-1}) \\ f(x_1, \ldots, x_{n-1}, x_n + 1) = \\ = h(x_1, \ldots, x_n, f(x_1, \ldots, x_{n-1}, \varphi_1(x_n + 1)), \ldots \\ \ldots, f(x_1, \ldots, x_{n-1}, \varphi_s(x_n + 1))), \end{cases}$$

также примитивно рекурсивна. (Так при $n > 1$; для $n = 1$ аналогично (сформулировать!).) [Указание. Доказать сначала примитивную рекурсивность функции

$$\prod_{t=0}^{x_n} p_t^{f(x_1, \ldots, x_{n-1}, t)}.$$

40) Пользуясь теоремой о возвратной рекурсии (см. предыдущую задачу), доказать, что функция $F(x)$, определяемая равенствами $F(0) = 0$, $F(1) = 1$, $F(n+2) = F(n) + F(n+1)$, примитивно рекурсивна[67].

41) Доказать теорему об одновременной рекурсии: Если $(n-1)$-местные функции $g_1, \ldots, g_s$ и $(n+s)$-местные функции $h_1, \ldots, h_s$ примитивно рекурсивны, то таковы же и $n$-местные функции $f_1, \ldots, f_s$, определяемые равенствами

$$\begin{cases} f_1(x_1, \ldots, x_{n-1}, 0) = g_1(x_1, \ldots, x_{n-1}) \\ f_1(x_1, \ldots, x_{n-1}, x_n + 1) = h_1(x_1, \ldots, x_n, f_1(x_1, \ldots, x_n), \ldots f_s(x_1, \ldots, x_n)) \end{cases}$$

(Так при $n > 1$; для $n = 1$ аналогично (сформулировать!).)

42) Расположив всевозможные упорядоченные пары натуральных чисел в последовательность таким образом, чтобы пара $(m, n)$ предшествовала паре $(m', n')$ тогда и только тогда, когда либо $m + n < m' + n'$, либо $m + n = m' + n'$ и $m < m'$, назовем номер пары в этой последовательности ее *канторовским номером* и будем обозначать его $C(m, n)$ (при этом $C(0, 0) = 0$). Первый и второй члены пары с номером $k$ обозначим соответственно $L(k)$ и $R(k)$. Доказать, что функции $L$, $R$ и $C$ примитивно рекурсивны. [Указание. Для $L$ и $R$ воспользоваться одновременной рекурсией (задача 41) и затем для $C$ — ограниченной минимизацией.]

43) Доказать, что функция $[e \cdot n]$ ($e$ — основание натуральных логарифмов) примитивно рекурсивна. [Указание. Рассмотреть функцию $S_n$, определяемую равенствами $S_0 = 0$, $S_{n+1} = (n+1) \cdot S_n + 1$.]

44) Пусть $a$ — действительное число. Обозначим через $\psi_a(n)$ ($n = 1, 2, \ldots$) $n$-й знак после запятой бесконечной десятичной дроби, представляющей $a$, и положим $\psi_a(0) = [a]$. Доказать, что функции $\psi_{\sqrt{2}}$, $\psi_e$, $\psi_\pi$ примитивно рекурсивны.

45) Доказать, что следующие функции и предикаты примитивно рекурсивны (в нижеследующих определениях функций и предикатов числа отождествляются с их записями в девятеричной системе без нуля):

(а) Длина слова $x$:

[67] Значения этой функции называются *числами Фибоначчи*.

(б) Обращение слова $x$;

(в) «Проекция» $x$ на заданный подалфавит $A'$ алфавита $\{a_1, \ldots, a_s\}$ (т. е. слово, получаемое из $x$ вычеркиванием символов, не принадлежащих $A'$);

(г) Subst$(x, y, z)$ (см. пример 10 из § 7.3);

(д) «$x$ есть симметричное слово»;

(е) «$x$ есть периодическое слово (т. е. $x = z^n$ для некоторого слова $z$ и некоторого $n = 2, 3, 4, \ldots$)».

46) *Функцией Аккермана*[68] (см. [Гильберт — Бернайс 1979], гл. VII, § 3, п. 2) называется двуместная функция $A$, определяемая равенствами

$$\begin{cases} A(0, y) = 2y + 1 \\ A(x + 1, 0) = A(x, 1) \\ A(x + 1, y + 1) = A(x, A(x + 1, y)). \end{cases}$$

Процедура, позволяющая вычислять значения этой функции, очевидна. Доказать (последовательно), что:

(а) $A(x, y) > y$ для любых $x$ и $y$;

(б) функция $A$ монотонна по обеим переменным;

(в) Для любой п. р. ф. $f(x_1, \ldots, x_n)$ найдется такое число $z$, что $f(x_1, \ldots, x_n) < A(z, \max(x_1, \ldots, x_n))$ для любых $x_1, \ldots, x_n$;

(г) Функция $A(y, y)$ мажорирует любую одноместную п. р. ф. $\varphi$ в том смысле, что $\varphi(y) < A(y, y)$ для всех достаточно больших $y$ (и, следовательно $A(x, y)$ не примитивно рекурсивна — что, впрочем, нетрудно вывести и непосредственно из (в));

(д) Не существует разнозначной одноместной п. р. ф., множество значений которой совпадало бы с множеством значений функции $A(y, y)$.

47) Доказать, что для любого $n$ существует $n$-местная ч. р. ф., которую нельзя доопределить до о. р. ф. [Указание. См. замечание 1 после формулировки теоремы 3 из § 7.9.]

48) (а) Доказать, что если для машины Тьюринга, вычисляющей $n$-местную функцию $f$, существует такая $n$-местная п. р. ф. $\varphi$, что для любых $x_1, \ldots, x_n$, для которых определено $f(x_1, \ldots, x_n)$, длина соответствующего полного вычисления машины не превосходит $\varphi(x_1, \ldots, x_n)$, то функция

$$\bar{f}(x_1, \ldots, x_n) = \begin{cases} f(x_1, \ldots, x_n), & \text{если } f(x_1, \ldots, x_n) \text{ определено} \\ 0, & \text{если } f(x_1, \ldots, x_n) \text{ не определено} \end{cases}$$

примитивно рекурсивна.

(б) То же с заменой длины вычисления числом используемых в вычислении ячеек (равным числу ячеек на ленте в заключительной ситуации).

49) Доказать, что если машины Тьюринга удовлетворяет для некоторого $n$ условию задачи 48а или 48б, то область определения $n$-местной функции, вычисляемой этой машиной, есть примитивно рекурсив-

[68] В. Аккерман (Wilhelm Ackermann) — немецкий математик, ученик Д. Гильберта.

ное множество (т. е. ее характеристическая функция примитивно рекурсивна).

50) (а) Доказать, что для всякой п. р. ф. существует вычисляющая ее машина Тьюринга, удовлетворяющая обоим условиям задачи 48.

(б) То же для функции с примитивно рекурсивной областью определения, доопределимой до п. р. ф.

51) (а) Доказать, что характеристическая функция предиката $T_1(i, z, x_1, \ldots, x_n)$ может быть вычислена с помощью машины Тьюринга, у которой число шагов правильного вычисления мажорируется линейной функцией от $i + z$, а число используемых в вычислении ячеек — логарифмической. [Указание. Сначала оценить зависимость числа используемых ячеек от длины слова $i + z$.]

(б) То же для использованного в доказательстве основной леммы предиката $T'(i, z, y)$.

Замечание. Результаты задач 48 и 51 дают другое доказательство основной леммы.

52) Указать пример разрешимого множества, не являющегося примитивно рекурсивным.

53) Доказать, что $n$-местная о. р. ф. $f$ тогда и только тогда может быть представлена в виде $\mu y P(x_1, \ldots, x_n, y)$ с примитивно рекурсивным $P$, когда график $f$ является примитивно рекурсивным множеством.

54) Доказать, что график функции Аккермана (см. задачу 46) примитивно рекурсивен.

55) Указать пример о. р. ф., график которой не является примитивно рекурсивным.

ГЛАВА

8

# ФОРМАЛЬНАЯ АРИФМЕТИКА. ГРАНИЦЫ ФОРМАЛИЗАЦИИ МАТЕМАТИКИ

## § 8.1. ФОРМАЛЬНАЯ АРИФМЕТИКА

1. В § 6.3 мы рассмотрели ряд примеров прикладных логических исчислений, предназначенных для формализации понятий группы, кольца, поля, упорядоченного множества и т. п. Однако наряду с этими чрезвычайно общими понятиями современная математика продолжает пользоваться также более старыми и более конкретными — такими, как число, точка, прямая, плоскость, к которым в конечном счете восходят и все более абстрактные понятия. Возникает вопрос, в какой мере эти «конкретные» понятия можно формализовать средствами математической логики. А так как все эти, да и все остальные математические концепции так или иначе опираются на понятие натурального числа, первым шагом на пути решения этого вопроса должна быть попытка формализовать арифметику натуральных чисел. Такая попытка действительно была предпринята (в основном по инициативе Д. Гильберта) в первой трети XX в.— и привела к совершенно неожиданным результатам. Изложением этих результатов мы и займемся в настоящей главе.

Если читатель не знаком с пеановской арифметикой, ему следует, прежде чем двигаться дальше, изучить пункт 3 приложения III.

2. Начнем с построения прикладного логического исчисления на основе $G_1$, которое естественно будет считать формальной версией арифметики натуральных чисел. Мы будем называть это исчисление *формальной арифметикой* и обозначать Ar.

Чтобы задать логическое исчисление на основе $G_1$ (см. § 6.2), нужно перечислить его предикатные и функциональные символы, символы предметных констант и аксиомы. Для исчисления Ar эти компоненты таковы:

I. Ar имеет один двуместный предикатный символ $F_1^2$, один одноместный функциональный символ $f_1^1$, два двуместных функциональных символа $f_1^2$ и $f_2^2$ и один символ предметной константы $a_1$. Мы будем в дальнейшем вместо $F_1^2(t_1, t_2)$ писать $t_1 = t_2$, вместо $f_1^1(t)$ — $t'$, вместо $f_1^2(t_1, t_2)$ — $t_1 + t_2$, вместо $f_2^2(t_1, t_2)$ — $t_1 \cdot t_2$ (или $t_1 t_2$) и вместо $a_1$ — 0. Содержательно $t'$ будет означать число, непосредственно следующее за $t$; смысл остальных обозначений ясен.

II. Аксиомы исчисления Ar задаются схемами:[1]

$(r)\ x = x;$

$(s)\ x = y \supset y = x;$

$(t)\ x = y \& y = z \supset x = z;$

$(\alpha_1)\ x = y \supset x' = y';$

$(\alpha_2)\ x' = y' \supset x = y;$

$(\alpha_3)\ \neg \exists x(x' = 0);$

$(\alpha_4)\ \mathfrak{A}(0) \& \forall x(\mathfrak{A}(x) \supset \mathfrak{A}(x')) \supset \forall x \mathfrak{A}(x);$

$(\alpha_5)\ x + 0 = x;$

$(\alpha_6)\ x + y' = (x + y)';$

$(\alpha_7)\ x \cdot 0 = 0;$

$(\alpha_8)\ x \cdot y' = x \cdot y + x.$

Здесь $x$, $y$, $z$ — произвольные переменные; в схеме $(\alpha_4)$ $\mathfrak{A}(x)$ — произвольная формула в алфавите исчисления Ar и $\mathfrak{A}(0)$, $\mathfrak{A}(x')$ — формулы, полученные из $\mathfrak{A}(x)$ заменой всех вхождений $x$ вхождениями термов 0 и $x'$ соответственно. Все остальные схемы аксиом — простейшие (см. с. 238), и мы будем их называть просто аксиомами (ср. сноску на той же странице).

Комментарий. В аксиомах $(\alpha_1) - (\alpha_4)$ легко узнать аксиомы Пеано (см. Приложение III), однако аксиома индукции здесь ослаблена: в ней идет речь не о произвольном свойстве натуральных чисел, как в неформальной пеановской арифметике, а только о таком, которое можно выразить на языке узкого исчисления предикатов (т. е. с помощью формулы исчисления Ar). О последствиях этого вынужденного ослабления принципа индукции см. ниже, в пункте 7 настоящего параграфа. Для «формального нуля» мы пользуемся

[1] В схеме $(\alpha_8)$ (и далее, когда нужно) мы пользуемся общепринятым соглашением о порядке арифметических действий.

обозначением 0, чтобы отличать его от «неформального» (обозначаемого 0). Аксиомы $(\alpha_7) - (\alpha_8)$ — это рекурсивные определения суммы и произведения (ср. § 7.8 и Приложение III).

Замечания. 1) Все аксиомы исчисления Ar, содержащие свободные переменные, сохраняют силу при замене этих переменных произвольными термами.

Это непосредственно следует из правил B∀ и У∀.

2) Чтобы доказать, что формула $\forall x\mathfrak{A}(x)$ — теорема исчисления Ar, достаточно, ввиду аксиомы $(\alpha_4)$ (и правил BK и УИ), установить, что в нем являются теоремами формулы $\mathfrak{A}(0)$ и $\forall x(\mathfrak{A}(x)\supset\mathfrak{A}(x'))$. Такой способ доказательства мы будем называть *формальной индукцией*, а доказательства теорем $\mathfrak{A}(0)$ и $\forall x(\mathfrak{A}(x)\supset\mathfrak{A}(x'))$ — *базисом* (индукции) и *индукционным шагом*[2].

В качестве примера формальной индукции выведем следующую (формальную) теорему (символ $\vdash$ здесь и далее, если не оговорено противное, означает $\vdash_{\mathrm{Ar}}$):

$$(1)\ \vdash \forall x(x = 0 \vee \exists y\,(x = y')).$$

Доказательство. Базис: $\vdash 0 = 0 \vee \exists y(0 = y')$ ввиду аксиомы $(r)$, замечания 1 и правила ВД. Индукционный шаг: Ввиду $(r)$ и замечания 1 $\vdash x' = x'$, откуда по B∃ $\vdash \exists y(x' = y')$. Но из этой формулы по правилам исчисления $G_0$ и правилу B∀ выводима формула

$$\forall x(x = 0 \vee \exists y\,(x = y') \supset x' = 0 \vee \exists y\,(x' = y'))^3.$$

В дальнейшем мы не будем доказывать выводимости в Ar так подробно; в частности, не будем явно ссылаться на правила исчисления $G_0$ (кроме наиболее сложных случаев). Восстановление опущенных деталей будет предоставляться читателю.

3. Чтобы иметь право считать логическое исчисление формальной версией арифметики натуральных чисел, мы во всяком случае должны быть уверены, что в нем доказуемы, во-первых, основные свойства равенства и, во-вторых, основные свойства сложения и умножения. Поэтому сейчас нам прежде всего необходимо убедиться, что исчисление Ar удовлетворяет этим требованиям. Первое из них означает, что Ar есть исчисление на основе $G_1$ с равенством. Чтобы установить это, достаточно — ввиду теоремы 5 из § 6.3 и того, что

---

[2] Таким образом, термины «базис» и «индукционный шаг» приобретают теперь наряду с обычным «неформальным» смыслом еще один, «формальный» (подобно терминам «теорема» и «доказательство»).

[3] Мы пользуемся здесь выводимостью $\mathfrak{C} \vdash_{G_0} \mathfrak{A} \supset \mathfrak{B} \vee \mathfrak{C}$. (Напомним, что ввиду полноты $G_0$ всякую выводимость в этом исчислении можно доказать с помощью истинностных таблиц.)

было сказано на с. 238 о ее применении, а также ввиду наличия в Ar аксиом $(r)$, $(s)$, $(t)$, $(\alpha_1)$ — установить, что:

(2) $\vdash x = y \supset x + z = y + z$;

(3) $\vdash x = y \supset z + x = z + y$;

(4) $\vdash x = y \supset x \cdot z = y \cdot z$;

(5) $\vdash x = y \supset z \cdot x = z \cdot y$.

Второе требование означает, что:

(6) $\vdash x + (y + z) = (x + y) + z$;

(7) $\vdash x + y = y + x$;

(8) $\vdash x + z = y + z \supset x = y$;

(9) $\vdash x \cdot (y \cdot z) = (x \cdot y) \cdot z$;

(10) $\vdash x \cdot y = y \cdot x$;

(11) $\vdash (x + y) \cdot z = x \cdot z + y \cdot z$;

(12) $\vdash \neg(z = 0) \& x \cdot z = y \cdot z \supset x = y$.

Доказывать теоремы (2) — (12) нам будет удобнее не в том порядке, в каком мы их записали. По ходу доказательства придется вывести также несколько вспомогательных теорем; некоторые из них имеют и самостоятельное значение. Бóльшая часть доказательств будет проводиться с помощью формальной индукции.

Доказательство (2). Базис: $\vdash x = y \supset x + 0 = y + 0$ ввиду аксиом $(\alpha_5)$, $(s)$ и $(t)$; подробности восстанавливаются без труда. Индукционный шаг: чтобы доказать

$$\vdash \forall z((x = y \supset x + z = y + z) \supset (x = y \supset x + z' = y + z')),$$

достаточно убедиться, что $\vdash x + y = y + z \supset x + z' = y + z'$[4]; но это ввиду $(\alpha_6)$, $(s)$ и $(t)$ вытекает из $\vdash x + z = y + z \supset (x + z)' = (y + z)'$, а последнее справедливо в силу $(\alpha_1)$ и замечания 1.

В дальнейшем ссылки на аксиомы $(s)$ и $(t)$ и на замечание 1 будут, как правило, опускаться.

Далее нам понадобятся три вспомогательные теоремы:

(13) $\vdash x + 0' = x'$;

(14) $\vdash 0 + x = x$;

(15) $\vdash x + y' = x' + y$.

[4] Если импликация $\mathfrak{B} \supset \mathfrak{C}$ истинна, то истинна, очевидно, и импликация $(\mathfrak{A} \supset \mathfrak{B}) \supset (\mathfrak{A} \supset \mathfrak{C})$.

Теорема (13) легко выводится из $(\alpha_5)$, $(\alpha_1)$ и $(\alpha_6)$. Докажем (14). Базис: $0 + 0 = 0$ по $(\alpha_5)$. Индукционный шаг: достаточно доказать $0 + x = x \vdash 0 + x' = x'$. Но по $(\alpha_1)$ $0 + x = x \vdash (0 + x)' = x'$, а по $(\alpha_6)$ $\vdash 0 + x' = (0 + x)'$. Доказательство (15) получается так: $\vdash x + 0' = x' + 0$ ввиду (13) и $(\alpha_5)$: $x + y' = x' + y \vdash x + y'' = x' + y'$, поскольку: $\vdash x + y'' = (x + y')'$ по $(\alpha_6)$; $x + y' = x' + y \vdash (x + y')' = (x' + y)'$ по $(\alpha_1)$; $\vdash (x' + y)' = x' + y'$ снова по $(\alpha_6)$.

Теперь мы можем доказать (7). Базис: $\vdash x + 0 = 0 + x$ ввиду $(\alpha_5)$ и (14). Индукционный шаг: $x + y = y + x \vdash x + y' = y' + x$, поскольку: $x + y = y + x \vdash (x + y)' = (y + x)'$ по $(\alpha_1)$; $\vdash (y + x)' = y + x'$ по $(\alpha_6)$; $\vdash y + x' = y' + x$ по (15); $\vdash (x + y)' = x + y'$ по $(\alpha_6)$.

Из (7) и (2) легко вывести (3); после этого можно доказать (4) так же, как (2), используя $(\alpha_7)$ и $(\alpha_8)$ вместо $(\alpha_5)$ и $(\alpha_6)$ соответственно, а вместо $(\alpha_1)$ применив последовательно (2) и (3).

Докажем, далее, (6). Базис: $\vdash x + (y + 0) = (x + y) + 0$, поскольку $\vdash x + (y + 0) = x + y$ (ввиду $(\alpha_5)$ и (3)) и $\vdash (x + y) + 0 = x + y$ (по $(\alpha_5)$). Индукционный шаг: $x + (y + z) = (x + y) + z \vdash x + (y + z') = (x + y) + z'$ вытекает из того, что: $\vdash x + (y + z') = x + (y + z)'$ (ввиду $(\alpha_6)$ и (3)); $\vdash x + (y + z)' = (x + (y + z))'$ (по $(\alpha_6)$); $x + (y + z) = (x + y) + z \vdash (x + (y + z))' = ((x + y) + z)'$ (по $(\alpha_1)$; $\vdash ((x + y) + z)' = (x + y) + z'$ (по $(\alpha_6)$).

Докажем (11). Базис: $\vdash (x + y)\cdot 0 = x\cdot 0 + y\cdot 0$, поскольку $\vdash (x + y)\cdot 0 = 0$ по $(\alpha_7)$, $\vdash x\cdot 0 + y\cdot 0 = 0 + y\cdot 0$ по $(\alpha_7)$ и (2), $\vdash 0 + y\cdot 0 = 0 + 0$ по $(\alpha_7)$ и (3); $\vdash 0 + 0 = 0$ по $(\alpha_5)$.
Индукционный шаг: выводимость

$$(x + y)\cdot z = x\cdot z + y\cdot z \vdash (x + y)\cdot z' = x\cdot z' + y\cdot z'$$

вытекает из следующих выводимостей

$\vdash (x + y)\cdot z' = (x + y)\cdot z + (x + y)$ по $(\alpha_8)$;
$(x + y)\cdot z = x\cdot z + y\cdot z \vdash (x + y)\cdot z + (x + y) = (x\cdot z + y\cdot z) + (x + y)$ (по (2));
$\vdash (x\cdot z + y\cdot z) + (x + y) = (x\cdot z + x) + (y\cdot z + y)$ (легко получается из (6), (7), (2) и (3); $\vdash (x\cdot z + x) + (y\cdot z + y) = x\cdot z' + y\cdot z'$ (из $(\alpha_8)$, (2) и (3)).

Следующие две вспомогательные теоремы читатель легко

докажет сам:

(16) $\vdash \mathbf{0}\cdot x = 0$;

(17) $\vdash \mathbf{0}'\cdot x = x$.

Теперь можно доказать (10). Базис: $\vdash x\cdot\mathbf{0} = \mathbf{0}\cdot x$ ввиду $(\alpha_7)$ и (16). Индукционный шаг: $x\cdot y = y\cdot x \vdash x\cdot y' = y'\cdot x$, поскольку $\vdash x\cdot y' = x\cdot y + x$ по $(\alpha_8)$; $x\cdot y = y\cdot x \vdash x\cdot y + x = y\cdot x + x$ по (2); $\vdash y\cdot x + x = y\cdot x + \mathbf{0}'\cdot x$ по (17) и (3); $\vdash y\cdot x + \mathbf{0}'\cdot x = (y + \mathbf{0}')\cdot x$ по (11); $\vdash (y + \mathbf{0}')\cdot x = y'\cdot x$ по (13) и (4).

Из (10) и (4) получаем теперь (5). Кроме того, из (10) и (11) вытекает

(18) $\vdash x\cdot(y + z) = x\cdot y + x\cdot z$.

Докажем (9). Базис: $\vdash x\cdot(y\cdot\mathbf{0}) = (x\cdot y)\cdot\mathbf{0}$, т. к. $\vdash x\cdot(y\cdot\mathbf{0}) = \mathbf{0}$ (ввиду $(\alpha_7)$ и (5)) и $\vdash (x\cdot y)\cdot\mathbf{0} = \mathbf{0}$ (по $(\alpha_7)$). Индукционный шаг: $x\cdot(y\cdot z) = (x\cdot y)\cdot z \vdash x\cdot(y\cdot z') = (x\cdot y)\cdot z'$, поскольку $\vdash x\cdot(y\cdot z') = x\cdot(y\cdot z + y)$ (ввиду $(\alpha_8)$ и (5)); $\vdash x\cdot(y\cdot z + y) = x\cdot(y\cdot z) + x\cdot y$ по (18)); $x\cdot(y\cdot z) = (x\cdot y)\cdot z \vdash x\cdot(y\cdot z) + x\cdot y = (x\cdot y)\cdot z + x\cdot y$ (по (2)); $\vdash (x\cdot y)\cdot z + x\cdot y = (x\cdot y)\cdot z'$ (по $(\alpha_8)$).

Доказательство теорем (8) и (12) мы отложим до конца следующего пункта.

Задача. Доказать, что:

(а) $\vdash x + y = \mathbf{0} \supset x = \mathbf{0} \& y = \mathbf{0}$;

(б) $\vdash x\cdot y = \mathbf{0} \supset x = \mathbf{0} \vee y = \mathbf{0}$:

(в) $\vdash x + y = x \supset y = \mathbf{0}$.

4. Теперь нам нужно формализовать отношение «меньше». Пользуясь тем, что для натуральных чисел $n < m$ тогда и только тогда когда $n$ можно представить в виде $m + k$, где $k \neq 0$, мы будем для произвольных термов $t$ и $u$ понимать выражение $t < u$ как сокращенную запись формулы $\exists z(y = t + z')$, где $z$ — произвольная переменная, не входящая в $t$ и $u$ (очевидно, для фиксированных $t$ и $u$ все такие формулы дедуктивно эквивалентны). Основные свойства отношения «меньше» выражаются следующими формальными теоремами:

(19) $\vdash \neg(x < x)$;

(19′) $\vdash x < y \supset \neg(x = y)$;

(20) $\vdash x < y \supset \neg(y < x)$;

(21) $\vdash x < y \& y < z \supset x < z$;

(22) $\vdash \neg(x = y) \supset x < y \vee y < x$;

(23) $\neg(\exists x)(x < \mathbf{0})$;

(24) $\vdash (x < y \supset x + z < y + z) \,\&\, (x + z < y + z \supset x < y)$;

(25) $\vdash \neg(z = 0) \supset (x < y \supset x \cdot z < y \cdot z) \,\&\, (x \cdot z < y \cdot z \supset x < y)$.

Докажем (19). Базис: чтобы доказать, что $\vdash \neg \exists z(0 = 0 + z')$, достаточно привести формулу $\exists z(0 = 0 + z')$ к противоречию, т. е. вывести из нее формулу, отрицание которой доказуемо в Ar. Но ввиду $(\alpha_5)$ и (7) $\exists z(0 = 0 + z') \vdash \exists z(z' = 0)$, а отрицание формулы $\exists z(z' = 0)$ есть аксиома $(\alpha_4)$. Индукционный шаг: достаточно установить, что $\exists z(x' = x' + z') \vdash \exists z(x = x + z')$, а это легко сделать с помощью $(\alpha_6)$, (7) и $(\alpha_2)$.

(19′) сразу получается из (19), если заметить, что $x < y$, $x = y \vdash x < x$[5].

(21) в подробной записи имеет вид $\vdash \exists z_1(y = x + z_1') \,\&$

$$\&\exists z_2(z = y + z_2') \supset \exists z_3(z = x + z_3'),$$

а это легко доказать с помощью (6)[6]. Далее, из (21) вытекает $\vdash x < y \,\&\, y < x \supset x < x$; это вместе с (19) дает $\vdash \neg(x < y \,\&\, y < x)$, что равносильно (20).

Часто бывает полезна следующая теорема (получаемая очевидным образом из (13)):

(26) $\vdash x < x'$.

Вместо (22) докажем равносильное утверждение $\vdash x = y \vee x < y \vee y < x$. Базис: $\vdash x = 0 \vee x < 0 \vee 0 < x$ вытекает из $\vdash x = 0 \vee 0 < x$, а это — из (1) и очевидной ввиду $(\alpha_5)$ и (7) выводимости $\exists y(x = y') \vdash 0 < x$. Индукционный шаг: выводимость $x = y \vee x < y \vee y < x \vdash x = y' \vee x < y' \vee y' < x$ получается из трех выводимостей: $x = y \vdash x < y'$; $x < y \vdash x < y'$; $y < x \vdash x = y' \vee y' < x$. Первая из них непосредственно вытекает из (26), вторая — из (26) и (21). Третью легко установить, если доказать, что $x = y + z' \vdash x = y' \vee y' < x$. Но эту последнюю выводимость ввиду (1) можно получить из следующих двух: $x = y + 0' \vdash x = y'$, вытекающей из (13), и $x = y + z_1'' \vdash x = y' + z_1'$, которую нетрудно получить, используя (13), (7), (6) и еще раз (13).

Чтобы доказать (23), достаточно заметить, что из $\exists x(x < 0)$ ввиду $(\alpha_6)$ выводимо $\exists x \exists z((x + z)' = 0)$, а это противоречит аксиоме $(\alpha_3)$.

---

[5] Ввиду того, что Ar, как доказано в предыдущем пункте, есть исчисление на основе $C_1$ с равенством, так что в нем справедливо условие (r) из § 6.3. Далее мы пользуемся этим без оговорок (см., например, доказательства теорем (22) и (24)).

[6] Используя также (2).

Далее нам понадобятся две вспомогательные теоремы:

(27) $\vdash x < y \supset x' < y'$;

(28) $\vdash x' < y' \supset x < y$.

Первую из них легко получить, если доказать, что $y = x + z' \vdash y' = x' + z'$, а это очевидным образом вытекает из $(\alpha_1)$, $(\alpha_6)$ и (15). Так же доказывается и вторая (с заменой $(\alpha_1)$ на $(\alpha_2)$).

Обращаясь теперь к (24) и рассматривая сначала первый член конъюнкции, видим, что в его доказательстве базис получается с помощью $(\alpha_5)$, а выводимость $x + z < y + z \vdash x' + z < y' + z$, на которой основывается индукционный шаг — с помощью (7) и (27): подробности предоставляются читателю. Для второго члена все делается так же (но вместо (27) используется (28)).

Остается доказать (25). Здесь в первом члене конъюнкции базис получается из аксиомы $(r)$, индукционный шаг — из $(\alpha_8)$, (24) и (21). Чтобы получить второй член, достаточно установить, что $\neg(x < y) \vdash \neg(x \cdot z < y \cdot z)$. Но из $\neg(x < y)$ ввиду (22) можно вывести $x = y \vee y < x$; из $x = y$ по (4) выводится $x \cdot z = y \cdot z$, а из $y < x$, поскольку первый член конъюнкции уже доказан, можно вывести $y \cdot z < x \cdot z$. Как из $x \cdot z = y \cdot z$, так и из $y \cdot z < x \cdot z$ выводится $\neg(x \cdot z < y \cdot z)$. Подробности читатель может восстановить сам.

Теперь, располагая теоремами о свойствах отношения «меньше», мы без труда докажем теоремы (8) и (12). Чтобы доказать (8), достаточно установить, что $\neg(x = y) \vdash \neg(x + z = y + z)$; но ввиду (22) и (24) имеем $\neg(x = y) \vdash (x + z < y + z) \vee (y + z < x + z)$, а из (19′) получается $x + z < y + z \vee y + z < x + z \vdash \neg(x + z = y + z)$. Точно так же (с использованием (25) вместо (24)) доказывается (12).

Аналогично отношению «меньше» можно формализовать отношение «меньше или равно». Именно, мы будем для произвольных термов $t$ и $u$ понимать выражение $t \leq u$ как сокращенную запись формулы $t < u \vee t = u$. Читателю предоставляется доказать, что

(29) $\vdash x \leq y \vee y \leq x$;

(30) $\vdash x \leq y \& y \leq z \supset x \leq z$;

(31) $\vdash 0 \leq x$;

(32) $\vdash (x \leq y \supset x < y') \& (x < y') \supset x \leq y)$.

Иногда мы будем вместо $t < u$ писать $u > t$ и вместо $t \leq u$ — $y \geq t$.

Замечание. Читатель, несомненно, уже понял, что в доказательствах теорем (6) — (28) воспроизводятся в формализованном виде обычные доказательства соответствующих предложений «неформальной» пеановской арифметики (Приложение III, пункт 3).

Задача. Доказать, что:

(а) $\vdash \forall x \exists y (x < y)$;

(б) $\vdash \forall x \neg \exists y (x < y \& y < x')$;

(в) $\vdash x \leq x + y$;

(г) $\vdash \neg (y = 0) \supset x \leq x \cdot y$;

(д) $\vdash \neg (y = 0) \supset x < x + y$.

5. Особую роль в исчислении Ar играют термы $0$, $0'$, $0''$ и т. д., соответствующие конкретным натуральным числам. Эти термы принято называть *цифрами*. Цифру $0^{\prime\ldots\prime}$, содержащую $n$ штрихов, мы будем для краткости обозначать $\boldsymbol{n}$.

Заметим, что:

(33) $\vdash x + 1 = x'$;

(34) $\vdash x \cdot 1 = x$.

((33) совпадает с (13); (34) получается из (17) и (10).)

В дальнейшем нам понадобятся следующие утверждения о цифрах:

Утверждение 1. Для любых натуральных чисел $m$ и $n$:

(а) $\vdash \boldsymbol{m + n = m + n}$; (б) $\boldsymbol{m \cdot n = m \bullet n}$.

(например, $\vdash 2 + 2 = 4$, $\vdash 2 \cdot 2 = 4$; $\boldsymbol{m \bullet n}$ (с «жирной» точкой) означает $\mathbf{0}$ с $m \cdot n$ штрихами в отличие от $\boldsymbol{m \cdot n}$ — терма, содержащего функциональный символ $\cdot$; аналогичный смысл имеет выражение $\boldsymbol{m + n}$).

Доказательство. Справедливость (а) мы докажем индукцией[7] по $n$. Базис: поскольку $\boldsymbol{m + 0}$ — то же самое, что $\boldsymbol{m}$, по $(\alpha_5)$ имеем $\vdash \boldsymbol{m + 0 = m + 0}$. Индукционный шаг: т. к. $\boldsymbol{n + 1}$ совпадает с $\boldsymbol{n'}$, по $(\alpha_6)$ имеем $\vdash \boldsymbol{m + n + 1 = (m + n)'}$; в то же время по предположению индукции $\vdash \boldsymbol{m + n = m + n}$, откуда ввиду $(\alpha_1)$ $\vdash \boldsymbol{(m + n)' = (m + n)'}$; таким образом, $\vdash \boldsymbol{m + n + 1 = (m + n)'}$. но $\boldsymbol{(m + n)'}$ — это не что иное, как $\boldsymbol{(m + n) + 1}$ или, иначе, $\boldsymbol{m + (n + 1)}$. Аналогично доказывается (б).

Утверждение 2. Если $m < n$, то $\vdash \boldsymbol{m < n}$.

Доказательство. Пусть $m < n$. Тогда, полагая $k = n - m - 1$, имеем $n = m + (k + 1)$, откуда по утверждению 1 $\vdash \boldsymbol{n = m + k + 1}$ или, иначе, $\vdash \boldsymbol{n = m + k'}$, но отсюда сразу получается $\vdash \exists z (\boldsymbol{n = m + z'})$, т. е. $\vdash \boldsymbol{m < n}$.

[7] Само собой, здесь имеется в виду не формальная, а обычная математическая индукция.

Утверждение 3. Если $m \neq n$, то $\vdash \neg(\boldsymbol{m} = \boldsymbol{n})$.

Это утверждение непосредственно вытекает из предыдущего ввиду (19′).

Утверждение 4. Для любого натурального числа $n$

$$\vdash (x < \boldsymbol{n} + \boldsymbol{1} \supset x = \boldsymbol{0} \vee \cdots \vee x = \boldsymbol{n}) \,\&$$

$$\& \,(x = \boldsymbol{0} \vee \cdots \vee x = \boldsymbol{n} \supset x < \boldsymbol{n} + \boldsymbol{1}).$$

Читатель легко докажет это (неформальной) индукцией, используя (23) и (32).

Задача. Доказать, что:

(а) $\vdash x + 2 = x''$,

(б) $\vdash x \cdot y = x \supset x = 0 \vee y = 1$;

(в) если $m \leq n$, то $\vdash \boldsymbol{m} \leq \boldsymbol{n}$.

6. Для дальнейшего нам нужно формализовать теорему о делении с остатком и основные факты теории делимости.

Теореме о делении с остатком отвечает формальная теорема

$$(35)\ \vdash \forall x \forall y(\neg(y = 0) \supset \exists! z_1 \exists! z_2(x = y \cdot z_1 + z_2 \& z_2 < y)),$$

доказательство которой можно получить следующим образом. Прежде всего нетрудно видеть, что (35) получается с помощью правил $G_i$ и аксиом $(r)$, $(s)$, $(t)$ из

$$(35')\ \vdash \neg(y = 0) \supset \exists z_1 \exists z_2(x = y \cdot z_1 + z_2 \& z_2 < y)$$

и

$$(35'')\ y \cdot z_1 + z_2 = y \cdot z_3 + z_4 \& z_2 < y \& z_4 < y \vdash z_1 = z_3 \& z_2 = z_4.$$

В доказательстве (35′) воспользуемся формальной индукцией по $x$. Ее базис легко получить из очевидного утверждения $\vdash 0 = y \cdot 0 + 0$. Индукционный шаг: достаточно доказать, что

$$\exists z_1 \exists z_2 \exists z_3(x = y \cdot z_1 + z_2 \& y = z_2 + z_3') \vdash$$

$$\vdash \exists z_1 \exists z_2(x' = y \cdot z_1 + z_2 \& z_2 < y).$$

Для этого, в свою очередь, достаточно вывести правую часть из формулы $x = y \cdot z_1 + z_2 \& y = z_2 + z_3'$. Но из этой последней ввиду (1) выводима дизъюнкция $(x = y \cdot z_1 + z_2 \& y = z_2 + 0') \vee (x = y \cdot z_1 + z_2 \& \& \exists z_4(y = z_2 + z_4''))$; из первого члена этой дизъюнкции нетрудно вывести формулу $x' = y \cdot z_1' + 0 \& 0 < y$, а из второго — $x' = y \cdot z_1 + z_2' \& \& z_2' < y$; каждой из этих двух формул очевидным образом достаточно, чтобы вывести ту формулу, которая нам нужна.

Переходя к утверждению (35″), заметим, что его легко получить из двух более простых:

$$y\cdot z_1 + z_2 = y\cdot z_3 + z_4 \& z_2 < y \& z_4 < y \vdash z_1 = z_3$$

и

$$y\cdot z + z_1 = y\cdot z + z_2 \& z_1 < y \& z_2 < y \vdash z_1 = z_2.$$

Второе из этих утверждений очевидно. Чтобы доказать первое, достаточно, ввиду (22), привести к противоречию конъюнкцию

$$y\cdot z_1 + z_2 = y\cdot z_3 + z_4 \& z_2 < y \& z_4 < y \& z_1 < z_3.$$

Но из ее первого и последнего членов выводится формула $\exists z_5(y\cdot z_1 + z_2 = y\cdot(z_1 + z_5') + z_4)$, а из этой последней — $\exists z_5(z_2 = y\cdot z_5' + z_4)$. Однако $\vdash y\cdot z_5' \geq y$ (ввиду $(\alpha_8)$ и свойств отношения $<$), и мы приходим к противоречию со вторым членом нашей конъюнкции.

Легко понять, что формальное доказательство теоремы о делении с остатком, путь построения которого мы сейчас наметили, является попросту формализованной записью ее обычного доказательства. Так же обстоит дело и с основными фактами теории делимости. Понимая выражение $u/t$ как сокращенную запись формулы $\exists x(t = u\cdot x)$, нетрудно показать, что:

(36) $\vdash x/x$;

(37) $\vdash 1/x$;

(38) $\vdash x/0$;

(39) $\vdash y/x \& z/y \supset z/x$;

(40) $\vdash y/x \& x/y \supset x = y$;

(41) $\vdash y/x \supset y\cdot z/x\cdot z$;

(42) $\vdash y/x_1 \& y/x_2 \supset y/(x_1 + x_2)$;

(43) $\vdash y/x \& \neg(x = 0) \supset y \leq x$.

Доказательство утверждений (36) — (43) предоставляется читателю.

Теперь нетрудно было бы и любое утверждение, доказываемое в элементарных курсах теории чисел (см., например, [Бухштаб 1960]), записать в виде формулы исчисления Ar и построить соответствующее формальное доказательство.

7. Что можно сказать о моделях формальной арифметики? Поскольку в нашем распоряжении имеются обычные, «неформальные» натуральные числа, и мы умеем их складывать и умножать (причем мы постоянно пользуемся ими в самых разнообразных нематемати-

ческих задачах, в том числе чисто практических, и они нас никогда не подводят), мы можем рассмотреть интерпретацию множества формул исчисления Ar, в которой основным множеством является множество натуральных чисел и символам $=$, $0$, $'$, $+$, $\cdot$ отвечают соответственно равенство, нуль, прибавление единицы, сложение и умножение. Все аксиомы исчисления Ar превратятся в этой интерпретации в истинные предложения обычной арифметики, и, следовательно,— по теореме 5 из § 6.2[8] — она будет моделью исчисления Ar. Эту модель, ради которой и построено наше исчисление, мы будем называть *стандартной моделью* (или *стандартной интерпретацией*) исчисления Ar. Но единственна ли эта модель? Всякому, кто впервые знакомится с формальной арифметикой, хотелось бы, без сомнения, чтобы это было так, и на то же самое настраивает обычная пеановская арифметика, которая, как легко убедиться, имеет только одну нормальную модель (с точностью до изоморфизма)[9]. Действительно, в этой арифметике очевидной индукцией доказывается, что всякое натуральное число есть нуль с каким-то количеством штрихов или без них, и поэтому, если $E_1$, $E_2$ — основные множества двух нормальных моделей пеановской арифметики и $0_1$, $0_2$ — их нули, то отображение, сопоставляющее произвольному элементу $0_1^{\prime\prime\ldots\prime} \in E_1$ элемент $E_2$, представляющий собой $0_2$ с тем же числом штрихов, оказывается биективным, и легко проверить, что оно изоморфно относительно операций, $'$, $+$ и $\cdot$. Однако для исчисления Ar такое доказательство не проходит (почему?), и можно показать, что если это исчисление непротиворечиво, то наряду со стандартной моделью оно должно иметь и другие нормальные модели, не изоморфные ей. Существование такой нестандартной модели мы докажем сейчас следующим несложным, хотя и довольно искусственным рассуждением. Добавим к алфавиту исчисления Ar новый символ предметной константы $c$ и к множеству аксиом — всевозможные формулы вида $\neg(n = c)$, где $n$ — произвольное натуральное число. Из непротиворечивости Ar вытекает непротиворечивость нового исчисления: если бы в нем существовало доказательство константы $\Lambda$, то, заменив в этом доказательстве все вхождения $c$ вхождениями некоторой не встречающейся в нем цифры $n_0$, мы получили бы вывод константы

[8] В этой теореме речь идет о множестве замкнутых формул, но, связав во всех аксиомах Ar все свободные переменные кванторами общности, мы, очевидно, получим равносильное исчисление. (Ср. сноску в конце пункта 4 § 6.3.)

[9] В курсах теории числовых систем говорят просто «имеет только одну модель», поскольку в обычной «неформальной» математике рассматриваются только нормальные модели. Пример ненормальной модели исчисления Ar см. в задаче 8 в конце этой главы.

$Л$ в Ar из некоторых формул вида $7(\boldsymbol{n} = \boldsymbol{n}_0)$, где $n \neq n_0$; но все такие формулы являются в Ar теоремами (см. выше утверждение 3), так что $Л$ оказалась бы доказуемой формулой и в Ar. Ввиду теоремы 2 из § 6.2 и теоремы 4 из § 6.3 новое исчисление имеет конечную или счетную нормальную модель, которая тем самым является и нормальной моделью исчисления Ar. Впрочем, конечной эта модель быть не может, т. к. всякая нормальная модель Ar бесконечна (в самом деле, по утверждению 3 для любых различных $m$ и $n$ имеем $\vdash 7(\boldsymbol{m} = \boldsymbol{n})$, и потому — см. § 6.3, пункт 6 — в любой нормальной модели Ar цифрам $\boldsymbol{m}$ и $\boldsymbol{n}$ отвечают различные элементы). В то же время, если бы существовало изоморфное отображение $\Psi$ этой модели на стандартную, то для любого натурального $n$ было бы $\Psi(\widetilde{n}) = n$, где $\widetilde{n}$ — элемент новой модели, отвечающий цифре $\boldsymbol{n}$[10]; но если $\gamma$ — элемент, отвечающий символу $c$, то $\gamma \neq \widetilde{n}$, каково бы ни было $n$, и поэтому $\Psi(\gamma)$ не равно никакому натуральному числу $n$, вопреки определению стандартной модели.

Таким образом, хотя в исчислении Ar, как мы видели выше (см. конец предыдущего пункта), можно вывести все теоремы, доказываемые в элементарных учебниках теории чисел, не говоря уже о школьных учебниках арифметики[11], это исчисление не дает идеальной формализации обычной арифметики натуральных чисел. Далее мы увидим, что и стандартную модель оно описывает не идеально, и что ее неполная адекватность своему прототипу не может быть «исправлена» добавлением каких-то аксиом, т. к. имеет глубокие причины, коренящиеся в самой природе формальных моделей как таковых. Но сначала нам придется рассмотреть ряд технических вопросов, к чему мы сейчас и перейдем.

[10] Поскольку, с одной стороны, цифре $\boldsymbol{n}$ отвечает в стандартной модели число $n$, с другой — при любом изоморфном соответствии между двумя моделями Ar элементы, отвечающие в этих моделях одной и той же цифре, должны соответствовать друг другу.

[11] Это не относится к тем теоретико-числовым теоремам, для которых известны лишь доказательства с использованием методов теории функций комплексного переменного.

