Московский государственный университет имени М.В. Ломоносова

КЛАССИЧЕСКИЙ УНИВЕРСИТЕТСКИЙ УЧЕБНИК

А.Н. Колмогоров, А.Г. Драгалин

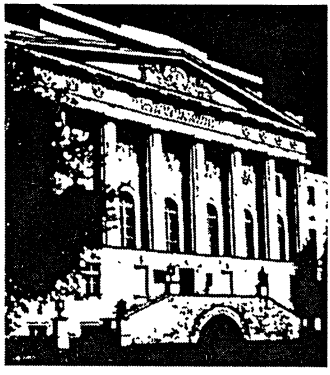
МАТЕМАТИЧЕСКАЯ ЛОГИКА

Серия