## § 8.2. ПРЕДСТАВЛЕНИЕ В ФОРМАЛЬНОЙ АРИФМЕТИКЕ ПРЕДИКАТОВ И ФУНКЦИЙ

1. Пусть $\mathfrak{A} = \mathfrak{A}(x_1, ..., x_n)$ — формула исчисления Ar, не содержащая свободных переменных, отличных от $x_1, ..., x_n$, и $\Psi(x_1, ..., x_n)$ — $n$-местный предикат, определенный на натуральном ряде. Мы будем говорить, что формула $\mathfrak{A}$ *представляет предикат* $\Psi$, если для любых $n$ натуральных чисел $k_1, ..., k_n$:

(1) $\vdash \mathfrak{A}(\boldsymbol{k}_1, ..., \boldsymbol{k}_n)$, если $\Psi(k_1, ..., k_n) \equiv И$;

(2) $\vdash \neg\mathfrak{A}(\boldsymbol{k}_1, ..., \boldsymbol{k}_n)$, если $\Psi(k_1, ..., k_n) \equiv Л$.

Будем говорить также, что формула $\mathfrak{A}(x_1, ..., x_n, x_{n+1})$ того же исчисления, не содержащая свободных переменных, отличных от $x_1, ..., x_{n+1}$, *представляет* всюду определенную числовую *функцию*[12], если для любых натуральных $k_1, ..., k_n$:

(3) $\vdash \exists! x_{n+1}\mathfrak{A}(\boldsymbol{k}_1, ..., \boldsymbol{k}_n, x_{n+1})$;

(4) $\vdash \mathfrak{A}(\boldsymbol{k}_1, ..., \boldsymbol{k}_n, \boldsymbol{l})$, где $l = f(k_1, ..., k_n)$.

Если для некоторого предиката или функции существует представляющая формула, мы будем называть этот предикат (функцию) *представимым (-ой) в формальной арифметике.*

Замечание. Условие (3) можно заменить условием

(3′) $\vdash \forall y(\mathfrak{A}(\boldsymbol{k}_1, ..., \boldsymbol{k}_n, y) \supset y = \boldsymbol{l})$, где $l = f(k_1, ..., k_n)$.

В самом деле: из (4) и (3′) по ВК и В∃ получается

$$\exists x_{n+1}(\mathfrak{A}(\boldsymbol{k}_1, ..., \boldsymbol{k}_n, x_{n+1}) \,\&\, \forall y(\mathfrak{A}(\boldsymbol{k}_1, ..., \boldsymbol{k}_n, y) \supset y = x_{n+1})),$$

а это и есть (3); с другой стороны, чтобы вывести (3′) из (3) и (4), достаточно вывести противоречие из (3), (4) и дополнительной гипотезы $\exists y(\mathfrak{A}(\boldsymbol{k}_1, ..., \boldsymbol{k}_n, y) \& \neg(y = \boldsymbol{l}))$, где $l = f(k_1, ..., k_n)$, но из этой гипотезы и из (4) очевидным образом выводится

$$\exists y \exists z(\mathfrak{A}(\boldsymbol{k}_1, ..., \boldsymbol{k}_n, y) \& \mathfrak{A}(\boldsymbol{k}_1, ..., \boldsymbol{k}_n, z) \& \neg(y = z)).$$

[12] Мы называем функцию *числовой*, если она отображает некоторое подмножество натурального ряда или какой-то его декартовой степени в натуральный ряд (ср. с. 295).

в то время как из (3) легко вывести формулу

$$\forall y \forall z(\mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, y) \& \mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, z) \supset y = z).$$

**Примеры.** 1) Предикат $x_1 = x_2$ представляется формулой $x_1 = x_2$. Действительно, если $k_1 = k_2$, то цифры $\boldsymbol{k}_1$ и $\boldsymbol{k}_2$ совпадают, и $\vdash \boldsymbol{k}_1 = \boldsymbol{k}_2$ по аксиоме $(r)$, а если $k_1 \neq k_2$, то $\vdash \neg(\boldsymbol{k}_1 = \boldsymbol{k}_2)$ по утверждению 3 предыдущего параграфа.

2) Аналогичным образом легко доказать, что формула $\neg(x_1 = x_2)$ представляет предикат $x_1 \neq x_2$.

3) Предикат $x_1 < x_2$ представляется формулой $x_1 < x_2$: при $k_1 < k_2$ по утверждению 2 предыдущего параграфа имеем $\vdash \boldsymbol{k}_1 < \boldsymbol{k}_2$, а при $k_1 \geq k_2$ либо $k_1$ и $k_2$ совпадают, откуда $\vdash \neg(\boldsymbol{k}_1 < \boldsymbol{k}_2)$ ввиду (19) из того же параграфа, либо $\vdash \boldsymbol{k}_2 < \boldsymbol{k}_1$, откуда $\vdash \neg(\boldsymbol{k}_1 < \boldsymbol{k}_2)$ ввиду (20).

4) Все исходные п. р. ф. (см. § 7.8) представимы в формальной арифметике. Именно:

*(i)* функция $0(x_1)$ представляется формулой $x_2 = 0$. В самом деле, ввиду аксиомы $(r)$ имеем $\vdash 0 = 0 \& \forall y(y = 0 \supset y = 0)$, откуда с помощью B∃ получается $\vdash \exists! x_2(x_2 = 0)$, а формула $\mathfrak{A}(\boldsymbol{k}_1, \boldsymbol{l})$ из условия (4) для любого $k_1$ имеет вид $\boldsymbol{0} = \boldsymbol{0}$ и доказуема также ввиду $(r)$.

*(ii)* Функция $S(x_1) = x_1 + 1$ представляется формулой $x_2 = x_1'$, поскольку, с одной стороны, справедливо $\vdash \exists! x_2(x_2 = x_1')$ или, подробнее, $\vdash \exists x_2(x_2 = x_1' \& \forall y(y = x_1' \supset y = x_2))$ (это получается по правилу B∃ из очевидного утверждения $\vdash x_1' = x_1' \& \forall y(y = x_1' \supset y = x_1')$), с другой — для любого $k_1$ имеет место $\vdash \boldsymbol{k}_1' = \boldsymbol{k}_1'$.

*(iii)* Теперь читатель легко убедится, что функция $e^n_r(x_1, \ldots, x_n)$ представляется формулой $x_{n+1} = x_r$.

Лемма. Предикат тогда и только тогда представим в формальной арифметике, когда представима его характеристическая функция.

Доказательство. Если формула $\mathfrak{A}(x_1, \ldots, x_n)$ представляет предикат $F(x_1, \ldots, x_n)$, то функция $\chi_F$ представляется формулой $\mathfrak{A}(x_1, \ldots, x_n) \& x_{n+1} = 1 \vee \neg\mathfrak{A}(x_1, \ldots, x_n) \& x_{n+1} = 0$. Обратно, если формула $\mathfrak{B}(x_1, \ldots, x_n, x_{n+1})$ представляет функцию $\chi_F$, то предикат $F$ представляется формулой $\mathfrak{B}(x_1, \ldots, x_n, 1)$. Подробности читатель восстановит сам.

Задачи. 1) Доказать, что функции $x_1 + x_2$, $x_1 \cdot x_2$, $|x_1 - x_2|$ представимы в формальной арифметике.

2) Доказать, что если предикаты $F$ и $G$ представимы в формальной арифметике, то представимы и предикаты $F \& G$, $F \vee G$, $F \supset G$, $\neg F$.

3) Доказать, что если функция $f(x_1, \ldots, x_n)$ представима в формальной арифметике, то представим и предикат $F(x_1, \ldots, x_{n+1}) \equiv x_{n+1} = f(x_1, \ldots, x_n)$.

2. В дальнейшем нам понадобится

**Теорема.** Всякая общерекурсивная функция представима в формальной арифметике[13].

**Доказательство.** Мы уже знаем (см. выше пример 4), что в формальной арифметике представимы все исходные п. р. ф. Поэтому достаточно установить, что операторы подстановки, рекурсии и минимизации сохраняют свойство представимости в формальной арифметике (последний — в случае, когда результат его применения есть всюду определенная функция).

Для подстановки и минимизации это делается довольно просто. Пусть $n$-местные функции $f_1, \ldots, f_m$ и $m$-местная функция $g$ представляются соответственно формулами $\mathfrak{A}_1 = \mathfrak{A}_1(x_1, \ldots, x_{n+1}), \ldots, \mathfrak{A}_m = \mathfrak{A}_m(x_1, \ldots, x_{n+1})$, $\mathfrak{B} = \mathfrak{B}(x_1, \ldots, x_{m+1})$. Тогда нетрудно убедиться, что функция $h$, получаемая из $f_1, \ldots, f_m, g$ подстановкой, представляется формулой $\mathfrak{C} = \mathfrak{C}(x_1, \ldots, x_{n+1}) = \exists y_1 \cdots \exists y_m | \mathfrak{A}_1(x_1, \ldots, x_n, y_1) \& \ldots \& \mathfrak{A}_m(x_1, \ldots, x_n, y_m) \& \mathfrak{B}(y_1, \ldots, y_m, x_{n+1}) |$.

В самом деле: (а) условие (4) для формулы $\mathfrak{C}$ выводится из соответствующих условий для $\mathfrak{A}_1, \ldots, \mathfrak{A}_m, \mathfrak{B}$ с помощью правил ВК и В$\exists$: (б) присоединив к условиям (3′) для $\mathfrak{A}_1, \ldots, \mathfrak{A}_m, \mathfrak{B}$ в качестве дополнительной гипотезы формулу, отличающуюся от формулы $\mathfrak{C}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, x_{n+1})$ отсутствием приставки $\exists y_1 \cdots \exists y_m$, нетрудно вывести равенство $x_{n+1} = \boldsymbol{l}$, где $l = h(k_1, \ldots, k_n)$, после чего очевидным образом — с помощью У$\exists$, ВИ и В$\forall$ — получается вывод условия (3′) для $\mathfrak{C}$ из соответствующих условий для $\mathfrak{A}_1, \ldots, \mathfrak{A}_m, \mathfrak{B}$.

Далее, если предикат $F(x_1, \cdots, x_n, x_{n+1})$ представляется формулой $\mathfrak{A} = \mathfrak{A}(x_1, \ldots, x_n, x_{n+1})$ и функция $f(x_1, \ldots, x_n) = \mu x_{n+1} F(x_1, \ldots, x_n, x_{n+1})$ всюду определена, то эта функция представляется формулой $\mathfrak{B} = \mathfrak{B}(x_1, \ldots, x_n, x_{n+1}) = \mathfrak{A}(x_1, \ldots, x_n, x_{n+1}) \& \forall y (y < x_{n+1} \supset \neg \mathfrak{A}(x_1, \ldots, x_n, y))$. Действительно, пусть $k_1, \ldots, k_n$ — произвольные натуральные числа, и $f(k_1, \ldots, k_n) = l$. Тогда, чтобы получить условие (4) для формулы $\mathfrak{B}$, достаточно доказать, что $(i) \vdash \mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, \boldsymbol{l})$ и $(ii) \vdash \forall y (y < \boldsymbol{l} \supset \neg \mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, y))$. Но $(i)$ есть условие (1) для $\mathfrak{A}$, а $(ii)$ при $l = 0$ получается из (23) предыдущего параграфа и при $l = j + 1$ из утверждения 4 того же параграфа и условия (2) для $\mathfrak{A}$. С другой стороны, из

[13] В следующем параграфе мы убедимся, что если формальная арифметика непротиворечива, то справедливо и утверждение, обратное этой теореме.

того же (*ii*) легко получить (*iii*) $\vdash y < \boldsymbol{l} \supset 7\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, y)$ и в то же время $\vdash y > \boldsymbol{l} \supset \exists z(z < y \& \mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, z))$ (ввиду условия (1) для $\mathfrak{A}$), откуда очевидным образом получается $\vdash y > \boldsymbol{l} \supset 7\forall z(z < y \supset \supset 7\mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, z))$ и далее (*iv*) $\vdash y > \boldsymbol{l} \supset 7\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, y)$. Но из (*iii*) и (*iv*) ввиду (22) из предыдущего параграфа вытекает $\vdash 7(y = \boldsymbol{l}) \supset \supset 7\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, y)$, а отсюда с помощью контрапозиции и $B\forall$ выводится условие (3′) для $\mathfrak{B}$.

Переходя к оператору рекурсии, рассмотрим сначала *β-функцию Гёделя*: $\beta(x_1, x_2, x_3) = r(x_2 \cdot (x_3 + 1) + 1, x_1)$. ($r(x, y)$ — остаток от деления $y$ на $x$, см. с. 332). Эта функция — очевидно, примитивно рекурсивная — обладает следующим замечательным свойством: какова бы ни была конечная последовательность натуральных чисел $k_0, k_1, \ldots, k_n$, найдутся такие натуральные $a$ и $b$, что $\beta(a, b, i) = k_i$ для каждого $i = 0, \ldots, n$. Доказательство этого свойства основывается на так называемой *китайской теореме об остатках*[14]: для любых попарно взаимно простых натуральных чисел $m_1, \ldots, m_k$ и любых $k$ натуральных чисел $c_1, \ldots, c_k$ существует такое натуральное число $x$, что $x \equiv c_i \pmod{m_i}$ для каждого $i = 1, \ldots, k$. Именно, положим: $\max(n, k_0, \ldots, k_n) = N$; $N! = b$; $b \cdot (i + 1) + 1 = z_i$ $(i = 0, \ldots, n)$. Числа $z_i$ попарно взаимно просты. В самом деле, если бы нашлись такие $i_1, i_2$, $0 \leq i_1 < i_2 \leq n$, и такое простое число $p$, что $z_{i_1}$ и $z_{i_2}$ делились бы на $p$, то на $p$ делилась бы и разность $z_{i_2} - z_{i_1} = b(i_2 - i_1)$ и, следовательно, поскольку $b$ делится на $i_2 - i_1$, число $p$ было бы делителем числа $b$; но тогда разность $z_{i_1} - b(i_1 + 1) = 1$ также делилась бы на $p$. По китайской теореме об остатках найдется такое $a$, что для каждого $i = 0, \ldots, n$ число $k_i$ сравнимо с $a$ по модулю $z_i$, а это, поскольку $k_i < z_i$, означает, что $r(z_i, a) = k_i$. Но $r(z_i, a) = r(b \cdot (i + 1) + 1, a) = \beta(a, b, i)$.

Нетрудно доказать также, что функция $\beta$ представима в формальной арифметике. Представляющей формулой для нее служит

$$\mathfrak{G}(x_1, x_2, x_3, x_4) = \exists y[x_1 = (x_2 \cdot (x_3 + 1) + 1) \cdot y + x_4 \&$$

$$\& x_4 < x_2 \cdot (x_3 + 1) + 1].$$

[14] Доказательство этой теоремы можно найти в любом учебнике теории чисел (см., например, [Бухштаб 1960]). «Китайской теоремой об остатках» ее называют потому, что соответствующая задача впервые встречается в трактате древнекитайского математика Сунь-цзы (III в. н.э.) в следующей форме: «Имеются вещи, число их неизвестно. Если считать их тройками, то остаток 2, если считать их пятерками, то остаток 3, если считать их семерками, то остаток 2. Спрашивается, сколько вещей?» (См. [Березкина 1980], с. 186.)

Действительно: если $\beta(k_1, k_2, k_3) = k_4$, то $(i) k_4 < k_2 \cdot (k_3 + 1) + 1$ и найдется такое $k_5$, что $(ii) k_1 = (k_2 \cdot (k_3 + 1) + 1) k_5 + k_4$; из $(i)$ и $(ii)$ ввиду утверждений 1 и 2 предыдущего параграфа следует $(iii) \vdash \boldsymbol{k}_4 < \boldsymbol{k}_2 \cdot (\boldsymbol{k}_3 + 1) + 1$ и $(iv) \vdash \boldsymbol{k}_1 = (\boldsymbol{k}_2 \cdot (\boldsymbol{k}_3 + 1) + 1) \cdot \boldsymbol{k}_5 + \boldsymbol{k}_4$; из $(iv)$ вытекает $(v) \vdash \exists y [\boldsymbol{k}_1 = (\boldsymbol{k}_2 \cdot (\boldsymbol{k}_3 + 1) + 1) \cdot y + \boldsymbol{k}_4]$, а из $(iii)$ и $(v)$ очевидным образом получается $\mathfrak{G}(\boldsymbol{k}_1, \boldsymbol{k}_2, \boldsymbol{k}_3, \boldsymbol{k}_4)$ (условие (4)). Что касается условия (3), то ввиду (35) из предыдущего параграфа формула $\mathfrak{G}$ удовлетворяет даже более сильному условию: $\vdash \exists! x_4 \mathfrak{G}(x_1, x_2, x_3, x_4)$ (оно понадобится нам в дальнейшем).

Доказанные свойства $\beta$-функции позволяют представлять в формальной арифметике предикаты, отвечающие утверждениям о конечных последовательных натуральных чиссл. Именно это и нужно, чтобы доказать, что оператор рекурсии сохраняет представимость: ведь при рекурсии каждое следующее значение функции определяется последовательностью предыдущих значений. Мы проведем доказательство для случая функции $n$ переменных при $n > 1$; для $n = 1$ доказательство проводится совершенно аналогично (с очевидными упрощениями).

Итак, пусть функция $f(x_1, \ldots, x_n)$ удовлетворяет рекурсивным равенствам

$$\begin{cases} f(x_1, \ldots, x_{n-1}, 0) = g(x_1, \ldots, x_{n-1}) \\ f(x_1, \ldots, x_{n-1}, x_n + 1) = h(x_1, \ldots, x_{n-1}, x_n, f(x_1, \ldots, x_n)). \end{cases}$$

и функции $g(x_1, \ldots, x_{n-1})$ и $h(x_1, \ldots, x_{n+1})$ представляются соответственно формулами $\mathfrak{A}(x_1, \ldots, x_n)$ и $\mathfrak{B}(x_1, \ldots, x_{n+2})$. Чтобы получить представляющую формулу для $f$, воспользуемся тем, что равенство $f(x_1, \ldots, x_{n-1}, x_n) = x_{n+1}$ справедливо тогда и только тогда, когда существует конечная последовательность $c_0, \ldots, c_{x_n}$, такая, что $c_0 = g(x_1, \ldots, x_{n-1})$, $c_{x_n} = x_{n+1}$ и $c_{i+1} = h(x_1, \ldots, x_{n-1}, i, c_i)$ для каждого $i = 0, \ldots, x_n - 1$, а это, в свою очередь, равносильно существованию таких $a$ и $b$, что $\beta(a, b, 0) = g(x_1, \ldots, x_{n-1})$, $\beta(a, b, x_n) = x_{n+1}$ и для каждого $i = 0, \ldots, x_n - 1$ выполняется равенство $\beta(a, b, i + 1) = h(x_1, \ldots, x_{n-1}, i, \beta(a, b, i))$. Таким образом мы приходим к формуле

$$\mathfrak{C} = \mathfrak{C}(x_1, \ldots, x_{n+1}) = \exists y_1 \exists y_2 [\exists z_1 (\mathfrak{G}(y_1, y_2, 0, z_1) \,\&$$

$$\& \, \mathfrak{A}(x_1, \ldots, x_{n-1}, z_1)) \& \mathfrak{G}(y_1, y_2, x_n, x_{n+1}) \& \forall z (z < x_n \supset$$

$$\supset \exists z_2 \exists z_3 (\mathfrak{G}(y_1, y_2, z, z_2) \& \mathfrak{G}(y_1, y_2, z', z_3) \,\&$$

$$\& \, \mathfrak{B}(x_1, \ldots, x_{n-1}, z, z_2, z_3))) ].$$

Докажем, что эта формула в самом деле представляет функцию $f$. Пусть $f(k_1, \ldots, k_n) = l$. Будем обозначать выражение, стоящее в формуле $\mathfrak{E}$ в квадратных скобках, через $\mathfrak{D}$ или $\mathfrak{D}(y_1, y_2, x_1, \ldots, x_{n+1})$; положим также $f(k_1, \ldots, k_{n-1}, i) = l_i$ $(i = 0, \ldots, k_n)$ (так что $l_{k_n} = l$). Пусть $a$ и $b$ — числа, для которых $\mathfrak{Z}(a, b, i) = l_i$ при любом $i = 0, \ldots, k_n$. Чтобы доказать $\vdash \mathfrak{E}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, \boldsymbol{l})$ (условие (4) для функции $\mathfrak{E}$), достаточно проверить, что $\vdash \mathfrak{D}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, \boldsymbol{l})$, а для этого, в свою очередь, достаточно установить доказуемость каждого из трех конъюнктивных членов последней формулы в отдельности. Доказуемость первого члена следует из $\mathfrak{G}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{0}, \boldsymbol{l}_0)$ (условие (4) для $\mathfrak{G}$) и $\mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{l}_0)$ (условие (4) для $\mathfrak{A}$). Второй член есть $\mathfrak{G}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{k}_n, \boldsymbol{l})$; его доказуемость следует из условия (4) для $\mathfrak{G}$. Чтобы установить доказуемость третьего члена, достаточно установить доказуемость его подкванторного выражения, представляющего собой импликацию с посылкой $z < \boldsymbol{k}_n$; эта последняя цель — ввиду утверждения 4 предыдущего параграфа и правил УД и ВИ — будет достигнута, если мы покажем, что для любого $i < k_n$ имеет место выводимость $z = \boldsymbol{i} \vdash \mathfrak{E}$, где $\mathfrak{E}$ — заключение упомянутой импликации. Пусть теперь $\tilde{\mathfrak{E}}$ — формула, полученная из подкванторного выражения формулы $\mathfrak{E}$ заменой переменных $z$, $z_2$, $z_3$ цифрами $\boldsymbol{i}$, $\boldsymbol{l}_i$, $\boldsymbol{l}_{i+1}$ соответственно. Ввиду правила В$\exists$ и того факта, что наше исчисление Ar есть исчисление на основе $G_1$ с равенством, для доказательства выводимости $z = \boldsymbol{i} \vdash \mathfrak{E}$ достаточно установить, что формула $\tilde{\mathfrak{E}}$ доказуема. Но $\tilde{\mathfrak{E}} = \mathfrak{G}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{i}, \boldsymbol{l}_i) \& \mathfrak{G}(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{i}+1, \boldsymbol{l}_{i+1}) \& \mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, \boldsymbol{l}_i, \boldsymbol{l}_{i+1})$; первые два члена этой конъюнкции доказуемы в силу условия (4) для $\mathfrak{G}$, третий — в силу того же условия для $\mathfrak{B}$.

Остается доказать, что формула $\mathfrak{E}$ удовлетворяет условию (3′). Мы докажем это (неформальной) индукцией по числу $k_n$, которое для большего удобства будем обозначать $i$. Итак, мы докажем индукцией по $i$, что формула $\mathfrak{E}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, z) \supset z = \boldsymbol{l}_i$, где $l_i = f(k_1, \ldots, k_{n-1}, i)$, является теоремой.

Базис. Легко показать (это предоставляется читателю) что трехчленная конъюнкция $\mathfrak{D}(y_1, y_2, \boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{0}, z)$ дедуктивно эквивалентна конъюнкции двух своих первых членов. Отсюда по теореме о замене дедуктивно эквивалентных формул следует, что формула $\mathfrak{E}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{0}, z) \supset z = \boldsymbol{l}_0$ дедуктивно эквивалентна формуле $\exists y_1 \exists y_2 [\exists z_1 (\mathfrak{G}(y_1, y_2, 0, z_1) \& \mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, z_1)) \& \mathfrak{G}(y_1, y_2, 0, z)] \supset z = \boldsymbol{l}_0$, так что достаточно установить доказуемость этой последней. Но ввиду условия (3′) для формулы $\mathfrak{A}$ имеем $\mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, z_1) \vdash z_1 = \boldsymbol{l}_0$ и тем более $\mathfrak{G}(y_1, y_2, 0, z_1) \& \mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, z_1) \& \mathfrak{G}(y_1, y_2, 0, z) \vdash z_1 = \boldsymbol{l}_0$.

В то же время ввиду условия (3) для $\mathfrak{G}$ справедливо $\mathfrak{G}(y_1, y_2, 0, z_1)\&\mathfrak{G}(y_1, y_2, 0, z) \vdash z = z_1$. Отсюда $\mathfrak{G}(y_1, y_2, 0, z_1)\&\mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, z_1)\&\mathfrak{G}(y_1, y_2, 0, z) \vdash z = \boldsymbol{l}_0$. В последней выводимости левую часть можно связать квантором существования по $z_1$ (правило У$\exists$), из-под которого можно затем вынести $\mathfrak{G}(y_1, y_2, 0, z)$ (по (11) из § 6.1), после чего, применив еще два раза У$\exists$, получаем $\exists y_1 \exists y_2 | \exists z_1(\mathfrak{G}(y_1, y_2, 0, z_1)\&\mathfrak{A}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, z_1))\&\mathfrak{G}(y_1, y_2, 0, z) | \vdash z = \boldsymbol{l}_0$; остается применить ВИ.

Индукционный шаг. Пусть $\vdash \mathfrak{C}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, z) \supset z = \boldsymbol{l}_i$, или, что то же самое, $\mathfrak{C}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, z) \vdash z = \boldsymbol{l}_i$. Покажем, что в этом случае $\mathfrak{C}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}+1, z) \vdash z = \boldsymbol{l}_{i+1}$. Сначала докажем, что $\mathfrak{C}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}+1, z) \vdash \exists w(\mathfrak{C}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, w)\&\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, w, z))$. Для произвольного натурального числа $j$ и произвольного терма $t$ будем обозначать через $\mathfrak{D}_j(t)$ формулу $\mathfrak{D}(y_1, y_2, \boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{j}, t)$. Ввиду утверждения 2 предыдущего параграфа $\vdash \boldsymbol{i} < \boldsymbol{i}+1$; поэтому из третьего конъюнктивного члена формулы $\mathfrak{D}_{i+1}(z)$ и тем более из самой этой формулы выводима формула $\exists w \exists w_1(\mathfrak{G}(y_1, y_2, \boldsymbol{i}, w)\&\mathfrak{G}(y_1, y_2, \boldsymbol{i}+1, w_1)\&\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, w, w_1))$ и, следовательно, также $\exists w_1 | \mathfrak{G}(y_1, y_2, \boldsymbol{i}+1, w_1)\&\exists w(\mathfrak{G}(y_1, y_2, \boldsymbol{i}, w)\&\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, w, w_1)) |$, а из этой последней формулы и формулы $\mathfrak{G}(y_1, y_2, \boldsymbol{i}+1, z)$, являющейся вторым конъюнктивным членом формулы $\mathfrak{D}_{i+1}(z)$, можно, принимая во внимание, что $\vdash \exists! x \mathfrak{G}(y_1, y_2, \boldsymbol{i}+1, x)$ (усиленное условие (3) для $\mathfrak{G}$, см. выше, с. 377) вывести формулу $\exists w(\mathfrak{G}(y_1, y_2, \boldsymbol{i}, w)\&\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, w, z))$. [Действительно, в любом исчислении на основе $G_1$ с равенством для любых формул $\mathfrak{M}$ и $\mathfrak{N}$ справедлива выводимость $\mathfrak{M}(y), \exists z(\mathfrak{M}(z)\&\mathfrak{N}(z)), \exists! x \mathfrak{M}(x) \vdash \mathfrak{N}(y)$, где $x$, $y$, $z$ — переменные, свободные для подстановки вместо друг друга в $\mathfrak{M}$ и $\mathfrak{N}$; доказательство предоставляется читателю в качестве упражнения.] Таким образом, $\mathfrak{D}_{i+1}(z) \vdash \exists w(\mathfrak{G}(y_1, y_2, \boldsymbol{i}, w)\&\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, w, z))$. Далее, т. к. первые конъюнктивные члены формул $\mathfrak{D}_i(w)$ и $\mathfrak{D}_{i+1}(z)$ совпадают, а из третьего члена $\mathfrak{D}_{i+1}(z)$ выводится третий член $\mathfrak{D}_i(w)$ (ввиду утверждения 2 и соотношения (21) из предыдущего параграфа), имеем $\mathfrak{D}_{i+1}(z) \vdash \mathfrak{Q}\&\exists w(\mathfrak{G}(y_1, y_2, \boldsymbol{i}, w)\&\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, w, z))$, где $\mathfrak{Q}$ — конъюнкция первого и третьего членов $\mathfrak{D}_i(w)$; из правой части этой выводимости, внося $\mathfrak{Q}$ под квантор, можно вывести $\exists w(\mathfrak{D}_i(w)\&\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, w, z))$. Отсюда, пользуясь правилами В$\exists$ и У$\exists$, получаем $\exists y_1 \exists y_2 \mathfrak{D}_{i+1}(z) \vdash \exists y_1 \exists y_2 \exists w(\mathfrak{D}_i(w)\&\mathfrak{B}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}, w, z))$. Но левая часть последней выводимости есть как раз $\mathfrak{C}(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n-1}, \boldsymbol{i}+1, z)$, а из правой легко вывести

$\exists w(\mathfrak{C}(k_1, \ldots, k_{n-1}, i, w)\&\mathfrak{B}(k_1, \ldots, k_{n-1}, i, w, z))$.

Теперь уже нетрудно завершить индукционный шаг. Используя замечание, сделанное выше в квадратных скобках, мы видим, что $\exists w(\mathfrak{C}(k_1, \ldots, k_{n-1}, i, w)\&\mathfrak{B}(k_1, \ldots, k_{n-1}, i, w, z))$, $\mathfrak{C}(k_1, \ldots, k_{n-1}, i, l_i)$, $\exists! y\mathfrak{C}(k_1, \ldots, k_{n-1}, i, y) \vdash \mathfrak{B}(k_1, \ldots, k_{n-1}, i, l_i, z)$. Но в левой части этой выводимости первая формула выводится, как мы только что доказали, из $\mathfrak{C}(k_1, \ldots, k_{n-1}, i+1, z)$, а остальные две являются теоремами (вторая — ввиду уже доказанного условия (4) для $\mathfrak{C}$, третья — ввиду того же условия и предположения индукции). Поэтому $\mathfrak{C}(k_1, \ldots, k_{n-1}, i+1, z) \vdash \mathfrak{B}(k_1, \ldots, k_{n-1}, i, l_i, z)$; однако по условию (3') для формулы $\mathfrak{B}$ имеем $\mathfrak{B}(k_1, \ldots, k_{n-1}, i, l_i, z) \vdash z = l_{i+1}$. Этим завершается индукционный шаг, а тем самым и доказательство теоремы.

Вспоминая лемму, доказанную в начале параграфа, непосредственно получаем

Следствие. Всякий рекурсивный предикат представим в формальной арифметике.

## § 8.3. АРИФМЕТИЗАЦИЯ ВЫВОДОВ

1. Сейчас мы занумеруем формулы и деревья выводов в исчислении Ar аналогично тому, как это было сделано в §§ 7.7 и 7.9 для машин Тьюринга и тьюринговых вычислений. Как и там, нумерация будет основана на использовании представления чисел в системе счисления без нуля.

Будем кодировать слова в алфавите исчисления Ar словами в алфавите $\{a_1, \ldots, a_{20}\}$ следующим образом (ср. кодирование машин Тьюринга в § 7.5): *кодом переменной* $x_n$ будет слово $a_1^n$; *кодами символов* 0, =, ′, +, ·, &, ∨, ⊃, ¬, $\Lambda$, ∀, ∃, (,), , — символы $a_2, \ldots, a_{16}$ соответственно[15]; *кодом слова* $\alpha_1 \cdots \alpha_s$, где $\alpha_i$ — элементарные символы, будет слово $\varkappa(\alpha_1) \cdots \varkappa(\alpha_s)$, где $\varkappa(\alpha_i)$ — код символа $\alpha_i$; *кодом пустого слова* будет оно само.

Стандартный номер (см. начало § 7.7) кода слова в алфавите Ar будет называться просто *номером* этого слова. Как и в §§ 7.7, 7.9, мы часто будем отождествлять номер слова с его кодом и вместо $a_1$, $a_2$ и т. д. будем иногда писать 1, 2 и т. д.

[15] Символы $a_{17}, \ldots, a_{20}$ понадобятся нам ниже для кодирования выводов.

Далее нам понадобятся некоторые функции и предикаты, определенные при доказательстве основной леммы в § 7.9 и являющиеся, как было установлено там же, примитивно рекурсивными[16]. Точнее, мы будем пользоваться только первыми одиннадцатью введенными там (на с. 346—347) функциями и предикатами, т. е. теми, которые относятся только к свойствам чисел (или слов) как таковых, а не нумеруемых объектов. К этим функциям и предикатам мы присоединим некоторые другие и докажем, что они также примитивно рекурсивны. Как и в § 7.9, функции обычно будут обозначаться сочетаниями строчных русских букв, предикаты — прописных. (Но иногда будут использоваться латинские и греческие буквы.)

1) ПЕР($x$) — «$x$ есть номер переменной».

$$\text{ПЕР}(x) \equiv \neg(x = 0)\&\underset{z\le x}{\neg\exists} z\ (\text{ВХОД}(x, z)\&(z = 2\vee\dots\vee z = 20)).$$

(Здесь перечислены все «цифры» нашей системы счисления, кроме единицы, служащей для кодирования переменных.)

2) КВТ($x$) — «$x$ есть номер "квазитерма", т. е. выражения, которое либо есть переменная или символ 0, либо имеет вид $+(u, v)$, или $\cdot(u, v)$, или $(u)'$, где $u$, $v$ — произвольные слова[17].»

Чтобы доказать, что этот предикат примитивно рекурсивен, введем следующие вспомогательные функции $a_1(u, v)$, $a_2(u, v)$, $b(u)$: произвольным словам $u$, $v$ (отождествляемым с их номерами) функция $a_1$ сопоставляет слово $+(u, v)$ (отождествляемое с его номером), а функция $a_2$ — слово $\cdot(u, v)$; функция $b$ произвольному слову $u$ сопоставляет номер слова $'(u)$. Примитивная рекурсивность этих функций очевидна.

Теперь определение предиката КВТ можно записать так:

$$\text{КВТ}(x) \equiv \text{ПЕР}(x)\vee x = 2\vee\underset{u\le x}{\exists u}\ \underset{v\le x}{\exists v}(x = a_1(u, v)\vee x = a_2(u, v))\vee$$

$$\vee\underset{u\le x}{\exists u}(x = b(u)).$$

(Число 2 — номер символа 0.)

3) ТМ($x$) — «$x$ есть номер терма)»:

$$\text{ТМ}(x) \equiv \text{КВТ}(x)\&\underset{z\le x}{\forall z}(\text{ВХОД}(x, z)\&\text{КВТ}(z)\supset\text{ПЕР}(z)\vee z =$$

$$= 2\vee\underset{u\le z\,v\le z}{\exists u\exists v}(z = a_1(u, v)\vee z = a_2(u, v))\vee\underset{u\le z}{\exists u}(z = b(u))).$$

[16] Тот факт, что сейчас мы пользуемся двадцатеричной системой счисления вместо девятеричной, не имеет, разумеется, никакого значения.

[17] Напомним, что обозначениями $u + v$, $u \cdot v$, $u'$ мы пользуемся лишь для удобства чтения вместо $+(u, v)$, $\cdot(u, v)$, $'(u)$.

Это представление основано на том очевидном факте, что слово является термом тогда и только тогда, когда, во-первых, оно есть квазитерм, и, во-вторых, непосредственные составляющие любого входящего в него неэлементарного квазитерма — тоже квазитермы.)

4) Аналогичным образом нетрудно доказать примитивную рекурсивность предиката ФМ$(x)$ — «$x$ есть номер формулы».

5) цф$(n)$ — функция, сопоставляющая натуральному числу $n$ номер цифры $\boldsymbol{n}$:

$$\begin{cases} \text{цф}(0) = 2 \\ \text{цф}(n+1) = b(\text{цф}(n)). \end{cases}$$

(Здесь $b$ — функция, введенная перед определением предиката КВТ.)

Для дальнейшего нам понадобится теперь уточнить понятие вхождения. Именно, мы будем называть *вхождением слова $y$ в слово $x$* упорядоченную тройку слов (или чисел) $(u, y, v)$, такую, что $uyv = x$.

6) ОБЛКВ $(x, u, y, v, z)$ — «вхождение $(u, y, v)$ слова с номером $y$ в формулу с номером $x$ содержится в области действия квантора по переменной с номером $z$»:

$$\text{ОБЛКВ}(x, u, y, v, z) \equiv \text{ФМ}(x)\&\text{ПЕР}(z)\&$$

$$\&x = \text{произв}_3(u, y, v)\&\underset{u \le x}{\exists w}\ \underset{w_1 \le x}{\exists w_1}\ \underset{w_2 \le x}{\exists w_2}\ \underset{t_1 \le x}{\exists t_1}\ \underset{t_2 \le x}{\exists t_2}\ \underset{q \le x}{\exists q}$$

$$|x = \text{произв}_3(t_1, w, t_2)\&\text{ФМ}(w)\&w = \text{произв}_5(q, z, w_1, y, w_2)\&$$

$$\&(q = 12 \vee q = 13)\&u = \text{произв}_4(t_1, q, z, w_1)\&v = \text{произв}(w_2, t_2)|.$$

(Числа 12 и 13 — номера символов $\forall$ и $\exists$.)

7) СВВХ $(x, u, y, v)$ — «тройка слов с номерами $u$, $y$, $v$ представляет собой свободное вхождение переменной с номером $y$ в формулу с номером $x$»:

$$\text{СВВХ}(x, u, y, v) \equiv \text{ФМ}(x)\&\text{ПЕР}(y)\&x = \text{произв}_3(u, y, v)\&$$

$$\&\neg\text{ОБЛКВ}(x, u, y, v, y).$$

8) СВ$(x, y)$ — «переменная с номером $y$ входит свободно в формулу с номером $x$»:

$$\text{СВ}(x, y) \equiv \underset{u \le x}{\exists u}\ \underset{v \le x}{\exists v}\ \text{СВВХ}(x, u, y, v).$$

9) СВП$(x, y, z)$ — «терм с номером $z$ свободен для подстановки вместо переменной с номером $y$ в формулу с номером $x$»:

$$\text{СВП}(x, y, z) \equiv \text{ФМ}(x)\&\text{ПЕР}(y)\&\text{ТМ}(z)\&$$

$$\&\neg\exists_{u\le x}\,\exists_{v\le x}\,\exists_{w\le x}\,(\text{СВВХ}(x, u, y, v)\&$$

$$\&\,\text{ОБЛКВ}(x, u, y, v, w)\&\text{ВХОД}(z, w)).$$

10) зам$(x, y, z)$: если $x$ — номер формулы $\mathfrak{A}$, $y$ — номер переменной $x_i$ и $z$ — номер терма $t$, свободного для подстановки в $\mathfrak{A}$ вместо $x_i$, то зам$(x, y, z)$ — номер формулы $\mathfrak{A}^t_i$; в противном случае зам$(x, y, z) = 0$.

Чтобы доказать, что функция зам примитивно рекурсивна, докажем сначала примитивную рекурсивность трех вспомогательных функций:

$h_1(x, y, n)$ — номер начала формулы с номером $x$ до $n$-го свободного вхождения переменной с номером $y$ (если число таких вхождений меньше $n$, то $h_1(x, y, n) = x$; если $x$ — не номер формулы или $y$ — не номер переменной, то $h_1(x, y, n) = 0$):

$$h_1(x, y, 0) = 0$$

$$h_1(x, y, n+1) = \mu_{z\le x}\,[\text{ФМ}(x)\&\text{ПЕР}(y)\&\text{НАЧ}(z, h_1(x, y, n))\&$$

$$\&\neg(z = h_1(x, y, n))\&(\exists_{u\le x}\,\text{СВВХ}(x, z, y, u)\vee z = x)\&$$

$$\&\neg\exists_{v\le x}\,\exists_{w\le x}\,[\text{НАЧ}(v, h_1(x, y, n))\&\neg(v = h_1(x, y, n))\&$$

$$\&\,\text{НАЧ}(z, v)\&\neg(v = z)\&\text{СВВХ}(x, v, y, w)\,]].$$

$h_2(x, y, n)$ — номер куска формулы с номером $x$ между $n$-м и $n+1$-м свободными вхождениями переменной с номером $y$ (или конца формулы после $n$-го вхождения, если число таких вхождений равно $n$; если же их меньше $n$, а также если $x$ — не номер формулы или $y$ — не номер переменной, то $h_2(x, y, n) = 0$):

$$h_2(x, y, n) = \mu_{u\le x}\,[h_1(x, y, n+1) = \text{произв}_3(h_1(x, y, n), y, u)\,]].$$

$h_3(x, y, z, n)$ — номер результата замены в слове с номером $h_1(x, y, n)$ всех свободных вхождений[18] переменной с номером $y$ вхождениями терма с номером $z$, свободного для подстановки в формулу с

[18] Подразумеваются вхождения, свободные в формуле с номером $x$.

номером $x$ вместо переменной с номером $y$:

$$h_3(x, y, z, 0) = 0$$

$$h_3(x, y, z, n + 1) = \text{произв}_3(h_3(x, y, z, n),$$

$$z \cdot sg(x \dot{-} h_1(x, y, z, n)) \cdot h_2(x, y, n)) \cdot \text{свп}(x, y, z),$$

где свп — характеристическая функция предиката СВП.

Теперь ясно, что $\text{зам}(x, y, z) = h_3(x, y, z, \underset{n \le x}{\mu n}(h_1(x, y, n) = x))$.

11) $\text{зам}'_n(i, j_1, \ldots, j_n)$ $(n = 1, 2, \cdots)$: если $i$ — номер формулы $\mathfrak{A}(x_1, \ldots, x_n)$ (здесь $x_1, \ldots, x_n$, как всегда — не «метапеременные», а настоящие переменные!) и $j_1, \ldots, j_n$ — номера термов $t_1, \ldots, t_n$, свободных для подстановки в $\mathfrak{A}$ вместо $x_1, \ldots, x_n$ соответственно, то $\text{зам}'_n(i, j_1, \ldots, j_n)$ есть номер формулы $\mathfrak{A}(t_1, \ldots, t_n)$; в противном случае $\text{зам}'_n(i, j_1, \ldots, j_n) = 0$.

Примитивную рекурсивность этой функции можно доказать так. Используя функции $\text{новпер}'_n(y, z_1, \ldots, z_n)$ — номер $i$-й (в порядке возрастания номеров) переменной, не входящей в формулу с номером $y$ и в термы с номерами $z_1, \ldots, z_n$, — примитивная рекурсивность которой устанавливается без труда, легко доказать примитивную рекурсивность функций $\text{зам}''_n(i, j_1, \ldots, j_n)$, отличающихся от $\text{зам}'_n$ тем, что вместо $x_1, \ldots, x_n$ подставляются не термы $t_1, \ldots, t_n$, а первые (по порядку номеров) $n$ переменных, не входящих в формулу $\mathfrak{A}$ и в термы $t_1, \ldots, t_n$. Например, $\text{зам}''_2(i, j_1, j_2) = \text{зам}(\text{зам}(i, c_1, \text{новпер}'_2(i, j_1, j_2)), c_2, \text{новпер}'_2(i, j_1, j_2))$, где $c_1, c_2$ — номера переменных $x_1, x_2$. Далее, формулу с номером $\text{зам}'_n(i, j_1, \ldots, j_n)$ можно получить из формулы с номером $\text{зам}''_n(i, j_1, \ldots, j_n)$ путем $n$-кратной последовательной подстановки термов с номерами $j_1, \ldots, j_n$ вместо переменных с номерами $\text{новпер}'_n(i, j_1, \ldots, j_n), \ldots, \text{новпер}''_n(i, j_1, \ldots, j_n)$. Примитивную рекурсивность соответствующей функции доказать нетрудно. Подробности предоставляются читателю. (Он без труда поймет также, почему нельзя воспользоваться последовательной подстановкой непосредственно вместо $x_1, \ldots, x_n$.)

12) $\text{общ}(x, y)$, $\text{сущ}(x, y)$: если $x$ — номер формулы $\mathfrak{A}$ и $y$ — номер переменной $x_i$, то $\text{общ}(x, y)$ и $\text{сущ}(x, y)$ — номера формул $\forall x_i \mathfrak{A}$ и $\exists x_i \mathfrak{A}$ соответственно; в противном случае их значения равны нулю.

Примитивная рекурсивность этих функций очевидна.

2. Перейдем к кодированию и нумерации деревьев вывода. В кодах деревьев будут участвовать символы $a_{17}$, $a_{18}$, $a_{19}$, $a_{20}$, вместо которых мы для удобства будем писать соответственно $b$, $c$, $d$, $e$.

1) *Кодом элементарного дерева вывода* (дерева высоты 1) будет слово $ubv_1c\ldots v_kc$, где $u$ — код формулы, записанной в дереве под чертой, и $v_1, \ldots, v_k$ — коды формул, записанных над чертой (в том порядке, как они записаны); код дерева, отвечающего правилу ИТ, имеет вид $ubc$, где $u$ — код некоторой формулы вида $\mathfrak{A} \vee \neg\mathfrak{A}$.

2) Пусть $n > 1$ и для каждого дерева вывода высоты $< n$ определен код. Для произвольного слова $w$, содержащего вхождения символа $e$, будем обозначать через $r(w)$ наибольший конец $w$, начинающийся вхождением $e$ и не содержащий вхождений $b$, $c$, $d$; если таких концов нет, то $r(w)$ — пустое слово. Пусть теперь: $D$ — дерево вывода высоты $n + 1$; $D_1, \ldots, D_k$ $(k = 1, 2, \ldots)$ деревья и/или формулы, записанные в $D$ непосредственно над самой нижней чертой (слева направо); $f$ — корень $D$; $g_1, \ldots, g_s (s = 0, 1, \cdots)$ — формулы, устраняемые на последнем шаге вывода, отвечающего дереву $D$. Тогда кодом дерева $D$ будет слово $ubv_1\alpha_1 \cdots bv_k\alpha_k r(v_k) \cdots r(v_k)w$, где: $u$ — код формулы $f$; $v_i$ — код дерева или формулы $D_i$; $\alpha_i$ есть $d$, если $D_i$ — дерево, и $c$, если $D_i$ — формула; $w = ew_1 \cdots ew_s$, где $w_j$ — код формулы $g_j$ (если $s = 0$, то $w$ — пустое слово).

Таким образом, если $q$ — код дерева вывода, то «главная часть» $q$, т. е. слово, получаемое из $q$ вычеркиванием всех кусков вида $r(w)$, есть «линейная запись» дерева, а $r(q)$ — перечень кодов его увядших листьев, разделенных вхождениями $e$. Полный список листьев дерева состоит из всех формул, коды которых входят в $q$ таким образом, что за ними следуют вхождения $c$. Начало $q$ до первого вхождения $b$ есть код корня дерева.

Стандартный номер кода дерева вывода мы будем называть просто *номером этого дерева*.

Теперь нам нужно рассмотреть некоторые функции и предикаты, связанные с деревьями вывода, и доказать, что они примитивно рекурсивны. Для этого будут использоваться те же технические приемы, что и в § 7.9 и в пункте 1 настоящего параграфа, и мы позволим себе не приводить всех деталей; при желании читатель восстановит их без большого труда.

1) $Д(x)$ — «$x$ есть номер формулы или дерева вывода».

Здесь и далее, говоря о дереве вывода, мы подразумеваем дерево, отвечающее выводу, в котором не применяется правило тривиальной выводимости. Поскольку это правило, как мы показали на с. 169, избыточно, на объем отношения выводимости такое ограничение не влияет.

Доказательство примитивной рекурсивности предиката Д будет основано на том, что «главные части» используемых нами кодов деревьев вывода представляют собой «скобочные структуры», построенные так же, как термы и формулы; коды листьев занимают в

них места элементарных термов и атомных формул, коды остальных входящих в вывод формул — места функциональных и предикатных символов, символ $b$ играет роль левой скобки, символы $c$ и $d$ — роль правой скобки. Поэтому мы можем определить предикат Д подобно тому, как было сделано выше для предиката ТМ. Однако это будет сложнее, потому что, во-первых, нужно учитывать увядание листьев, и во-вторых — это главное,— в отличие от терма и формулы, где «заголовок» может быть произвольным функциональным, соответственно предикатным символом, в коде дерева «заголовок» (код корня) зависит от вида поддеревьев, из которых это дерево «собрано».

В доказательстве примитивной рекурсивности предиката Д мы будем использовать введенную на с. 385 функцию $r(u)$, примитивная рекурсивность которой почти очевидна, и еще несколько функций и предикатов, также, как нетрудно проверить, примитивно рекурсивных:

кор$(x)$ («корень дерева $x$») — начало слова $x$ до первого вхождения $b$ (само это вхождение в кор$(x)$ не входит); если вхождений $b$ нет, то кор$(x) = x$;

бк$(x)$ («$x$ без корня») — конец слова $x$, остающийся после вычеркивания кор$(x)$;

$p(u_1, u_2, u_3)$, $q(u_1, u_2)$, $s(u)$: функция $p$ сопоставляет словам $u_1$, $u_2$, $u_3$ слово $bu_1\alpha_1bu_2\alpha_2bu_3\alpha_3r(u_1)r(u_2)r(u_3)$, где $\alpha_i$ есть буква $c$, если $u_i$ не содержит вхождений $b$, и буква $d$ в противном случае; $q$ и $s$ — аналогичные функции двух и одной переменной;

$\theta_\&(u, v)$, $\theta_\vee(u, v)$, $\theta_\supset(u, v)$, $\theta_\neg(u)$: функция $\theta_\&$ сопоставляет номерам слов $u$, $v$ номер слова $(u)\&(v)$; $\theta_\vee$, $\theta_\supset$ и $\theta_\neg$ определяются аналогично;

ЛС$(x, y)$ — «$x$ содержит вхождение слова $byc$, а $y$ непусто и не содержит вхождений $b$, $c$, $d$, $e$»;

УЛ$(x, y)$ — «$x$ содержит вхождение слова $eye$ или оканчивается словом $ey$, а $y$ не содержит вхождений $b$, $c$, $d$, $e$».

$$ЗЛ(x, y) \equiv ЛС(x, y)\&\neg УЛ(x, y).$$

(Если $x$ — номер дерева вывода, то ЛС$(x, y)$ означает, что $y$ есть номер одного из его листьев, УЛ$(x, y)$ — что $y$ есть номер одного из его увядших листьев, ЗЛ$(x, y)$ — что $y$ есть номер одного из его зеленых листьев.)

Далее мы определим предикат КВД$(x)$, аналогичный рассмотренному выше предикату КВТ$(x)$. Именно, КВД$(x)$ означает, что $x$ есть либо код формулы, либо слово, отличающееся от кода дерева тем, что

$v_1, \ldots, v_k$ могут быть произвольными словами (но $u$ и $v$ связаны с $v_1, \ldots, v_k$ так же, как в коде дерева). Мы положим

$$\text{КВД}(x) \equiv \text{ФМ}(x) \vee (\text{А}_{\text{вк}}(x) \vee \ldots \vee \text{А}_{\text{уэ}}(x) \,|\&B(x)\,|,$$

где $B(x)$ означает, что $\alpha_i$ есть $c$ тогда и только тогда, когда $v_i$ есть код формулы (записать это нерудно) и где дизъюнктивные члены $A_{\text{вк}}, \ldots, A_{\text{уэ}}$ отвечают четырнадцати логическим правилам исчисления Ar — или, безразлично, исчисления $G_1$.

Мы выпишем в явном виде только некоторые дизъюнктивные члены; остальные читатель сможет записать сам.

$$A_{\text{вк}}(x) \equiv \underset{u\le x}{\exists u}\ \underset{v\le x}{\exists v}\ |\text{бк}(x) = \psi(u, v)\&\text{кор}(x) =$$

$$= \theta_8(\text{кор}(u), \text{кор}(v))\,|;$$

$$A_{\text{ук}}(x) \equiv A'_{\text{ук}}(x) \vee A''_{\text{ук}}(x,), \text{ где: } A'_{\text{ук}}(x) \equiv$$

$$\equiv \underset{u\le x}{\exists u}\ \underset{z\le x}{\exists z}\,|\text{бк}(x) = s(u)\&\text{кор}(u) = \theta_8(\text{кор}(x), z)\,|;$$

$A''_{\text{ук}}$ определяется точно так же с заменой $\theta_8(\text{кор}(x), z)$ на $\theta_8(z, \text{кор}(x))$;

$$A_{\text{уд}}(x) \equiv \underset{u\le x}{\exists u}\ \underset{v\le x}{\exists v}\ \underset{w\le x}{\exists w}\ \underset{z_1\le x}{\exists z_1}\ \underset{z_2\le x}{\exists z_2}\ |\text{бк}(x) =$$

$$= \text{произв}_5(p(u, v, w), e, z_1, e, z_2)\&\text{кор}(x) = \text{кор}(u) = \text{кор}(v)\&$$

$$\&\text{ЗЛ}(u, z_1)\&\text{ЗЛ}(u, z_2)\&\text{кор}(w) = \theta_9(z_1, z_2);$$

$$A_{\text{во}}(x) \equiv \underset{u\le x}{\exists u}\ \underset{z\le x}{\exists z}\ |\text{бк}(x) = \text{произв}_3(s(u), e, z)\&$$

$$\&\text{ЗЛ}(u, z)\&\text{кор}(u) = 11\&\text{кор}(x) = \theta_7(z)\,|$$

(число 11 — номер символа $Л$);

$$A_{\text{вв}}(x\,) \equiv \underset{u\le x}{\exists u}\ \underset{z\le x}{\exists z}\ |\text{бк}(x) = s(u)\&\text{кор}(x) =$$

$$= \text{общ}(\text{кор}(u), z)\&\,\neg\underset{w\le x}{\exists w}\ (\text{ЗЛ}(u, w)\&\text{СВ}(w, z))\,|;$$

$$A_{\text{вэ}}(x) \equiv \underset{u\le x}{\exists u}\ \underset{v\le x}{\exists v}\ \underset{z\le x}{\exists z}\ \underset{w\le x}{\exists w}\ |\text{бк}(x) = s(u)\&$$

$$\&\text{кор}(u) = \text{зам}(v, z, w)\&\text{кор}(x) = \text{сущ}(v, z)\,|.$$

Смысл приведенных записей легко понять. Например, в представляющей формуле для $\text{А}_{\text{уд}}$ первый конъюнктивный член в квадратных скобках означает, что в дереве с номером $x$ над самой нижней чертой записаны деревья с номерами $u$, $v$ и $w$ и что на последнем шаге

соответствующего вывода устраняются гипотезы с номерами $z_1$ и $z_2$; смысл остальных членов ясен непосредственно.

Теперь предикат Д можно получить из КВД аналогично тому, как ТМ получается из КВТ: слово удовлетворяет условию Д тогда и только тогда, когда оно удовлетворяет условию КВД и для всякого входящего в него слова, удовлетворяющего условию КВД и не являющегося кодом формулы, его «компоненты» тоже удовлетворяют условию КВД. Соответствующая запись, из которой следует примитивная рекурсивность Д, громоздка, но очевидна.

2) $\text{АКС}(z)$ — «$z$ есть номер аксиомы исчисления Ar».

Этот предикат можно представить в виде дизъюнкции одиннадцати предикатов, отвечающих схемам аксиом исчисления Ar:

$$\text{АКС}(z) \equiv \text{АКС}_1(z) \vee \text{АКС}_2(z) \vee \dots \vee \text{АКС}_{\sigma_8}(z),$$

где для каждого $\xi = 1, \dots, \sigma_8$ $\text{АКС}_\xi(z)$ означает «$z$ есть номер аксиомы, образованной по схеме $(\xi)$». Запись предикатов $\text{АКС}_\xi$, отвечающих простейшим схемам, очевидна: например,

$$\text{АКС}_1(z) \equiv \underset{j_1 \le z}{\exists j_1} \; \underset{j_2 \le z}{\exists j_2} \; [\text{ПЕР}(j_1)\&\text{ПЕР}(j_2)\&z = \text{зам}_2(i_1, j_1, j_2)],$$

где $i_1$ — номер формулы $x_1 = x_2 \supset x_2 = x_1$. Что касается предиката $\text{АКС}_{a_4}$, то с помощью функций $\theta_\&$, $\theta_\supset$, общ, $b$ и зам ($b$ — функция, определенная на с. 381) легко выразить функцию $\psi(i, j)$, которая всякому $i$, являющемуся номером формулы $\mathfrak{A}$, и всякому $j$, являющемуся номером переменной $x$, сопоставляет номер формулы $\mathfrak{A}(0)\&\forall x(\mathfrak{A}(x) \supset \mathfrak{A}(x')) \supset \forall x \mathfrak{A}(x)$; но

$$\text{АКС}_{a_4}(z) \equiv \underset{i \le z}{\exists i} \; \underset{j \le z}{\exists j} \; (z = \psi(i, j)).$$

3) $\text{ДОК}(x, y)$ — «$x$ есть номер теоремы и $y$ — номер ее доказательства»:

$$\text{ДОК}(x, y) \equiv \text{Д}(y)\&\text{кор}(y) = x\&\underset{z \le y}{\forall z} \; (\text{ЗЛ}(z) \supset \text{АКС}(z)).$$

4) $d(y)$ — функция, сопоставляющая каждому $y$, являющемуся номером формулы $\mathfrak{A}$, номер формулы $\mathfrak{A}|^{x_1}_{y}$, и равная нулю для остальных $y$:

$$d(y) = \text{зам}(y, 1, \text{цф}(y)).$$

5) $W_1(y, z)$ — «$y$ есть номер формулы $\mathfrak{A}(x_1)$, содержащей свободное вхождение переменной $x_1$ и не содержащей свободных вхождений

других переменных, а $z$ — номер доказательства формулы $\mathfrak{A}(y)$» (так что $\mathfrak{A}(y)$ есть теорема):

$$W_1(y, z) \equiv \text{СВ}(y, 1)\&\underset{v\le y}{\forall v}\ (\text{СВ}(y, v)\supset v = 1\&\text{ДОК}(d(y), z).$$

б) $W_2(y, z)$ — «$y$ есть номер формулы $\mathfrak{A}(x_1)$, содержащей свободное вхождение переменной $x_1$ и не содержащей вхождений других переменных, а $z$ — номер доказательства формулы $\neg\mathfrak{A}(y)$ (так что $\neg\mathfrak{A}(y)$ есть теорема):

$$W_2(y, z) \equiv \text{СВ}(y, 1)\&\underset{v\le y}{\forall v}\ (\text{СВ}(y, v)\supset v = 1)\&\text{ДОК}(\theta_7(d(y)), z).$$

3. Теперь мы можем доказать, что если формальная арифметика непротиворечива, то справедливо утверждение, обратное теореме предыдущего параграфа: всякая функция, представимая в формальной арифметике, общерекурсивна.

Пусть функция $f(x_1, \ldots, x_n)$ представляется формулой $\mathfrak{A}_0 = \mathfrak{A}_0(x_1, \ldots, x_{n+1})$, имеющей номер $i_0$. Рассмотрим функцию $\varphi_0(k_1, \ldots, k_{n+1})$, сопоставляющую любым натуральным числам $k_1, \ldots, k_{n+1}$ номер формулы $\mathfrak{A}_0(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n+1})$; эта функция представляется в виде $\text{зам}^{n}_{n+1}(i_0, \text{цф}(k_1), \ldots, \text{цф}(k_{n+1}))$ и, следовательно, примитивно рекурсивна. Далее нам понадобится функция $\chi(p)$, которая в случае, когда $p$ — номер какого-либо доказательства формулы вида $\mathfrak{A}_0(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_{n+1})$, где $k_1, \ldots, k_{n+1}$ — произвольные натуральные числа, принимает значение $k_{n+1}$, а в остальных случаях обращается в нуль. Ее можно представить в виде

$$\chi(p) = \underset{k\le p}{\mu k}\ [\underset{q\le p}{\exists q}\ (\text{ДОК}(q, p)\&\underset{k_1\le p}{\exists k_1}\ldots\underset{k_n\le p}{\exists k_n}\ (q = \varphi_0(k_1, \ldots, k_n, k))\ ]$$

(потому что для заданного $p$ может существовать не более одного $q$, удовлетворяющего условию ДОК$(q, p)$, а для заданного $q$ — не более одного набора $k_1, \ldots, k_n$, удовлетворяющего условию $q = \varphi_0(k_1, \ldots, k_n, k)$[19]); следовательно, $\chi$ также примитивно рекурсивна.

По условию (4) (см. начало предыдущего параграфа) для любых $k_1, \ldots, k_n$ доказуема формула $\mathfrak{A}_0(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, \boldsymbol{l})$, где $l = f(k_1, \ldots, k_n)$. В то же время при условии непротиворечивости исчисления Ar ни при каком $m \ne f(k_1, \ldots, k_n)$ формула $\mathfrak{A}_0(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, \boldsymbol{m})$ не может быть доказуемой: ввиду условия (3′) из $\vdash \mathfrak{A}_0(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, \boldsymbol{m})$ вытекает $\vdash \boldsymbol{m} = \boldsymbol{l}$, но по утверждению 3 из § 8.1 при $m \ne l$ должно быть также

[19] Поскольку никакое число не может быть номером более чем одной формулы.

$\vdash 7(\boldsymbol{m} = \boldsymbol{l})$. Поэтому всякое число $p$, для которого существует такое $m$, что $p$ есть доказательство формулы $\mathfrak{A}_0(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, \boldsymbol{m})$ — иначе говоря, всякое $p$, удовлетворяющее условию $\exists m$ ДОК $(\mathfrak{q}_0(k_1, \ldots, k_n, m), p)$ — является номером некоторого доказательства формулы $\mathfrak{A}_0(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, \boldsymbol{l})$. Отсюда следует, что для всякого такого $p$ справедливо равенство $\chi(p) = l = f(k_1, \ldots, k_n)$. В сформулированном только что условии для $p$ можно ограничить квантор $\exists m$ числом $p$ (т. к. номер доказательства формулы $\mathfrak{A}_0(\boldsymbol{k}_1, \ldots, \boldsymbol{k}_n, \boldsymbol{m})$, очевидно, больше $m$), и мы получаем равенство

$$f(k_1, \ldots, k_n) = \chi\left(\mu p\left[\exists_{m \leq p} m \text{ ДОК}(\mathfrak{q}_0(k_1, \ldots, k_n, m), p)\right]\right).$$

Таким образом, всюду определенная функция $f$ выражается через примитивно рекурсивные функции и оператор минимизации; следовательно, она общерекурсивна.

Объединяя доказанное утверждение с теоремой предыдущего параграфа, мы видим теперь, что если формальная арифметика непротиворечива, то класс функций, в ней представимых, совпадает с классом общерекурсивных функций.

Наконец, теперь легко видеть, что предикат, заданный на множестве натуральных чисел, тогда и только тогда представим в формальной арифметике,— при условии ее непротиворечивости,— когда он рекурсивен. В самом деле, по лемме из § 8.2 предикат тогда и только тогда представим в формальной арифметике, когда представима его характеристическая функция, а это по только что доказанному равносильно ее общерекурсивности, т. е. рекурсивности предиката.

Задачи. 1) Видоизменить конструкцию этого пункта таким образом, чтобы получить из нее новое доказательство теоремы Клини о нормальной форме для случая всюду определенных функций.

2) Какие функции представимы в противоречивом логическом исчислении, алфавит которого совпадает с алфавитом Ar?

## § 8.4. ТЕОРЕМА ГЁДЕЛЯ О НЕПОЛНОТЕ

1. Насколько адекватна формальная арифметика для описания содержательной арифметики натуральных чисел? Этот вопрос, к обсуждению которого мы сейчас переходим, можно уточнить так (ср. начало § 5.4): является ли исчисление Ar семантически пригодным и семантически полным?

В конце пункта 4 параграфа 6.3 мы уточнили понятия семантической пригодности и семантической полноты для исчислений на основе $G_1$ следующим образом: семантическая пригодность исчисления означает, что все интерпретации определенного класса — те, для описания которых это исчисление предназначается — служат для него моделями, а семантическая полнота — что всякая его формула, истинная во всех интерпретациях этого класса, является в нем теоремой. Но исчисление Ar предназначено для описания всего лишь одной интерпретации — той, которую мы в § 8.1 (пункт 7) назвали стандартной. Эта интерпретация является для него моделью, и, таким образом, оно семантически пригодно.

Прежде чем переходить к несравненно более сложному вопросу о семантической полноте, вспомним, что в § 6.2 мы ввели еще дедуктивную полноту, означающую, что любая замкнутая формула либо доказуема, либо опровержима (т. е. доказуемо ее отрицание). Это понятие также представляет интерес в семантическом аспекте, хотя оно и определяется в чисто дедуктивных терминах. Прежде всего, легко видеть, что для семантически пригодных исчислений дедуктивная полнота влечет семантическую: если бы в семантически пригодном и дедуктивно полном исчислении некоторая истинная формула $\mathfrak{A}$ оказалась недоказуемой, то ее замыкание[20] $\mathfrak{A}'$ также было бы истинной и недоказуемой формулой; но тогда была бы доказуема и, следовательно, истинна формула $\neg\mathfrak{A}'$, однако ни при каком разумном понимании истинности формулы $\mathfrak{A}'$ и $\neg\mathfrak{A}'$ не могут быть истинны одновременно. В то же время обратное неверно. В самом деле, если хотя бы для одной замкнутой формулы $\mathfrak{A}$ семантически пригодного исчисления $L$ среди его «запланированных» интерпретаций — тех, для описания которых оно предназначено — найдутся две, в одной из которых $\mathfrak{A}$ истинна, а в другой невыполнима, то ни одна из формул $\mathfrak{A}$ и $\neg\mathfrak{A}$ не может быть доказуемой в $L$ и, следовательно, $L$ не является дедуктивно полным. Но уже в исчислении $G_1$, которое, как мы доказали в § 6.2, семантически полно и для которого «запланированы» все интерпретации, можно указать сколько угодно замкнутых формул, истинных в одних интерпретациях и невыполнимых в других (см. хотя бы примеры в § 4.1), так что $G_1$ дедуктивно неполно. То же справедливо для семантически полных исчислений, рассмот-

[20] *Замыканием* формулы $\mathfrak{A}(z_1, \ldots, z_k)$, содержащей свободные переменные $z_1, \ldots, z_k$ и не содержащей других свободных переменных, называется формула $\forall z_1 \ldots \forall z_k \mathfrak{A}(z_1, \ldots, z_k)$; замыкание замкнутой формулы совпадает с ней самой. Легко видеть, что если $\mathfrak{A}$ — формула некоторого исчисления $L$ на основе $G_1$ и $\mathfrak{A}'$ — ее замыкание, то: а) $\vdash_L \mathfrak{A}$ тогда и только тогда, когда $\vdash_L \mathfrak{A}'$; б) какова бы ни была интерпретация формулы $\mathfrak{A}$, эта формула истинна в ней тогда и только тогда, когда истинна $\mathfrak{A}'$.

ренных в § 6.3, пункт 4 (примеры 1—3). Существуют, например, группы, в которых истинна формула $\forall x(x + x + x = 0)$, равно как и группы, где истинно ее отрицание — и уже отсюда следует, что элементарная теория групп дедуктивно неполна; легко подобрать нужные формулы и для других исчислений из § 6.3. Мы видим, таким образом, что дедуктивная неполнота этих исчислений — естественное следствие разнообразия их моделей: исчисление, предназначенное для описания математических объектов с существенно разными свойствами, не только не может, но и «не должно» быть дедуктивно полным. Но если исчисление построено ради описания одной модели, его семантическая полнота влечет дедуктивную и, следовательно, равносильна ей: ведь если в таком исчислении некоторая замкнутая формула $\mathfrak{A}$ не доказуема, то из семантической полноты следует, что она не является истинной в его единственной «запланированной» модели; поэтому формула $\neg\mathfrak{A}$ истинна в этой модели и, значит, доказуема.

Задача. а) Доказать, что исчисление, полученное из элементарной теории групп добавлением аксиомы $\forall x(x + x + x = 0)$, имеет с точностью до изоморфизма единственную модель.

б) Убедиться, что это исчисление дедуктивно полно.

Таким образом, для формальной арифметики оба понятия полноты совпадают по объему, и мы можем в дальнейшем интересоваться только одним из них. Нам удобно будет исследовать вопрос о дедуктивной полноте, которую мы будем называть теперь просто *полнотой*.

Если бы формальная арифметика была полной, это значило бы, что всякое истинное арифметическое предложение, выразимое на ее языке (т. е., в сущности, на языке узкого исчисления предикатов), было бы в ней доказуемо, а всякое ложное — опровержимо[21]; это было бы очень «хорошее» и «естественное» свойство, и в свое время многие из математиков, занимавшихся логическими основаниями своей науки, надеялись, что формальная арифметика полна и это удастся доказать. Но в 1931 г. 25-летний К. Гёдель получил сенсационный результат: оказалось, что если формальная арифметика обладает некоторым простым свойством, которое он назвал $\omega$-непротиворечивостью (и которое следует из семантической пригодности, если только в стандартной интерпретации нет противоречий), то она неполна, и, более того, можно указать конкретное предложение, выразимое на языке формальной арифметики и истинное, но не доказуемое в ней. А в 1936 г. Дж. Б. Россер показал, что в теореме Гёделя можно заменить $\omega$-непротиворечивость обычной непротиво-

[21] Напомним, что предложениям отвечают в исчислении на основе $G_1$ з а м к н у т ы е формулы.

речивостью (ценой некоторого усложнения доказательства и самого примера истинной недоказуемой формулы). Эту теорему называют обычно теоремой Гёделя о неполноте, а иногда просто «теоремой Гёделя», потому что это самая знаменитая из его теорем (и одна из самых знаменитых математических теорем вообще). Сейчас мы докажем ее в обеих формах — в первоначальной и в форме Россера.

2. Пусть $L$ — исчисление, алфавит которого содержит алфавит формальной арифметики, и пусть, какова бы ни была его формула $\mathfrak{A} = \mathfrak{A}(x)$, если для любого натурального $n$ в $L$ доказуема формула $\mathfrak{A}(\boldsymbol{n})$, то не может быть доказуемой формула $\exists x 7\mathfrak{A}(x)$. Такое исчисление называется *ω-непротиворечивым*.

Понятно, что если в стандартной модели, в которой каждый элемент основного множества отвечает некоторой цифре, нет противоречий, то формальная арифметика ω-непротиворечиво.

Теорема 1. *Если логическое исчисление на основе $G_1$ ω-непротиворечиво*, то оно непротиворечиво.

Доказательство. Чтобы убедиться в непротиворечивости исчисления на основе $G_1$, достаточно, ввиду леммы 2 из § 6.2, найти в нем хотя бы одну недоказуемую формулу. Но в ω-непротиворечивом исчислении не может быть доказуемой никакая формула вида $\exists x 7\mathfrak{A}(x)$, где $\mathfrak{A}(x)$ — доказуемая формула, поскольку вместе с $\mathfrak{A}(x)$ доказуема, очевидно, любая формула вида $\mathfrak{A}(\boldsymbol{n})$.

По поводу обратного утверждения см. замечание в конце этого пункта.

Рассмотрим теперь введенный в конце пункта 2 предыдущего параграфа предикат $W_1$. Поскольку он примитивно рекурсивен, по следствию из теоремы § 8.2 существует представляющая его формула $\mathfrak{B}_1(x_1, x_2)$ исчисления Ar. Будем обозначать через $\mathfrak{G}_1$ или $\mathfrak{G}_1(x_1)$ формулу $7\exists x_2 \mathfrak{B}_1(x_1, x_2)$. Пусть $m_1$ — номер этой формулы; формулу $\mathfrak{G}(\boldsymbol{m}_1)$ — иначе $7\exists x_2 \mathfrak{B}_1(\boldsymbol{m}_1, x_2)$ — обозначим $\mathfrak{G}_1'$. Вспоминая, что означает предикат $W_1$, видим, что для всякого натурального $n$ формула $\mathfrak{G}_1(\boldsymbol{n})$ имеет (в стандартной интерпретации) следующий смысл: «Не существует такого натурального числа $z$, чтобы $n$ было номером какой-либо формулы $\mathfrak{A}(x_1)$ с одной свободной переменной $x_1$, а $z$ — номером доказательства формулы $\mathfrak{A}(\boldsymbol{n})$». А поскольку $m_1$ как раз есть номер формулы $\mathfrak{G}(x_1)$, содержащей одну свободную переменную $x_1$, формула $\mathfrak{G}_1(\boldsymbol{m}_1) = \mathfrak{G}_1'$ означает: «Не существует натурального числа, являющегося номером доказательства формулы $\mathfrak{G}_1(\boldsymbol{m}_1)$» — или, что то же самое: «Не существует доказательства формулы $\mathfrak{G}_1(\boldsymbol{m}_1)$», т. е. «$\mathfrak{G}_1(\boldsymbol{m}_1)$ — не теорема». Таким образом, формула $\mathfrak{G}_1'$ выражает утверждение о своей собственной недоказуемости — подобно тому, как предложение, фигурирую-

щее в парадоксе лжеца (см. Введение) выражает утверждение о своей собственной ложности. Это предложение, как мы видели, не может быть ни истинным, ни ложным — и по аналогии естественно ожидать, что формула, утверждающая свою собственную недоказуемость, не будет ни доказуемой, ни опровержимой. Сейчас мы покажем, что это действительно так.

**Теорема 2 (теорема Гёделя о неполноте в первоначальной форме).** (а) Если исчисление Ar непротиворечиво, то формула $\mathfrak{G}_1'$ недоказуема в нем; (б) если исчисление Ar $\omega$-непротиворечиво, то в нем недоказуема также и формула $\neg\mathfrak{G}_1'$.

**Доказательство.** (а) Пусть формула $\mathfrak{G}_1' = \mathfrak{G}_1(\boldsymbol{m}_1)$ доказуема, и пусть $n_1$ — номер какого-либо ее доказательства. Тогда по смыслу предиката $W_1$ предложение $W_1(m_1, n_1)$ истинно и, следовательно, доказуема формула $\mathfrak{W}_1(\boldsymbol{m}_1, \boldsymbol{n}_1)$. В то же время вместе с формулой $\mathfrak{G}_1' = \neg\exists x_2 \mathfrak{W}_1(\boldsymbol{m}_1, x_2)$ доказуема и формула $\forall x_2 \neg\mathfrak{W}_1(\boldsymbol{m}_1, x_2)$, а из нее по УУ выводится $\neg\mathfrak{W}_1(\boldsymbol{m}_1, \boldsymbol{n}_1)$. Таким образом, обе формулы $\mathfrak{W}_1(\boldsymbol{m}_1, \boldsymbol{n}_1)$ и $\neg\mathfrak{W}_1(\boldsymbol{m}_1, \boldsymbol{n}_1)$ оказались доказуемыми, что невозможно, если Ar непротиворечиво.

(б) Если исчисление Ar $\omega$-непротиворечиво и в нем доказуема формула $\neg\mathfrak{G}_1'$, то формула $\mathfrak{G}_1' = \mathfrak{G}_1(\boldsymbol{m}_1)$ в нем недоказуема (потому что по теореме 1 Ar в этом случае непротиворечиво), так что никакое число $n$ не является номером ее доказательства и, следовательно, для любого $n$ предложение $W_1(m_1, n)$ ложно. Поэтому для любого $n$ доказуема формула $\neg\mathfrak{W}_1(\boldsymbol{m}_1, \boldsymbol{n})$. С другой стороны, вместе с формулой $\neg\mathfrak{G}_1' = \neg\neg\exists x_2 \mathfrak{W}_1(\boldsymbol{m}_1, x_2)$ доказуема и формула $\exists x_2 \neg\neg\mathfrak{W}_1(\boldsymbol{m}_1, x_2)$. Но в $\omega$-непротиворечивом исчислении эта формула не может быть доказуемой, если для любого $n$ доказуема $\neg\mathfrak{W}_1(\boldsymbol{m}_1, \boldsymbol{n})$.

Замкнутые формулы, недоказуемые и неопровержимые в некотором исчислении, принято называть *неразрешимыми предложениями* этого исчисления. Мы доказали, таким образом, что $\mathfrak{G}_1'$ — неразрешимое предложение формальной арифметики.

В стандартной интерпретации, как уже было замечено, формула $\mathfrak{G}_1'$ даст предложение «формула $\mathfrak{G}_1'$ недоказуема». Но мы только что доказали, что это предложение истинно. Итак, $\mathfrak{G}_1'$ может служить также и примером недоказуемой истинной формулы.

Соблазнительно подумать: быть может, в нашей формальной арифметике просто не хватает каких-то аксиом, и именно поэтому в ней нельзя доказать все истинные арифметические предложения — так же, как нельзя доказать все истинные предложения евклидовой геометрии, не пользуясь пятым постулатом? Но нетрудно понять, что это не так. В самом деле, при доказательстве теоремы Гёделя мы

пользовались только тем, что, во-первых, в исчислении представимы все рекурсивные предикаты, и, во-вторых, некоторые предикаты, связанные с выводимостью в этом исчислении (рассмотренные в § 8.3), рекурсивны. Однако из определения представимости предиката непосредственно следует, что всякий предикат, представимый в исчислении Ar, представим и в любом его расширении; что же касается предикатов, связанных с выводимостью, то для любого простого расширения Ar с помощью конечного или даже бесконечного, но разрешимого множества формул приведенное в § 8.3 доказательство рекурсивности этих предикатов можно повторить слово в слово с той только разницей, что в выражении для предиката АКС добавятся новые дизъюнктивные члены. Следовательно, теорема останется справедливой и для исчисления, полученного добавлением к Ar любого разрешимого множества новых аксиом. Можно, например, присоединить в качестве новой аксиомы саму формулу $\mathfrak{G}_1'$; тогда мы получим неразрешимое предложение, которое строится так же, как $\mathfrak{G}_1'$, но, разумеется, не совпадает с ним, потому что понятие доказуемости будет теперь другое и, следовательно, предикат $W_1$ и представляющая его формула $\mathfrak{W}_1$ также изменятся.

Замечание. В предположении обычной непротиворечивости исчисления Ar можно не только провести доказательство утверждения (а) теоремы 2, но и показать, пользуясь этим утверждением (и рассуждая, как в доказательстве утверждения (б)), что для любого $n$ в Ar доказуема формула $\neg\mathfrak{W}_1(\boldsymbol{m}_1, \boldsymbol{n})$. Тем более все эти формулы будут доказуемы в простом расширении Ar с помощью формулы $\neg\mathfrak{G}_1' = \neg\neg\exists x_2\mathfrak{W}_1(\boldsymbol{m}_1, x_2)$, которое мы обозначим $L$. Но в $L$ доказуема также и формула $\exists x_2\neg\neg\mathfrak{W}_1(\boldsymbol{m}_1, x_2)$. Таким образом, если Ar непротиворечиво, то $L$ $\omega$-противоречиво. С другой стороны, ввиду утверждения (а) теоремы 2 из непротиворечивости Ar по лемме 3 из § 6.2 следует, что $L$ также непротиворечиво. Итак, при условии непротиворечивости исчисления Ar у него имеется непротиворечивое и в то же время $\omega$-противоречивое простое расширение.

3. Обратимся теперь к теореме Гёделя в форме Россера. Рассмотрим введенный вместе с предикатом $W_1$ примитивно рекурсивный предикат $W_2$ и представляющую его формулу $\mathfrak{W}_2(x_1, x_2)$. Будем обозначать через $\mathfrak{G}_2$ или $\mathfrak{G}_2(x_1)$ формулу

$$\forall x_1(\mathfrak{W}_1(x_1, x_2)\supset\exists x_3(x_3 < x_2\&\mathfrak{W}_2(x_1, x_3))).$$

Пусть $m_2$ — номер этой формулы; формулу $\mathfrak{G}_2(\boldsymbol{m}_2)$, подробнее

$$\forall x_2(\mathfrak{W}_1(\boldsymbol{m}_2, x_2)\supset\exists x_3(x_3 < x_2\&\mathfrak{W}_2(\boldsymbol{m}_2, x_3))),$$

обозначим $\mathfrak{G}_2'$. Вспоминая, что означают предикаты $W_1$ и $W_2$, видим

(ср. начало предыдущего пункта), что формула $\mathfrak{G}_2(\boldsymbol{m}_2) = \mathfrak{G}_2'$ имеет (в стандартной интерпретации) следующий смысл: «Для любого натурального числа, являющегося номером доказательства формулы $\mathfrak{G}_2(\boldsymbol{m}_2)$, существует меньшее натуральное число, являющееся номером доказательства формулы $\neg\mathfrak{G}_2(\boldsymbol{m}_2)$». Таким образом, формула $\mathfrak{G}_2'$ утверждает, что если она доказуема, то доказуемо и ее отрицание (и притом найдется доказательство отрицания, номер которого меньше номера доказательства самой формулы).

**Теорема 3 (теорема Гёделя о неполноте в форме Россера).** Если исчисление Ar непротиворечиво, то в нем недоказуемы формулы $\mathfrak{G}_2'$ и $\neg\mathfrak{G}_2'$.

Доказательство. (а) Пусть формула $\mathfrak{G}_2'$ доказуема, и пусть $n_2$ — номер какого-либо ее доказательства. Тогда предложение $W_1(m_2, n_2)$ истинно и, следовательно, доказуема формула $\mathfrak{W}_1(\boldsymbol{m}_2, \boldsymbol{n}_2)$. Из этой формулы и из формулы $\mathfrak{W}_1(\boldsymbol{m}_2, \boldsymbol{n}_2) \supset \exists x_3(x_3 < \boldsymbol{n}_2 \& \mathfrak{W}_2(\boldsymbol{m}_2, x_3))$, непосредственно выводимой из $\mathfrak{G}_2'$, выводится формула $\exists x_3(x_3 < \boldsymbol{n}_2 \& \& \mathfrak{W}_2(\boldsymbol{m}_2, x_3))$, а из этой последней (с помощью утверждения 4 из § 8.1 и теоремы о замене дедуктивно эквивалентных формул) — формула

$$\exists x_3((x_3 = 0 \vee x_3 = 1 \vee \dots \vee x_3 = \boldsymbol{n}_2 - 1) \& \mathfrak{W}_2(\boldsymbol{m}_2, x_3));$$

из нее, в свою очередь, выводится формула

$$\exists x_3(x_3 = 0 \& \mathfrak{W}_2(\boldsymbol{m}_2, x_3) \vee \dots \vee x_3 = \boldsymbol{x}_2 - 1 \& \mathfrak{W}_2(\boldsymbol{m}_2, x_3))$$

и далее, поскольку Ar — исчисление на основе $G_1$ с равенством, формула $\exists x_3(\mathfrak{W}_2(\boldsymbol{m}_2, 0) \vee \dots \vee \mathfrak{W}_2(\boldsymbol{m}_2, \boldsymbol{n}_2 - 1))$. В последней формуле квантор можно отбросить (т. к. формула $\mathfrak{A}$, не содержащая свободных вхождений $x$, дедуктивно эквивалентна формуле $\exists x\mathfrak{A}$ — ср. доказательство теоремы 2 из § 6.2, пункт (е) индукционного шага), так что дизъюнкция $\mathfrak{W}_2(m_2, 0) \vee \dots \vee \mathfrak{W}_2(\boldsymbol{m}_2, \boldsymbol{n}_2 - 1)$ оказывается доказуемой. Но если Ar непротиворечиво, то формула $\neg\mathfrak{G}_2' = \neg\mathfrak{G}_2(\boldsymbol{m}_2)$ недоказуема (поскольку мы допустили, что доказуема $\mathfrak{G}_2'$); поэтому для любого натурального $n$ предложение $W_2(m_2, n)$ ложно и, следовательно, доказуема формула $\neg\mathfrak{W}_2(\boldsymbol{m}_2, \boldsymbol{n})$. В частности, доказуемы все формулы $\neg\mathfrak{W}_2(\boldsymbol{m}_2, 0)$, ..., $\neg\mathfrak{W}_2(\boldsymbol{m}_2, \boldsymbol{n}_2 - 1)$; поэтому доказуема их конъюнкция, а из нее можно вывести отрицание дизъюнкции $\mathfrak{W}_2(\boldsymbol{m}_2, 0) \vee \dots \vee \mathfrak{W}_2(\boldsymbol{m}_2, \boldsymbol{n}_2 - 1)$, которая, как мы видели, также доказуема. Итак, доказуемость формулы $\mathfrak{G}_2'$ несовместима с непротиворечивостью Ar.

(б) Пусть доказуема формула $\neg\mathfrak{G}_2'$. Мы покажем, что тогда $\mathfrak{G}_2'$

также доказуема, что опять-таки несовместимо с непротиворечивостью Ar. Достаточно устаиовить доказуемость формулы

$$\mathfrak{D} = \forall x_1(\neg\mathfrak{B}_1(\boldsymbol{m}_2, x_2) \vee \exists x_3(x_3 < x_2 \& \mathfrak{B}_2(\boldsymbol{m}_2, x_3))),$$

т. к. она, очевидно, дедуктивно эквивалентна $\mathfrak{G}_2'$. А для этого достаточно, в свою очередь, убедиться, что доказуемо подкванторное выражение этой формулы, которое мы обозначим $\mathfrak{D}'$.

Пусть $k$ — номер какого-либо доказательства формулы $\neg\mathfrak{G}_2'$. Из доказуемости (22) § 8.1 следует, что $\vdash x_2 \leq \boldsymbol{k} \vee \boldsymbol{k} < x_2$. Поэтому, если мы покажем, что $x_2 \leq \boldsymbol{k} \vdash \mathfrak{D}'$ и $\boldsymbol{k} < x_2 \vdash \mathfrak{D}'$, то по правилам УД и Т сможем получить $\vdash \mathfrak{D}'$. Но из доказуемости $\neg\mathfrak{G}_2'$ и непротиворечивости Ar следует, что формула $\mathfrak{G}_2' = \mathfrak{G}_2(\boldsymbol{m}_2)$ недоказуема; поэтому для любого натурального $n$ предложение $W_1(m_2, n)$ ложно и, значит, доказуема формула $\neg\mathfrak{B}_1(\boldsymbol{m}_1, \boldsymbol{n})$. В частности, доказуемы все формулы $\neg\mathfrak{B}_1(\boldsymbol{m}_2, 0)$, ..., $\neg\mathfrak{B}_1(\boldsymbol{m}_2, \boldsymbol{k})$, а вместе с ними и формулы $x_2 = 0 \supset \neg\mathfrak{B}_2(\boldsymbol{m}_2, x_2)$, ..., $x_2 = \boldsymbol{k} \supset \neg\mathfrak{B}_2(\boldsymbol{m}_2, x_2)$ (поскольку Ar есть исчисление на основе $G_1$ с равенством). Отсюда с помощью УИ и УД получается $x_2 = 0 \vee \cdots \vee x_2 = \boldsymbol{k} \vdash \neg\mathfrak{B}_1(\boldsymbol{m}_2, x_2)$. Но формула $x_2 = 0 \vee \cdots \vee x_2 = \boldsymbol{k}$ дедуктивно эквивалентна $x_2 \leq \boldsymbol{k}$ (ввиду утверждения 4 из § 8.1 и легко проверяемой дедуктивной эквивалентности формул $x < y + 1$ и $x \leq y$); таким образом, из формулы $x_2 \leq \boldsymbol{k}$ выводится первый член дизъюнкции $\mathfrak{D}'$, а значит, и она сама. С другой стороиы, поскольку $k$ — номер доказательства формулы $\neg\mathfrak{G}_2' = \neg\mathfrak{G}_2(m_2)$, предложение $W_2(m_2, k)$ истинно и, следовательно, доказуема формула $\mathfrak{B}_2(\boldsymbol{m}_2, \boldsymbol{k})$. Поэтому из $\boldsymbol{k} < x_2$ выводима формула $\boldsymbol{k} < x_2 \& \mathfrak{B}_2(\boldsymbol{m}_2, \boldsymbol{k})$, а из нее выводится $\exists x_3(x_3 < x_2 \& \mathfrak{B}_2(\boldsymbol{m}_2, x_3))$ — второй член дизъюнкции $\mathfrak{D}'$. Этим завершается доказательство теоремы.

Как и первоначальная форма, теорема Гёделя в форме Россера остается справедливой для любого простого расширения Ar с помощью рекурсивного множества формул. Действительно, в доказательстве этой теоремы мы пользовались, кроме представимости всех рекурсивных предикатов и рекурсивности предикатов, связанных с выводимостью (ср. соответствующее место предыдущего пункта), только доказуемостью (22) из § 8.1, утверждением 4 из того же параграфа и дедуктивной эквивалентностью формул $x < y + 1$ и $x \leq y$, т. е. доказуемостью некоторых формул; но всякая формула, доказуемая в Ar, доказуема и в любом его расширении. Таким образом, не только при условии ω-непротиворечивости, но и при условии обычной непротиворечивости неполноту формальной арифметики нельзя «исправить» добавлением новых аксиом.

**4.** Изложенный только что результат Гёделя вызвал в свое время у математиков немалое удивление, и такое же удивление он вызывает у свежего человека сейчас. Изучая математику, мы со школьных лет привыкаем к мысли, что она обосновывает свои истины путем строгих логических рассуждений, исходя из немногих простых посылок — аксиом. И чем больше мы погружаемся в ее изучение, тем ближе нам кажется идеал построения ее как единой дедуктивной системы. А так как все разделы математики так или иначе зависят от арифметики натуральных чисел, для осуществления идеала прежде всего необходимо построить формальную дедуктивную систему, полностью описывающую эту арифметику. Построение такой системы было одной из главных задач, которые ставили перед собой создатели теории логических исчислений[22] и казалось, что все средства для ее решения уже налицо: математики научились не только изображать арифметические утверждения в виде конечных последовательностей знаков строго определенного вида, но и доказательства этих утверждений представлять как формальные преобразования таких последовательностей, выполняемые чисто механически по очень простым правилам, хорошо отображающим принятые в обычной, не формализованной математике способы рассуждений; поэтому представлялось почти несомненным, что все арифметические утверждения, истинность которых можно доказать обычными рассуждениями, могут быть получены путем механических преобразований. Но каким бы очевидным ни казалось это утверждение, это была всего лишь гипотеза, которую нужно было проверить; математики давно уже привыкли признавать истинным только то, что строго доказано, и знали, что очевидность может оказаться обманчивой — хотя бывает это редко. И вот произошел как раз такой редкий случай. Гёдель доказал — вполне строго,— что гипотеза, представлявшаяся столь правдоподобной, на самом деле неверна: не все истинные арифметические предложения можно получить «механическим» путем из аксиом, и никакое расширение системы аксиом в этом не поможет. Итак, надежды на построение математики в виде формальной дедуктивной системы не оправдались: никакая формальная система, допускающая «механизацию» выводов, не может исчерпать даже арифметику натуральных чисел — и тем более всю математику.

Важнейший методологический вывод из этого факта состоит в том, что математические рассуждения в принципе не могут быть

---

[22] Программа обоснования математики в рамках строго формальной дедуктивной системы была выдвинута в начале нынешнего столетия Д. Гильбертом, стоявшим в вопросах обоснования математики на позициях формализма (см. Введение). (Следует заметить, впрочем, что сами формалисты так себя не называли.)

полностью сведены к механическим выкладкам. Выше (§ 5.5, пункт 5) говорилось о трудностях, с которыми связана реальная автоматизация процесса вывода в логическом исчислении; но оказывается, что даже если отвлечься от этих трудностей, автоматизация математических рассуждений невозможна, т. к. не все эти рассуждения можно формализовать с помощью логических исчислений. И даже доказательство теорем элементарной арифметики не всегда можно свести к формальным выкладкам. Сходный вывод можно сделать из существования неразрешимых алгоритмических проблем (см. § 7.6): для ряда задач «вычислительного» характера, в том числе очень просто формулируемых, нет никакого способа решать их в общем виде с помощью одних лишь механических выкладок. Итак: теорема Гёделя, равно как и факт существования неразрешимых алгоритмических проблем, показывает, что из математики в принципе невозможно изгнать содержательные рассуждения, заменив их формальными выкладками.

Несколько иначе можно сформулировать основной методологический вывод из теоремы Гёделя следующим образом: процесс рассуждения невозможно полностью математизировать, т. е. представить вполне адекватным образом в виде математической модели, и это справедливо даже для самых простых и самых строгих рассуждений — математических доказательств.

Можно, правда, спросить: имеем ли мы право делать из теоремы Гёделя выводы, относящиеся к любым способам формализации арифметики натуральных чисел — в ней ведь идет речь только об одном способе? Но легко понять, что для таких сомнений нет основания. В самом деле, свойства натуральных чисел, выражаемые аксиомами формальной арифметики, безусловно должны быть признаны истинными — иначе это будут уже не натуральные числа, а что-то другое. Столь же несомненным представляется, что правила вывода, действующие в исчислении Ar (или, что то же самое, в $G_1$), должны быть признаны законными с содержательной точки зрения. Поэтому всякое логическое исчисление, претендующее на роль формального эквивалента арифметики натуральных чисел, должно иметь среди своих основных или производных правил все правила исчисления Ar и среди своих аксиом или теорем все его аксиомы; следовательно, в таком исчислении должны быть доказуемы все формулы, доказуемые в Ar. Кроме того, мы, без сомнения, признáем пригодным для формализации арифметики только такое исчисление, в котором правила вывода будут обеспечивать рекурсивность отношения выводимости и множество аксиом будет рекурсивным. Но для любого исчисления с рекурсивным отношением выводимости и рекурсивным множеством аксиом, в котором доказуемы все формулы, доказуемые

в Ar, можно доказать теорему Гёделя (в обеих формах) так же, как для Ar.

Стоит еще заметить, что из теоремы Гёделя никоим образом не вытекает существование таких математических утверждений, которые нельзя было бы ни доказать, ни опровергнуть никаким математическим рассуждением. Неразрешимое предложение, существование которого устанавливается теоремой Гёделя, в действительности истинно[23], и его истинность доказывается одновременно с неразрешимостью как раз при доказательстве теоремы Гёделя. Ни для какого математического утверждения мы не располагаем доказательством его содержательной неразрешимости, т. е. недоказуемости и неопровержимости содержательными средствами (а не в каком-то логическом исчислении)[24]. Более того, следующее простое соображение показывает, что для широкого класса утверждений, включающего в себя, например, Великую теорему Ферма, доказательство содержательной неразрешимости невозможно[25]. Если Великая теорема Ферма неверна, т. е. существуют такие целые положительные числа $a, b, c, n$, где $n > 2$, что $a^n + b^n = c^n$, то проверка этого равенства будет доказательством того факта, что теорема неверна; поэтому если бы было найдено доказательство ее содержательной неразрешимости, она не могла бы быть неверной. Таким образом, предположение о существовании доказательства невозможности ни доказать, ни опровергнуть теорему Ферма приводит к противоречию, поскольку из такого доказательства немедленно получилось бы доказательство самой теоремы Ферма[26]. Ясно, что это соображение применимо к любому утверждению вида

$$\forall z_1 \cdots \forall z_n \; A(z_1, \ldots, z_n) \text{ или } \exists z_1 \cdots \exists z_n \; A(z_1, \ldots, z_n),$$

где $A$ — рекурсивный предикат.

5. Еще одно замечательное следствие из теоремы Гёделя состоит в том, что если исчисление Ar (или любое его простое расширение с помощью рекурсивного множества формул) непротиворечиво, то его

---

[23] Это означает (см. конец пункта 4 параграфа 6.3 и начало настоящего параграфа), что оно истинно в стандартной интерпретации формальной арифметики.

[24] Неразрешимость утверждения не следует смешивать с неразрешимостью алгоритмической проблемы. В первом случае речь идет о невозможности решить данную конкретную задачу, а во втором — всего лишь о невозможности решить целый класс задач одним способом (поэтому алгоритмические проблемы часто называют *массовыми проблемами*).

[25] Это соображение неоднократно приводил в устных беседах П.С. Новиков (именно на примере теоремы Ферма).

[26] (Добавлено в 1996 г.) Это было написано до того, как Великая теорема Ферма была доказана. Мы сохраняем этот пример, т. к. он очень нагляден и приводится лишь с иллюстративной целью.

непротиворечивость не может быть формально доказана в самом этом исчислении. Действительно, по теореме Гёделя из непротиворечивости Ar следует недоказуемость в нем формулы $\mathfrak{G}'_1$, и в то же время по лемме 2 из § 6.2 из недоказуемости в Ar хотя бы одной формулы следует его непротиворечивость. Таким образом, недоказуемость формулы $\mathfrak{G}'_1$ в исчислении Ar является необходимым и достаточным условием его непротиворечивости; однако формальным выражением недоказуемости формулы $\mathfrak{G}'_1$ в Ar служит сама эта формула — а она недоказуема в исчислении Ar, если только оно непротиворечиво!

Разумеется, формула $\mathfrak{G}'_1$ лишь косвенно выражает утверждение о непротиворечивости исчисления Ar. Но это утверждение можно выразить на его (исчисления Ar) собственном языке также и непосредственно — например, с помощью формулы

$$\neg\exists x_1\exists x_2\exists x_3\exists x_4(\mathfrak{D}(x_1, x_2)\&\mathfrak{D}(x_3, x_4)\&\mathfrak{N}(x_1, x_3)),$$

где $\mathfrak{D}$ и $\mathfrak{N}$ — формулы, представляющие соответственно предикат ДОК и функцию $\theta_7$ из § 8.3. Действительно, в стандартной интерпретации эта формула — мы обозначим ее НЕПР — имеет следующий смысл: «Не существует таких натуральных чисел $k_1$, $k_2$, $k_3$, $k_4$, чтобы $k_1$ и $k_3$ были номерами теорем исчисления Ar, а $k_2$ и $k_4$ — соответственно номерами их доказательств, и при этом теорема с номером $k_3$ была отрицанием теоремы с номером $k_1$», или проще: «Не существует двух теорем исчисления Ar, одна из которых есть отрицание другой». Можно доказать, что из формулы НЕПР выводима в Ar формула $\mathfrak{G}'_1$; отсюда ввиду теоремы 2 немедленно следует, что если Ar непротиворечиво, то формула НЕПР в нем недоказуема (и то же верно для любого простого расширения Ar с помощью рекурсивного множества формул). Это последнее утверждение носит название второй теоремы Гёделя; оно было впервые опубликовано К. Гёделем в той же статье [Gödel 1931], что и теорема о неполноте.

Таким образом, формула НЕПР, непосредственно выражающая на языке исчисления Ar его непротиворечивость, не может быть доказана в этом исчислении, если оно в действительности непротиворечиво. Доказательство этого факта, т. е. доказательство выводимости НЕПР$\vdash \mathfrak{G}'_1$, представляет собой, по существу, перевод на формальный язык тех содержательных рассуждений, которыми мы при доказательстве теоремы 2 установили, что из непротиворечивости Ar (являющейся в стандартной интерпретации смыслом формулы НЕПР) вытекает недоказуемость $\mathfrak{G}'_1$ (являющаяся в той же интерпретации смыслом $\mathfrak{G}'_1$). В полном изложении это доказательство громоздко; мы его приводить не будем. Подробное доказательство вто-

рой теоремы Гёделя имеется в книге [Гильберт — Бернайс 1982] (гл. V, §§ 1, 2) и в Добавлении I (написанном А.С. Есениным-Вольпиным) к книге [Клини 1957].

## § 8.5. ТЕОРЕМЫ ТАРСКОГО И ЧЁРЧА

1. В предыдущем параграфе мы показали, что если в конструкции, приводящей при неформальных рассуждениях к парадоксу лжеца, заменить истинность доказуемостью, то перевод такой конструкции на язык формальной арифметики не дает парадокса, но позволяет построить неразрешимое предложение, т. е. замкнутую формулу, которую нельзя ни доказать, ни опровергнуть. А что получится, если попытаться перевести на язык формальной арифметики т у с а м у ю конструкцию, которая приводит к парадоксу лжеца?

Излагая этот парадокс во Введении, мы еще не пользовались логической символикой. С ее помощью парадокс можно сформулировать так. Пусть $И(p)$ — предикат, определенный на множестве предложений и означающий «Предложение $p$ истинно», и $M(t, p)$ — предикат, в котором первая переменная пробегает моменты времени и вторая — предложения, означающий «В момент времени $t$ критянин произносит предложение $p$» (мы считаем для простоты, что произнесение предложения — «моментальный» акт). Тогда, если в некоторый момент времени $t_0$ критянин произнесет предложение $\forall p(M(t_0, p) \supset \neg И(p))$, то, обозначив это предложение $p_0$, мы увидим, что — поскольку $M(t_0, p_0)$ истинно — из истинности предложения $p_0$ следует истинность предложения $\neg И(p_0)$, т. е. ложность $p_0$, а из ложности $p_0$ — ложность $\neg И(p_0)$, т. е. истинность $p_0$[27]. Теперь понятно, в чем трудность формализации этого рассуждения: в формальном выражении того обстоятельства, что предложение $p_0$ произносится именно в момент $t_0$. Ведь критянин говорит в каждый момент то, что ему вздумается сказать, так что формализовать предикат $M(t, p)$ было бы затруднительно.

Эту трудность можно если не преодолеть, то обойти следующим образом. Допустим, что наш критянин наряду с обычными предложениями произносит также предложения вида $p(t)$, где $t$ — переменная, пробегающая моменты времени. Иначе говоря, он не

[27] Поскольку $p_0$ есть единственное предложение, произносимое критянином в момент $t_0$. (Естественно считать, что он не может произнести в один момент более одного предложения.)

только высказывает истинные или ложные предложения, но еще и описывает свойства моментов времени. Тогда, если в некоторый момент времени $t_1$ он опишет свойство $C_0$ моментов времени, состоящее в том, что если в момент $t$ он описывает какое-то свойство, то сам момент $t$ этим свойством не обладает, то из допущения, что момент $t_1$ обладает свойством $C_0$, следует, что он им не обладает, а из допущения, что $t_1$ им не обладает — что он им обладает. Такой усложненный вариант парадокса лжеца не столь выразителен и нагляден, как первоначальный, зато его нетрудно перевести на формальный язык. Для этого: а) заменим предикат $И(p)$ предикатом $И_1(t)$, определенным на множестве моментов времени и означающим «Если в момент $t$ критянин произносит предложение, то оно истинно»; б) введем предикат $П(t, t')$, также определенный на множестве моментов времени и означающий «Если в момент $t$ критянин описывает некоторое свойство $C$ моментов времени, то в момент $t'$ он произносит предложение „Момент $t$ обладает свойством $C$“»; в) допустим, что если в момент $t$ описывается некоторое свойство, то существует момент $t'$, для которого $П(t, t')$ истинно. Тогда свойство $C_0$, о котором говорилось выше, будет выражаться формулой $\forall t'(П(t, t') \supset \neg И_1(t'))$, и совершенно аналогично тому, как выше мы видели, что предложение $p_0 = \forall p(M(t_0, p) \supset \neg И(p))$ не истинно и не ложно, теперь мы видим, что таково же предложение $C_0(t_1) = \forall t'(П(t_1, t') \supset \neg И_1(t'))$ (поскольку по допущению в) существует момент $t_2$, для которого $П(t, t_2)$ истинно). Однако в отличие от выражения для $p_0$ выражение для $C_0(t)$ не содержит затруднившего нас предиката $M(t, p)$, и вдобавок в нем участвуют переменные только одного сорта — пробегающие моменты времени. Разумеется, предикат $П(t, t')$ тоже зависит от произвола критянина; но если критянин захочет облегчить нам задачу, он постарается строить свою речь так, чтобы зависимость между $t$ и $t'$ была не слишком сложной. Это особенно легко сделать, если отождествить моменты времени с натуральными числами; тогда достаточно попросить критянина высказывать только такие предложения и описывать только такие свойства, которые выражаются формулами формальной арифметики, причем моментом произнесения каждой формулы должен быть ее номер. (Заодно стоит на всякий случай попросить его произносить также и формулы с несколькими свободными переменными.) Сможет ли он тогда описать свойство $C_0$ — иначе говоря, можно ли это свойство выразить формулой формальной арифметики? Безусловно, можно, если существуют формулы формальной арифметики $\Omega(x_1, x_2)$ с двумя свободными переменными $x_1$ и $x_2$ и $\Re(x_2)$ с одной свободной переменной $x_2$, выражающие (в стандартной интерпретации) соответственно преди-

каты $\Pi$ и $И_1$; тогда свойство $C_0$ будет выражаться, очевидно, формулой $\forall x_2(\mathfrak{Q}(x_1, x_2) \supset 7\mathfrak{R}(x_2))$, которую мы обозначим $\mathfrak{C}_0(x_1)$. Но это быстро приводит нас к противоречию. В самом деле, пусть $c$ — номер формулы $\mathfrak{C}_0(x_1)$ и $d$ — номер формулы $\mathfrak{C}_0(\boldsymbol{c})$. Тогда предложение $\mathfrak{Q}(\boldsymbol{c}, \boldsymbol{d})$ истинно[28]; но если при этом истинно также и предложение $\mathfrak{C}_0(\boldsymbol{c}) = \forall x_2(\mathfrak{Q}(\boldsymbol{c}, x_2) \supset 7\mathfrak{R}(x_2))$, то вместе с ним истинна и импликация $\mathfrak{Q}(\boldsymbol{c}, \boldsymbol{d}) \supset 7\mathfrak{R}(\boldsymbol{d})$, так что из истинности $\mathfrak{Q}(\boldsymbol{c}, \boldsymbol{d})$ вытекает ложность $\mathfrak{R}(\boldsymbol{d})$, но $\mathfrak{R}(\boldsymbol{d})$ ложно тогда и только тогда, когда ложно предложение с номером $d$, т. е. $\mathfrak{C}_0(\boldsymbol{c})$; если же $\mathfrak{C}_0(\boldsymbol{c})$ ложно, то $7\mathfrak{R}(\boldsymbol{d})$ истинно (по смыслу формулы $\mathfrak{R}$) и поэтому истинна импликация $\mathfrak{Q}(\boldsymbol{c}, \boldsymbol{d}) \supset 7\mathfrak{R}(\boldsymbol{d})$; а отсюда следует — поскольку для всякого числа $n$, отличного от $d$, предложение $\mathfrak{Q}(\boldsymbol{c}, \boldsymbol{n})$ ложно — что истинно также и предложение $\forall x_2(\mathfrak{Q}(\boldsymbol{c}, x_2) \supset \mathfrak{R}(x_2)) = \mathfrak{C}_0(\boldsymbol{c})$.

Проведенное сейчас рассуждение ничем, кроме терминологии, не отличается от того, которое выше привело нас к парадоксу лжеца (в усложненном варианте). Но теперь, после формализации, оно превращается в обычное доказательство от противного и приводит не к парадоксу, а всего лишь к выводу, что наше допущение о существовании формул $\mathfrak{Q}$ и $\mathfrak{R}$, выражающих в стандартной интерпретации предикаты $\Pi$ и $И_1$, было неверно. Однако формула, выражающая $\Pi$, существует. В самом деле, в § 8.3 (конец пункта 2) мы доказали рекурсивность функции $d(y)$, которая всякому числу $y$, являющемуся номером формулы $\mathfrak{A}(x_1)$ с одной свободной переменной $x_1$, сопоставляет номер формулы $\mathfrak{A}(\boldsymbol{y})$, а вместе с этой функцией рекурсивен предикат $d(y) = z$, равносильный $\Pi(y, z)$; поэтому по теореме из § 8.2 существует формула $\mathfrak{Q}(x_1, x_2)$ исчисления Ar с двумя свободными переменными $x_1$, $x_2$, такая, что для любых чисел $m$, $n$ имеет место $\vdash \mathfrak{Q}(\boldsymbol{m}, \boldsymbol{n})$, если $n = d(m)$, и $\vdash 7\mathfrak{Q}(\boldsymbol{m}, \boldsymbol{n})$, если $n \neq d(m)$; но поскольку стандартная интерпретация является моделью исчисления Ar, из доказуемости формулы $\mathfrak{Q}(\boldsymbol{m}, \boldsymbol{n})$ вытекает ее истинность в стандартной модели, а из доказуемости ее отрицания — ее ложность. Таким образом, формула $\mathfrak{Q}$ выражает предикат $\Pi$. Следовательно, *не существует формулы, выражающей предикат* $И_1$.

Итак, мы доказали следующую теорему:

**Теорема 1 (теорема Тарского)**[29]. Не существует формулы формальной арифметики $\mathfrak{R}(x_1)$ с одной свободной переменной $x_1$, такой,

---

[28] Под истинностью и ложностью в этом рассуждении подразумевается истинность и ложность в стандартной интерпретации (так что истинность $\mathfrak{Q}(\boldsymbol{c}, \boldsymbol{d})$ означает истинность $И(c, d)$, и т.п.).

[29] А. Тарский (Alfred Tarski, 1902—1983) — польский логик и математик (с 1939 г. жил в США).

что для произвольного натурального $n$ предложение $\mathfrak{R}(n)$ истинно в стандартной интерпретации тогда и только тогда, когда $n$ есть номер замкнутой формулы формальной арифметики, истинной в стандартной интерпретации.

(Доказывая эту теорему, мы незаметно потеряли из вида критянина. Если снова встретим его когда-нибудь — поблагодарим за помощь!)

Назовем множество натуральных чисел $M$ *арифметическим*, если существует формула формальной арифметики $\mathfrak{A}(x_1)$ с одной свободной переменной $x_1$, такая, что $n \in M$ тогда и только тогда, когда формула $\mathfrak{A}(n)$ истинна в стандартной интерпретации. С помощью этого понятия теорему Тарского можно сформулировать так:

Теорема 1′. Множество номеров формул формальной арифметики, истинных в стандартной интерпретации, не является арифметическим.

Содержательно эта теорема означает, что понятие истинности в формальной арифметике невозможно определить внутри самой формальной арифметики.

2. Рассуждения, которыми доказывается теорема Тарского, легко перенести из плана истинности в план доказуемости. Тогда получается следующая теорема:

Теорема 2. Предикат «быть номером доказуемой формулы формальной арифметики» не представим в формальной арифметике, если она непротиворечива.

Доказательство. Допустим, что существует формула $\mathfrak{B} = \mathfrak{B}(x_1)$, представляющая этот предикат, т. е. такая, что для всякого числа $n$, являющегося номером какой-либо формулы $\mathfrak{A}$, имеет место $\vdash \mathfrak{B}(n)$, если $\mathfrak{A}$ доказуема, и $\vdash \neg\mathfrak{B}(n)$, если $\mathfrak{A}$ не доказуема. Обозначим через $\mathfrak{P}(x_1, x_2)$ формулу, представляющую функцию $d(x_1)$[30], и рассмотрим формулу

$$\mathfrak{D}(x_1) = \forall x_2(\mathfrak{P}(x_1, x_2) \supset \neg\mathfrak{B}(x_2)).$$

Пусть $k$ — номер этой формулы. Рассмотрим теперь формулу

$$\mathfrak{D}(k) = \forall x_2(\mathfrak{P}(k, x_2) \supset \neg\mathfrak{B}(x_2));$$

ее номер обозначим через $l$.

Допустим теперь, что формула $\mathfrak{D}(k)$ доказуема. Вместе с ней доказуема и формула $\mathfrak{P}(k, l) \supset \neg\mathfrak{B}(l)$; но, поскольку $l = d(k)$ и формула $\mathfrak{P}$ представляет функцию $d$, имеем $\vdash \mathfrak{P}(k, l)$, откуда $\vdash \neg\mathfrak{B}(l)$; но тогда, если формальная арифметика непротиворечива, невозможно

[30] А не предикат $d(x_1) = x_2$, как в предыдущем пункте.

$\vdash \mathfrak{B}(l)$, а отсюда по определению формулы $\mathfrak{B}$ следует, что формула с номером $l$, т. е. $\mathfrak{D}(k)$, недоказуема.

С другой стороны, если $\mathfrak{D}(k)$ недоказуема, то недоказуема и формула $\mathfrak{P}(k, l) \supset \neg\mathfrak{B}(l)$. (Действительно, поскольку $\mathfrak{P}$ представляет функцию $d$ и $d(k) = l$, имеем $\vdash \forall x_2(\mathfrak{P}(k, x_2) \supset x_2 = l)$ (условие (3′) в начале § 8.2), а из этой формулы и формулы $\mathfrak{P}(k, l) \supset \neg\mathfrak{B}(l)$ легко вывести $\mathfrak{D}(k)$.) Поэтому недоказуема и $\neg\mathfrak{B}(l)$ (см. (8) в § 5.3); между тем по определению формулы $\mathfrak{B}$ в случае, когда формула с номером $l$, т. е. $\mathfrak{D}(k)$, недоказуема, формула $\neg\mathfrak{B}(l)$ должна быть доказуемой. Полученное противоречие завершает доказательство.

Из доказанной сейчас теоремы и теоремы из § 8.2 немедленно вытекает

Следствие. Множество номеров теорем формальной арифметики неразрешимо. Иначе говоря: не существует алгоритма, позволяющего по номеру формулы формальной арифметики (или, безразлично, по самой формуле[31]) узнавать, является ли эта формула доказуемой.

Замечания. 1) В доказательстве теоремы 2 из всех свойств формальной арифметики (исчисления Ar) использовано только то, что в ней представима функция $d$. Поэтому теорема 2 — и вместе с ней отмеченное нами следствие из нее — справедлива для любого непротиворечивого исчисления на основе $G_1$ с равенством, алфавит которого совпадает с алфавитом Ar[32] и в котором представимы все рекурсивные функции. В частности, теорема 2 сохраняет силу для любого непротиворечивого простого расширения исчисления Ar.

2) Множество номеров формул формальной арифметики, истинных в стандартной интерпретации, также неразрешимо (см. в конце главы задачу 18а).

3) Легко видеть, что множество номеров теорем формальной арифметики перечислимо. В самом деле, оно совпадает с множеством значений частично рекурсивной функции $\mu x Д\text{ОК}(x, y)$.

3. Логическое исчисление называют *разрешимым*, если существует алгоритм, позволяющий по любой его формуле узнать, является ли она теоремой (иначе — если множество его теорем разрешимо).

Пользуясь этим понятием, мы можем сформулировать следствие из теоремы 2 так: формальная арифметика неразрешима.

Что можно сказать о разрешимости исчислений, рассматривавшихся в предыдущих главах? Исчисление предложений разрешимо,

---

[31] Поскольку существуют алгоритмы, позволяющие находить по формуле ее номер и формулу по номеру (точнее — для всякого натурального числа узнавать, является ли оно номером формулы, и если да — строить эту формулу).

[32] Совпадение алфавитов необходимо для того, чтобы не изменилось определение номера формулы.

т. к. его формула тогда и только тогда является теоремой, когда она тождественно истинна, а свойство формулы быть тождественно истинной проверяемо. Что же касается исчисления предикатов, то оно неразрешимо. Сейчас мы займемся доказательством этого факта. Предварительно рассмотрим еще одно логическое исчисление с тем же алфавитом и теми же правилами вывода, что и Ar, и следующими аксиомами:

$(\rho_1)\ x_1 = x_1;$

$(\rho_2)\ x_1 = x_2 \supset x_2 = x_1;$

$(\rho_3)\ x_1 = x_2 \& x_2 = x_3 \supset x_1 = x_3;$

$(\rho_4)\ x_1 = x_2 \supset x_1' = x_2';$

$(\rho_5)\ x_1' = x_2' \supset x_1 = x_2;$

$(\rho_6)\ \neg\exists x_1(x_1' = 0);$

$(\rho_7)\ \neg(x_1 = 0) \supset \exists x_2(x_1 = x_2');$

$(\rho_8)\ x_1 + 0 = x_1;$

$(\rho_9)\ x_1 + x_2' = (x_1 + x_2)';$

$(\rho_{10})\ x_1 \cdot 0 = 0;$

$(\rho_{11})\ x_1 \cdot x_2' = x_1 \cdot x_2 + x_1;$

$(\rho_{12})\ x_1 = x_2 \supset (x_1 + x_3 = x_2 + x_3 \& x_3 + x_1 = x_3 + x_2);$

$(\rho_{13})\ x_1 = x_2 \supset (x_1 \cdot x_3 = x_2 \cdot x_1 \& x_3 \cdot x_1 = x_3 \cdot x_2);$

$(\rho_{14})\ x_1 = x_2 \cdot x_3 + x_4 \& x_4 < x_2 \& x_1 = x_2 \cdot x_5 + x_6 \& x_6 < x_2 \supset x_4 = x_6$

(единственное достатка; знак < понимается здесь как сокращение — см. § 8.1, пункт 4);

$(\rho_{15})\ x_1 + x_2 = x_2 + x_1.$

Это исчисление (введенное Р. Робинсоном[33]) мы будем обозначать $R$. Аксиомы $(\rho_1) - (\rho_6)$, $(\rho_8) - (\rho_{11})$ отличаются от схем $(r)$, $(s)$, $(t)$, $(\alpha_1) - (\alpha_3)$, $(\alpha_5) - (\alpha_8)$ исчисления Ar только тем, что метапеременные $x$, $y$, $z$ заменены конкретными переменными $x_1$, $x_2$, $x_3$. Это различие, как мы знаем, несущественно, так что фактически $R$ отличается от Ar только тем, что схема $(\alpha_4)$ («аксиома индукции») заменена пятью новыми аксиомами. Исчисление $R$ слабее, чем Ar

[33] Собственно, Р. Робинсоном было предложено исчисление с аксиомами $(\rho_1) - (\rho_{13})$ (см. ниже комментарий).

(см. задачу 19 в конце главы), но все же, как мы увидим, достаточно сильно, чтобы представить в нем все рекурсивные функции. Поэтому для него сохраняет силу теорема 2 (см. замечание 1 в конце предыдущего пункта) и, следовательно, оно неразрешимо. В то же время, поскольку множество его аксиом конечно, из его неразрешимости нетрудно будет вывести неразрешимость исчисления с тем же алфавитом совсем без аксиом (не считая закона исключенного третьего) — т. е. исчисления предикатов с «арифметическим» алфавитом,— а затем и «настоящего» исчисления предикатов. Таков план, к реализации которого мы теперь приступим.

Заметим прежде всего, что по теореме 5 из § 6.3 $R$ есть исчисление на основе $G_1$ с равенством (примеиимость этой теоремы обеспечивается аксиомами $(\rho_1) - (\rho_4)$, $(\rho_{12})$, $(\rho_{13})$). Далее, поскольку все аксиомы $(\rho_1) - (\rho_{15})$ являются теоремами исчисления Ar, всякая теорема исчисления $R$ будет теоремой и в Ar. Обратное неверно (см. задачу 19 в конце главы), но все же многие теоремы Ar остаются теоремами в $R$. В частности, для $R$ сохраняют силу утверждения 1—4 из § 8.1. Утверждения 1 и 2 доказываются так же, поскольку в их доказательствах используются только аксиомы $(r)$, $(s)$, $(t)$, $(\alpha_1)$, $(\alpha_5) - (\alpha_8)$, фактически имеющиеся и в $R$, а также (3) из § 8.1, очевидным образом вытекающее из $(\rho_{12})$[34]. Докажем утверждение 3. Пусть $m \neq n$; для определенности положим $m < n$. Нам достаточно привести к противоречию утверждение $\vdash \boldsymbol{m} = \boldsymbol{n}$. Однако, поскольку в нашем случае $n > 0$, по определению цифры терм $\boldsymbol{n}$ совпадает с $(\boldsymbol{n-1})'$. Поэтому при $m = 0$ утверждение $\vdash \boldsymbol{m} = \boldsymbol{n}$ противоречит аксиоме $(\rho_6)$, а при $m \neq 0$ из этого утверждения, равносильного тогда $\vdash (\boldsymbol{m-1})' = (\boldsymbol{n-1})'$, ввиду аксиомы $(\rho_5)$ следует $\vdash \boldsymbol{m-1} = \boldsymbol{n-1}$, затем $\vdash \boldsymbol{m-2} = \boldsymbol{n-2}$ и т. д. — и, наконец, $\vdash \boldsymbol{0} = \boldsymbol{n-m}$, что опять-таки, поскольку $n - m > 0$, противоречит аксиоме $(\rho_6)$. В утверждении 4 доказуемость первого члена конъюнкции мы установим неформальной индукцией. Ее базис состоит в доказательстве того, что $\vdash x < \mathbf{1} \supset x = \mathbf{0}$, подробнее $\vdash \exists z(\mathbf{1} = x + z') \supset x = \mathbf{0}$. Но из $\exists z(\mathbf{1} = x + z')$, легко вывести $\exists z(\mathbf{1} = (x + z)')$ (ввиду $(\rho_9)$. Отсюда, поскольку $\mathbf{1}$ есть $\mathbf{0}'$, выводится $\exists z(\mathbf{0} = x + z)$ (ввиду $(\rho_5)$), откуда затем можно вывести $x = \mathbf{0}$ следующим способом: из $\mathbf{0} = x + z$ и $\neg(z = \mathbf{0})$ с использованием $(\rho_7)$ и $(\rho_9)$ выводится $\exists y(\mathbf{0} = (x + y)')$, что противоречит аксиоме $(\rho_6)$; поэтому $\mathbf{0} = x + z \vdash z = \mathbf{0}$, откуда с использованием $(\rho_8)$ получается $\mathbf{0} = x + z \vdash \mathbf{0} = x$ и далее $\mathbf{0} = x + z \vdash x = \mathbf{0}$; остается применить УЭ. Индукционный шаг

[34] (3) из 8.1 используется в доказательстве пункты б) утверждения 1.

будет очевиден, если доказать, что $x < \boldsymbol{n}+2 \vdash x < \boldsymbol{n}+1 \vee x = \boldsymbol{n}+1$. Но из $x < \boldsymbol{n}+2$, т. е. из $\exists z(\boldsymbol{n}+2 = x + z')$, с помощью $(\rho_9)$ и $(\rho_5)$ выводится $\exists z(\boldsymbol{n}+1 = x + z)$; чтобы вывести из этой формулы дизъюнкцию $x < \boldsymbol{n}+1 \vee x = \boldsymbol{n}+1$, достаточно вывести ее из $\boldsymbol{n}+1 = x + z$; но из $\boldsymbol{n}+1 = x + z$ с дополнительной гипотезой $z = 0$ выводится $x = \boldsymbol{n}+1$, а с дополнительной гипотезой $\neg(x = 0)$ выводится (с помощью $(\rho_7)$) $\exists y(\boldsymbol{n}+1 = x + y')$, т. е. $x < \boldsymbol{n}+1$; остается применить ВД и ИТ. Доказуемость второго члена конъюнкции в утверждении 4 будет установлена, если мы убедимся, что при $m < n$ справедлива выводимость $x = \boldsymbol{m} \vdash x < \boldsymbol{n}$, но это немедленно вытекает из утверждения 2.

Для дальнейшего нам понадобятся еще две доказуемости:

(*) $\vdash_R \boldsymbol{0} \leq x$;

(**) $\vdash_R x \leq \boldsymbol{n} \vee \boldsymbol{n} \leq x$ ($n$ — любое натуральное число).

Чтобы доказать (*), заметим, что формула $y \leq z$, как легко видеть, дедуктивно эквивалентна (в $R$, как, впрочем, и в Ar) формуле $\exists w(z = y + w)$. Поэтому достаточно убедиться, что $\vdash \exists w(x = 0 + w)$; но это сразу следует из $(\rho_8)$ и $(\rho_{15})$.

Для доказательства (**) воспользуемся неформальной индукцией. Базис обеспечивается доказуемостью (*). Проведем индукционный шаг. Пусть для некоторого $n$ справедливо $\vdash x \leq \boldsymbol{n} \vee \boldsymbol{n} \leq x$. Чтобы доказать $\vdash x \leq \boldsymbol{n}+1 \vee \boldsymbol{n}+1 \leq x$, заметим сначала, что, поскольку из $(\rho_7)$ следует $\vdash x = 0 \vee \exists y(x = y')$, достаточно убедиться, что $x = 0 \vdash x \leq \boldsymbol{n}+1 \vee \boldsymbol{n}+1 \leq x$ и $\exists y(x = y') \vdash x \leq \boldsymbol{n}+1 \vee \boldsymbol{n}+1 \leq x$. Но первая из этих двух выводимостей очевидным образом вытекает из (*), а вторую можно получить так: поскольку из первого члена дизъюнкции $y \leq \boldsymbol{n} \vee \boldsymbol{n} \leq y$, доказуемой ввиду предположения индукции, можно с помощью $(\rho_{15})$, $(\rho_9)$ и $(\rho_4)$ вывести $y' \leq \boldsymbol{n}+1$, а из второго таким же способом $\boldsymbol{n}+1 \leq y'$, имеем $\vdash y' \leq \boldsymbol{n}+1 \vee \boldsymbol{n}+1 \leq y'$, а отсюда уже легко получается нужная выводимость.

Теперь можно убедиться, что проведенное в § 8.2 доказательство теоремы о представимости в исчислении Ar рекурсивных функций остается в силе для исчисления $R$. Из всех свойств исчисления Ar (не считая того, что оно есть исчисление на основе $G_1$ с равенством) мы пользовались в этом доказательстве только утверждениями 1, 2 и 4 из § 8.1, справедливыми, как мы видели, и для $R$, и доказуемостями (21), (22), (23) и (35) из того же параграфа. Но при этом (21) использовалось только для того, чтобы вывести $x < \boldsymbol{i}+1$ из $x \leq \boldsymbol{i}$ (см. с. 379), а это легко сделать непосредственно с помощью $(\rho_9)$; (22) использовалось только для того, чтобы получить

$\neg(y = l) \vdash y < l \vee y > l$ (см. с. 376), а это равносильно только что установленной доказуемости (**); (23) справедливо и для $R$ (следует из $(\rho_6)$ и $(\rho_9)$); наконец, (35) (существование и единственность остатка) используется только при доказательстве усиленного условия (3) для формулы $\mathfrak{G}$ (см. с. 377), а это последнее также используется только один раз (с. 379), и притом таким образом, что вместо него можно воспользоваться доказуемостью

$$\vdash \forall y \forall z(\mathfrak{G}(x_1, x_2, x_3, y) \& \mathfrak{G}(x_1, x_2, x_3, z) \supset y = z),$$

для получения которой достаточно единственности остатка, т. е. аксиомы $(\rho_{14})$. Подробную проверку читатель может провести сам.

Итак, в исчислении $R$ представимы все рекурсивные функции. Поэтому — см. замечание 1 в конце предыдущего пункта — мы можем считать доказанной следующую теорему:

**Теорема 3.** Если исчисление $R$ непротиворечиво, то оно неразрешимо.

**Замечания.** 1) Эта теорема справедлива и для любого простого расширения $R$.

2) Представимость в $R$ всех рекурсивных функций позволяет также повторить для этого исчисления доказательство теоремы Гёделя (как в первоначальной форме, так и в форме Россера).

**Комментарий.** Доказательство неполноты и неразрешимости исчисления Робинсона в его первоначальном виде (с аксиомами $(\rho_1)$ — $(\rho_{13})$) можно найти в книге [Клини 1957]. Аксиома $(\rho_{14})$ добавлена ради упрощения рассуждений Э. Мендельсоном [Мендельсон 1971]. Аксиома $(\rho_{15})$ добавлена с той же целью автором этих строк. Без нее нетрудно обойтись, если понимать $t < u$ как сокращение для $\exists z(u = z' + t)$ (так и сделано в книге [Клини 1957]), но автору неизвестно, можно ли доказать утверждения (*) и (**), не пользуясь коммутативностью сложения, если $t < u$ означает $\exists z(u = t + z')$, как в нашей книге (и в книге [Мендельсон 1971], где утверждение (**) сформулировано без доказательства). Читатель без труда убедится, что в приведенных нами доказательствах использование $(\rho_{15})$ станет излишним, если понимать $t < u$ как $\exists z(u = z' + t)$.

Далее мы позволим себе считать исчисление $R$ непротиворечивым — что представляется весьма вероятным, поскольку интуитивно ясно, что все аксиомы этого исчисления верны в стандартной интерпретации (и эту интуицию можно считать более убедительной, чем для Ar, так как множество аксиом конечно), и в самой этой интерпретации, по-видимому, нет противоречий[35]. В о в с е х

[35] Имеются, впрочем, и доказательства непротиворечивости $R$. См., например, [Клини 1957], § 79.

дальнейших формулировках условие непротиворечивости $R$ будет подразумеваться.

Перейдем теперь к выполнению второй части плана, намеченного на с. 408.

Лемма 1. Если исчисление на основе $G_1$ разрешимо, то всякое его простое расширение с помощью конечного множества формул также разрешимо.

Доказательство. Пусть $L$ — исчисление на основе $G_1$ и $L'$ — его простое расширение с помощью конечного множества формул $\Gamma$. Достаточно рассмотреть случай, когда $\Gamma$ состоит из одной формулы $\mathfrak{A}$ и, более того, когда эта формула замкнута[36]. Но в этом случае по лемме 1 из § 6.2 формула $\mathfrak{B}$ тогда и только тогда будет теоремой исчисления $L'$, когда она выводима в $L$ из $\mathfrak{A}$, а это, в свою очередь, справедливо тогда и только тогда, когда в $L$ доказуема формула $\mathfrak{A} \supset \mathfrak{B}$. Поэтому из алгоритма проверки доказуемости в $L$ немедленно получается алгоритм проверки доказуемости в $L'$.

Следствие. Если исчисление на основе $G_1$ имеет неразрешимое простое расширение с помощью конечного множества формул, то оно и само неразрешимо.

Из этого следствия и теоремы 3 непосредственно вытекает

Теорема 4. Исчисление $G_1^{Ar}$, полученное из $R$ изъятием всех аксиом, кроме ИТ, (иначе — полученное из $G_1$ ограничением алфавита символами, входящими в алфавит исчисления Ar) неразрешимо.

Обозначим теперь через $G_1^-$ исчисление, полученное из $G_1$ изъятием из алфавита всех функциональных символов и символов предметных констант с соответствующим изменением определения формулы (*«чистое исчисление предикатов»*).

Лемма 2. Существует алгоритм, позволяющий по любой формуле $\mathfrak{A}$ исчисления $G_1$ построить формулу $\mathfrak{A}'$ исчисления $G_1^-$ таким образом, что $\vdash_{G_1} \mathfrak{A}$ тогда и только тогда, когда $\vdash_{G_1^-} \mathfrak{A}'$.

Доказательство. Для формулы $\mathfrak{A}$, не содержащей функциональных символов и символов предметных констант, положим $\mathfrak{A}' = \mathfrak{A}$. В общем случае формула $\mathfrak{A}'$ строится следующим образом. Пусть $a_i$ — первый входящий в $\mathfrak{A}$ символ предметной константы (если таковой имеется), $F_j^1$ — первый не входящий в $\mathfrak{A}$ одноместный предикатный символ и $x_k$ — первая не входящая в $\mathfrak{A}$ переменная. Обозначим через $\mathfrak{A}^*$ результат замены в формуле $\mathfrak{A}$ всех вхождений символа $a_i$

[36] Действительно, во всяком исчислении на основе $G_1$ (ввиду правил ВА и УА) формула тогда и только тогда является теоремой, когда это верно для ее замыкания. Поэтому, заменяя одну из аксиом исчисления ее замыканием, мы не изменяем множества его теорем.

вхождениями переменной $x_k$ и положим $\mathfrak{A}_1 = \exists x_k F^1_j(x_k) \supset \supset \exists x_k (F^1_j(x_k) \& \mathfrak{A}^*)$. Нетрудно видеть, что формула $\mathfrak{A}_1$ тогда и только тогда всюду истинна, когда всюду истинна формула $\mathfrak{A}$. В самом деле: а) Пусть $\mathfrak{A}$ всюду истинна, $I_1$ — произвольная интерпретация формулы $\mathfrak{A}_1$ и $\Phi$ — предикат, сопоставляемый в этой интерпретации символу $F^1_j$. Тогда, если предикат $\Phi$ тождественно ложен, формула $\mathfrak{A}_1$ очевидным образом истинна в $I_1$; в противном случае, рассмотрев интерпретацию $I$ формулы $\mathfrak{A}$, в которой всем входящим в обе формулы предикатным и функциональным символам и символам предметных констант сопоставляется то же, что в интерпретации $I_1$, а символу $a_i$ — элемент $b$ основного множества[37], такой, что $\Phi(b) \equiv И$, сразу видим, что из истинности $\mathfrak{A}$ в $I$ вытекает истинность $\mathfrak{A}_1$ в $I_1$. б) Пусть $\mathfrak{A}_1$ всюду истинна, $I$ — произвольная интерпретация формулы $\mathfrak{A}$ и $b$ — элемент, сопоставляемый в этой интерпретации символу $a_i$. Рассмотрев интерпретацию $I_1$ формулы $\mathfrak{A}_1$, в которой всем символам, входящим в обе формулы, сопоставляется то же, что в $I$, а символу $F^1_j$ — предикат $\Phi$, такой, что $\Phi(b) \equiv И$ и $\Phi(z) \equiv Л$ для всех $z \neq b$, немедленно убеждаемся, что из истинности $\mathfrak{A}_1$ в $I_1$ следует истинность $\mathfrak{A}$ в $I$. Далее, если в формуле $\mathfrak{A}_1$ еще есть символы предметных констант, повторяем описанное преобразование — и так до тех пор, пока не получим формулу $\mathfrak{B}$, не содержащую символов предметных констант и всюду истинную тогда и только тогда, когда всюду истинна $\mathfrak{A}$. Если в формуле $\mathfrak{B}$ есть функциональные символы, поступим следующим образом. Пусть $n$ — наименьшее число, для которого формула $\mathfrak{A}$ содержит $n$-местные функциональные символы, и пусть $f^n_{i_1}, \ldots, f^n_{i_m}$ — все эти символы в порядке возрастания нижних индексов, и $F^{n+1}_{j_1}, \ldots, F^{n+1}_{j_m}$ — первые $m$ не входящих в $\mathfrak{B}$ $(n+1)$-местных предикатных символов в аналогичном порядке. Сопоставим каждому символу $f^n_{i_k}$ предикатный символ $F^{n+1}_{j_k}$. Рассмотрим теперь самый левый входящий в $\mathfrak{B}$ терм вида $f^n_i(t_1, \ldots, t_n)$, такой, что термы $t_1, \ldots, t_n$ не содержат вхождений функциональных символов. Пусть $F^{n+1}_i$ — предикатный символ, сопоставленный функциональному символу $f^n_i$, и $x_s$ — первая не входящая в $\mathfrak{B}$ переменная. Обозначим через $\mathfrak{B}^*$ результат замены в формуле $\mathfrak{B}$ всех вхождений терма $f^n_i(t_1, \ldots, t_n)$ вхождениями переменной $x_s$ и положим

$$\mathfrak{B}_1 = \exists x_s F^{n+1}_i(t_1, \ldots, t_n, x_s) \supset \exists x_s (F^{n+1}_i(t_1, \ldots, t_n, x_s) \& \mathfrak{B}^*).$$

[37] Основное множество интерпретации $I$ — то же, что у $I_1$.

Аналогично предыдущему[38] нетрудно видеть, что формула $\mathfrak{B}_1$ тогда и только тогда всюду истинна, когда это верно для $\mathfrak{B}$. Если формула $\mathfrak{B}_1$ еще содержит вхождения функциональных символов, повторим это преобразование, и так до тех пор, пока не получим формулу $\mathfrak{A}'$, не содержащую предметных констант и функциональных символов и всюду истинную тогда и только тогда, когда это верно для $\mathfrak{A}$. Описанный способ построения $\mathfrak{A}'$, очевидно, является алгоритмом. Но по теореме 3′ из § 6.2 формула $\mathfrak{A}$ всюду истинна тогда и только тогда, когда она доказуема в $G_1$, а формула $\mathfrak{A}'$ — тогда и только тогда, когда она доказуема в $G_1^-$.

Теперь уже без труда получается

**Теорема 5 (теорема Чёрча).** Исчисление предикатов с функциональными символами и символами предметных констант и чистое исчисление предикатов (исчисления $G_1$ и $G_1^-$) неразрешимы.

Доказательство. Рассмотрим произвольную формулу исчисления $G_1^{Ar}$ — иначе говоря, произвольную формулу исчисления $G_1$, содержащую только символы из алфавита Ar. Доказуемость этой формулы в $G_1^{Ar}$ равносильна ее всюду-истинности (ввиду теоремы 3′ из § 6.2). Но и доказуемость ее в $G_1$ равносильна ее всюду-истинности; таким образом, формула исчисления $G_1^{Ar}$ тогда и только тогда доказуема в $G_1^{Ar}$, когда она доказуема в $G_1$[39]. Поэтому алгоритм, распознающий доказуемость формул в $G_1$, распознавал бы ее и в $G_1^{Ar}$. Но по теореме 4 для $G_1^{Ar}$ такого алгоритма нет; следовательно, его нет и для $G_1$. Отсюда ввиду леммы 2 немедленно вытекает, что такой алгоритм невозможен и для $G_1^-$.

4. Исчисление Робинсона, использованное нами для доказательства теоремы Чёрча, представляет и самостоятельный интерес: изучив его, мы убедились, что и конечно аксиоматизируемое «арифметическое» исчисление, не содержащее аксиомы индукции, может быть неполным. Но для доказательства теоремы Чёрча можно с таким же успехом использовать любое другое неразрешимое конечно аксиоматизируемое исчисление на основе $G_1$. Рассмотрим, например, логическое исчисление $\Pi_{\text{II}}$, получаемое из элементарной теории полугрупп (§ 6.3, пункт 4) присоединением в качестве новых аксиом всех определяющих соотношений ассоциативного исчисления $H_M$ с неразрешимой проблемой эквивалентности (§ 7.6, пункт 3), записанных в виде равенств термов ($q_i a_j = q_j a_k$ и т. д.). Формула вида

[38] С небольшими усложнениями, разобраться в которых предоставляется читателю.

[39] Этот факт можно доказать и чисто синтаксически (см. задачу 22 в конце главы).

$w = w'$, где $w$ и $w'$ — замкнутые термы, т. е. по существу, слова в алфавите ассоциативного исчисления $И_M$, доказуема в $П_н$, очевидно, тогда и только тогда, когда $w$ и $w'$ эквивалентны в $И_M$. А так как алгоритма, распознающего эквивалентность слов в $И_M$, не существует, $П_н$ — неразрешимое исчисление. Из этого факта с помощью лемм 1 и 2 можно вывести теорему Чёрча точно так же, как это было сделано выше с использованием факта неразрешимости $R$.

5. В ряде специальных вопросов представляет интерес *исчисление одноместных предикатов*, т. е. исчисление — обозначим его $G_1^-$ — получаемое изъятием из алфавита $G_1^-$ всех многоместных предикатных символов с соответствующим изменением определения формулы. (В частности, этого исчисления достаточно для обоснования аристотелевской силлогистики — см. § 6.5.) В отличие от «всего» $G_1^-$ чистое исчисление одноместных предикатов разрешимо. Покажем это. Поскольку для $G_1^-$ справедлива теорема о полноте (см. теорему 3′ из § 6.2), достаточно найти алгоритм, распознающий всюду-истинность. Для этого мы докажем следующую теорему:

Теорема 6. Формула исчисления $G_1^-$, содержащая $k$ различных предикатных символов, тогда и только тогда всюду истинна, когда она истинна во всякой ее интерпретации, основное множество которой содержит не более $2^k$ элементов.

Из этой теоремы легко получается нужный алгоритм, поскольку истинность формулы во всех интерпретациях с основным множеством не более чем из $2^k$ элементов проверяема: на множестве из $m$ элементов существует ровно $2^m$ попарно неравносильных одноместных предикатов (см. задачу на с. 135), так что каждому из $k$ предикатных символов можно сопоставить одноместный предикат на $m$-элементном множестве $2^m$ способами, что дает $2^{mk}$ неизоморфных интерпретаций для мощности $m$, а всего $2^k + 2^{2k} + \ldots 2^{2^k \cdot k}$ интерпретаций, для каждой из которых можно непосредственно проверить, истинна ли в ней данная формула (см. замечание 2 на с. 132).

Доказательство теоремы 6. Пусть $\mathfrak{A}$ — формула исчисления $G_1^-$, содержащая предикатные символы $F_{l_1}^1, \ldots, F_{l_k}^1$. Мы покажем, что для произвольной интерпретации $I$ этой формулы существует другая интерпретация $I'$ с основным множеством не более чем из $2^k$ элементов, в которой формула $\mathfrak{A}$ тогда и только тогда истинна, когда она истинна в $I$. Отсюда сразу будет следовать, что если формула истинна во всех интерпретациях с не более чем $2^k$-элементными основными множествами, то она всюду истинна. Обратное утверждение тривиально.

Итак, пусть $I$ — произвольная интерпретация формулы $\mathfrak{A}$, $M$ —

ее основное множество и $\Phi_1, \ldots, \Phi_k$ — предикаты, отвечающие в ней символам $F^1_{j_1}, \ldots, F^1_{j_k}$. Сопоставим каждому $a \in M$ $k$-мерный булев вектор $r^a = r^a_1 \cdots r^a_k$, где $r^a_i$ есть истинностное значение предложения $\Phi_i(a)$. Будем писать $a \sim b$, если $r^a = r^b$. Очевидно, отношение $\sim$ есть отношение эквивалентности. Обозначим через $M'$ фактор-множество $M/\sim$ и через $\Phi'_i (i = 1, \ldots, k)$ одноместный предикат на множестве $M'$, сопоставляющий каждому классу $A \in M$ предложение: «Если $a \in A$, то $\Phi_i(a)$». Пусть теперь $I'$ — интерпретация с основным множеством $M'$, в которой каждому символу $F^1_{j_i}$ отвечает предикат $\Phi'_i$. Индукцией по сложности формулы нетрудно доказать, что если формула $\mathfrak{B} = \mathfrak{B}(y_1, \ldots, y_s)$ исчисления $G^-_{\pi}$ со свободными переменными $y_1, \ldots, y_s$, не содержащая предикатных символов, отличных от $F^1_{j_1}, \ldots, F^1_{j_s}$, переходит в интерпретациях $I$ и $I'$ в предикаты $\Phi(y_1, \ldots, y_s)$ и $\Phi'(y_1, \ldots, y_s)$ соответственно, то для любых $a_1, \ldots, a_s \in M$ истинностное значение предложения $\Phi(a_1, \ldots, a_s)$ совпадает с истинностным значением предложения $\Phi'(A_1, \ldots, A_s)$, где $A_1, \ldots, A_s$ — те классы эквивалентности, которым принадлежат соответственно $a_1, \ldots, a_s$. (В частности, если $\mathfrak{B}$ замкнута, то соответствующие ей в $I$ и в $I'$ предложения одновременно истинны или ложны.) Отсюда следует, что формула $\mathfrak{A}$ тогда и только тогда истинна в $I$, когда она истинна в $I'$. Подробности предоставляются читателю.

Естественно возникает вопрос: останется ли исчисление $G^-_{\pi}$ разрешимым, если к одноместным предикатам присоединить двуместные? Ответ на этот вопрос — отрицательный; более того, фиксировав какой-либо двуместный предикатный символ, можно указать алгоритм, позволяющий по любой формуле чистого исчисления предикатов построить другую формулу, содержащую вхождения только этого фиксированного предикатного символа и всюду истинную тогда и только тогда, когда всюду истинна исходная формула. (Это теорема Л. Кальмара; ее доказательство имеется в книге [Чёрч 1960], § 47.) В то же время для многих частных классов формул чистого исчисления предикатов доказано существование алгоритмов, распознающих всюду-истинность. (Некоторые из этих классов рассмотрены в § 46 книги [Чёрч 1960]; более полное изложение этого вопроса, отражающее новые результаты, см. в статье [Маслов 1968] и книге [Dreben — Goldfarb 1979].

В заключение упомянем о замечательной теореме, доказанной М. Пресбургером: формальная арифметика без умножения (т. е. исчисление, получаемое из Ar изъятием символа умножения и аксиом $(\alpha_7)$ и $(\alpha_8)$ с соответствующим изменением определения формулы)

полна и разрешима. Доказательство см. в книге [Гильберт — Бернайс 1979], гл. VII, § 4.

## Задачи и упражнения

1) Показать, что в исчислении Ar

а) $\vdash x \cdot y = 1 \supset x = 1 \& y = 1$;

б) $\vdash \exists z(z + z = x) \vee \exists z((z + z)' = x)$.

2) Доказать (8) и (12) из § 8.1 непосредственно, не пользуясь отношением $<$. [Указание. Доказательство (12) провести индукцией по $z$, применив внутри индукционного шага индукцию по $x$ или по $y$ и использовав (8).]

3) Показать, что в исчислении Ar:

а) $\vdash \neg(x = 0) \supset x + x > x$;

б) $\vdash \neg(x = 0) \& \neg(x = 1) \supset x \cdot x > x$.

4) Показать, что в исчислении Ar:

а) $\vdash x + x = 2 \cdot x$;

б) $\vdash x \geq 2 \& y \geq 2 \supset x + y \leq x \cdot y$;

в) $\vdash x + y = x \cdot y \supset x = 0 \& y = 0 \vee x = 2 \& y = 2$,

г) $\vdash \exists z(n = m + z)$, если $m \leq n$, и $\vdash \neg\exists z(n = m + z)$, если $m > n$;

д) $\vdash \exists z(n = m \cdot z)$, если $n$ делится на $m$, и $\vdash \neg\exists z(n = m \cdot z)$, если $n$ не делится на $m$.

5) Показать, что всякая бескванторная замкнутая формула исчисления Ar либо доказуема в нем, либо опровержима (т. е. доказуемо ее отрицание).

6) Добавим к исчислению Ar новый одноместный функциональный символ $f^1_2$ и новые аксиомы $f^1_2(0) = (0)$, $f^1_2(x') = x$. Показать, что в полученном исчислении:

а) $\vdash x = y \supset f^1_2(x) = f^1_2(y)$;

б) $\vdash x > 0 \supset (f^1_2(x))' = x$.

7) Добавим к исчислению Ar новый двуместный функциональный символ $f^2_3$, причем вместо $f^2_3(t_1, t_2)$ будем писать $t_1^{t_2}$, и новые аксиомы $x^0 = 1$, $x^{y'} = x^y \cdot x$. Показать, что в полученном исчислении:

а) $\vdash x = y \supset x^z = y^z$;

б) $\vdash x = y \supset z^x = z^y$;

в) $\vdash x^{y+z} = x^y \cdot x^z$;

г) $\vdash x^{y \cdot z} = (x^y)^z$;

д) если $m^n = p$, то $\vdash m^n = p$.

8) Рассмотрим следующую интерпретацию системы аксиом Ar:

основным множеством служит множество всевозможных конечных множеств целых положительных чисел; равенство означает равномощность; 0 есть $\varnothing$; $X'$ есть множество, получаемое добавлением к $X$ наименьшего числа, не принадлежащего $X$; $X + Y$ есть $\varnothing$, если $X = Y = \varnothing$, и $\{1, 2, \ldots, |X| + |Y|\}$ в противном случае; $X \cdot Y$ есть $\varnothing$, если $X = \varnothing$ или $Y = \varnothing$, и $\{1, 2, \ldots, |X| \cdot |Y|\}$ в противном случае. Показать, что эта интерпретация является (ненормальной) моделью исчисления Ar. [Указание. Для доказательства аксиомы индукции убедиться, что для всякого предиката $\Phi(X_1, \ldots, X_k)$, сопоставляемого в данной интерпретации какой-либо формуле исчисления Ar, существует такой предикат $\Phi'(n_1, \ldots, n_k)$, определенный на множестве натуральных чисел, что $\Phi(X_1, \ldots, X_k) \equiv \equiv \Phi'(|X_1|, \ldots, |X_k|)$.]

9) Показать, что аксиома индукции не выводима из остальных аксиом исчисления Ar. [Указание. Рассмотреть следующую интерпретацию: основным множеством служит множество многочленов с целыми коэффициентами, старшие коэффициенты которых неотрицательны; нуль, равенство, сложение и умножение имеют обычный смысл; штрих означает прибавление единицы. Для опровержения аксиомы индукции взять в качестве $\mathfrak{A}(x)$ формулу, означающую существование частного и остатка от деления $x$ на 2.]

10) Будем говорить, что формула формальной арифметики $\mathfrak{A}(x_1, \ldots, x_n, x_{n+1})$, не содержащая свободных переменных, отличных от $x_1, \ldots, x_{n+1}$, *сильно представляет* всюду определенную числовую функцию $f(x_1, \ldots, x_n)$, если для любых натуральных $k_1, \ldots, k_n$ выполняется условие (4) из § 8.2 и, кроме того, $\vdash \exists! x_{n+1} \mathfrak{A}(x_1, \ldots, x_n, x_{n+1})$. Функция, для которой существует сильно представляющая ее формула формальной арифметики, называется *сильно представимой в формальной арифметике*. Доказать, что:

а) Все исходные п. р. ф. сильно представимы в формальной арифметике;

б) То же для $\beta$-функции Гёделя;

в) Операторы подстановки и рекурсии сохраняют свойство сильной представимости в формальной арифметике.

(Таким образом, этим свойством обладают все п.р.ф.)[40]

11) а) Изменить описанный в § 8.3 способ кодирования деревьев вывода, обходясь вместо четырех дополнительных символов $b$, $c$, $d$, $e$ только одним.

б) То же, обходясь совсем без дополнительных символов.

В обоих случаях предикаты Д, ДОК, $W_1$, $W_2$ и функция $d$ должны остаться примитивно рекурсивными.

12) По аналогии с описанным в § 8.3 способом кодирования деревьев вывода в Ar закодировать деревья вывода в исчислении $G_1$ так, чтобы предикаты Д и ДОК были примитивно рекурсивны.

---

[40] Во втором английском издании книги Э. Мендельсона, с первого издания которой сделан русский перевод [Мендельсон 1971], приведен — без доказательства и без библиографической ссылки — результат Дайсона [V. H. Dyson], доказавшего, что сильная представимость равносильна представимости в смысле § 8.2.

13) а) Определив подходящим образом код и номер конечного множества формул исчисления Ar (при этом не обязательно, чтобы каждое такое множество имело только один номер), доказать, что предикат $\text{ВЫВ}(x, y, z)$ — «$x$ есть номер конечного множества формул, $y$ — номер формулы, выводимой из этого множества, и $z$ — номер вывода формулы с номером $y$ из множества с номером $x$» примитивно рекурсивен.

б) То же для исчисления $G_1$.

14) Доказать, что функция замык($x$), сопоставляющая каждому $x$, являющемуся номером формулы исчисления Ar, номер ее замыкания, и равная нулю для остальных значений $x$, примитивно рекурсивна.

15) Доказать, что множество теорем произвольного логического исчисления на основе $G_1$ с перечислимым множеством аксиом перечислимо.

16) Доказать, что всякое дедуктивно полное логическое исчисление на основе $G_1$ с перечислимым множеством аксиом разрешимо.

17) Логическое исчисление, алфавит которого содержит алфавит формальной арифметики, называется *$\omega$-полным*, если, какова бы ни была его формула $\mathfrak{A} = \mathfrak{A}(x)$, из доказуемости $\mathfrak{A}(n)$ для любого натурального $n$ следует доказуемость формулы $\forall x \mathfrak{A}(x)$. Показать, что если исчисление Ar непротиворечиво, то оно $\omega$-неполно. [Указание. Рассмотреть формулу $\neg\mathfrak{Bew}_1(m_1, x)$ из доказательства теоремы Гёделя.]

18) а) Доказать, что множество номеров формул формальной арифметики, истинных в стандартной интерпретации, неразрешимо, если только в этой интерпретации нет противоречий. [Указание. Рассмотреть расширение исчисления Ar с помощью множества формул, истинных в стандартной интерпретации, и воспользоваться соображениями, изложенными в последнем абзаце пункта 3 § 8.4.]

б) Доказать, что это множество не может совпадать с множеством номеров теорем какого-либо непротиворечивого рекурсивно аксиоматизируемого (т. е. получаемого добавлением разрешимого множества аксиом) простого расширения исчисления Ar.

19) Доказать, что исчисление $R$ слабее исчисления Ar (т. е. не всякая теорема Ar есть теорема $R$). [Указание. Воспользоваться интерпретацией, описанной в указании к задаче 9.]

20) Показать, что аксиома $(\rho_{14})$ не выводима из остальных аксиом исчисления $R$. [Указание. Добавить к множеству натуральных чисел новый объект $b$ и положить: $b' = b$; $x + b = b + x = b$ для любого $x$; $x \cdot b = b \cdot x = b$ для любого $x \neq 0$; $0 \cdot b = b \cdot 0 = 0$.]

21) Два логических исчисления называются *совместимыми*, если исчисление, полученное объединением их алфавитов и множеств аксиом, непротиворечиво. Показать, что всякое исчисление, имеющее тот же алфавит, что и $R$, и совместимое с $R$, неразрешимо.

22) Не пользуясь теоремой о полноте, доказать, что если $\Gamma$ — множество формул исчисления $G_1^{\text{Ar}}$, $\mathfrak{A}$ — формула исчисления $G_1^{\text{Ar}}$ и $\Gamma \vdash_{G_1} \mathfrak{A}$, то $\Gamma \underset{G_1^{\text{Ar}}}{\vdash} \mathfrak{A}$. [Указание. Преобразовать вывод, заменяя вхождения символов, отсутствующих в алфавите Ar, вхождениями подходящих формул и термов в этом алфавите.]

ПРИЛОЖЕНИЕ I

# ОТНОШЕНИЯ ЭКВИВАЛЕНТНОСТИ И ПОРЯДКА

**1.** Среди используемых в математике отношений, весьма разнообразных по своим свойствам, можно выделить отдельные особенно важные типы; некоторые из них мы сейчас рассмотрим. Все эти отношения бинарны, и для каждого из них область отправления совпадает с областью прибытия. Поэтому слово *«отношение»* в настоящем приложении будет означать бинарное отношение, заданное на некотором непустом множестве (являющемся, таким образом, для данного отношения как областью отправления, так и областью прибытия).

**2.** Отношение $R$ называется *рефлексивным*[1], если оно удовлетворяет условию $\forall x(xRx)$ (т. е. если каждый элемент соответствующего множества находится в этом отношении к самому себе).

Отношение $R$ называется *симметричным*[2], если оно удовлетворяет условию $\forall x \forall y(xRy \supset yRx)$.

Легко видеть, что отношение тогда и только тогда симметрично, когда оно совпадает со своим обратным, т. е. удовлетворяет условию $\forall x \forall y[(xRy \supset xR^{-1}y) \& (xR^{-1}y \supset xRy)]$. (Для доказательства достаточно вспомнить, что $xR^{-1}y$ означает то же, что $yRx$.)

Отношение $R$ называется *транзитивным*[3], если оно удовлетворяет условию $\forall x \forall y \forall z(xRy \& yRz \supset xRz)$.

Примеры.

1) Отношение равенства действительных чисел является, очевидно, рефлексивным, симметричным и транзитивным: всякое число равно самому себе; если $a = b$, то $b = a$; если $a = b$ и $b = c$, то $a = c$.

---

[1] От лат. *reflexus* — «обратное движение, поворот». Ср. «рефлексия», «рефлекс», «рефлектор».

[2] Употребление здесь слова «симметричный» хорошо согласуется с другими случаями употребления слов «симметричный», «симметрия» (от греческого συμμετρία — «соразмерность, правильное соотношение») в математике и в обычном русском языке.

[3] От лат. *transitus* — «переход, прохождение». Ср. «транзит», «транзитный».

2) Отношение $\leq$, заданное на том же множестве действительных чисел $\mathbf{R}$ (в дальнейшем символ $\mathbf{R}$ всегда будет иметь тот же смысл) рефлексивно (всегда $a \leq a$) и транзитивно (если $a \leq b$ и $b \leq c$, то $a < c$), но не симметрично (из $a \leq b$ не следует $b \leq a$; например, $1 \leq 2$ верно, а $2 \leq 1$ неверно).

3) Отношение $<$, заданное на $\mathbf{R}$, не рефлексивно и не симметрично, но транзитивно.

4) Отношение конгруэнтности (на «школьном» языке — равенства) треугольников рефлексивно, симметрично и транзитивно.

5) То же справедливо для отношения подобия треугольников.

6) То же верно для отношения равносильности формул логики предложений.

7) Заданное на множестве формул логики предложений отношение «быть следствием» рефлексивно и транзитивно, но не симметрично (доказать это, подобрав подходящий пример).

8) Заданное на множестве всех подмножеств фиксированного непустого множества отношение «быть подмножеством» рефлексивно и транзитивно, но не симметрично.

9) Заданное на том же множестве отношение «быть истинным подмножеством» не рефлексивно и не симметрично, но транзитивно.

10) Отношение равенства множеств рефлексивно, симметрично и транзитивно.

11) Заданное на множестве прямых в пространстве отношение «иметь общие точки» рефлексивно и симметрично, но не транзитивно.

12) Заданное на том же множестве отношение «не иметь общих точек» не рефлексивно и не транзитивно, но симметрично.

13) Заданное на том же множестве отношение параллельности симметрично, но не рефлексивно и не транзитивно (импликация $a \| b \& b \| c \supset a \| c$ ложна, если $a \| b$ и $c$ совпадает с $a$).

14) Заданное на том же множестве отношение «$x$ параллельна $y$ или совпадает с $y$» рефлексивно, симметрично и транзитивно.

15) Пусть $a$, $b$ — целые числа и $m$ — целое положительное число. Говорят, что $a$ и $b$ *сравнимы по модулю* $m$, и пишут $a \equiv b (\mathrm{mod}\ m)$, если разность $a - b$ делится на $m$, или, что то же самое, если $a$ и $b$ дают при делении на $m$ одинаковые остатки. При любом $m$ отношение сравнимости по модулю $m$ рефлексивно ($a - a = 0$ и 0 делится на $m$), симметрично (если $a - b$ делится на $m$, то и $b - a$ делится на $m$) и транзитивно (если $a - b$ и $b - c$ делятся на $m$, то и $a - c = (a - b) + (b - c)$ делится на $m$).

16) Заданное на $\mathbf{R}$ отношение «быть противоположным числом» симметрично, но не рефлексивно и не транзитивно.

17) Пусть $Q$ — отношение, заданное на $\mathbf{R}$ следующим образом: $xQy$ означает $xy > 0 \vee x = y = 0$. Легко проверить, что это отношение рефлексивно, симметрично и транзитивно.

18) Заданное на множестве целых чисел $\mathbf{Z}$ (в дальнейшем символ $\mathbf{Z}$ всегда будет иметь тот же смысл) отношение делимости рефлексивно и транзитивно, но не симметрично.

19) Пусть $D$ — отношение, заданное на $\mathbf{Z}$ следующим образом: $xDy$ означает, что $x$ делится на $y$ и при этом $|x| > |y|$. Это отношение не рефлексивно и не симметрично, но транзитивно.

20) Заданное на произвольном множестве людей, среди которых есть хотя бы двое, один из которых — потомок другого, отношение «быть потомком» не рефлексивно и не симметрично, но транзитивно.

Для большей наглядности сведем разобранные примеры в таблицу (+ означает наличие свойства, − — его отсутствие).

Таблица 1

| № | Отношение | Рефл. | Симм. | Транз. |
|---|---|---|---|---|
| 1 | Равенство чисел | + | + | + |
| 2 | $\leq$ | + | − | + |
| 3 | $<$ | − | − | + |
| 4 | Конгруэнтность | + | + | + |
| 5 | Подобие | + | + | + |
| 6 | Равносильность | + | + | + |
| 7 | Быть следствием | + | − | + |
| 8 | Быть подмножеством | + | − | + |
| 9 | Быть истинным подмножеством | − | − | + |
| 10 | Равенство множеств | + | + | + |
| 11 | Иметь общие точки | + | + | − |
| 12 | Не иметь общих точек | − | + | − |
| 13 | $\|\|$ | − | + | − |
| 14 | $\|\|$ или $=$ | + | + | + |
| 15 | $a \equiv b (\mathrm{mod} m)$ | + | + | + |
| 16 | Быть противоположным числом | − | + | − |
| 17 | $Q$ | + | + | + |
| 18 | Делимость | + | − | + |
| 19 | $D$ | − | − | + |
| 20 | Быть потомком | − | − | + |

Задачи. 1) Исследовать на рефлексивность, симметричность и транзитивность следующие отношения:

а-д) Отношения $Q_1$, $Q_2$, $Q_3$, $Q_4$, $Q_5$, заданные на R следующим образом: $xQ_1y$ означает $xy > 0$, $xQ_2y$ — $xy \geq 0$, $xQ_3y$ — $xy < 0$, $xQ_4y$ — $xy \leq 0$, $xQ_5y$ — $x \leq y + 1$.

е) Отношение $S$, заданное на множестве $E^*$ «формальных слов» из русских букв (см. задачу 16 в конце гл. 2): $xSy$ означает, что последняя буква слова $x$ совпадает с первой буквой слова $y$.

2) Убедиться, что каждая из восьми мыслимых комбинаций наличия и отсутствия свойств рефлексивности, симметричности и транзитивности осуществляется для некоторого отношения.

3. Исключительно важную роль играют в математике отношения, являющиеся одновременно рефлексивными, симметричными и транзитивными. Такие отношения называются *отношениями эквивалентности* или просто *эквивалентностями*.

Эквивалентностями являются, например, следующие отношения (см. табл. 1): равенство действительных чисел; конгруэнтность треугольников; подобие треугольников; равносильность формул логики предложений; равенство множеств; параллельность или совпадение прямых; сравнимость целых чисел по заданному модулю; отношение $Q$.

Сейчас мы докажем теорему, из которой будет ясно, чем обусловлена исключительная роль отношений эквивалентности. Чтобы ее сформулировать, введем следующее понятие. Пусть $M$ — произвольное множество и $\{K_\alpha\}$ — какая-то система подмножеств $M$, т. е. некоторое множество, элементы которого являются подмножествами $M$. Говоря, что система $\{K_\alpha\}$ является *разбиением* множества $M$ (иначе: множества $K_\alpha$ *образуют разбиение* множества $M$, или: имеется *разбиение $M$ на* множества $K_\alpha$), если каждый элемент $M$ принадлежит одному и только одному из $K_\alpha$ — или, что то же самое, если множества $K_\alpha$ попарно не пересекаются[4] и их объединение совпадает с $M$.

Теорема. Если $R$ — отношение эквивалентности, заданное на произвольном непустом множестве $M$, то существует такое разбиение $\{K_\alpha\}$ множества $M$, что, каковы бы ни были $x, y \in M$, тогда и только тогда $xRy$, когда $x$ и $y$ принадлежат одному и тому же множеству $K_\alpha$.

Доказательство. Пусть $a$ — произвольный элемент множества $M$. Обозначим через $M_a$ множество $\{x | x \in M \& xRa\}$. Ввиду рефлек-

[4] Это значит, что не пересекаются никакие два из них (если они различны).

сивности отношения $R$ имеем $a \in M_a$, и поэтому объединение всех $M_a$ содержит $M$; но поскольку любое $M_a$ содержится в $M$, это объединение совпадает с $M$. Если мы теперь покажем, что любые два различных множества вида $M_a$ не пересекаются — т. е., что из $M_a \neq M_b$ следует $M_a \cap M_b = \varnothing$, — тем самым будет доказано, что множества $M_a$ образуют разбиение $M$. Докажем это от противного. Пусть $a, b \in M$, $M_a \neq M_b$ и $M_a \cap M_b \neq \varnothing$, т. е. существует хотя бы один элемент $c$ множества $M$, такой, что $cRa$ и $cRb$. Если $z$ — произвольный элемент $M_a$, то $zRa$; отсюда и из $cRa$ ввиду симметричности и транзитивности $R$ вытекает $zRc$, а из $zRc$ и $cRb$ следует $zRb$, т. е. $z \in M_b$. Итак, мы доказали, что $M_a \subset M_b$; точно так же можно доказать, что $M_b \subset M_a$. Таким образом, $M_a = M_b$, вопреки предположению.

Остается показать, что для любых $x, y \in M$ тогда и только тогда $xRy$, когда $x$ и $y$ принадлежат одному и тому же множеству полученного разбиения. Но если $x, y \in M_a$, то $xRa$ и $yRa$, откуда $xRy$; обратно. если $xRy$, то $x \in M_y$, но $y$ также принадлежит $M_y$. Доказательство теоремы закончено.

Разбиение $\{K_\alpha\}$, существование которого утверждается только что доказанной теоремой, называется *разбиением на классы эквивалентности (по отношению $R$)* или *фактор-множеством множества $M$ по отношению $R$* и обозначается $M/R$.

Ясно, что справедливо и обратное утверждение: если $\{K_\alpha\}$ — произвольное разбиение множества $M$ и $xRy$ означает, что $x$ и $y$ принадлежат одному и тому же множеству разбиения $\{K_\alpha\}$, то $R$ есть отношение эквивалентности, а $\{K_\alpha\}$ совпадает с фактор-множеством $M/R$.

Примеры:

1) Для отношения равенства действительных чисел каждое множество $K_\alpha$ состоит из одного числа, так что все классы эквивалентности одноэлементны.

2) Для отношения равносильности формул логики предложений каждый класс эквивалентности состоит из всех формул, представляющих одну и ту же булеву функцию.

3) Для отношения сравнимости по модулю $m$ каждый класс эквивалентности состоит из всех чисел, дающих при делении на $m$ заданный остаток. Такие «классы равноостаточных чисел» принято называть *классами вычетов по модулю $m$*. Поскольку остаток от деления целого числа на $m$ может принимать $m$ различных значений: 0, 1, ..., $m - 1$ — имеется ровно $m$ классов вычетов по модулю $m$:

$\{mk \mid k = 0, \pm 1, \pm 2, \ldots\}$, $\{mk + 1 \mid k = 0, \pm 1, \pm 2, \ldots\}$, ..., $\{mk + (m-1) \mid k = 0, \pm 1, \pm 2, \ldots\}$.

Например, при $m = 2$ один класс состоит из четных чисел, другой — из нечетных.

4) Для отношения $Q$ имеем три класса эквивалентности: $\mathbf{R}_+$, $\mathbf{R}_-$, $\{0\}$, где $\mathbf{R}_+$, соответственно $\mathbf{R}_-$, означает множество положительных (отрицательных) действительных чисел.

Для остальных эквивалентностей из табл. 1 читатель найдет классы эквивалентности сам.

Задача. Доказать, что следующие отношения, заданные на $\mathbf{R}$, являются отношениями эквивалентности; для каждого из них найти классы эквивалентности и изобразить их схематически на чертеже:

а) $R_1$: $xR_1y$ означает $|x| = |y|$;

б) $R_2$: $xR_2y$ означает $[x] = [y]$;

в) $R_3$: $xR_3y$ означает $x - [x] = y - [y]$

(иначе: разность $x - y$ есть целое число).

4. Отношение $R$ называется *антирефлексивным*, если оно удовлетворяет условию $\forall x \neg(xRx)$ (т. е. никакой элемент не находится в этом отношении к самому себе).

Отношение $R$ называется *антисимметричным*, если оно удовлетворяет условию $\forall x \forall y(xRy \supset \neg(yRx))$.

Исследуем на антирефлексивность и антисимметричность отношения из табл. 1 (разумеется, на антирефлексивность нужно исследовать только нерефлексивные отношения, а на антисимметричность — несимметричные).

1) Отношение $\leq$ не антисимметрично: из $a \leq b$ не следует $\neg(b \leq a)$.

2) Отношение $<$ антирефлексивно (никакое число не меньше самого себя) и антисимметрично (если $a < b$, то не может быть $b < a$).

3) Отношение «быть следствием» для формул логики предложений не антисимметрично.

4) То же справедливо для отношения «быть подмножеством».

5) Отношение «быть истинным подмножеством» антирефлексивно и антисимметрично.

6) Отношение «не иметь общих точек» антирефлексивно.

7) То же верно для отношения параллельности.

8) Отношение «быть противоположным числом» не антирефлексивно (так как число 0 противоположно самому себе).

9) Отношение делимости не антисимметрично.

10) Отношение $D$ антирефлексивно и антисимметрично.

11) То же верно для отношения «быть потомком».

Присоединим к этим примерам еще один:

12) Заданное на множестве $Б$ букв русского алфавита отношение «алфавитного предшествования»: буква «а» предшествует всем остальным, буква «б» — всем, кроме «а» и «б», буква «в» — всем, кро-

ме «а», «б» и «в», и т. д.— очевидно, антирефлексивно и антисимметрично. (Заметим также, что это отношение транзитивно).

Разобранные примеры сведем в новую таблицу, в которой повторим также столбец для транзитивности.

Таблица 2

| № | Отношение | Антирефл. | Антисимм. | Транз. |
|---|---|---|---|---|
| 1 | $\leq$ | – | – | + |
| 2 | $<$ | + | + | + |
| 3 | быть следствием | – | – | + |
| 4 | быть подмножеством | – | – | + |
| 5 | быть истинным подмножеством | + | + | + |
| 6 | не иметь общих точек | + | – | – |
| 7 | $\|\|$ | + | – | – |
| 8 | быть противоположным числом | – | – | – |
| 9 | делимость | – | – | + |
| 10 | $D$ | + | + | + |
| 11 | быть потомком | + | + | + |
| 12 | алфавитное предшествование | + | + | + |

Задача. Исследовать на антирефлексивность и антисимметричность отношения из задачи 1 в конце пункта 2.

Отношения, являющиеся одновременно антирефлексивными, антисимметричными и транзитивными, называются *отношениями порядка* или просто *порядками*.

Если отношение порядка $R$ удовлетворяет дополнительному условию $\forall x \forall y (x \neq y \supset xRy \vee yRx)$ (т. е. если любые два различных элемента соответствующего множества «сравнимы в смысле $R$»), оно называется *отношением линейного порядка* (или просто *линейным порядком*).

Множество, на котором задано отношение порядка (соответственно — линейного порядка), называется *упорядоченным* (соответственно — *линейно упорядоченным*) *множеством*[5]. Более строго, (линейно) упорядоченным множеством называется упорядоченная

[5] В другой терминологии, в настоящее время менее употребительной, то, что мы назвали отношением порядка и упорядоченным множеством, называют отношением частичного порядка и частично упорядоченным множеством, а то, что мы назвали отношением линейного порядка и линейно упорядоченным множеством — просто отношением порядка и упорядоченным множеством. Кроме того, вместо «отношение линейного порядка» и «линейно упорядоченное множество» иногда говорят «отношение полного порядка» и «полностью упорядоченное множество».

пара $(M, R)$, где $M$ — множество и $R$ — заданное на $M$ отношение (линейного) порядка.

Из отношений, включенных в табл. 2, порядками являются: $<$, «быть истинным подмножеством», $D$, «быть потомком», алфавитное предшествование. Легко видеть, что первый и последний из этих порядков линейны, а остальные нелинейны (точнее, отношения «быть истинным подмножеством» и «быть потомком» не являются линейными порядками, если они заданы: первое — на множестве всех подмножеств множества, состоящего не менее чем из двух элементов, второе — на множестве людей, в которое входят хотя бы два человека, ни один из которых не является потомком другого[6].

Задача. Доказать, что следующие отношения, заданные на $\mathbf{R}$, являются порядками:

а) $U_1$: $xU_1y$ означает $|x| < |y|$;

б) $U_2$: $xU_2y$ означает $[x] < [y]$;

в) $U_3$: $xU_3y$ означает $x - [x] < y - [y]$;

г) $U_4$: $xU_4y$ означает $|x| < |y| \vee |x| = |y| \& x < y$;

д) $U_5$: $xU_5y$ означает $x = 0 \& y \neq 0 \vee xy \neq 0 \& x < y$.

Какие из этих порядков линейны?

**Замечания.** 1) Не все мыслимые комбинации наличия и отсутствия свойств антирефлексивности, антисимметричности и транзитивности действительно возможны (ср. задачу 2 в конце пункта 2). Именно, всякое антисимметричное отношение антирефлексивно, а всякое, являющееся антирефлексивным и транзитивным, — антисимметрично. В самом деле:

(а) Из условия антисимметричности вытекает, что для любого элемента $a$ соответствующего множества из $aRa$ должно следовать $\neg(aRa)$; поэтому $aRa$ невозможно.

(б) Пусть отношение $R$ антирефлексивно и транзитивно, и пусть $aRb$. Тогда $bRa$ невозможно, поскольку из $aRb$ и $bRa$ по транзитивности следует $aRa$.

Таким образом, отношение порядка можно было бы определить проще, а именно либо как антирефлексивное и транзитивное отношение, либо как антисимметричное и транзитивное.

2) Непосредственно из определений легко вывести, что отношение, обратное для антирефлексивного (антисимметричного, транзитивного) отношения, также антирефлексивно (антисимметрично, транзитивно). Отсюда следует, что отношение, обратное для поряд-

[6] Название «линейный порядок» отражает тот факт, что в достаточно простых случаях элементы линейно упорядоченного множества можно наглядно изображать точками прямой линии так, что $xRy$ изображается как «$x$ левее $y$». В то же время, например, для отношения «быть потомком» подобное наглядное изображение («родословное дерево») «не укладывается» на прямой.

ка, также является порядком. Столь же легко усмотреть, что отношение, обратное для линейного порядка, также есть линейный порядок. Поэтому, например, отношение $>$ (обратное для $<$) является линейным порядком; отношение «быть предком» (обратное для «быть потомком») есть порядок.

Рассмотрим еще один пример линейного порядка. Пусть $Б$ — множество букв русского алфавита, $R$ — заданное на $Б$ отношение алфавитного предшествования (см. выше пример 12) и $Б^*$ — множество формальных слов в алфавите $Б$ (т. е. конечных последовательностей элементов $Б$: см. задачу 16 в конце гл. 2). (Одним из элементов $Б^*$ является *пустое слово* $\Lambda$, не содержащее никаких букв.) Будем говорить, что: а) слово $x$ является *префиксом* слова $y$, если существует непустое слово $z$, такое, что $y = xz$; б) слово $y$ *отходит вниз от слова* $x$ *на* $i$*-м шаге*, если существуют такое слово $u$ длины $i-1$[7] и такие непустые слова $x_1$ и $y_1$, что $x = ux_1$, $y = uy_1$ и первая буква слова $x_1$ предшествует первой букве слова $y_1$ в смысле отношения $R$. (Например, слово «лес» — префикс слова «леска», пустое слово — префикс всякого непустого; слово «ворон» отходит вниз от слова «воробей» на пятом шаге и от слова «бор» на первом шаге.) Если слово $x$ является префиксом слова $y$ или слово $y$ на каком-нибудь шаге отходит вниз от слова $x$, мы будем говорить, что слово $x$ *лексикографически предшествует слову* $y$, и писать $xR^*y$. Лексикографическое предшествование, называемое также *лексикографическим* (или *словарным*) *порядком* — это то самое отношение, с помощью которого принято упорядочивать слова в словарях[8]. Мы покажем сейчас, что оно действительно есть порядок, и притом линейный.

Поскольку из определения непосредственно следует, что отношение лексикографического предшествования антирефлексивно и любые два различных слова сравнимы в смысле этого отношения (т. е. одно из них лексикографически предшествует другому), достаточно доказать транзитивность. Пусть $xR^*y$, $yR^*z$. Возможны четыре случая:

а) $x$ является префиксом $y$ и $y$ — префиксом $z$. Тогда, очевидно, $x$ является префиксом $z$.

б) $x$ является префиксом $y$ и существует такое $i$, что на $i$-м шаге $z$ отходит вниз от $y$. Пусть длина $x$ равна $l$. Если при этом $i \leq l$, то $z$ на $i$-м шаге отходит вниз от $x$, а если $i > l$, то $x$ является префиксом $z$.

в) Существует такое $j$, что на $j$-м шаге $y$ отходит вниз от $x$, и $y$

[7] *Длиной слова* называется число вхождений букв в него. Например, слово «лампа» имеет длину 5, пустое слово — длину 0.

[8] Ср. сноску на с. 74 (где рассматривался лексикографический порядок для слов одинаковой длины, содержащих только буквы $И$ и $Л$). Там же см. объяснение термина

является префиксом $z$. В этом случае $z$ также отходит вниз от $x$ на $j$-м шаге.

г) Существуют такие $i$ и $j$, что на $i$-м шаге $y$ отходит вниз от $x$ и на $j$-м — $z$ от $y$. Тогда $z$ отходит вниз от $x$ на $k$-м шаге, где $k = \min(i, j)$.

Итак, в любом случае из $xR^*y$ и $yR^*z$ следует $xR^*z$. Доказательство окончено.

Замечание. При построении отношения $R^*$ и во всех последующих рассуждениях конкретная природа множества $E$ и отношения $R$ не играла никакой роли — использовался только тот факт, что $R$ есть линейный порядок. Поэтому лексикографический порядок можно определить, исходя из произвольного линейного порядка, заданного на каком-либо множестве. Например, если исходить из отношения $<$, заданного на множестве R, то, обозначая соответствующий лексикографический порядок через $<^*$ и пользуясь обычными обозначениями для упорядоченных систем чисел, играющих теперь роль «слов», имеем: $(3, 6, -2) <^* (3, 8)$; $(-1, 4, 0) <^* (0, -5, -1)$ и т. п.

5. Пусть $M$ — произвольное непустое множество, $R$ — заданное на $M$ отношение и $M'$ — непустое подмножество $M$. Определим отношение $R'$ следующим образом: $xR'y$ означает, что $x, y \in M'$ и $xRy$. Иначе говоря, $R'$ есть отношение, заданное на множестве $M'$ и отличающееся от $R$ только дополнительным условием $x, y \in M'$. Мы будем говорить, что $R'$ есть *отношение $R$, ограниченное множеством $M'$*. Например, отношение равенства целых чисел можно рассматривать как отношение равенства действительных чисел, ограниченное множеством целых чисел.

Ясно, что если отношение рефлексивно (антирефлексивно, симметрично, антисимметрично, транзитивно), то оно остается рефлексивным — соответственно антирефлексивным, симметричным, антисимметричным, транзитивным — при любом ограничении; сохраняется при ограничении также и свойство $\forall x \forall y (x \neq y \supset yRy \vee Rx)$. Поэтому всякая эквивалентность остается при любом ограничении эквивалентностью, порядок — порядком и линейный порядок — линейным порядком. Например, равенство рациональных чисел, равенство целых чисел и т. п.— отношения эквивалентности. Точно так же отношение $<$ для рациональных чисел, для целых чисел и т. п. остается линейным порядком. Часто рассматриваются также ограниченные отношения лексикографического порядка — например, лексикографический порядок на множестве упорядоченных $n$-ок действительных чисел при фиксированном $n$. (В частности, для упорядоченных пар действительных чисел лексикографическое предшествование можно определить так: пара $(x, y)$ предшествует паре $(x', y')$, если либо $x < x'$, либо $x = x'$ и $y < y'$.) Все такие ограниченные лексикографические порядки линейны.

Задача. Порядок R называется *плотным*, если он удовлетворяет

условию $\forall x \forall y (xRy \supset \exists z(xRz \& zRy))$. Привести примеры плотных и неплотных порядков. Сохраняется ли свойство плотности при любом ограничении?

## Задачи и упражнения

1) Исследовать на рефлексивность, антирефлексивность, симметричность, антисимметричность и транзитивность следующие отношения:

(а) заданное на $\mathbb{R}$ отношение $P_1$: $xP_1y$ означает «$x + y$ — целое число»;

(б) заданное на $\mathbb{R}$ отношение $P_2$: $xP_2y$ означает $|x - y| = 1$;

(в) заданное на множестве целых положительных чисел отношение $P_3$: $xP_3y$ означает «$x$ есть наименьший отличный от единицы делитель $y$»;

(г) заданное на том же множестве отношение $P_4$: $xP_4y$ означает $x = y + 1$;

(д) заданное на множестве $Б$ букв русского алфавита отношение $P_5$: $xP_5y$ означает «в слове "бесконечность" имеется вхождение буквы $x$, непосредственно предшествующее вхождению буквы $y$» (например $eP_5c$, $eP_5ч$).

2) Сформулировать в геометрических терминах свойства графика заданного на $\mathbb{R}$ отношения, необходимые и достаточные для того, чтобы это отношение было: (а) рефлексивным; (б) антирефлексивным; (в) симметричным; (г) антисимметричным.

3) Доказать, что следующие отношения являются эквивалентностями и найти классы эквивалентности:

(а) заданное на $\mathbb{R}$ отношение $x \approx y \vee x + y = 0$;

(б) заданное на $\mathbb{R}\setminus\{0\}$ отношение $x = y \vee xy = 1$;

(в) заданное на множестве $\mathbb{Z}^2$ отношение $\sim$: $(a, b) \sim (c, d)$ означает $a + d = b + c$;

(г) заданное на $\mathbb{Z} \times (\mathbb{Z}\setminus\{0\})$ отношение $\approx$: $(a, b) \approx (c, d)$ означает $ad = bc$.

4) Доказать, что каждое из следующих отношений, заданных на множестве $S$ функций, отображающих множество положительных действительных чисел в себя, является эквивалентностью:

(а) $f(1) = g(1)$;

(б) $\lim\limits_{x \to +\infty} (f(x) - g(x)) = 0$;

(в) «$\lim\limits_{x \to +\infty} (f(x) - g(x))$ существует и конечен»;

(г) $\lim\limits_{x \to +\infty} \dfrac{f(x)}{g(x)} = 1$;

(д) «$\lim\limits_{x \to +\infty} \dfrac{f(x)}{g(x)}$ существует, конечен и отличен от нуля»;

(е) $\exists a (a > 0 \& \exists x_0 \forall x (x > x_0 \supset |f(x) - g(x)| < a))$;

(ж) $\exists a \exists b (0 < a < b \& \exists x_0 \forall x (x > x_0 \supset a < \frac{f(x)}{g(x)} < b))$;

(з) $\exists k (k \leq 0 \& \exists x_0 \forall x (x > x_0 \supset \frac{1}{x^k} \leq \frac{f(x)}{g(x)} \leq x^k))$.

5) Пусть $F$ — произвольное отображение непустого множества $A$ в непустое множество $B$, и $R_F$ — следующее заданное на $A$ отношение: $xR_Fy$ означает, что $F(x) = F(y)$.

(а) Доказать, что $R_F$ — отношение эквивалентности;

(б) Для каждого из перечисленных ниже отношений подобрать функцию $F$ с числовыми значениями таким образом, чтобы данное отношение совпало с $R_F$: равенство действительных чисел; сравнимость по модулю $m$; отношение $Q$ (пример 17 в пункте 2).

6) Попытаться естественным образом определить понятие «антитранзитивного отношения». Привести примеры таких отношений.

7) Доказать, что следующие заданные на $\mathbf{R}$ отношения являются отношениями линейного порядка:

(а) $0 < x < y \vee y < x < 0 \vee x < 0 < y \vee x = 0 \& y \neq 0$;

(б) $x - |x| < y - |y| \vee x - |x| = y - |y| \& |x| < |y|$.

8) Доказать, что следующие отношения, заданные на $\mathbf{Z} \setminus \{0\}$, являются отношениями порядка, но не линейного порядка:

(а) «Число различных делителей $x$ больше числа различных делителей $y$»;

(б) то же для числа различных простых делителей;

(в) «$x$ делится на $y^2$ и $|x| > 1$».

9) Пусть $\prec$ — следующее отношение, заданное на $\mathbf{Z}^2$: $(a, b) \prec (c, d)$ означает $a + b < c + d \vee a + b = c + d \& a < c$. Доказать, что $\prec$ — линейный порядок.

10) Доказать, что следующие отношения, заданные на $S$ (см. задачу 4), являются отношениями порядка, но не линейного порядка:

(а) $f(1) < g(1)$;

(б) $\exists x_0 \forall x (x > x_0 \supset f(x) < g(x))$;

(в) $\lim\limits_{x \to +\infty} \frac{f(x)}{g(x)} = 0$;

(г) «$\lim\limits_{x \to +\infty} \frac{f(x)}{g(x)}$ существует и меньше единицы»;

(д) $\exists x_0 \forall x (x > x_0 \supset 2^{f(x)} < g(x))$.

11) Пусть $f$ — функция, отображающая $\mathbf{R}$ в себя и удовлетворяющая условиям $\forall x \forall y (x < y \supset f(x) < f(y))$ и $\forall x (x \leq f(x))$, и пусть $x <_f y$ означает $f(x) < y$.

(а) Доказать, что $<_f$ есть порядок.

(б) Всегда ли этот порядок является линейным?

12) Пусть $A$, $B$ — произвольные непустые множества, $F$ — отображение $A$ в $B$, $Q$ — порядок на $B$, и пусть $xQ_{[F]}y$ означает $F(x)QF(y)$.

(а) Доказать, что $Q_{[F]}$ — порядок на $A$.

(б) Показать на примерах, что $Q_{[F]}$ может не быть линейным порядком, даже если $Q$ является таковым.

13) (а) Что представляет собой рефлексивное функциональное отношение?

(б) Указать примеры функциональных отношений порядка.

(в) На каких множествах возможны функциональные отношения линейного порядка?

ПРИЛОЖЕНИЕ

II

# МОЩНОСТЬ МНОЖЕСТВА

1. В главе 1 было рассмотрено много примеров множеств. Некоторые из этих множеств к о н е ч н ы — например, $\{1\}$, $\{1, 2\}$, $\{1, 2, \ldots, 1000\}$, $\{a, б, в\}$, $\varnothing$,— другие б е с к о н е ч н ы — например, множество действительных чисел, множество целых чисел, множество четных чисел, множество нечетных чисел. Что такое «конечное» и «бесконечное» множество, мы не определяли, но для любого «достаточно просто заданного» множества читатель без труда скажет, конечно оно или бесконечно[1]. Для конечного множества имеет смысл вопрос: «сколько в нем элементов?»; ответ на этот вопрос выражается целым неотрицательным числом[2]. Поэтому конечные множества можно сравнивать по числу элементов: например, множества $\{1, 2, 3\}$ и $\{a, б, в\}$ состоят из одинакового числа элементов, а во множестве $\left\{1, \frac{1}{2}, \frac{1}{3}\right\}$ больше элементов, чем в $\{1, 2\}$.

Может показаться, что для бесконечных множеств «количественное сравнение» невозможно: нет смысла спрашивать, в каком из двух бесконечных множеств больше элементов. Однако это не так. Создатель теории множеств Георг Кантор[3] ввел понятие м о щ н о с т и м н о ж е с т в а, позволяющее сравнивать любые множества по «ко-

[1] Примером «не просто заданного» множества может служить множество таких простых чисел $p$, для которых $p + 2$ также простое. Неизвестно, конечно это множество или бесконечно («проблема близнецов» — см. с. 52).

[2] Мы не всегда можем точно указать это число, но уверены в его существовании, если знаем, что множество конечно.

[3] Георг Кантор (Georg Cantor, 1845—1918) — немецкий математик, был профессором университета в Галле. Его идеи, которые впоследствии изменили лицо математики, долгое время оставались непризнанными и находили противников даже среди очень крупных математиков. Ныне канторова теория множества образует фундамент здания математики.

Содержание настоящего Приложения почти все восходит к работам Кантора — вплоть до идей доказательств.

личеству элементов». При этом понятие целого неотрицательного числа оказалось частным случаем понятия мощности. Поэтому удобно начать изучение этого последнего понятия с анализа первого.

Читателю хорошо известно различие между количественными и порядковыми числами[4]. Первые выражаются количественными числительными: один, два, три, ... — и служат для обозначения количества; вторые выражаются порядковыми числительными: первый, второй, третий, ... — и служат для обозначения места предмета в некотором ряду однородных «вещей». Нас будут сейчас интересовать только количественные числа.

Попробуем проанализировать значение некоторого конкретного (количественного) числа — скажем, «пять». Что означают такие предложения, как «У меня на руке пять пальцев». «У цветка яблони пять лепестков» и т. п.? В каждом из этих предложений утверждается, что некоторое множество — состоящее из пальцев руки, из лепестков цветка и т. п. — обладает свойством «состоять из пяти элементов»; и этим свойством исчерпывается то, что есть общего между всеми такими множествами. Поэтому число пять можно трактовать как некоторое *свойство множеств*. Легко заметить, далее, что между любыми двумя множествами, обладающими этим свойством, можно установить взаимно однозначное соответствие — иначе говоря, каждое из этих множеств можно биективно отобразить на каждое другое,— в то время как между множеством, обладающим свойством «состоять из пяти элементов», и множеством, не обладающим этим свойством, взаимно однозначное соответствие невозможно. То же и для любого другого числа: два конечных множества состоят из одинакового числа элементов тогда и только тогда, когда между ними можно установить взаимно однозначное соответствие. Поэтому мы можем назвать два конечных множества «равночисленными», если между ними можно установить взаимно однозначное соответствие, и *определить* число элементов конечного множества как *то общее, что имеется у всех множеств, равночисленных данному*. Форма этого определения может показаться необычной, но пусть читатель попробует подумать — какое еще содержание может иметь понятие количественного числа? Тот факт, что понятие взаимно однозначного соответствия (биективного отображения) логически проще понятия числа, подтверждается, в частности, следующим: 1) Дети, еще не освоившиеся как следует с употреблением чисел, считают по пальцам, т. е. выполняют биективные отображения различных множеств

[4] Под числами здесь и далее до конца этого пункта подразумеваются целые положительные числа.

на множества, состоящие из пальцев рук. 2) У народностей, не знакомых с абстрактным счетом[5], меновая торговля основывалась на непосредственном установлении взаимно однозначного соответствия между множествами «единиц товара» (например, продавцы раскладывали шкурки, а покупатели клали рядом с каждой шкуркой, скажем, нож).

2. Сделаем теперь простое наблюдение: при определении равночисленности множеств мы не пользовались тем, что они конечны. Поэтому можно ввести аналогичное понятие для произвольных множеств. При этом мы заменим термин «равночисленность» другим — *равномощность*. Итак, мы будем говорить, что множество $A$ *равномощно*[6] множеству $B$, если существует биективное отображение $A$ на $B$ (иначе: если между $A$ и $B$ можно установить взаимно однозначное соответствие). Вместо «$A$ равномощно $B$» будем писать также $A \sim B$. Докажем, что отношение равномощности множеств есть отношение эквивалентности.

1) Каждое множество можно биективно отобразить на себя: нужным отображением является хотя бы тождественное. Таким образом, отношение равномощности рефлексивно.

2) Если $f$ есть биективное отображение $A$ на $B$, то существует обратное отображение $f^{-1}$, область определения которого совпадает с множеством значений $f$, т. е. с $B$, а множество значений — с областью определения $f$, т. е. с $A$. Таким образом, $f^{-1}$ отображает $B$ на $A$, т. е. $f^{-1}$ сюръективно. В то же время, поскольку $f^{-1}(b) = a$ означает то же, что $b = f(a)$, а для каждого $a \in A$ имеется только одно $b \in B$, такое, что $b = f(a)$, отображение $f^{-1}$ инъективно. Следовательно, $f^{-1}$ есть биективное отображение $B$ на $A$. Итак, из существования биективного отображения $A$ на $B$ следует существование биективного отображения $B$ на $A$, т. е. отношение равномощности симметрично.

3) Если $f$ — биективное отображение $A$ на $B$ и $g$ — биективное отображение $B$ на $C$, то $f \circ g$ есть биективное отображение $A$ на $C$. Действительно, если бы некоторое $c \in C$ имело два разных прообраза при отображении $f \circ g$ — скажем, $a_1$ и $a_2$, $a_1 \neq a_2$, — то в силу инъективности $f$ было бы $f(a_1) \neq f(a_2)$, откуда в силу инъективности $g$ сле-

[5] В языках народностей, познакомившихся с ним лишь недавно, числительные нередко подразделяются на параллельные ряды, каждый из которых служит для счета предметов только одного определенного вида. Например, в нивхском языке имеется около тридцати разрядов количественных числительных — для счета мелких круглых предметов, для счета длинных предметов, для счета лодок, для счета нарт и т. д. (см. [Крейнович 1973]).

[6] Иногда вместо «равномощно» говорят «эквивалентно».

довало бы $g(f(a_1)) \neq g(f(a_2))$; но по предположению $g(f(a_1)) = g(f(a_2)) = c$. Таким образом, $f \circ g$ биективно. Итак, из существования биективных отображений $A$ на $B$ и $B$ на $C$ следует существование биективного отображения $A$ на $C$, т. е. отношение равномощности транзитивно.

Определим теперь понятие мощности — обобщение понятия количественного числа[7]:

*Мощность множества* есть то общее, что имеется у всех множеств, равномощных данному.

Мощность множества $A$ мы будем обозначать $|A|$.

Теперь необходимо выяснить, что значит, что два множества имеют одну и ту же мощность. По точному смыслу определения это должно означать: то общее, что есть у всех множеств, равномощных одному из двух данных — обозначим его $A$ — совпадает с тем общим, что есть у всех множеств, равномощных другому данному множеству — скажем, $B$. Но это, в свою очередь, означает, что множества, равномощные $A$, неотличимы от множеств, равномощных $B$ — иначе говоря, что $A$ и $B$ удовлетворяют следующему условию: ($\alpha$) всякое множество, равномощное множеству $A$, равномощно и множеству $B$, а всякое множество, равномощное $B$, равномощно $A$. А поскольку равномощность есть отношение эквивалентности, условие ($\alpha$) равносильно более простому условию ($\beta$) $A \sim B$. (Доказать это!) Итак: Два множества имеют одну и ту же мощность тогда и только тогда, когда они равномощны[8]. Иначе говоря, $|A| = |B|$ означает то же, что $A \sim B$.

Рассмотрим теперь несколько примеров. При этом — и всюду дальше — наряду с ранее употреблявшимися обозначениями $\mathbf{Z}$, $\mathbf{R}$ мы будем пользоваться следующими: $\mathbf{N}$ для натурального ряда чисел (т. е. множества $\{0, 1, 2, \ldots\}$[9]); $\mathbf{Q}$, $\mathbf{Q}_+$, $\mathbf{Q}_-$ — для множеств всех рациональных чисел, всех положительных рациональных чисел и всех отрицательных рациональных чисел соответственно; $\mathbf{R}_+$, $\mathbf{R}_-$ — для множеств всех положительных и всех отрицательных действительных чисел соответственно; $\mathbf{Z}_+$, $\mathbf{Z}_-$ — аналогично.

---

[7] Мощности часто называют также *кардинальными числами* (от латинского грамматического термина *numeralia cardinalia* — количественные числительные, букв. «основные числительные»; *cardinalis* — «основной, главный» (от *cardo* — «ось», «дверной крюк»), ср. русское «кардинальный» — «самый важный, существенный, основной»).

[8] «$A$ и $B$ равномощны» означает то же, что «$A$ равномощно $B$» (или «$B$ равномощно $A$»). Симметричные отношения очень часто выражаются подобным образом: «прямые $l_1$ и $l_2$ параллельны», «Миша и Гриша — братья» и т. п.

[9] Чаще натуральными числами называют только целые положительные числа. Однако мы в этой книге начинаем отсчет натуральных чисел с нуля.

Пример 1. $\mathbf{Z}_+ \sim \mathbf{Z}_-$. Действительно, если положить $f(n) = -n$, то $f$ будет биективным отображением $\mathbf{Z}_+$ на $\mathbf{Z}_-$.

Пример 2. $\mathbf{N} \sim \mathbf{Z}_+$. Биективное отображение осуществляется функцией $f(n) = n + 1$:

$$\begin{array}{l} \mathbf{N} = \{0, 1, 2, 3, \ldots\}; \\ \qquad\quad \downarrow\ \downarrow\ \downarrow\ \downarrow \\ \mathbf{Z}_+ = \{1, 2, 3, 4, \ldots\}. \end{array}$$

Пример 3. Множество $\mathbf{Z}$ равномощно множеству четных чисел и множеству нечетных чисел (и, следовательно, эти множества равномощны между собой). Биективные отображения осуществляются функциями $f(n) = 2n$, $g(n) = 2n + 1$:

$$\begin{array}{l} \ldots, -4, -2, 0, 2, 4, \ldots \\ \qquad\ \uparrow\ \ \uparrow\ \uparrow\ \uparrow\ \uparrow \\ \ldots, -2, -1, 0, 1, 2, \ldots \\ \qquad\ \downarrow\ \ \downarrow\ \downarrow\ \downarrow\ \downarrow \\ \ldots, -3, -1, 1, 3, 5, \end{array}$$

Пример 4. $\mathbf{N} \sim \mathbf{Z}$. Биективное отображение осуществляется следующей функцией $f$: $f(2n) = n$, $f(2n + 1) = -(n + 1)$:

$$\begin{array}{l} 0,\ 1,\ 2,\ 3,\ 4,\ 5, 6, \ldots \\ \downarrow\ \downarrow\ \downarrow\ \ \downarrow\ \ \downarrow\ \ \downarrow\ \downarrow \\ 0, -1, 1, -2, 2, -3, 3, \ldots \end{array}$$

Пример 5. Для любых действительных чисел $a$, $b$, $c$, $d$, таких, что $a < b$ и $c < d$, отрезки $[a, b]$ и $[c, d]$ равномощны; то же верно для интервалов $(a, b)$ и $(c, d)$. Биективное отображение ($[a, b]$ на $[c, d]$ (или, безразличио, $(a, b)$ на $(c, d)$): $f(x) = \dfrac{d - c}{b - a}(x - a) + c$ (см. рис. 11).

Пример 6. $\mathbf{R} \sim \mathbf{R}_+$. Биективное отображение: $f(x) = 2^x$.

Пример 7. $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \sim \mathbf{R}$. Биективное отображение: $f(x) = tg\, x$.

Из примеров 5, 6 и 7 видно, что множества $\mathbf{R}$ и $\mathbf{R}_+$ равномощны любому интервалу.

**Пример 8.** Множество точек полуокружности, не включающее ее концов, соответственно включающее концы, равномощно множеству точек ее диаметра, не считая концов, соответственно считая концы — а значит, и любому интервалу, соответственно отрезку (пример 5). Способ установления взаимно однозначного соответствия ясен из рис. 12.

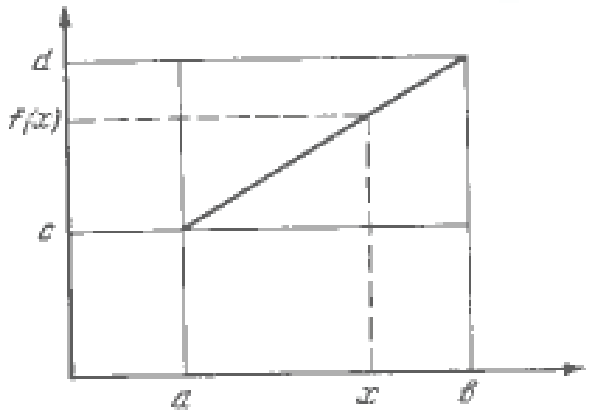



Рис. 11

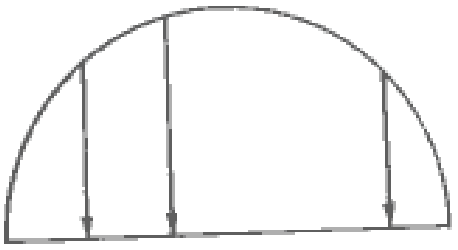


Рис. 12

**Пример 9.** Множество точек окружности равномощно множеству точек полуинтервала. Действительно, окружность можно представить в виде объединения двух непересекающихся полуокружностей, одна из которых включает концы, а другая — нет, а полуинтервал в виде объединения отрезка и не пересекающегося с ним интервала (например, $[0,2) = [0,1] \cup (1,2)$). Остается воспользоваться примером 8.

**Пример 10.** Множество точек полуокружности, не считая концов, равномощно R. Способ установления взаимно однозначного соответствия ясен из рис. 13.

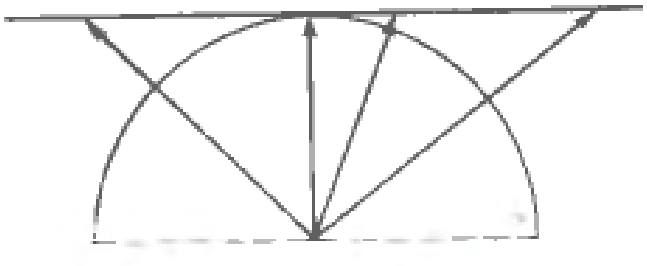


Рис. 13

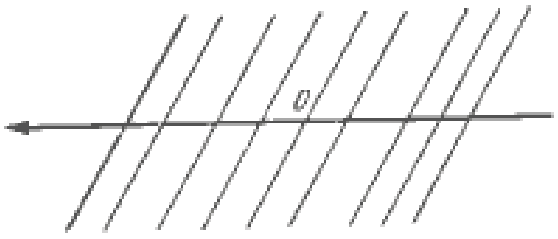



Рис. 14

Примеры 8 и 10 дают еще одно доказательство равномощности интервала и множества действительных чисел.

**Пример 11.** Множество прямых на плоскости, параллельных заданной прямой, равномощно R. Доказательство ясно из рис. 14.

**Пример 12.** Множество точек полусферы[10] без ограничивающей ее окружности равномощно множеству внутренних точек круга. Доказательство аналогично примеру 8.

**Пример 13.** То же множество равномощно множеству точек плоскости. Доказательство аналогично примеру 10.

Из примеров 12 и 13 следует, что множество точек плоскости равномощно множеству внутренних точек круга (*открытому кругу*).

Задача. Доказать, что:

а) $\mathbf{Z} \sim \mathbf{Z}\setminus\{0\}$;

б) $\mathbf{N} \sim \{-3, -2, -1, 0, 1, 2, \ldots\}$;

в) $\mathbf{N} \sim \mathbf{N}\cup\{а, б\}$;

г) $\mathbf{N}$ равномощно множеству натуральных чисел, дающих при делении на 3 остаток 2;

д) $\mathbf{R}_+ \sim R_+\setminus(0, 1]$;

е) $\mathbf{R} \sim (\mathbf{R}\setminus[-1, 1])\cup\{0\}$;

ж) $\mathbf{R}\setminus\{2, 3, 4\} \sim (-\infty, -1)\cup(0, 1)\cup(5, 7)\cup(\infty, +\infty)$;

з) $\mathbf{Q} \sim \mathbf{Q}\setminus(-1, 0]$;

и) $\mathbf{R}$ равномощно множеству точек синусоиды.

**Замечание.** Примеры 2, 3, 4, 6, 7 показывают, что множество может быть равномощно своей истинной части. Тому, кто имеет опыт обращения лишь с конечными множествами, такая возможность должна казаться удивительной; и действительно, скоро мы увидим, что она характерна именно для бесконечных множеств.

3. Но что такое бесконечное множество, как его определить? Понятно, что для этого достаточно сформулировать определение конечного множества. Чтобы это сделать, мы воспользуемся идеей построения конечных множеств «шаг за шагом», начиная с пустого, путем добавления элементов по одному. Эта идея приводит к индуктивному определению (ср. определения формулы в §§ 5.2 и 6.1). Чтобы его сформулировать, определим предварительно понятия пустого множества и атомного множества[11]: множество $M$ называется *пустым*, если оно не имеет элементов, т. е. удовлетворяет условию $\neg\exists x(x\in M)$, и *атомным*, если оно не пусто и не имеет

[10] *Сферой* мы называем поверхность шара, *полусферой* — одну из двух частей, на которые делит сферу окружность большого круга.

[11] Мы предпочитаем этот термин напрашивающемуся «одноэлементное», так как последний включает в себя слово «один», а число «один» — более сложный объект, определяемый именно через понятие атомного множества (см. ниже).

различных элементов, т. е. удовлетворяет условию $\exists x(x \in M \& \& \forall y(y \in M \supset y = x))$.

Теперь индуктивное определение *конечного множества* можно сформулировать так:

(а) Пустое множество конечно.

(б) Если $A$ — конечное множество и $B$ — атомное множество, то множество $A \cup B$ конечно.

(в) Множество может быть конечным только в силу (а) или (б).

Множество, не являющееся конечным, естественно назвать *бесконечным*.

Из определения конечного множества непосредственно ясно следующее: если мы хотим доказать, что все конечные множества обладают каким-либо свойством, то нам достаточно установить, что, во-первых, этим свойством обладает пустое множество, и, во-вторых, если какое-то множество обладает этим свойством, то им обладает и объединение данного множества с произвольным атомным множеством.

Применим это соображение к доказательству следующих утверждений:

**Теорема 1.** Множество, равномощное конечному множеству, также конечно.

**Доказательство.** I. Очевидно, между пустым и непустым множеством взаимно однозначное соответствие невозможно. Поэтому множество, равномощное пустому, также пусто и, следовательно, конечно. II. Пусть множество $A$ обладает тем свойством, что всякое равномощное ему множество конечно, и пусть $Q$ — произвольное атомное множество. Нам нужно доказать, что тем же свойством обладает множество $A \cup Q$. Если $Q \subset A$ (т. е. единственный элемент $Q$ принадлежит $A$), это очевидно, т. к. тогда $A \cup Q = A$. В противном случае произвольное множество $C$, равномощное $A \cup Q$, можно представить в виде $C = A_1 \cup Q_1$, где $A_1 \sim A$, $Q_1 \sim Q$, $A_1 \cap Q_1 = \varnothing$. Но $A_1$ по условию конечно, а $Q_1$ — атомное (очевидно, всякое множество, равномощное атомному, — также атомное). Поэтому $C$ конечно (по пункту (б) определения).

Следствие. Множество, равномощное бесконечному множеству, также бесконечно.

**Теорема 2.** Всякое подмножество конечного множества конечно.

**Доказательство.** I. Для пустого множества утверждение справедливо, т. к. у него есть только одно подмножество — оно само. II. Если множество $A$ обладает тем свойством, что всякое его подмножество конечно, и $Q$ — атомное множество, то всякое подмножество множества $A \cup Q$ либо содержится в $A$ — и тогда оно конечно по условию, —

либо представляется в виде $A' \cup Q$, где $A' \subset A$, — и тогда оно конечно по пункту (б) определения конечного множества.

**Следствие.** Множество, содержащее бесконечное подмножество, бесконечно.

**Теорема 3.** Объединение, пересечение, разность и декартово произведение двух конечных множеств суть конечные множества.

**Доказательство.** Поскольку множества $A \cap B$ и $A \setminus B$ содержатся в $A$, утверждение теоремы для пересечения и разности следует из теоремы 2. Докажем его для объединения. I. Объединение произвольного конечного множества $A$ с пустым множеством конечно, т. к. оно совпадает с $A$. II. Пусть множество $B$ обладает тем свойством, что для произвольного конечного множества $A$ объединение $A \cup B$ конечно. Тогда этим же свойством обладает и объединение $B$ с произвольным атомным множеством $Q$. В самом деле, $A \cup (B \cup Q) = (A \cup B) \cup Q$; но $A \cup B$ конечно по условию, а поэтому и $(A \cup B) \cup Q$ конечно (пункт (б) определения). Остается доказать утверждение для декартова произведения, что мы сейчас и сделаем. I. Для любого $A$ множество $A \times \varnothing$ пусто и, следовательно, конечно. II. Если множество $B$ обладает тем свойством, что для любого конечного множества $A$ декартово произведение $A \times B$ конечно, то множество $A \times (B \cup Q)$, где $A$ — конечное множество и $Q$ — атомное множество, состоящее из единственного элемента $q$, можно представить в виде $(A \times B) \cup A_q$, где $A_q$ — множество всевозможных упорядоченных пар вида $(a, q)$, $a \in A$. Очевидно, $A_q$ равномощно $A$ и потому конечно (теорема 1). Поэтому и $(A \times B) \cup A_q$ конечно — как объединение двух конечных множеств.

**Теорема 4.** Конечное множество не может быть равномощно своей истинной части.

**Доказательство.** I. Для пустого множества утверждение теоремы справедливо просто потому, что у него нет истинных частей. II. Пусть утверждение верно для некоторого множества $A$, и пусть $Q = \{q\}$ — атомное множество; докажем то же утверждение для $A \cup Q$. Если $q \in A$, оно очевидно, так как в этом случае $A \cup Q = A$. Пусть $q \notin A$ и утверждение для $A \cup Q$ не имеет места, т. е. существует биективное отображение $g$: $A \cup Q \xrightarrow{на} C$, где $C$ — истинная часть $A \cup Q$. Возможны два случая: 1) $q \notin C$, т. е. $C \subset A$. Тогда множество $C \setminus \{g(q)\}$, являющееся истинной частью $C$, будет также и истинной частью $A$; но функция $g$ биективно отображает $A$ на $C \setminus \{g(q)\}$, что противоречит предположению. 2) $q \in C$. Поскольку $C$ — истинная часть $A \cup Q$, найдется такое $a \in A \cup Q$, что $a \notin C$ (в данном случае $a \in A$). Положим $g^{-1}(q) = d$ и «исправим» отображение $g$: «перенесем» образ $d$ из $q$ в $a$. «Исправленное» отображение по-прежнему биективно, его областью определения остается $A \cup Q$, но множеством значений будет теперь $(C \setminus \{q\}) \cup \{a\}$, не содержащее $q$. Далее рассуждаем, как в случае 1.

**4.** Мощности конечных множеств — это не что иное, как натуральные числа. (См. сноску 9 на с. 435!). В частности, мощность пустого множества — это число 0, мощность атомного множества — число 1, мощность множества вида $A \cup B$, где $A$ и $B$ атомные и $A \cap B = \varnothing$ — число 2, и т. д.

Нетрудно было бы систематически построить арифметику натуральных чисел, понимая их как мощности конечных множеств. Мы этого делать не будем. (Впрочем, ниже мы определим для произвольных мощностей отношение «меньше», сумму и произведение, частными случаями которых являются соответствующие понятия для натуральных чисел.) Не будем мы и уточнять понятия рационального и действительного числа; для наших целей достаточно тех сведений о них, которые имеются в школьном курсе математики.

Множество N всех натуральных чисел — называемое, как известно, *натуральным рядом чисел* или просто *натуральным рядом* — представляет собой простейший пример бесконечного множества. В самом деле, оно равномощно своей истинной части (см. хотя бы пример 2 в предыдущем пункте[12]) и, следовательно, по теореме 4 не может быть конечным.

Множества, равномощные натуральному ряду, называются *счетными*. По следствию из теоремы 1 все они бесконечны; при этом они занимают среди бесконечных множеств особое место ввиду следующего факта:

**Теорема 5.** Множество тогда и только тогда бесконечно, когда оно содержит счетное подмножество.

**Доказательство.** (а) Пусть $M$ — произвольное бесконечное множество. Поскольку $M$ не пусто (пункт (а) определения конечного множества), оно содержит некоторый элемент $a_0$. Поскольку множество $\{a_0\} = \varnothing \cup \{a_0\}$ конечно (пункт (б) определения конечного множества), $M$ не совпадает с $\{a_0\}$ и, значит, содержит элемент $a_1 \neq a_0$. Множество $\{a_0, a_1\} = \{a_0\} \cup \{a_1\}$ также конечно (в силу того же пункта (б)); поэтому $M \neq \{a_0, a_1\}$; следовательно, в $M$ имеется элемент $a_2$, отличный от $a_0$ и от $a_1$; а так как $\{a_0, a_1, a_2\} = \{a_0, a_1\} \cup \{a_2\}$ конечно, то $M \neq \{a_0, a_1, a_2\}$ и в $M$ найдется элемент $a_3$, отличный от $a_0$, от $a_1$ и от $a_2$. Таким же образом для каждого натурального числа $n$ в $M$ можно найти элемент $a_n$, причем $m \neq n \supset a_m \neq a_n$. Полагая $f(n) = a_n$, видим, что $f$ есть биективное отображение N на $\{a_0, a_1, a_2, \cdots\}$, так что множество $\{a_0, a_1, a_2, \cdots\}$ счетно. Итак, мы доказали, что произвольное бесконечное множество содержит счетное подмножество.

[12] Можно также биективно отобразить N на множество четных — или нечетных — натуральных чисел аналогично примеру 3.

(б) Обратное утверждение вытекает из бесконечности счетного множества и следствия из теоремы 2.

Мощность натурального ряда — или, что то же самое, мощность произвольного счетного множества — принято обозначать $\aleph_0$[13].

В дальнейшем мы часто будем обозначать произвольное счетное множество через $\{a_0, a_1, a_2, \ldots\}$ (или $\{b_0, b_1, b_2, \cdots\}$ и т. п.), подразумевая при этом, что выбрано некоторое биективное отображение натурального ряда на данное множество и образ числа $n$ обозначен через $a_n$. В этом случае часто говорят, что элементы множества занумерованы натуральными числами. Иногда удобнее нумеровать их целыми положительными числами, т. е. обозначать множество, например, через $\{a_1, a_2, a_3, \cdots\}$.

Теперь нетрудно заметить, что необходимое условие конечности, которое дает теорема 4, в действительности является также и достаточным — иначе говоря, имеет место

**Теорема 6.** Множество тогда и только тогда бесконечно, когда оно равномощно своей истинной части.

**Доказательство.** Ввиду теоремы 4 достаточно установить, что всякое бесконечное множество равномощно некоторой своей истинной части. Пусть множество $M$ бесконечно. По теореме 5 $M$ содержит счетное подмножество $M_1 = \{a_0, a_1, a_2, \cdots\}$. Если положить $g(a_n) = a_{2n}$ и (в случае, когда $M \setminus M_1 \neq \varnothing$) $g(x) = x$ для $x \in M \setminus M_1$, то $g$ будет биективным отображением $M$ на множество $(M \setminus M_1) \cup \{a_0, a_2, a_4, \cdots\}$, являющееся истинной частью $M$.

**Замечание.** Характеристическое свойство бесконечных множеств, которое дает теорема 6, принимают иногда в качестве определения бесконечного множества.

Установим теперь несколько свойств счетных множеств.

**Теорема 7.** Всякое подмножество счетного множества конечно или счетно.

**Доказательство.** Пусть $M = \{a_0, a_1, a_2, \cdots\}$ — счетное множество и $M_1 \subset M$. Если $M_1$ пусто, оно конечно. Если $M_1$ не пусто, пусть $n_0$ — наименьшее число, для которого $a_{n_0} \in M_1$. Если $M_1 = \{a_{n_0}\}$, то $M_1$ конечно. В противном случае пусть $n_1$ — наименьшее число, для которого $a_{n_1} \in M_1 \setminus \{a_{n_0}\}$. Если $M_1 = \{a_{n_0}, a_{n_1}\}$, то $M_1$ конечно. В противном случае пусть $n_2$ — наименьшее число, для которого $a_{n_2} \in M_1 \setminus \{a_{n_0}, a_{n_1}\}$, и т. д. При продолжении этого процесса возможны два случая: 1) Найдется такое $k$, что $M_1 = \{a_{n_0}, \ldots, a_{n_k}\}$. Тогда $M_1$ конечно.

[13] $\aleph$ (читается «алеф») — первая буква еврейского алфавита.

2) $M_1 = \{a_{n_0}, a_{n_1}, a_{n_2}, \cdots\}$. Тогда, полагая $f(k) = a_{n_k}$ $(k = 0, 1, 2...)$, получаем биективное отображение N на $M_1$; значит, $M_1$ счетно.

**Теорема 8.** Мощность бесконечного множества не меняется при объединении с конечным или счетным множеством.

**Доказательство.** Пусть $A$ — бесконечное множество и $B$ — конечное или счетное множество. Читатель без труда докажет, что $A \cup B = A \cup (B \setminus A)$[14]: по теореме 7 множество $B \setminus A$ конечно или счетно. По теореме 5 множество $A$ содержит счетное подмножество $C = \{c_0, c_1, c_2, \cdots\}$. Рассмотрим два случая: 1) $B \setminus A$ конечно. Можно считать, что $B \setminus A \neq \varnothing$ (иначе $A \cup B = A$). Пусть $B \setminus A = \{b_0, b_1, ..., b_k\}$. Определим функцию $g$, полагая $g(b_0) = c_0$, $g(b_1) = c_1$, ..., $g(b_k) = c_k$, $g(c_0) = c_{k+1}$, $g(c_1) = c_{k+2}$, ... и $g(x) = x$ для $x \in A \setminus C$. Очевидно, $g$ есть биективное отображение множества $A \cup B = ((B \setminus A) \cup C) \cup (A \setminus C)$ на $A = C \cup (A \setminus C)$.

2) $B \setminus A$ счетно, $B \setminus A = \{b_0, b_1, b_2, \cdots\}$. Полагая $g(b_n) = c_{2n}$, $g(c_n) = c_{2n+1}$ и $g(x) = x$ для $x \in A \setminus C$, снова получаем биективное отображение $A \cup B$ на A.

**Теорема 9.** Объединение конечного числа множеств, одно из которых счетно, а остальные конечны или счетны, есть счетное множество.

Эта теорема для случая двух множеств является частным случаем предыдущей; случай трех множеств получается очевидным образом из случая двух, и т. д.[15]

**Теорема 10.** Декартово произведение конечного числа счетных множеств счетно.

**Доказательство.** (а) Рассмотрим сначала произведение двух сомножителей. Пусть $A = \{a_0, a_1, a_2, \cdots\}$ и $B = \{b_0, b_1, b_2, \cdots\}$ — счетные множества. Расположим элементы множества $A \times B = \{(a_i, b_j) | i, j = 0, 1, ...\}$ в последовательность следующим образом: сначала запишем (единственную) пару, у которой сумма индексов при $a$ и $b$ равна нулю, затем две пары, у которых эта сумма равна 1, затем три пары, у которых она равна 2, и т. д., а в каждой группе пар с одинаковыми суммами индексов (см. рис. 15, где эти группы изображены наклонными полосами) упорядочим пары по возрастанию индекса при $a$. В результате получим последовательность:

$$(a_0, b_0), (a_0, b_1), (a_1, b_0), (a_0, b_2), (a_1, b_1), (a_2, b_0), (a_0, b_3), \ldots .$$

---

[14] Это верно для л ю б ы х множеств $A$ и $B$.

[15] Строгое доказательство для общего случая должно проводиться по индукции (см. Приложение III).

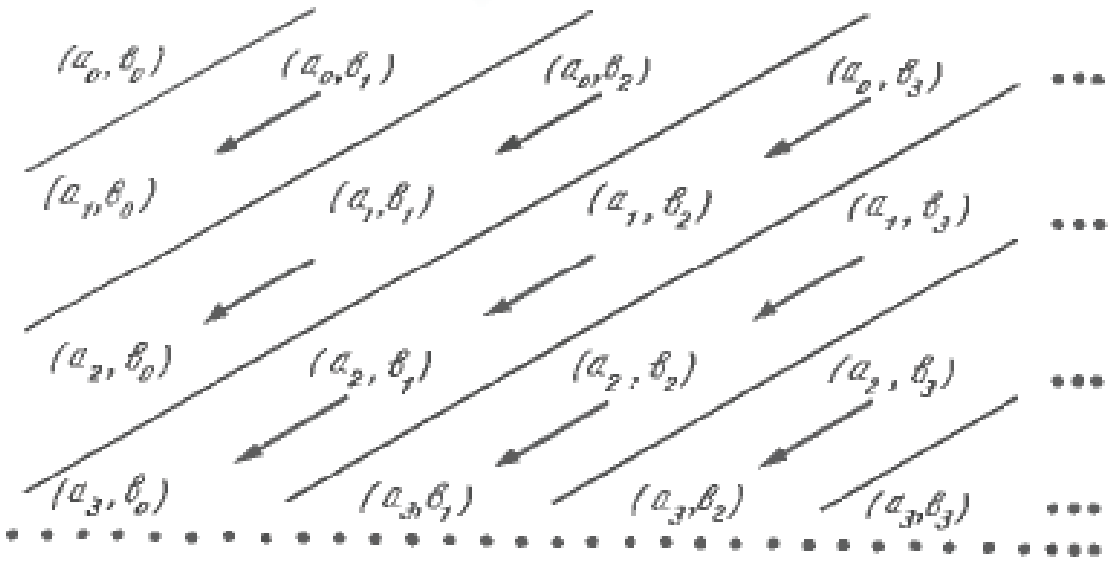



Рис. 15

Если теперь для каждого $n = 0, 1, 2, \ldots$ положить $f(n)$ равным $n$-му по порядку члену этой последовательности, то $f$ будет биективным отображением $\mathbb{N}$ на $A \times B$.

(б) Легко видеть, что $A_1 \times \cdots \times A_n \times A_{n+1} \sim (A_1 \times \cdots \times A_n) \times A_{n+1}$ (достаточно сопоставить каждой упорядоченной системе $(a_1, \ldots, a_n, a_{n+1})$ где $a_i \in A_i$, пару $((a_1, \ldots, a_n), a_{n+1})$). Поэтому из результата для случая двух сомножителей сразу получается аналогичный результат для трех, далее так же для четырех и т. д.

Важный пример. Множества $\mathbb{Q}$, $\mathbb{Q}_+$, $\mathbb{Q}_-$ счетны. Достаточно доказать это для $\mathbb{Q}_+$, так как между $\mathbb{Q}_+$ и $\mathbb{Q}_-$ очевидным образом устанавливается взаимно однозначное соответствие, а тогда из равенства $\mathbb{Q} = \mathbb{Q}_+ \cup \mathbb{Q}_- \cup \{0\}$ будет следовать счетность $\mathbb{Q}$. Но каждое положительное рациональное число единственным образом представляется в виде несократимой дроби, так что $\mathbb{Q}_+$ равномощно подмножеству $P$ множества $\mathbb{Z}_+^2$, состоящему из пар вида $(m, n)$, где $m$ взаимно просто с $n$. Поскольку $P$ бесконечно (хотя бы потому, что содержит все пары вида $(m, 1)$), оно в силу теорем 10 и 7 счетно.

**Теорема 11.** Объединение счетного числа конечных или счетных множеств конечно или счетно.

Доказательство. Пусть $A_0, A_1, A_2, \ldots$ — конечные или счетные множества и $A = \bigcup_{n=0}^{\infty} A_n$. Рассмотрим сначала случай, когда $A_n$ попарно не пересекаются. Каждому $a \in A$ сопоставим упорядоченную пару натуральных чисел следующим способом. Пусть $A_i$ — тот член объединения, которому принадлежит $a$ (поскольку члены объединения попарно не пересекаются, $A_i$ определяется единственным образом).

Множество $A_i$ можно представить либо в виде $\{a_{i0}, \cdots a_{ik_i}\}$ (если оно конечно), либо в виде $\{a_{i0}, a_{i1}, a_{i2}, \cdots\}$ (если оно счетно); в обоих случаях найдется такое $j$, что $a = a_{ij}$. Пару $(i, j)$ мы и сопоставим элементу $a$ и обозначим ее $f(a)$. Тем самым мы получаем отображение $f$ множества $A$ во множество $\mathbf{N}^2$; из способа построения отображения ясно, что оно инъективно — иначе говоря, что оно является биективным отображением множества на некоторое подмножество $\mathbf{N}^2$. Итак, $A$ равномощно подмножеству $\mathbf{N}^2$; но всякое подмножество $\mathbf{N}^2$ конечно или счетно (теоремы 10 и 7).

Переходя к общему случаю, положим $B_0 = A_0$, $B_1 = A_0 \setminus A_1$, $B_2 = A_2 \setminus (A_0 \cup A_1)$, $B_3 = A_3 \setminus (A_0 \cup A_1 \cup A_2)$ и т. д.; положим также $B = \bigcup_{n=0}^{\infty} B_n$. Легко доказать, пользуясь методом математической индукции, что $B_0 \cup B_1 \cup \cdots \cup B_n = A_0 \cup A_1 \cup \cdots \cup A_n$ $(n = 0, 1, \ldots)$, откуда $B = A$. Столь же легко доказывается, что множества $B_n$ попарно не пересекаются. Тем самым задача сводится к предыдущему случаю.

Пример. Множество $V^*$ всех слов в конечном или счетном алфавите $V$ счетно. В самом деле, множество слов в алфавите $V$, имеющих заданную длину $n > 1$, есть не что иное, как декартова степень $V^n$. Если алфавит $V$ конечен, то $V^n$ также конечно (подсчет мощности $V$ см. в Приложении III, пример 2 на с. 460), а если $V$ — счетное множество, $V^n$ по теореме 10 также счетно. Но $V^* = \bigcup_{n=0}^{\infty} V^n$ (мы полагаем здесь $V^1 = V$ и обозначаем через $V^0$ множество, состоящее из одного лишь пустого слова). А отсюда, поскольку $V^*$ в любом случае бесконечно (потому что для любого $a \in V$ оно содержит все слова вида $aa...a$), по теореме 11 следует, что оно счетно.

Замечание. В частности, множество конечных последовательностей натуральных чисел счетно, т. к. его можно рассматривать как множество слов в алфавите $\mathbf{N}$.

Задача. Доказать, что следующие множества счетны:

а) простых чисел;

б) составных чисел;

в) рациональных чисел, принадлежащих интервалу $(0, 1)$;

г) десятично рациональных чисел (т. е. чисел, представимых в виде конечных десятичных дробей);

д) точек плоскости, обе координаты которых рациональны;

е) точек пространства, все три координаты которых рациональны;

ж) многочленов с целыми коэффициентами;

з) многочленов с рациональными коэффициентами.

5. Бесконечные множества, не являющиеся счетными, принято называть *несчетными*. Существование несчетных множеств вытекает из следующей теоремы:

**Теорема 12.** Множество **R** несчетно.

Доказательство. Поскольку **R** заведомо бесконечно (хотя бы потому, что содержит **N**), достаточно показать, что оно не является счетным. А так как $\mathbf{R} \sim (0, 1)$ (пункт 2, замечание после примера 7), достаточно доказать это для (0, 1).

Допустим, что множество (0, 1) счетно. Тогда положительные действительные числа, меньшие единицы,— т. е. бесконечные десятичные дроби с целой частью 0, не оканчивающиеся девятками и отличные от нуля,— можно занумеровать целыми положительными числами, так что (0, 1) будет представлено в виде $\{a_1, a_2, \cdots\}$. Обозначая $j$-й десятичный знак дроби $a_i$ через $\alpha_{ij}$, получаем:

$$a_1 = 0, \alpha_{11}\, \alpha_{12} \cdots \alpha_{1j} \cdots$$

$$a_2 = 0, \alpha_{21}\, \alpha_{22} \cdots \alpha_{2j} \cdots$$

. . . . . .

$$a_i = 0, \alpha_{i1}\, \alpha_{i2} \cdots \alpha_{ij} \cdots$$

. . . . . .

Фиксируем теперь для каждого $j = 1, 2, \ldots$ некоторую цифру $\beta_j$, отличную от $\alpha_{jj}$, от нуля и от девятки. Рассмотрим бесконечную десятичную дробь $b = 0, \beta_1\beta_2\ldots\beta_j\ldots$. Среди ее десятичных знаков нет ни одной девятки и ни одного нуля; поэтому она является положительным действительным числом, меньшим 1, и, значит, должна совпасть с некоторым $a_{i_0}$, откуда $\beta_j = \alpha_{i_0 j}$ для любого $j = 1, 2, \ldots$. В частности, должно быть $\beta_{i_0} = \alpha_{i_0 i_0}$, но это невозможно — мы выбирали $\beta_{i_0}$ как раз так, чтобы оно было отлично от $\alpha_{i_0 i_0}$. Итак, предположение о счетности (0, 1) привело нас к противоречию.

Мощность множества **R** — отличную, как мы доказали, от $\aleph_0$ — называют *мощностью континуума*[16] и обозначают латинской буквой $c$.

**Задача.** Пользуясь теоремой 8, доказать, что мощность множества иррациональных чисел равна $c$.

6. Для произвольных мощностей можно определить операции *сложения* и *умножения*, частными случаями которых являются сложение и умножение натуральных чисел. Чтобы определить сложе-

[16] *Континуумом* (от лат. *continuum* — «непрерывное») иногда называют само множество **R**.

ние, вспомним, что детям его объясняют с помощью примеров вроде такого: «У Вани два яблока, а у Тани три. Сколько яблок у них вместе? Пять. Значит, 2 + 3 = 5». Перевод на «взрослый» язык даст следующее определение суммы мощностей (пригодное для мощностей любых множеств, не обязательно конечных!): мощность $\rho$ называется *суммой мощностей* $\mu$ и $\nu$ (обозначение: $\rho = \mu + \nu$), если существуют такие множества $A$ и $B$, что $|A| = \mu$, $|B| = \nu$, $A \cap B = \varnothing$ и $|A \cup B| = \rho$. (Можно доказать, что в этом случае для л ю б ы х двух множеств $A_1$ и $B_1$, таких, что $|A_1| = \mu$, $|B_1| = \nu$ и $A_1 \cap B_1 = \varnothing$, будет $|A_1 \cup B_1| = \rho$). Произведение (любых) мощностей определяется также в согласии со «школьным» пониманием этого термина («$m \cdot n$ есть сумма $n$ слагаемых, равных $m$»): мощность $\rho$ называется *произведением мощности* $\mu$ *на мощность* $\nu$ (обозначение: $\rho = \mu \cdot \nu$ или $\rho = \mu\nu$), если существует такое множество $B$ мощности $\nu$, элементами которого являются попарно непересекающиеся множества, каждое из которых имеет мощность $\mu$, что мощность объединения всех множеств-элементов $B$ равна $\rho$. (Можно доказать, что тогда для л ю б о г о множества мощности $\nu$, элементами которого являются попарно непересекающиеся множества мощности $\mu$, мощность объединения всех его элементов равна $\rho$.)

Нетрудно убедиться, что обе эти операции ассоциативны и коммутативны, и умножение дистрибутивно по отношению к сложению. (Ассоциативность и коммутативность сложения тривиальным образом следуют из соответствующих свойств объединения множеств; на доказательствах остальных свойств мы останавливаться не будем.)

**Примеры.** 1) $n + \aleph_0 = \aleph_0$ для любого натурального числа $n$. В самом деле, полагая $A_n = \{k \mid k \in \mathbf{N} \& k < n\}$, $B_n = \{k \mid k \in \mathbf{N} \& k \geq n\}$, имеем $|A_n| = n$, $|B_n| = \aleph_0$, $A_n \cap B_n = \varnothing$; но $A_n \cup B_n = \mathbf{N}$, так что $|A_n \cup B_n| = \aleph_0$.

2) $\aleph_0 + \aleph_0 = \aleph_0$. Действительно, полагая

$A = \{0, 2, 4, \ldots\}$, $B = \{1, 3, 5, \ldots\}$, имеем $|A| = |B| = \aleph_0$, $A \cap B = \varnothing$, $A \cup B = \mathbf{N}$.

3) $n \cdot \aleph_0 = \aleph_0$ для любого натурального $n \neq 0$: полагая $A_k = \{kn, kn + 1, \ldots, kn + (n - 1)\}$ для каждого $k = 0, 1 \ldots$ и обозначая через $B$ множество, элементами которого являются всевозможные $A_k$, видим, что $|B| = \aleph_0$, $|A_k| = n$ для любого $k$, множества $A_k$ попарно не пересекаются и объединение их есть $\mathbf{N}$.

4) $\aleph_0 \cdot \aleph_0 = \aleph_0$: обозначая через $D_n$, где $n$ — фиксированное натуральное число, множество всевозможных упорядоченных пар вида $(m, n)$ где $m \in \mathbf{N}$, видим, что множества $D_n$ попарно не пересе-

каются, мощность каждого из них равна $\aleph_0$ и объединение их есть $N^2$. Но по теореме 10 $|N^2| = \aleph_0$.

Дальнейшие примеры см. ниже (с. 451, 453).

Замечание. Из приведенных примеров видно, что «мощностные уравнения» $\xi + \aleph_0 = \aleph_0$ и $\xi \cdot \aleph_0 = \aleph_0$ имеют бесконечно много решений [17]. Поэтому для произвольных мощностей нельзя определить ни вычитание, ни деление.

Задачи. 1) Пользуясь определением конечного множества, доказать, что сумма и произведение натуральных чисел — натуральные числа.

2) Доказать, что $\mu \cdot 0 = 0 \cdot \mu = 0$ для любой мощности $\mu$.

3) доказать равенство $\aleph_0 \cdot n = \aleph_0$, не пользуясь коммутативностью умножения.

7. Теперь мы можем вернуться к вопросу о сравнении произвольных множеств «по количеству элементов».

Это значит, что мы должны определить для произвольных мощностей отношение «меньше». Для натуральных чисел это делается очевидным образом: естественно считать, что натуральное число $m$ меньше натурального числа $n$, если (произвольное) множество мощности $m$ равномощно истинной части (произвольного) множества мощности $n$. (Это тоже перевод на «взрослый» язык «детского» объяснения: чтобы узнать, чего на столе больше — чашек или блюдец, нужно попытаться каждую чашку поставить на блюдце, и если блюдец не хватит — значит, чашек больше, а если останутся лишние блюдца — больше блюдец.) Но если бы мы попробовали распространить это определение на общий случай, то ввиду теоремы 6 всякая бесконечная мощность[18] оказалась бы меньше самой себя. Во избежание этого нужно дополнить определение требованием, чтобы множества, мощности которых сравниваются, не были равномощны.

Итак; если $\mu$ и $\nu$ — произвольные мощности, говорят, что $\mu$ *меньше* $\nu$ (иначе: $\nu$ *больше* $\mu$) и пишут $\mu < \nu$ (или $\nu > \mu$), если, каковы бы ни были множества $A$ и $B$, такие, что $|A| = \mu$ и $|B| = \nu$, множество $A$ равномощно некоторой истинной части множества $B$ и не равномощно самому $B$. Из того факта, что равномощность есть отношение эквивалентности, легко выводится, что $\mu < \nu$ тогда и только тогда, когда существуют множества $A$ и $B$, такие, что $|A| = \mu$, $|B| = \nu$ и $A$ равномощно некоторой истинной части $B$, но не равномощно самому $B$.

---

[17] В действительности это верно для любых уравнений вида $\xi + \mu = \mu$ и $\xi \cdot \mu = \mu$, где $\mu$ — мощность заданного бесконечного множества.

[18] *Конечными*, соответственно *бесконечными мощностями* мы будем называть мощности конечных (бесконечных) множеств.

Теперь наша ближайшая задача — установить, что введенное только что отношение $<$ есть порядок. Для этого нам понадобится следующая теорема, представляющая и большой самостоятельный интерес:

**Теорема 13** (теорема Кантора — Бернштейна)[19]. Если $A \sim B' \subset B$ и $B \sim A' \subset A$, то $A \sim B$.

Иногда эту теорему формулируют иначе:

**Вторая формулировка теоремы Кантора — Бернштейна.** Если $A_2 \subset A_1 \subset A_0$ и $A_0 \sim A_2$, то $A_0 \sim A_1 \sim A_2$.

**Доказательство равносильности формулировок.** Пусть справедлива теорема в первой формулировке. Тогда, если $A_2 \subset A_1 \subset A_0$ и $A_0 \sim A_2$, имеем: 1) $A_1 \sim A_1 \subset A_0$; 2) $A_0 \sim A_2 \subset A_1$. Отсюда $A_1 \sim A_0$. Таким образом, из первой формулировки следует вторая. Обратно, пусть справедлива теорема во второй формулировке, и пусть $A \sim B' \subset B$ и $B \sim A' \subset A$. Тогда существуют биективные отображения $f$: $A \xrightarrow{на} B'$ и $g$: $B \xrightarrow{на} A'$ (рис. 16). Определим отображение $h$: $A \to A'$, положив для каждого $a \in A$: $h(a) = g(f(A))$. Обозначая множество значений $h$ через $A''$, имеем $A'' \subset A'$. Очевидно, $h$ взаимно однозначно. Следовательно, $A'' \sim A$; отсюда и из $A'' \subset A' \subset A$ вытекает $A \sim A'$, но по условию $A' \sim B$, так что $A \sim B$. Итак, из второй формулировки следует первая.

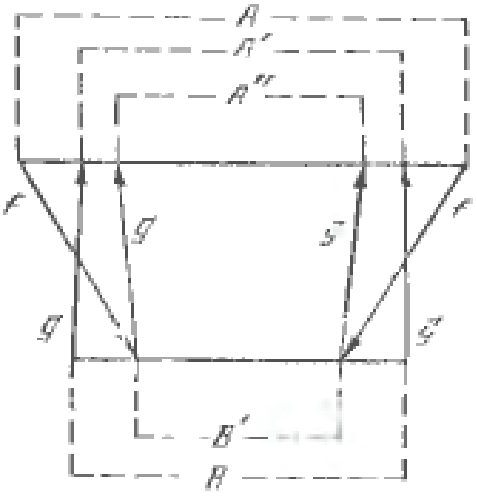



Рис. 16

**Доказательство теоремы.** Докажем теорему во второй формулировке. Пусть $A_2 \subset A_1 \subset A_0$ и $A_0 \sim A_2$. Существует биективное отображение $f$: $A \xrightarrow{на} A_2$. Имеем $A_2 = f(A_0)$[20]. Определим последовательность множеств $A_3$, $A_4$, $A_5$, ... следующим образом: $A_3 = f(A_1)$, $A_4 = f(A_2)$, $A_5 = f(A_3)$ и т. д. Поскольку для любых $C$ и $D$ из $C \subset D$ следует $f(C) \subset f(D)$, имеем: $A_3 = f(A_1) \subset f(A_0) = A_2$; $A_4 = f(A_2) \subset f(A_1) = A_1$. Отсюда точно так же получаем $A_5 \subset A_4$, $A_6 \subset A_5$ и т. д. Мы получили, таким образом, бесконечную последовательность множеств

$$A_0 \supset A_1 \supset A_2 \supset A_3 \supset A_4 \supset A_5 \supset \ldots.$$

---

[19] Ф. Бернштейн (Felix Bernstein. 1878—1956) — немецкий математик, был профессором университета в Гёттингене.

[20] Через $f(M)$ мы обозначаем образ множества $M$ при отображении $f$.

где $A_{n+2} = f(A_n)$ для каждого $n = 0, 1, 2, \ldots$. Так как $f$ взаимно однозначно, легко видеть, что $f(A_n \setminus A_{n+1}) = A_{n+2} \setminus A_{n+3}$ $(n = 0, 1, 2, \ldots)$. Положив $D = \bigcap_{n=0}^{\infty} A_n$, будем иметь:

$$(*)\ A_0 = (A_0 \setminus A_1) \cup (A_1 \setminus A_2) \cup (A_3 \setminus A_4) \cup \cdots \cup D;$$
$$(**)\ A_1 = (A_1 \setminus A_2) \cup (A_3 \setminus A_4) \cup \cdots \cup D.$$

В самом деле: если $a \in A_0$, то либо $a$ принадлежит всем $A_n$, либо не всем. В первом случае $a \in D$; во втором, если $A_{n_0}$ — первое из $A_n$, которому $a$ не принадлежит, то $n_0 > 0$ и $a \in A_{n_0-1}$, так что $a \in A_{n_0-1} \setminus A_{n_0}$. Таким образом, $A_0$ содержится в правой части соотношения (*); обратное включение очевидно. Равенство (**) доказывается так же.

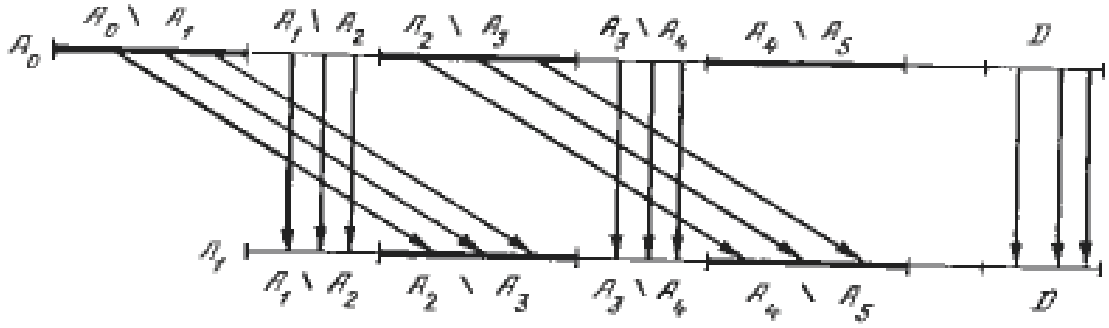



Рис. 17

Рассмотрим теперь множество

$$S = (A_1 \setminus A_2) \cup (A_3 \setminus A_4) \cup (A_5 \setminus A_6) \cup \cdots \cup D$$

(на рис. 17 жирными линиями отмечены разности, не содержащиеся в $S$) и определим на $A_0$ функцию $g$ следующим образом:

$$g(x) = \begin{cases} x, & \text{если } x \in S \\ f(x), & \text{если } x \notin S. \end{cases}$$

Имеем, очевидно:

$$g(A_0 \setminus A_1) = f(A_0 \setminus A_1) = A_2 \setminus A_3;$$
$$g(A_1 \setminus A_2) = A_1 \setminus A_2;$$
$$g(A_2 \setminus A_3) = f(A_2 \setminus A_3) = A_4 \setminus A_5;$$
$$g(A_3 \setminus A_4) = A_3 \setminus A_4;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$g(D) = D$$

(см. рис. 17).

Отсюда ввиду (*) и (**) получаем $g(A_0) = A_1$. Ясно, также, что $g$ взаимно однозначна. Итак, функция $g$ осуществляет биективное отображение $A_0$ на $A_1$; существование такого отображения нам и требовалось доказать.

Теорема Кантора — Бернштейна часто оказывается полезной при доказательстве равномощности множеств.

**Примеры.** 1) Поскольку $\mathbf{R}$ равномощно любому интервалу, всякое подмножество $\mathbf{R}$, содержащее какой-либо интервал, имеет мощность $c$. В частности, такова мощность любого отрезка и любого полуинтервала.

2) Поскольку $\mathbf{R}^2$ (множество точек плоскости) равномощно открытому кругу (замечание после примера 13 в пункте 2), всякое подмножество $\mathbf{R}^2$, содержащее какой-либо открытый круг, равномощно $\mathbf{R}^2$.

С помощью примера 1 легко показать, что: (а) $c + n = c$; (б) $c + \aleph_0 = c$; (в) $c + c = c$; (г) если $n \neq 0$, то $c \cdot n = c$; (д) $c \cdot \aleph_0 = c$. (Здесь $n$ — произвольное натуральное число). В самом деле, полагая $A = (1, 2)$, $B = \left\{1, \frac{1}{2}, \ldots, \frac{1}{2^{n-1}}\right\}$, имеем $|A| = c$, $|B| = n$, $A \cap B = \varnothing$, $|A \cup B| = c$; этим доказывается (а). Точно так же, заменяя множество $\left\{1, \frac{1}{2}, \ldots, \frac{1}{2^{n-1}}\right\}$ на $\left\{1, \frac{1}{2}, \frac{1}{4}, \cdots\right\}$, соответственно на $(0, 1)$, получим (б) и (в). Чтобы доказать (г), рассмотрим множество $B = \{(0,1), (1, 2), \ldots, (n - 1, n)\}$. Очевидно, $|B| = n$, элементы $B$ попарно не пересекаются, и их мощности, как и мощность их объединения, равны $c$. Аналогично с помощью множества $\{(), 1), (1, 2), (2, 3), \ldots\}$ получаем (д).

**Задача.** Не пользуясь коммутативностью умножения, доказать равенства $n \cdot c = c$, $\aleph_0 \cdot c = c$.

С помощью теоремы Кантора — Бернштейна может быть доказана

**Теорема 14 (теорема о сравнении мощностей)**[21]. Отношение «меньше» для мощностей есть порядок.

**Доказательство.** Достаточно установить, что наше отношение антирефлексивно и транзитивно (см. с. 426, замечание 1). Антирефлексивность очевидна, так как из $\mu < \mu$ по определению вытекало бы, что некоторое множество мощности $\mu$ не равномощно самому себе. Докажем транзитивность. Пусть $\mu_1 < \mu_2$ и $\mu_2 < \mu_3$. Тогда найдутся множества $A_1$, $A_2$, $A_3$, имеющие мощности $\mu_1$, $\mu_2$, $\mu_3$ соответственно и

[21] Иногда «теоремой о сравнении мощностей» называют саму теорему Кантора — Бернштейна.

такие, что: ($\alpha$) $A_1$ равномощно некоторому $A_2' \subset A_2$, $A_2 \neq A_2'$, а $A_2$ — некоторому $A_3' \subset A_3$, $A_3' \neq A_3$; ($\beta$) $A_1 \neq A_2$ и $A_2 \neq A_3$. Из ($\alpha$) следует, что $A_2$, а значит, и $A_1$, равномощно некоторому $A_3'' \subset A_3' \subset A_3$, $A_3'' \neq A_3$. В силу теоремы Кантора — Бернштейна $A_3'' \neq A_3$ — иначе было бы $A_3' \sim A_3$, откуда $A_2 \sim A_3$ вопреки ($\beta$). Но из $A_1 \sim A_3''$ и $A_3'' \neq A_3$ вытекает $A_1 \neq A_3$. Итак, $|A_1| < |A_3|$, т. е. $\mu_1 < \mu_3$.

Замечание. В действительности отношение «меньше» для мощностей является даже линейным порядком. Однако доказательство этого факта выходит за рамки нашей книги.

8. Займемся теперь сравнением конкретных мощностей.

Следующие две простые теоремы еще раз подчеркивают особую роль счетных множеств.

**Теорема 15.** $\aleph_0$ есть наименьшая из бесконечных мощностей.

Доказательство. Пусть $\mu$ — произвольная бесконечная мощность, отличная от $\aleph_0$, и $A$ — множество мощности $\mu$. По теореме 5 множество $A$ содержит счетное подмножество $B$. Но по определению отношения «меньше» из $A \neq B$ и $B \subset A$ следует $|B| < |A|$, т. е. $\aleph_0 < \mu$.

В частности, $\aleph_0 < c$.

**Теорема 16.** Любое натуральное число меньше $\aleph_0$.

Доказательство. Для любого натурального числа $n$ множество $\{k | k \in \mathbf{N} \& k < n\}$, имеющее мощность $n$, содержится в $\mathbf{N}$ и не равномощно ему (конечное и бесконечное множество не могут быть равномощны — см. теорему 1).

Из теорем 15 и 16 следует, что любая конечная мощность меньше любой бесконечной.

Существуют ли мощности, бо́льшие, чем $c$? В поисках таких мощностей кажется естественным обратиться к множеству точек плоскости — или, что то же самое, упорядоченных пар действительных чисел. По такому пути пошел сначала и сам Кантор, но результат был настолько неожиданным, что он первое время не мог поверить: оказалось, что множество точек плоскости равномощно множеству точек прямой. Сейчас мы это докажем:

**Теорема 17.** $|\mathbf{R}^2| = c$.

Доказательство. Поскольку $\mathbf{R}$ равномощно любому интервалу, а $\mathbf{R}^2$ — множеству внутренних точек любого квадрата (пример 2 после теоремы 13), достаточно показать, что $(0, 1) \sim ((0, 1))^2$. $|((0, 1))^2 = \{(x, y) | 0 < x < 1, 0 < y < 1\}$ есть множество внутренних точек квадрата, ограниченного прямыми $x = 0$, $x = 1$, $y = 0$, $y = 1$]. Для доказательства воспользуемся теоремой Кантора — Бернштейна. В квадрате $((0, 1))^2$ легко найти часть, равномощную интервалу $(0, 1)$:

можно взять, например, множество $\{(x, \frac{1}{2}) | 0 < x < 1\}$ (т. е. тот же интервал на прямой $y = \frac{1}{2}$). Остается найти в интервале часть, равномощную квадрату. Для этого рассмотрим произвольную точку $A = (x, y) \in ((0, 1))^2$, где $x = 0, \alpha_1\alpha_2\alpha_3 \ldots$, $y = 0, \beta_1\beta_2\beta_3 \ldots$, ($\alpha_i, \beta_i$ — десятичные цифры), и положим $f(A) = 0, \alpha_1\beta_1\alpha_2\beta_2\alpha_3\beta_3 \ldots$. Поскольку дроби $x$ и $y$ не оканчиваются девятками, дробь $f(A)$ также ими не оканчивается, т. е. является неотрицательным действительным числом. Очевидно, $f(A) < 1$. Кроме того, $f(A) \neq 0$ (иначе все десятичные знаки $f(A)$ были бы нулями, т. е. были бы нулями все знаки $x$ и $y$, что означало бы $x = y = 0$). Итак, $f(A) \in (0, 1)$. Мы получили отображение: $f$: $((0, 1))^2 \to (0, 1)$.

Это отображение инъективно: если $A_1 = (x_1, y_1)$, $A_2 = (x_2, y_2)$ и $f(A_1) = f(A_2) = 0, \gamma_1\gamma_2 \ldots$, то $0, \gamma_1\gamma_3\gamma_5 \ldots = x_1 = x_2$ и $0, \gamma_2\gamma_4\gamma_6 \cdots = y_1 = y_2$, так что $A_1 = A_2$. Поэтому, если $B$ — множество значений $f$, то $f$ отображает $((0, 1))^2$ на $B$ биективно; в то же время $B \subset (0, 1)$. Доказательство закончено.

**Следствия.** 1) Для любого $n = 1, 2, 3, \ldots$ $|\mathbb{R}^n| = c$. В частности, $\mathbb{R}^3$, т. е. множество точек трехмерного пространства, имеет мощность $c$.

Для доказательства достаточно вспомнить, что

$$A_1 \times \cdots \times A_n \times A_{n+1} \sim (A_1 \times \cdots \times A_n) \times A_{n+1}$$

(ср. часть (б) доказательства теоремы 10).

2) $c \cdot c = c$.

Это равенство выводится из теоремы 17 так же, как из теоремы 10 было выведено равенство $\aleph_0 \cdot \aleph_0 = \aleph_0$.

**Задача.** Доказать, что множество прямых на плоскости и множество прямых в (трехмерном) пространстве имеют мощность континуума.

Вернемся теперь к вопросу о существовании мощностей, бо́льших $c$. Следующая теорема дает на него положительный ответ — и, более того, позволяет утверждать, что для любой мощности можно найти бо́льшую.

**Теорема 18.** Для любого множества мощность множества его подмножеств больше его собственной мощности.

**Доказательство.** Пусть $A$ — произвольное множество и $B$ — множество подмножеств $A$. Нам нужно доказать, что: (а) $A$ равномощно некоторому $B' \subset B$; (б) $A \not\sim B$. Справедливость (а) устанавливается легко: если положить $g(a) = \{a\}$ для любого $a \in A$, то $g$ будет биективным отображением $A$ на множество одноэлементных подмножеств $A$. Утверждение (б) докажем от противного. Допустим, что

$A \sim B$. Тогда существует биективное отображение $f$: $A \xrightarrow{\text{на}} B$. Для каждого $a \in A$ его образ $f(a)$ есть некоторое множество $A_a \subset A$; при этом либо $a \in A_a$, либо $a \notin A_a$. В первом случае мы назовем элемент $a$ «хорошим», во втором — «плохим». Обозначим через $A^*$ множество всех «плохих» элементов $A$ и положим $a^* = f^{-1}(A^*)$. Элемент $a^*$, как всякий элемент $A$, должен быть либо «хорошим», либо «плохим». Но: если $a^*$ «хорош», это значит, что $a^* \in f(a^*) = A^*$, а так как $A^*$ по определению состоит из «плохих» элементов, то и $a^*$ «плох»; если $a^*$ «плох», это значит, что $a^* \notin f(a^*) = A^*$, а так как $A^*$ по определению содержит в с е «плохие» элементы, то $a^*$ «хорош». Итак, $a^*$ не может быть ни «хорошим», ни «плохим». Полученное противоречие завершает доказательство.

Замечание. Полезно обратить внимание на сходство проведенного рассуждения с доказательством теоремы 12. В основе обоих рассуждений лежит так называемый диагональный метод Кантора, широко используемый в теории множеств, а также в математической логике. (Ср. доказательство неразрешимости проблемы распознавания самоприменимости в § 7.6.)

Нетрудно доказать (см. ниже, с. 460) что если $A$ конечно, то мощность множества подмножеств $A$ равна $2^{|A|}$. Поэтому и в общем случае, если $|A| = \mu$, мощность множества подмножеств $A$ обозначают $2^{\mu}$. Полезна также

Теорема 19. $2^{\aleph_0} = c$. (Иначе: множество подмножеств натурального ряда равномощно $\mathbb{R}$).

Доказательство. Воспользуемся теоремой Кантора — Бернштейна, а также тем, что мощность множества $\mathbb{Z}_+$ равна $\aleph_0$, а мощность полуинтервала $[0, 1)$ равна $c$. Пусть $P$ — множество подмножеств $\mathbb{Z}_+$. Нам достаточно (а) найти в $[0, 1)$ часть, равномощную $P$, и (б) найти в $P$ часть, равномощную $[0, 1)$. Сделаем это так: (а) Пусть $Q$ — подмножество $[0, 1)$, состоящее из тех бесконечных десятичных дробей с целой частью 0, все десятичные знаки которых — нули и единицы. Тогда, сопоставляя каждому множеству $A \subset \mathbb{Z}_+$ дробь $0, \alpha_1\alpha_2\cdots\alpha_n\cdots$, где для каждого $n = 1, 2, \ldots$ $\alpha_n = 1$, если $n \in A$, и $\alpha_n = 0$, если $n \notin A$ (например, множеству $\{1, 3, 5, \ldots\}$ сопоставляется дробь $0,101010\ldots$, множеству $\{1, 2\}$ — дробь $0,11000\ldots = 0,11$, пустому множеству — $0,000\ldots = 0$, всему $\mathbb{Z}_+$ — $0,111\ldots$), получаем, очевидно, взаимно однозначное соответствие между $P$ и $Q$. (б) Сопоставим каждой бесконечной десятичной дроби $x = 0, \alpha_1\alpha_2\alpha_3\cdots \in [0, 1)$ множество $f(x) = \{1\alpha_1, 1\alpha_1\alpha_2, 1\alpha_1\alpha_2\alpha_3, \ldots\}$ (например, дроби $0,090909\ldots = \frac{1}{11}$ сопоставляется множество $\{10, 109, 1090,$

10909, ...}, дроби $0{,}25000... = \frac{1}{4}$ — множество {12, 125, 1250, 12500, 125000, ...}, дроби $0{,}141159... = \pi - 3$ — множество {11, 114, 1141, 11415, 114159, ...}, дроби $0{,}000... = 0$ — множество {10, 100, 1000, ...}). Если $x \neq y$, то $f(x) \neq f(y)$. Действительно, если $x = 0, \alpha_1\alpha_2 ...$, $y = 0, \beta_1\beta_2 \cdots$ и $x \neq y$, то хотя бы для одного $n$ должно быть $\alpha_n \neq \beta_n$; но тогда единственное $(n + 1)$-значное число, принадлежащее $f(x)$, не будет принадлежать $f(y)$. Поэтому $f$ отображает $[0, 1)$ на множество $f([0, 1)) \subset P$ биективно. Теорема доказана.

Естественно возникает вопрос: существуют ли мощности, промежуточные между $\aleph_0$ и $c$? Это так называемая *проблема континуума* — одна из самых знаменитых в истории математики задач[22]. Кантору не удалось ее решить, и в течение десятилетий это не удавалось никому. Впоследствии было установлено, что утверждение о несуществовании промежуточных мощностей невозможно ни доказать, ни опровергнуть, исходя из некоторой стандартной системы аксиом теории множеств[23] (о системах аксиом теории множеств см. во Введении).

На этом мы закончим наше краткое введение в теорию мощностей. Более подробное ее изложение в том же неформальном стиле, которого придерживались мы, можно найти, например, в книге [Александров 1977].

### Задачи и упражнения

1) Путем непосредственного установления взаимно однозначного соответствия доказать, что:

(а) множество окружностей, лежащих в одной плоскости и имеющих один и тот же центр, равномощно $\mathbf{R}_+$;

(б) множество прямоугольников, центры симметрии которых находятся в одной точке, а стороны параллельны двум заданным взаимно перпендикулярным прямым, равномощно $\mathbf{R}_+^2$;

(в) множество точек плоскости, из которого выброшена одна точка, равномощно множеству точек плоскости, лежащих вне некоторой окружности;

(г) каждое из множеств пункта (в) равномощно множеству точек, лежащих между двумя концентрическими окружностями;

(д) множество точек плоскости равномощно множеству точек сферы, из которой выброшена одна точка;

---

[22] Между прочим, она стояла на первом месте в списке важнейших математических проблем, составленном в 1900 г. Д. Гильбертом (см. с. 315).

[23] Недоказуемость этого утверждения была установлена в конце 30-х годов К. Гёделем, неопровержимость — в начале 60-х американским математиком П. Коэном (Paul G. Cohen, род. в 1934 г.). Изложение их результатов см. в книге [Манин 1979].

(е) множество подмножеств (произвольного) множества $M$ равномощно множеству отображений $M$ во множество $\{a, b\}$;

(ж) $(0, 1) \sim [0, 1]$.

2) Доказать, что если $A \setminus B \sim B \setminus A$, то $A \sim B$.

3) Доказать, что если $A \subset B$ и $A \sim A \cup (C \setminus B)$, то $B \sim B \cup C$.

4) Доказать, что следующие множества счетны:

(а) каждый класс вычетов по модулю $m$, где $m$ — произвольное целое положительное число;

(б) множество прямоугольных матриц с заданным числом строк и столбцов, элементы которых — целые, соответственно рациональные числа;

(в) множество всех прямоугольных матриц, элементы которых — целые, соответственно рациональные числа;

(г) множество интервалов с рациональными концами;

(д) множество окружностей с рациональными радиусами, центры которых имеют рациональные координаты;

(е) множество бесконечных десятичных дробей, оканчивающихся девятками.

5) Доказать, что всякое множество, элементами которого являются попарно непересекающиеся интервалы, лежащие на одной прямой, конечно или счетно.

6) Доказать, что множество точек разрыва монотонной функции конечно или счетно.

7) Положив в доказательстве теоремы 10 $A = B = \mathbf{N}$, обозначим первый и второй элементы пары $f(n)$ через $l(n)$ и $r(n)$ соответственно, а число $f^{-1}((a, b)) = C(a, b)$. (Функция $C$ осуществляет нумерацию пар натуральных чисел, число $C(a, b)$ есть номер пары $(a, b)$ в этой нумерации.) Найти явные выражения функций $C$, $l$ и $r$.

8) Доказать, что следующие множества имеют мощность континуума:

(а) множество точек параболы;

(б) множество точек окружности;

(в) множество точек сферы;

(г) множество треугольников на плоскости;

(д) множество комплексных чисел;

(е) множество квадратных трехчленов с действительными коэффициентами.

9) Дать непосредственное доказательство равномощности $\mathbf{R}^3$ и $\mathbf{R}$ (по аналогии с доказательством равномощности $\mathbf{R}^2$ и $\mathbf{R}$).

10) Доказать, что множество всевозможных последовательностей вида $a_0, a_1, a_2, \ldots$, где $a_i$ — действительные числа, имеет мощность континуума.

11) Доказать, что следующие множества имеют мощность континуума:

(а) множество многоугольников на плоскости;

(б) множество многогранников в трехмерном пространстве;

(в) множество многочленов с действительными, соответственно комплексными коэффициентами.

12) Доказать, что мощность декартова произведения двух множеств равна произведению мощностей сомножителей.

13) Если $a_0, a_1, a_2, \ldots$ и $b_0, b_1, b_2, \ldots$ — последовательности целых

положительных чисел и $\lim_{n\to\infty}\frac{b_n}{a_n}=0$, говорят, что последовательность $a_0, a_1, \ldots$ растет быстрее, чем $b_0, b_1, \ldots$ Доказать, что если множество $M$, состоящее из последовательностей целых положительных чисел, таково, что для каждой последовательности целых положительных чисел в нем найдется последовательность, растущая быстрее, то $M$ несчетно. [Указание: воспользоваться диагональным методом.]

14) Найти мощность множества возрастающих последовательностей натуральных чисел.

15) Найти мощность множества бесконечных десятичных дробей, не содержащих цифры 7, соответственно содержащих ее.

16) Можно ли построить несчетное множество, элементами которого являются окружности, расположенные в одной плоскости и такие, что каждая из них расположена вне всех остальных?

17) (а) Можно ли построить несчетное множество, элементами которого являются буквы П, расположенные в одной плоскости и попарно не пересекающиеся?

(б) тот же вопрос для букв Т.

18) Доказать, что множество всех функций действительной переменной имеет мощность $2^c$.

19) Доказать, что множество всех непрерывных функций действительной переменной имеет мощность $c$.

ПРИЛОЖЕНИЕ

**III**

# МЕТОД МАТЕМАТИЧЕСКОЙ ИНДУКЦИИ И ПЕАНОВСКАЯ АРИФМЕТИКА

1. В предыдущем приложении мы определили натуральные числа как мощности конечных множеств, а этим последним дали индуктивное определение, означающее, в сущности, что конечные множества — это все те множества, которые можно получить из пустого последовательным добавлением элементов по одному. Отсюда следует — поскольку мощность пустого множества есть нуль, а мощность множества, полученного из множества $A$ добавлением одного элемента (т. е. множества $A \cup Q$, где $Q$ — атомное множество и $A \cap Q = \varnothing$), равна $|A| + 1$,— что все натуральные числа можно получить из нуля последовательным прибавлением единицы. Поэтому, если мы хотим доказать, что все натуральные числа обладают некоторым свойством, то нам достаточно убедиться, во-первых, что этим свойством обладает число 0, и, во-вторых, что каково бы ни было натуральное число, если оно обладает этим свойством, то им обладает и число, на единицу большее. Это простое соображение играет исключительно важную роль не только в арифметике натуральных чисел, но и в математике в целом; оно называется *принципом математической индукции* и формулируется обычно следующим образом:

Если некоторое свойство натуральных чисел[1] справедливо для нуля и если для любого натурального числа $n$ из справедливости этого свойства для $n$ следует справедливость его для $n + 1$, то данное свойство справедливо для всех натуральных чисел.

На символическом языке математической логики принцип математической индукции записывается так:

$$B(0) \& \forall n(B(n) \supset B(n + 1)) \supset \forall k B(k),$$

где $B$ — произвольный одноместный предикат, определенный на N. Метод доказательства свойств натуральных чисел, основанный на

[1] То есть свойство, имеющее смысл для натуральных чисел.

принципе математической индукции, называется *методом математической индукции*[2]. Доказательство с помощью этого метода (его часто называют просто *доказательством по индукции*) состоит в том, что устанавливается справедливость нужного свойства для нуля — эта часть доказательства называется *базисом индукции*,— и доказывается, что для произвольного $n$ из предположения, что свойство справедливо для $n$, вытекает, что оно справедливо и для $n + 1$; эта часть доказательства называется *индукционным шагом*. Предположение, что свойство справедливо для $n$, называется *предположением индукции* (или *индуктивным предположением*).

**Пример.** Докажем методом математической индукции, что произвольное натуральное число $n$ обладает следующим свойством: каково бы ни было натуральное число $k > 0$, существуют такие натуральные числа $q$ и $r$, что $n = k \cdot q + r$ и $r < k$.

Базис. Если $n = 0$, то при любом $k$ можно положить $q = r = 0$. Индукционный шаг. Пусть для некоторого $n$ при любом $k > 0$ существуют такие $q$ и $r$, что $n = k \cdot q + r$ и $r < k$. Нам нужно доказать, что при любом $k > 0$ существуют такие $q_1$ и $r_1$, что $n + 1 = k \cdot q_1 + r_1$ и $r_1 < k$. Но если $r < k - 1$, то $r + 1 < k$ и $n + 1 = k \cdot q + (r + 1)$; если же $r = k - 1$, то $n + 1 = k \cdot q + k = k \cdot (q + 1) + 0$. Таким образом, в первом случае имеем $q_1 = q$, $r_1 = r + 1$, во втором $q_1 = q + 1$, $r_1 = 0$[3].

Методом математической индукции можно доказывать не только свойства натуральных чисел, но и свойства математических объектов любой природы, занумерованных натуральными числами. В самом деле, если $a_0, a_1, \ldots$ — последовательность, члены которой являются, например, действительными числами, и $C(x)$ — некоторое свойство действительных чисел, то, обозначив через $B(n)$ свойство натурального числа $n$, состоящее в том, что действительное число $a_n$ обладает свойством $C$, имеем:

$$\forall k B(k) \equiv \forall k C(a_k);\ B(0) \equiv C(a_0);\ \forall n (B(n) \supset B(n + 1)) \equiv$$

$$\equiv \forall n (C(a_n) \supset C(a_{n+1})).$$

Поэтому, чтобы доказать, что все члены последовательности $a_0, a_1, \ldots$

---

[2] Во Введении (сноска на с. 9) мы уже говорили, что математическая индукция представляет собой в действительности не индуктивный, а дедуктивный прием рассуждения. В самом деле, заключение о справедливости утверждения для общего случая делается здесь не из справедливости его для некоторых частных случаев, а из того, что оно справедливо для «начального случая» и что для любого случая из справедливости утверждения для него вытекает справедливость для следующего (разумеется, это имеет смысл лишь в предположении, что случаи соответствующим образом упорядочены).

[3] Нетрудно было бы также показать, что пара чисел $q$, $r$ определяется единственным образом.

обладают свойством $C$, достаточно установить, что им обладает $a_0$ (базис индукции) и что для любого $n$ из того, что $a_n$ обладает этим свойством, следует, что им обладает и $a_{n+1}$ (индукционный шаг). Чаще всего метод математической индукции именно так и используется.

**Примеры.** 1) Выведем формулу суммы геометрической прогрессии: $\sum_{k=0}^{n} aq^k = a\cdot\frac{q^{n+1}-1}{q-1}$, где $a$, $q$ — произвольные действительные или комплексные числа, но $q \neq 1$.

Базис $\sum_{k=0}^{0} aq^k = a = a\cdot\frac{q^1-1}{q-1}$. Индукционный шаг. Если для некоторого $n$ верно, что $\sum_{k=0}^{n} aq^k = a\cdot\frac{q^{n+1}-1}{q-1}$,

то $\sum_{k=0}^{n+1} aq^k = a\cdot\frac{q^{n+1}-1}{q-1} + aq^{n+1} = a\cdot\frac{q^{n+2}-1}{q-1}$.

2) Докажем, что число слов длины $n$ в алфавите, состоящем из $k$ букв (эти слова называют также *размещениями с повторениями* из $k$ элементов по $n$), равно $k^n$.

Базис. Слово длины 0 (пустое слово) единственно; но $1 = k^0$. Индукционный шаг. Из каждого слова длины $n$ можно получить, приписывая букву справа, $k$ различных слов длины $n+1$, и каждое слово длины $n+1$ можно получить таким способом только из одного слова длины $n$. Поэтому число слов длины $n+1$ в $k$ раз больше числа слов длины $n$, так что если слов длины $n$ имеется $k^n$, то слов длины $n+1$ будет $k^n\cdot k = k^{n+1}$.

3) Докажем, что число подмножеств конечного множества, состоящего из $n$ элементов, равно $2^n$.

Базис. Если $n = 0$, т. е. множество пусто, то у него только одно подмножество — оно само, и интересующее нас число равно $1 = 2^0$. Индукционный шаг. Пусть утверждение справедливо для некоторого $n$ и пусть $M$ — множество мощности $n+1$. Фиксировав некоторое $a_0 \in M$, разделим подмножества $M$ на два типа: (1) содержащие $a_0$ и (2) не содержащие $a_0$, т. е. являющиеся подмножествами множества $M\setminus\{a_0\}$. Подмножеств типа (2) по предположению индукции имеется $2^n$. Но подмножеств типа (1) ровно столько же, так как каждое подмножество типа (1) получается из некоторого и притом единственного подмножества типа (2) добавлением элемента $a_0$, и из каждого подмножества типа (2) получается этим способом одно и только одно

подмножество типа (1). Поэтому число всех подмножеств $M$ равно $2^n + 2^n = 2^{n+1}$.

Замечания. 1) Если мы хотим доказать, что все натуральные числа, бóльшие или равные некоторому $n_0$, обладают свойством $B$, для этого достаточно установить, что это свойство справедливо для $n_0$ и что для каждого $n \geq n_0$ из справедливости его для $n$ вытекает справедливость для $n + 1$. (В частности, при $n_0 = 1$ получается принцип математической индукции для множества целых положительных чисел.) В самом деле, если обозначить через $C(n)$ свойство натурального числа $n$, состоящее в том, что число $n + n_0$ обладает свойством $B$, имеем:

$$\forall k(k \geq n_0 \supset B(k)) \equiv \forall k C(k); \; B(n_0) \equiv C(0);$$

$$\forall n \,|\, n \geq n_0 \supset (B(n) \supset B(n+1))\,| \equiv \forall n(C(n) \supset C(n+1)).$$

В качестве примера можно привести доказательство того факта, что сумма углов плоского выпуклого $n$-угольника равна $\pi(n-2)$. Здесь $n \geq 3$; базисом индукции служит доказательство теоремы о сумме углов треугольника; индукционный шаг легко провести, разбив $(n+1)$-угольник диагональю на $n$-угольник и треугольник.

2) Чтобы доказать, что все натуральные числа, не превосходящие некоторого $n_0$, обладают свойством $B$, достаточно установить, что это свойство справедливо для нуля и что для каждого $n < n_0$ из справедливости его для $n$ вытекает справедливость для $n + 1$. В самом деле, полагая $C(n) \equiv B(n) \vee n > n_0$, имеем:

$$\forall k(k \leq n_0 \supset B(k)) \equiv \forall k C(k); \; B(0) \equiv C(0);$$

$$\forall n \,|\, n < n_0 \supset (B(n) \supset B(n+1))\,| \equiv \forall n(C(n) \supset C(n+1)).$$

Докажем, например, что для любых натуральных $n$ и $m$, таких, что $m \leq n$, число $m$-элементных подмножеств $n$-элементного множества (их часто называют *сочетаниями* из $n$ элементов по $m$), обозначаемое обычно $C_n^m$ или $\binom{n}{m}$, равно $\dfrac{n!}{m!(n-m)!}$. (В доказательстве $n$ и $m$ будут играть роль $n_0$ и $n$ соответственно.) При этом считается, что $0! = 1$. Базис очевиден, так как $C_n^0 = 1 = \dfrac{n!}{0!(n-0)!}$. Индукционный шаг. Пусть для некоторого $m < n$ равенство $C_n^m = \dfrac{n!}{m!(n-m)!}$ справедливо, и пусть $A$ — множество мощности $m$. Из каждого $m$-элементного подмножества $A$ можно получить, добавляя один из остальных $n - m$ элементов, $n - m$ различных $(m+1)$-элементных подмножеств; но каждое $(m+1)$-элементное подмножество

получается таким способом из $m+1$ различных $m$-элементных (например, подмножество $\{1, 2, 3\}$ множества $\{1, 2, 3, 4\}$ получается из подмножеств $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$). Поэтому

$$C_n^{m+1} = C_n^m \cdot \frac{n-m}{m+1} = \frac{n!}{m!(n-m)!} \cdot \frac{n-m}{m+1} = \frac{n!}{(m+1)![n-(m+1)]!}.$$

3) Утверждение, доказываемое по индукции, может содержать не одну, а несколько переменных, т. е. иметь вид $\forall x_1 \dots \forall x_s B(x_1, \dots, x_s)$, где $s > 1$. Тогда для проведения индукции его представляют, выбрав некоторую переменную $x_i$, в виде $\forall x_i(\forall x_1 \dots \forall x_{i-1} \forall x_{i+1} \dots \dots \forall x_s B(x_1, \dots, x_s))$ (см. выше пример на с. 459 и пример 2 на с. 460). В этом случае говорят, что утверждение доказывается индукцией по переменной $x_i$. Иногда при этом внутри базиса или индукционного шага проводится индукция по другой переменной.

Задачи. 1) Вывести формулу суммы арифметической прогрессии:

$$\sum_{k=0}^{n} (a + kd) = \frac{1}{2}(2a + nd) \cdot (n + 1).$$

2) Доказать, что число слов длины $n$ в $k$-буквенном алфавите, составленных из попарно различных букв (*размещений без повторений* из $n$ элементов по $k$), равно $k(k-1)\cdots(n-k+1)$.

3) Вывести формулу для числа сочетаний из $n$ элементов до $m$ индукцией по $n$.

4) Доказать, что $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

5) Доказать, что если $A$ и $B$ — непустые конечные множества, $|A| = a$, $|B| = b$, то число всевозможных отображений $A$ в $B$ равно $b^a$.

6) Вывести *биномиальную формулу Ньютона*: $(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$ ($a$, $b$ — произвольные действительные или комплексные числа, $n = 0, 1, \dots$).

2. В ряде случаев полезен следующий вариант принципа математической индукции — *принцип возвратной индукции*:

Если некоторое свойство натуральных чисел справедливо для нуля и если, каково бы ни было целое положительное $n$, из справедливости этого свойства для всех натуральных чисел, меньших $n$, следует справедливость его для $n$, то данное свойство справедливо для всех натуральных чисел.

На символическом языке:

$$B(0)\&\forall n(n > 0\&\forall m(m < n \supset B(m)) \supset B(n)) \supset \forall k B(k).$$

Этот принцип легко вывести из основной формы принципа математической индукции. Именно: пусть $B$ — свойство натуральных чисел, справедливое для нуля и такое, что для любого $n > 0$ из справедливости его для всех $m < n$ вытекает справедливость для $n$. Положим $C(n) \equiv \forall m(m \leq n \supset B(m))$. Очевидно, $C(0) \equiv B(0) \equiv И$. С другой стороны, $C(n) \equiv \forall m(m < n + 1 \supset B(m))$; поэтому, если для некоторого $n$ справедливо $C(n)$, то справедливо $B(n + 1)$; но $C(n)\&B(n + 1) \equiv C(n + 1)$. Итак, свойство $C$ справедливо для нуля, и из справедливости его для $n$ следует справедливость для $n + 1$. Поэтому свойство $C$ — и тем более $B$ — справедливо для всех натуральных чисел.

**Пример.** Докажем, что всякое натуральное число, большее единицы, может быть представлено, и притом единственным образом (с точностью до порядка сомножителей), в виде произведения простых чисел.

Обозначим через $B$ следующее свойство натуральных чисел: «число либо равно нулю или единице, либо представляется, и притом единственным образом, в виде произведения простых чисел» и докажем возвратной индукцией, что все натуральные числа обладают свойством $B$.

Базис очевиден: $B(0)$ истинно по определению свойства $B$. Индукционный шаг: пусть $n > 0$ и свойство $B$ справедливо для всех $m < n$. Тогда, если $n = 1$, то $B(n)$ истинно по определению $B$; если же $n > 1$, то в случае, когда $n$ — простое, истинность $B(n)$ очевидна; в противном случае, обозначая через $p$ произвольный простой делитель числа $n$ и полагая $q = \frac{n}{p}$, имеем $1 < q < n$; по предположению индукции отсюда следует, что $q$ представляется единственным образом в виде произведения простых чисел. Но из существования такого представления для $q$ немедленно вытекает существование его для $n = p \cdot q$, и если бы для $n$ существовали два разных представления, то, поскольку каждое из них содержало бы множитель $p$, сокращение на него дало бы два разных представления для $q$.

**Задачи.** 1) Будем рассматривать конечные последовательности, состоящие из левых и правых скобок, и дадим индуктивное определение *правильной последовательности скобок* следующим образом: (*i*) пустая последовательность правильна; (*ii*) если $\alpha$ — правильная последовательность, то последовательность $(\alpha)$ правильна; (*iii*) если $\alpha$, $\beta$ — правильные последовательности, то последовательность $\alpha\beta$ правильна; (*iv*) всякая правильная последовательность является та-

ковой в силу одного из пунктов (*i*) — (*iii*). Доказать возвратной индукцией по длине последовательности, что:

(а) в правильной последовательности скобок число левых скобок равно числу правых;

(б) если $\alpha$ — правильная последовательность скобок и $\beta$ — ее начало (т. е. существует такая последовательность $\gamma$, что $\alpha = \beta\gamma$), то число левых скобок в $\beta$ не меньше числа правых;

(в) для всякой непустой правильной последовательности скобок существует единственное взаимно однозначное соответствие между множествами входящих в нее левых и правых скобок, такое, что для любых двух соответствующих друг другу скобок заключенные между ними скобки образуют правильную последовательность.

2) Семейство $C$ непустых подмножеств непустого конечного линейно упорядоченного множества $A$ называется *бинарной системой составляющих* для $A$, если: (*i*) само $A$ и все одноэлементные подмножества $A$ принадлежат $C$; (*ii*) если $P, Q \in C$, то либо $P \cap Q = \varnothing$, либо $P \subset Q$, либо $Q \subset P$; (*iii*) если $M \in C$ и $M$ не одноэлементно, то существуют такие $P, Q \in C$, $P \neq Q$, что $M = P \cup Q$; (*iv*) если $M \in C$, $a, b \in M$, $c \in A$ и $a < c < b$, то $c \in M$. Доказать, что мощность бинарной системы составляющих для $A$ равна $2 \cdot |A| - 1$.

3) Доказать, что если $X$, $Y$ — слова в некотором алфавите, то слово $XY$ тогда и только тогда совпадает со словом $YX$, когда существуют такое слово $Z$ и такие натуральные $m$, $n$, что $X = Z^m$, $Y = Z^n$.

3. При аксиоматическом построении арифметики натуральных чисел принцип математической индукции, являющийся одним из важнейших их свойств, обычно включается в число аксиом. Наиболее употребительная система аксиом арифметики натуральных чисел, предложенная в конце XIX в. независимо немецким математиком Р. Дедекиндом (Richard Dedekind, 1831—1916) и итальянским математиком Дж. Пеано (см. § 6.6), известна под названием *системы Пеано*. Эта система лежит и в основе формальной арифметики, рассматриваемой в гл. 8. Ее неопределяемые объекты — *натуральное число* (в дальнейшем мы для краткости будем говорить просто «*число*») и нуль. Ее единственное неопределяемое отношение — «число $y$ *следует за* числом $x$» (обозначение: $y = x'$). Аксиом всего пять:

I. Нуль есть число.

II. Для всякого числа $x$ существует единственное число $y$, такое, что $y = x'$.

III. Если $x' = y'$, то $x = y$.

IV. Нуль не следует ни за каким числом.

V. (Аксиома индукции). Если $B$ — произвольное свойство чисел, справедливое для нуля и такое, что, каково бы ни было число $x$, из

справедливости свойства $B$ для $x$ следует справедливость его для $x'$, то свойство $B$ справедливо для всех чисел.

Систематическое построение арифметики натуральных чисел на основе системы Пеано можно найти в курсах теории числовых систем (см., например, [Ландау 1947], [Фефермаи 1971]). Здесь мы только введем сложение, умножение и отношение «меньше» и докажем некоторые из основных свойств этих понятий — с единственной целью облегчить чтение § 8.1.

**Утверждение 1.** Любое число или есть нуль, или следует за каким-либо числом.

**Доказательство.** Базис тривиален. Тривиален и индукционный шаг, поскольку, каково бы ни было число $x$, для числа $x'$ наше утверждение справедливо по самому определению этого числа, и поэтому из справедливости утверждения для $x$ следует справедливость его для $x'$ (так как импликация с истинным заключением истинна).

**Утверждение 2.** Существует единственная функция двух переменных, сопоставляющая каждым двум числам $x$, $y$ число $x + y$ таким образом, что выполняются условия:

$S1$. $x + 0 = x$;

$S2$. $x + y' = (x + y)'$.

**Доказательство.** Пусть $x$ — произвольное фиксированное число. Докажем, что для любого числа $z$ существует такое число $x + z$, что при $z = 0$ оно равно $x$, а если $z = y'$ для некоторого $y$, то $x + z = (x + y)'$. Базис. Достаточно положить по определению $x + 0 = x$. Индукционный шаг. Если наше утверждение справедливо для некоторого числа $z$, то, во всяком случае, число $x + z$ определено. Полагая по определению $x + z' = (x + z)'$, видим, что утверждение справедливо для $z'$. Остается доказать, что если $f(x, y)$ — функция, определенная на множестве чисел и удовлетворяющая условиям $(i)$ $f(x, 0) = x$ и $(ii)$ $f(x, y') = (f(x, y))'$, то $f(x, y) = x + y$ для любых $x$, $y$. Докажем это индукцией по $y$. Базис. $f(x, 0) = x + 0$ ввиду $S1$ и $(i)$. Индукционный шаг. Если для некоторого $y$ справедливо $f(x,y) = x + y$, то ввиду $S2$ и $(ii)$ имеем $f(x, y') = (f(x, y))' = (x + y)' = x + y'$. (Здесь мы воспользовались не только предположением индукции, но и аксиомой II, в силу которой из $f(x, y) = x + y$ следует $(f(x, y))' = (x + y)'$.)

**Утверждение 3.** $(x + y) + z = x + (y + z)$.

**Доказательство** проведем индукцией по $z$. Базис. Ввиду $S1$ $(x + y) + 0 = x + y = x + (y + 0)$. Индукционный шаг. Пусть для некоторого $z$ справедливо $(x + y) + z = x + (y + z)$. Тогда, используя $S2$, получаем: $(x + y) + z' = ((x + y) + z)' = (x + (y + z))' = x + (y + z)' = x + (y + z')$.

**Утверждение 4.** $0 + x = x$.

**Доказательство.** $0 + 0 = 0$ по $S1$; если $0 + x = x$, то по $S2$ $0 + x' = (0 + x)' = x'$.

Будем обозначать число $0'$ через $1$. Очевидно, $x + 1 = x + 0' = (x + 0)' = x'$. Нетрудно доказать также (индукцией; это предоставляется читателю), что $1 + x = x'$.

**Утверждение 5.** $x + y = y + x$.

**Доказательство** проведем индукцией по $y$. Базис. $x + 0 = x = 0 + x$ ввиду $S1$ и утверждения 4. Индукционный шаг. Если $x + y = y + x$, то, используя утверждение 3 и равенства $x + 1 = x'$, $1 + x = x'$, получаем: $x + y' = x + (1 + y) = (x + 1) + y = (1 + x) + y = 1 + (x + y) = 1 + (y + x) = (1 + y) + x = y' + x$.

**Утверждение 6.** Существует единственная функция двух переменных, сопоставляющая каждым двум числам $x$, $y$ число $x \cdot y$ таким образом, что выполняются условия:

$P1$. $x \cdot 0 = 0$;

$P2$. $x \cdot y' = x \cdot y + x$.

Доказательство (аналогичное доказательству утверждения 2) предоставляется читателю.

**Утверждение 7.** $(x + y) \cdot z = x \cdot z + y \cdot z$.

**Доказательство.** Базис. $(x + y) \cdot 0 = 0 = 0 + 0 = x \cdot 0 + y \cdot 0$ ввиду $P1$ и $S1$. Индукционный шаг. Пусть для некоторого $z$ справедливо $(x + y) \cdot z = x \cdot z + y \cdot z$. Тогда по $P1$ $(x + y) \cdot z' = (x + y) \cdot z + (x + y)$, но по предположению индукции $(x + y) \cdot z = x \cdot z + y \cdot z$, а ввиду утверждений 3 и 5 имеем $(x \cdot z + y \cdot z) + (x + y) = (x \cdot z + x) + (y \cdot z + y)$; последнее выражение по $P2$ равно $x \cdot z' + y \cdot z'$.

**Утверждение 8.** $0 \cdot x = 0$.

Доказательство предоставляется читателю.

Нетрудно доказать также, что $x \cdot 1 = 1 \cdot x = x$.

**Утверждение 9.** $x \cdot y = y \cdot x$.

Читатель докажет это утверждение сам (индукцией, используя $P1$, $P2$, утверждения 7 и 8 и равенства $1 \cdot x = x$, $x + 1 = x'$).

Из утверждений 7 и 9 следует

**Утверждение 10.** $x \cdot (y + z) = x \cdot y + x \cdot z$.

**Утверждение 11.** $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Доказательство предоставляется читателю.

**Определение.** Будем говорить, что число $x$ меньше числа $y$, и писать $x < y$, если существует такое число $z$, что $y = x + z'$.

**Утверждение 12.** Невозможно $x < x$.

**Доказательство.** Более подробно утверждение можно сформулировать так: ни для каких чисел $x$, $z$ невозможно равенство $x = x + z'$. Докажем его индукцией по $x$. Базис. Из равенства $0 = 0 + z'$ ввиду утверждения 4 следовало бы $0 = z'$, что противоречит аксиоме IV. Индукционный шаг. Пусть для некоторого $x$ равен-

ство $x = x + z'$ невозможно ни при каком $z$. Допустим, что для какого-то $z$ имеет место $x' = x' + z'$. Тогда ввиду утверждения 5 и S2 получим $x' = z' + x' = (z' + x)'$, откуда по аксиоме III $x = x + z'$, вопреки предположению индукции.

**Утверждение 13.** Если $x < y$ и $y < z$, то $x < z$.

**Доказательство.** Пусть $x < y$ и $y < z$, т. е. существуют такие числа $u$, $v$, что $y = x + u'$, $z = y + v'$. Тогда $z = (x + u') + v' = x + (u' + v') = x + (u' + v)'$. Отсюда по определению $x < z$.

Задачи. 1) Положив $0'' = 2$, доказать, что $x + x = x \cdot 2$.

2) Доказать, что если $x + y = 0$, то $x = y = 0$.

3) Доказать, что если $x \cdot y = 0$, то $x = 0$ или $y = 0$.

4) Доказать, что нуль есть наименьшее число (т. е. невозможно $x < 0$).

5) Доказать, что для любых $x$, $y$, $z$: (а) тогда и только тогда $x < y$, когда $x + z < y + z$; (б) если $z \neq 0$, то тогда и только тогда $x < y$, когда $x \cdot z < y \cdot z$.

6) Доказать, что ни для каких $x$, $y$ невозможно $x < y < x'$.

7) Для каждой из аксиом II—V доказать ее независимость от остальных, подобрав интерпретацию, в которой она не выполняется, а остальные выполняются.

8) Упорядоченное множество называется *вполне упорядоченным*, если в каждом его непустом подмножестве есть наименьший элемент. Доказать, что: (а) множество натуральных чисел вполне упорядочено отношением $<$; (б) из аксиом I — IV и условия, что множество натуральных чисел вполне упорядочено отношением $<$, следует аксиома V.

9) Сформулировать и доказать утверждение, аналогичное утверждениям 2 и 6, для операции возведения в степень.

# ЛИТЕРАТУРА

В настоящий список включены только работы, упоминаемые в тексте книги. Если работа, вышедшая на иностранном языке, издана также в русском переводе, указывается только этот последний.


*Александров П.С.* Введение в теорию множеств и общую топологию. М.: Наука, 1977.

Античные теории языка и стиля / Под общей ред. О.М. Фрейденберг. М.; Л.: ОГИЗ-Соцэкгиз. 1936; 2-е изд. СПб.: Алетейя, 1996.

*Апресян Ю.Д., Богуславский И.М., Иомдин Л.Л.* и др. Лингвистическое обеспечение системы ЭТАП-2. М.: Наука, 1989.

*Аристотель.* Сочинения: В 4 т. Т. 2. М.: Мысль, 1978.

*Березкина Э.И.* Математика древнего Китая. М.: Наука, 1980.

*Бухштаб А.А.* Теория чисел. М.: Учпедгиз. 1960; 2-е изд. М.: Просвещение, 1966.

*Гейтинг А.* Интуиционизм. М.: Мир, 1965.

*Генцен Г.* Исследования логических выводов // Математическая теория логического вывода. М.: Наука, 1967. С. 9—74.

*Генцен Г.* Непротиворечивость чистой теории чисел // Там же (а). С. 77—153.

*Генцен Г.* Новое изложение доказательства непротиворечивости для чистой теории чисел // Там же (б). С. 154—190.

*Гильберт Д., Аккерман В.* Основы теоретической логики. М.: Изд-во иностр. лит., 1947.

*Гильберт Д., Бернайс П.* Основания математики: Логические исчисления и формализация арифметики. М.: Наука, 1979.

*Гильберт Д., Бернайс П.* Основания математики: Теория доказательств. М.: Наука, 1982.

*Гиндикин С.Г.* Алгебра логики в задачах. М.: Наука, 1972.

*Гладкий А.В.* Формальные грамматики и языки. М.: Наука, 1973.

*Гладкий А.В.* О значении союза *или* // Семиотика и информатика / ВИНИТИ. М., 1979. Вып. 13. С. 196—214.

*Гладкий А.В.* О значении союза *если* // Семиотика и информатика / ВИНИТИ. М., 1982. Вып. 18. С. 43—75.

*Гладкий А.В., Бойдакова В.Н.* Об одной системе аксиом исчисления предложений // Математическая лингвистика и теория алгоритмов. Калинин, 1978. С. 35—40.

*Гладкий А.В., Дрейзин Ф.А.* К семантике русского отрицания // Wiener Slawistischer Almanach. Bd. 11. Wien, 1983. S. 123—152.

*Гудстейн Р.Л.* Математическая логика. М.: Изд-во иностр. лит., 1961.

*Ершов Ю. Л., Палютин Е. А.* Математическая логика. М.: Наука, 1979.

*Карри Х.Б.* Основания математической логики. М.: Мир, 1969.

*Клини С.К.* Введение в метаматематику. М.: Изд-во иностр. лит., 1957.

*Клини С.К.* Математическая логика. М.: Мир, 1973.

*Клини С.К.* Об истоках теории рекурсивных функций // Алгоритмы в современной математике и ее приложениях: В 2 ч. Ч. 2. Новосибирск, 1982.

*Клини С., Весли Р.* Основания интуиционистской математики. М.: Наука, 1978.

*Колмогоров А.Н., Драгалин А.Г.* Введение в математическую логику. М.: Изд-во МГУ, 1982.
*Колмогоров А.Н., Драгалин А.Г.* Математическая логика. Дополнительные главы. М.: Изд-во МГУ, 1984.
*Крейнович Е.А.* Нишгу. М.: Наука, 1973.
*Кузичева З.А.* Математическая логика // Математика XIX в. Математическая логика. Алгебра. Теория чисел. Теория вероятностей. М.: Наука, 1978. С. 11—38.
*Куратовский К., Мостовский А.* Теория множеств М.: Мир, 1970.
*Кушнер Б.А.* Лекции по конструктивному математическому анализу. М.: Наука, 1973.
*Лавров И.А., Максимова Л.Л.* Задачи по теории множеств и математической логике. М.: Наука, 1975.
*Ландау Э.* Основы анализа. М.: Изд-во иностр. лит., 1947.
*Лукасевич Я.* Аристотелевская силлогистика с точки зрения современной формальной логики. М.: Изд-во иностр. лит., 1959.
*Мальцев А.И.* Алгоритмы и рекурсивные функции. М.: Наука, 1965; 2-е изд. М.: Наука, 1986.
*Манин Ю.И.* Доказуемое и недоказуемое. М.: Сов. радио, 1979.
*Манин Ю.И.* Вычислимое и невычислимое. М.: Сов. радио, 1980.
*Марков А.А.* Теория алгорифмов // Тр. / Матем. ин-т АН СССР им. В.А. Стеклова. Т. 42„М., Л.: Изд-во АН СССР, 1954.
*Марков А.А.* О конструктивной математике // Тр. / Матем. ин-т АН СССР им. В.А. Стеклова. Т. 67. М.; Л.: Изд-во АН СССР, 1962. С. 8—14.
*Марков А..*1. Элементы математической логики. М.: Изд-во МГУ, 1984.
*Марков А.А., Нагорный Н.М.* Теория алгорифмов. м.: Наука, 1984.
*Мартин-Лёф П.* Очерки по конструктивной математике. М.: Мир, 1975.
*Маслов С.Ю.* Обратный метод установления выводимости для логических исчислений // Тр. / Матем. ин-т АН СССР им. В.А. Стеклова. Т. 98. М.: Изд-во АН СССР, 1968. С. 26—87.
*Маслов С.Ю.* Теория дедуктивных систем и ее применения. М.: Радио и связь, 1986.
*Мельчук И.А.* Опыт теории лингвистических моделей «Смысл ⇔ Текст». Семантика, синтаксис. М.: Наука, 1974.
*Мендельсон Э.* Введение в математическую логику. М. Наука, 1971. 2-е изд. М.: Наука, 1976.
*Монтегю Р.* Универсальная грамматика // Семиотика и информатика. м., 1985. Вып. 26. С. 105—136.
*Новиков П.С.* Элементы математической логики. М.: Физматгиз, 1959; 2-е изд. М.: Наука, 1973.
*Новиков П.С.* Об алгоритмической неразрешимости проблемы тождества слов в теории групп // Тр. / Матем. ин-т АН СССР им. В.А. Стеклова. Т. 44., М.: Изд-во АН СССР, 1955.
*Новиков П.С.* Конструктивная математическая логика с точки зрения классической. М.: Наука, 1977.
*Падучева Е.В.* О семантике синтаксиса. М.: Наука, 1974.
*Робинсон А.* Введение в теорию моделей и метаматематику алгебры. М.: Наука, 1967.
*Роджерс Х.* Теория рекурсивных функций и эффективная вычислимость. М.: Мир, 1972.
Справочная книга по математической логике. В 4 ч. / Под ред. Дж. Барвайса. Ч. I: Теория моделей. М.: Наука, 1982, Ч. II: Теория множеств. М.: Наука, 1982; Ч. III: Теория рекурсии. М.: Наука, 1982; Ч. IV: Теории доказательств и конструктивная математика. М.: Наука, 1983.
*Свяжкин Н.И.* Формирование математической логики. М.: Наука, 1967.
*Фейс Р.* Модальная логика. М.: Наука, 1974.
*Фефермен С.* Числовые системы: Основания алгебры и анализа. М.: Наука, 1971.

*Фреге Г.* Смысл и денотат // Семиотика и информатика / ВИНИТИ. М., Вып. 8. 1977. С. 181—210.

*Фреге Г.* Понятие и вещь // Семиотика и информатика / ВИНИТИ. М., 1978. Вып. 10. С. 188—205.

*Фреге Г.* Функция и понятие // Семиотика и информатика / ВИНИТИ. М., 1980. Вып. 14. С. 159—183.

*Френкель А.А., Бар-Хиллел И.* Основания теории множеств. М.: Мир, 1966.

*Циткин А.И.* Введение в грамматики Р. Монтегю // Семиотика и информатика / ВИНИТИ. М., 1985. Вып. 26. С. 137—153.

*Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем. М.: Наука, 1983.

*Чёрч А.* Введение в математическую логику. Т. I. М.: Изд-во иностр. лит., 1960.

*Шенфилд Дж.* Математическая логика. М.: Наука, 1975.

*Ashworth E. J.* Language and Logic in the Postmedieval Period. Dordrecht, 1974.

*Berka K., Kreiser L.* Logik-Texte. Kommentierte Auswahl zur modernen Logik. Berlin, 1971.

*Bole L., Borowik P.* Many-Valued Logics. Vol. I. Theoretical Foundations. Berlin; Heidelberg; N. Y., 1992.

*Bocheński I. M.* A History of Formal Logic. N. Y., 1970.

*Chellas B. F.* Modal Logic. An Introduction. Cambridge, 1993.

*Gödel K.* Die Vollständigkeit des logichen Aussagenkalküls // Monatshefte für Mathemauk und Physik. Bd. 37. 1930. S. 349—360. (Перепечатано в [Berka — Kreiser 1971], S. 283—294).

*Gödel K.* Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme // Monatshefte für Mathematik und Physik. Bd. 38. 1931. S. 173—198. (Частично перепечатано с комментариями в [Berka—Kreiser 1971], S. 321—325).

*Gödel K.* Eine Interpretation des intuitionistischen Aussagenkalküls // Ergebn. math. Koll. Bd. 4. 1933. S. 39—40. (Перепечатано в [Berka — Kreiser 1971], S. 187—188).

*Dreben B., Goldfarb W.* The Decision Problem. Reading, 1979.

*Hasenjäger G.* Eine Bemerkung zum Henkins Beweis für Vollständigkeit des Prädikatenkalküls det ersten Stufe // J. Symbolic Logic. Vol. 18. 1953, p. 42—48.

*Henkin L.* The Completeness of the First Order Functional Calculus // J. Symbolic Logic. Vol. 14. 1949, p. 159—166.

*McArthur R.P.* Temps Logic. Dordrecht, 1993.

*Pinborg J.* Die Entwicklung der Sprachtheorie im Mittelalter. Münster, 1967.

*Post E.L.* Formal Reduction of the General Combinatorial Decision Problem // Amer. J. Math. Vol. 65. 1943, p. 197—215.

*Prantl G.* Geschichte der Logik im Abendlande. Bd. I. Leipzig, 1855. (Фотомеханическая перепечатка: Graz, 1955.)

*Rice H.G.* Classes of Recursively Enumerable Sets and Their Decision Problems. // Trans. Amer. Math. Soc. Vol. 74. 1953, p. 358—366.

*Robinson R.M.* An Essentialy Undecidable Axiom System // Proc. Int. Cong. Math. Vol. 1. Cambridge, 1950, p. 729—730.

*Scholz H.* Geschichte der Logik. Berlin, 1931.

*Smullyan R.* First-Order Logic. Berlin; Heidelberg; N.-Y., 1968.

*Steinthal H.* Geschishte der Sprashwissenschaft bei der Griechen und Römern.Mit besonderer Rücksicht auf die Logik. Berlin, 1863; 2-te Aufl., Berlin, 1890 (Bd. I), 1891 (Bd. II). (Фотомеханич. перепечатка 2-го изд.: Hildesheim, 1961.)

# ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ


Аксиома 157
— собственная 239
Алгоритм 179
Алгоритмическая проблема 306
Алфавит 155
— внешний 283
— внутренний 283
— входной 286
— выходной 286
Антецедент 194
Аргумент 37
Ассоциативность дизъюнкции 97
— конъюнкции 97
— объединения 28
— пересечения 29

Базис индукции 362, 459
Биекция 42
Булева алгебра 270
Булев вектор 108

Введение дизъюнкции (ВД) 160
— импликации (ВИ) 160
— конъюнкции (ВК) 160
— общности (В∀) 210
— отрицания (ВО) 161
— существования (В∃) 210
Взаимно однозначное соответствие 42
Вместимость 45
Вхождение переменной в формулу свободное 77
— — — — связанное 77
— символа в слово 155
— слова в слово 382
Вывод 157, 164, 184
Выводимость 157
Высота дерева вывода 168, 196
Вычисление (правильное) 286
Вычитание множеств 27

Глубина вхождения подформулы в формулу 107, 145
График 34, 40, 44, 46

Декартова степень 32
Декартов квадрат 32
Декартово произведение 32
Дерево вывода 165, 168, 196, 253
— — элементарное 168
Дизъюнкция 65
— разделительная 124
— элементарная 104
— — полная 112
Дистрибутивность дизъюнкции по отношению к конъюнкции 97
— конъюнкции по отношению к дизъюнкции 97
— объединения по отношению к пересечению 29
— пересечения по отношению к объединению 29
Длина вывода 185
— слова 156
Д. н. ф — см. нормальная форма дизъюнктивная
Доказательство 157
— от противного 173
— разбором случаев 93, 124, 161
Дополнение 30

Зависимость формул в выводе 249
Задано (отношение на множестве) 34
Закон исключенного третьего 105, 161
— контрапозиции 99, 175
— — обратный 175
— — — ослабленный 203
— противоречия 105
— рефлексивности равенства 238
— симметричности равенства 238
— транзитивности импликации (ТИ) 176, 188
— — равенства 238
Законы Де Моргана 98
Замыкание формулы 391
Значение переменной 36

Идемпотентность дизъюнкции 97
— конъюнкции 98
Импликация 67
Индукционный шаг 362, 459
Интерпретация 129, 149
Инъекция 41
Истинностная таблица 64, 73
Истинностное значение 51

Исчисление 352
— ассоциативное 241
— — групповое 241
— естественного вывода 158
— логико-математическое 157
— логическое 155
— — генценовского типа 158
— — гильбертовского типа 157
— — дедуктивно полное 222
— — прикладное 157
— — разрешимое 406
— — (семантически) полное 178
— — семантически пригодное 178
— — чистое 157, 411
— на основе $G_1$ 222
— — — — с равенством 231
— одноместных предикатов 414
— предикатов узкое (исчисление предикатов 1-й ступени) 230
— — — с равенством 238
— предложений 158
— секвенциальное 193, 253
Итерация 328

Категорическое суждение 255
Квантор общности 60
— существования 60
Кванторный префикс (кванторная приставка) 147
Классы эквивалентности 423
К. н. ф.— *см.* нормальная форма конъюнктивная
Код машины Тьюринга 303
— переменной 380
— символа 302, 380
— слова 302, 380
Коммутативность дизъюнкции 97
— конъюнкции 97
— объединения 28
— пересечения 29
Композиция отображений 42
Конечный автомат 303
Конъюнкция 64
— элементарная 103
— — полная 108
К. н. ф. — см. нормальная форма конъюнктивная
Координата булева вектора 108
Корень дерева вывода 168, 196
Кортеж 31

Лексикографический порядок 74, 427
Лемма Линденбаума 222
— о противоположной формуле 112
Лист 165, 196
— зеленый 168
— увядший 168
Логика интуиционистская 163
— классическая 162
— конструктивная 163
Логические парадоксы 12

Матрица (формулы в п. н. ф.) 147
Машина Тьюринга 282
— — несамоприменимая 306
— — самоприменимая 306
— — универсальная 303
Метод математической индукции 459
Множество 21
— бесконечное 439
— значений 35
— конечное 439
— линейно упорядоченное 425
— основное 130, 149
— перечислимое 318
— пустое 25, 438
— разрешимое (рекурсивное) 317
— рекурсивно перечислимое — *см.* множество перечислимое
— универсальное 30
— упорядоченное 425
— функционально замкнутое 126
— — полное 122
Модель арифметики стандартная 371
— логического исчисления 223
— — — нормальная 232
— множества формул 132, 149
Мощность множества 435

Натуральное число 441, 464
Находятся в (отношении) 33
Начинается с квантора 77
— с отрицания 78
Непосредственная составляющая 101, 145
Непротиворечивость 184
Неразрешимое предложение 394
Номер вычисления 344
— дерева вывода 385
— машины Тьюринга 323
— п. р. ф. 337
— слова (стандартный) 316, 380
Нормализация модели 235
Нормальная форма дизъюнктивная (д. н. ф.) 103
— — — совершенная (с. д. н. ф.) 110
— — конъюнктивная (к. н. ф.) 104
— — — совершенная (с. к. н. ф.) 113
— — префиксная (п. н. ф.) 147

Область вторых элементов 34, 44
— действия квантора 76
— изменения переменной 36
— определения 35
— отправления 34
— первых элементов 34, 44
— прибытия 34
— третьих элементов 44
Образ 37
— множества 40
Общая часть множеств 25
Объединение множеств 25, 26
Ограничение (в кванторе) 83
Оператор минимизации 340
— ограниченной минимизации 335
— подстановки 330
— рекурсии 330
Операция бинарная 70
— унарная 70
Определение 79
— индуктивное 159
О. р. ф. — см. функция обращерекурсивная
Основа булевой функции 95
Основные равносильности логики предикатов 140
— — — предложений 97
Отделимость 324
Отношение 33
— антирефлексивное 424
— антисимметричное 424
— бинарное (двуместное) 44
— выводимости 156
— линейного порядка 425
— обратное 35
— ограниченное множеством 428
— порядка 425
— рефлексивное 421
— симметричное 421
— тернарное (трехместное) 44
— транзитивное 421
— эквивалентности 422
Отображает 39
Отображение 39
— биективное 41
— в 39
— взаимно однозначное 41
— инъективное 41
— на 39
— одно-однозначное 41
— сюръективное 39
— тождественное 42
Отождествление переменных 87
Отрицание 69
Парадокс Берри 14
— Кантора 13
— лжеца 13
— Рассела 14
— Ришара 14
Переменная 36
— зависимая 37, 45
— независимая 37, 45
— несущественная 94
— свободная 77
— связанная 77
— существенная 94
Переработка набора слов машиной 286
Пересечение множеств 25, 27
Перестановка (фигура заключения) 195
Перечисление элементов множества 23
Подмножество 22
— истинное (собственное) 23
Подразумеваемая часть суждения — см. презумпции
Подстановка 42
— терма в формулу 208
Подформула 100, 145
Полугруппа 241
— конечно определенная 242
— свободная 241
Правила введения и удаления логических символов 160
— вывода 156
— — логические 157
— — структурные 157
— образования формул 156, 209
— — термов 209
— преобразования формул 156
— производные 187
— чтения формул 71, 77
Правило безусловное 159, 163
— Дунса Скота (ДС) 107, 161
— modus ponens (MP) 185, 186, 249
— обобщения (Об) 248
— постановки двойного отрицания 172
— снятия двойного отрицания 98, 172
— транзитивности (Т) 160
— тривиальной выводимости (ТВ) 160
— условное 159, 163
— устранения теоремы (УТ) 188
П. н. ф. — см. нормальная форма пренексная
Предикат 56, 57
— вычислимый (рекурсивный) 287
— двуместный 57
— многоместный 57
— *n*-местный 57
— одноместный 56

— представимый в формальной арифметике 373
— примитивно рекурсивный 332
— рекурсивный — *см.* предикат вычислимый
— тождественно истинный 58
— — ложный 58
— трехместный 57
— характеристический 98
Предположение индукции 459
Представление предиката формулой 373
— функции формулой 373
Презумпция 257, 259
Приведение к д. н. ф. 103
— к к. н. ф. 104
— к нелепости 161
— к п. н. ф. 141
Применимость (машины Тьюринга) 286
Принадлежит 21
Принцип возвратной индукции 462
— двойственности 112
— математической индукции 458
Пробегает 36
Проблема Гильберта десятая 315
— распознавания применимости 307
— — самоприменимости 306
— — переработки слов 310
— тождества 311, 314
— эквивалентности 311
Проекция множества 62
Прообраз 37
— множества 41
— полный 37
Промежуточная гипотеза 166
Пропозициональные связки 69
Простое расширение исчисления 220
П. р. ф. — *см.* функция примитивно рекурсивная
Пункт индуктивного определения косвенный 159
— — — прямой 159

Равенство множеств 23
Равномощность 434
Равносильность предикатов 59, 135
— предложений 135
— формул 96, 136, 149
Разбавление 194
Разбиение множества 422
Разность множеств 25
Рекурсия 328

Свойство машин Тьюринга инвариантное 308
— — — нетривиальное 308
— подформульности 197, 254
— функций нетривиальное 309
— характеристическое 24
— элементарное 239
Связаны (отношением) 33
Связывание квантором 62
С. д. н. ф. — *см.* нормальная форма дизъюнктивная совершенная
С. к. н. ф. — *см.* нормальная форма конъюнктивная совершенная
Секвенция 193
— верхняя 194
— нижняя 194
Семантика 91
Сечение 195
Силлогизм 261
Символ константы 148, 207
— логический 158, 207
— предикатный 128, 207
— — двуместный 129
— — *k*-местный 207
— — нульместный 129
— — одноместный 129
— синтаксический 158, 207
— функциональный 148, 207
— элементарный 155
Синтаксис 154
Ситуация машины Тьюринга 285
— — — заключительная 285
— — — начальная 285
Следование семантическое 113, 139
Слово 155
Сложность формулы 159, 208
Соглашение о порядке действий 71, 76
Содержит 22
Сокращение 195
Сукцедент 194
Схема аксиом 163
— — простейшая 237
— секвенций 194
— теорем 163
— фигур заключения 194
— формул 163
Сюръекция 39

Тавтология 105
Тезис Чёрча-Тьюринга 297
Теорема (в логическом исчислении) 156
Теорема Гёделя вторая 401
— — о неполноте 394, 396
— — о полноте 228
— Генцена о дизъюнкции 206
— — основная 197, 254
— Кантора-Бернштейна 449

— китайская об остатках 376
— Лёвенгейма–Скулема 229
— о дедукции 187 250
— о замене дедуктивно эквивалентных формул 177, 216
— — — равносильных формул 101, 145
— о непротиворечивости исчисления $G_0$ 184
— о полноте исчисления $G_0$ 180
— о представлении булевой функции формулой 108
— о приведении к д. н. ф. 103
— — — к к. н. ф. 104
— о семантической пригодности исчисления $G_0$ 178
— — — — — — $G_1$ 217
— Поста 322
— Райса 308
— Тарского 404
— Чёрча 413
Терм 148, 208
— свободный для подстановки 208
Тождественные преобразования 100, 145
Тривиальное ограничение исчисления 220

Удаление дизъюнкции (УД) 160
— импликации (УИ) 160
— конъюнкции (УК) 160
— общности (У∀) 210
— отрицания (УО) 161
— существования (У∃) 210
Упорядоченная пара 31
Упорядоченная система 31
Утверждаемая часть суждения 259

Фактор-множество 423
Фигура заключения 194
— — логическая 195
— — структурная 194
Формальная арифметика 360
— индукция 362
— система (формальная теория) 155
Формула атомная 208
— доказуемая 156
— логики предикатов 76
— — — выполнимая 133, 149
— — — — в интерпретации 132, 149
— — — всюду истинная 133, 149
— — — замкнутая 77
— — — истинная в интерпретации 131, 149
— — предложений 70
— — — тождественно истинная 105
— — — — ложная 105
Функциональный элемент 120

Функция 37, 45
— булева 93
— — двойственная 125
— — линейная 126
— — монотонная 126
— — приведенная 94
— — самодвойственная 125
— — сохраняющая $И$ 126
— — — $Л$ 126
— — тождественно истинная 95
— — — ложная 95
— вычислимая (по Тьюрингу) 287
— обратная 40
— общерекурсивная (о. р. ф.) 341
— предметная 148
— представимая в формальной арифметике 373
— примитивно рекурсивная (п. р. ф.) 330
— характеристическая 332
— частично рекурсивная (ч. р. ф.) 341

Цифра 368

Часть 22
— истинная (собственная) 23
Ч. р. ф. — *см.* функция частично рекурсивная

Шаг вывода 166, 169
Штрих Шеффера 123

Эквивалентность дедуктивная 177, 216
— машин Тьюринга 308
Эквиваленция 68
Элемент 21
— отвечающий терму в интерпретации 247
Элементарная теория 238
— — абелевых групп 239
— — групп 239
— — колец 240
— — коммутативных колец 240
— — линейно упорядоченных множеств 240
— — полей 240
— — полугрупп 239
— — упорядоченных множеств 240
Элементарное предложение (в теории математических систем) 238
— — (в логике предложений) 70
Элементарный шаг вывода — *см.* шаг вывода

β-функция Гёделя 376
ω-непротиворечивость 393

# УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ


$И$ 51
$Л$ (истинностное значение) 51
$Л$ (в команде) 284
$П$ 284
$С$ 284
$\overline{A}$ 69
$\sim A$ 69
$|A|$ 435
$(a_1, a_2)$ 31
$(a_1, \ldots, a_n)$ 31
Ar 360
CA 30
$c$ 446
$F(a)$ 37
$F \circ G$ 42
$G$ 239
$G_0$ 158
$G_0'$ 190
$G_1$ 207
$G_1^-$ 411
$G_1^=$ 238
$G_1^{\Delta r}$ 411
$H_0$ 186
$H_1$ 248
$KR$ 239
$LOr$ 239
$M/R$ 423
$M[t_1, \ldots, t_n]$ 286
$n$ 368
$Or$ 239
$R$ (элементарная теория колец) 239
$R$ (исчисление Робинсона) 407
$R^{-1}$ 35
$S_0$ 194
$S_1$ 253
$t\|_y^x$ 236
$x^*$ 361, 464
$[x]$ 38
$xRy$ 33
$X|Y$ 123
$\mathfrak{A}^*$ 111
$\mathfrak{A}^\wedge$ 111
$\mathfrak{A}_\Gamma$ 77
$\mathfrak{A}_\Gamma^*$ 208
$\mathfrak{A}_y^x$ 236
$\beta(x_1, x_2, x_3)$ 376
$\varkappa(M)$ 303
$\varkappa(x)$ 302
$\Lambda$ 285
$\forall\alpha$ 316
$\aleph_0$ 442
$\in$ 22
$\notin$ 22
$\overline{\in}$ 22
$\subset$ 22
$=$ 23, 231
$\{\}$ 24
$\varnothing$ 25
$\cup$ 25
$\cap$ 25
$\setminus$ 25
$\times$ 31
$\overset{f}{\mapsto}$ 37
$\mapsto$ 37
$\rightarrow$ (отображение) 39
$\rightarrow$ (в секвенции) 194
$\rightarrow$ (в команде) 283
$\overset{n,a}{\rightarrow}$ 40
$\not\subset$ 47
$\doteq$ 52, 59, 135, 136
$\forall x$ 60
$\exists x$ 60
$\&$ 64
$\vee$ 65
$\supset$ 67
$\leftrightarrow$ 68
$\neg$ 69
$\Rightarrow$ 113, 139
$\downarrow$ 123
$\vdash_\Gamma$ 156
$\vdash$ 156
$\exists!x$ 238
$\#$ 283
$\square$ 302
$*$ 302
$|$ 295
$\sim$ 434
$\leq, \geq$ 27, 32 *


* По техническим причинам для отношений «меньше или равно» и «больше или равно» используются обозначения $\leq$, $\geq$.

# ОГЛАВЛЕНИЕ


ПРЕДИСЛОВИЕ . . . . . 5

ВВЕДЕНИЕ . . . . . 8

ГЛАВА 1. МНОЖЕСТВА, ОТНОШЕНИЯ И ФУНКЦИИ . . . . . 21

§ 1.1. Множества . . . . . 21
§ 1.2. Отношения и функции . . . . . 33

Задачи и упражнения . . . . . 47

ГЛАВА 2. СИМВОЛИЧЕСКИЙ ЯЗЫК . . . . . 51

§ 2.1. Предложения . . . . . 51
§ 2.2. Предикаты и кванторы . . . . . 54
§ 2.3. Пропозициональные связки . . . . . 63
§ 2.4. Формулы . . . . . 70

Задачи и упражнения . . . . . 86

ГЛАВА 3. СЕМАНТИКА ЛОГИКИ ПРЕДЛОЖЕНИЙ . . . . . 91

§ 3.1. Булевы функции. Равносильность формул . . . . . 91
§ 3.2. Тождественные преобразования. Нормальные формы. Тождественно истинные и тождественно ложные формулы . . . . . 100
§ 3.3. Представление произвольной булевой функции формулой. Совершенные нормальные формы. Двойственность . . . . . 108
§ 3.4. Семантическое следование . . . . . 113
§ 3.5. Приложения. Функциональная полнота . . . . . 117

Задачи и упражнения . . . . . 123

ГЛАВА 4. СЕМАНТИКА ЛОГИКИ ПРЕДИКАТОВ . . . . . 128

§ 4.1. Интерпретации и модели. Выполнимость, истинность и равносильность формул . . . . . 128
§ 4.2. Основные равносильности. Тождественные преобразования. Префиксная нормальная форма . . . . . 140
§ 4.3. Предметные функции и константы . . . . . 148

Задачи и упражнения . . . . . 150

ГЛАВА 5. СИНТАКСИС ЛОГИКИ ПРЕДЛОЖЕНИЙ . . . . . 154

§ 5.1. Общее понятие логического исчисления . . . . . 154
§ 5.2. Определение исчисления $G_0$ . . . . . 158
§ 5.3. Формальные выводы в исчислении $G_0$ . . . . . 164
§ 5.4. Семантическая пригодность и полнота исчисления $G_0$ . . . . . 178
§ 5.5. Другие варианты исчисления предложений . . . . . 184

Задачи и упражнения . . . . . 202

ГЛАВА 6. СИНТАКСИС ЛОГИКИ ПРЕДИКАТОВ . . . . . 207

§ 6.1. Исчисление $G_1$ . . . . . 207
§ 6.2. Семантическая пригодность и полнота исчисления $G_1$ . . . . . 217
§ 6.3. Исчисления на основе $G_1$ с равенством. Некоторые прикладные исчисления . . . . . 230
§ 6.4. Другие варианты узкого исчисления предикатов . . . . . 248
§ 6.5. Исчисление предикатов и аристотелевская силлогистика . . . . . 255
§ 6.6. Исторический комментарий к главам 2—6 . . . . . 268

Задачи и упражнения . . . . . 274

ГЛАВА 7. ЭЛЕМЕНТЫ ТЕОРИИ АЛГОРИТМОВ . . . . . 278

§ 7.1. Предварительные соображения . . . . . 278
§ 7.2. Машины Тьюринга . . . . . 281
§ 7.3. Примеры машин . . . . . 287
§ 7.4. Тезис Чёрча — Тьюринга . . . . . 297
§ 7.5. Универсальная машина Тьюринга . . . . . 301
§ 7.6. Неразрешимые алгоритмические проблемы . . . . . 306
§ 7.7. Разрешимые и перечислимые множества . . . . . 315
§ 7.8. Примитивно рекурсивные функции . . . . . 327
§ 7.9. Частично рекурсивные и общерекурсивные функции . . . . . 340

Задачи и упражнения . . . . . 352

ГЛАВА 8. ФОРМАЛЬНАЯ АРИФМЕТИКА. ГРАНИЦЫ ФОРМАЛИЗАЦИИ МАТЕМАТИКИ . . . . . 360

§ 8.1. Формальная арифметика . . . . . 360
§ 8.2. Представление в формальной арифметике предикатов и функций . . . . . 373
§ 8.3. Арифметизация выводов . . . . . 380
§ 8.4. Теорема Гёделя о неполноте . . . . . 390
§ 8.5. Теоремы Тарского и Чёрча . . . . . 402

Задачи и упражнения . . . . . 416

ПРИЛОЖЕНИЕ I. ОТНОШЕНИЯ ЭКВИВАЛЕНТНОСТИ И ПОРЯДКА . . . . . 419

Задачи и упражнения . . . . . 429

ПРИЛОЖЕНИЕ II. МОЩНОСТЬ МНОЖЕСТВА ..... 432

Задачи и упражнения ..... 455

ПРИЛОЖЕНИЕ III. МЕТОД МАТЕМАТИЧЕСКОЙ ИНДУКЦИИ И ПЕАНОВСКАЯ АРИФМЕТИКА ..... 458

ЛИТЕРАТУРА ..... 468

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ ..... 471

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ ..... 476

ГЛАДКИЙ АЛЕКСЕЙ ВСЕВОЛОДОВИЧ

# МАТЕМАТИЧЕСКАЯ ЛОГИКА

Художник *В.В. Суркоо*
Технический редактор *Г.П. Каренина*
Корректор *Т.М. Козлова*
Компьютерная верстка *Г.И. Гаврикова*

Лицензия ЛР № 020219 от 25.09.96.
Подписано в печать 20.05 98
Формат 60 × 90 $^{1}/_{16}$
Гарнитура Таймс
Усл. печ. 30,0 Уч.-изд. 30,0
Тираж 1000 экз.
Заказ 139.

Издательский центр
Российского государственного
гуманитарного университета
125267 Москва, Миусская пл., 6.
973-4200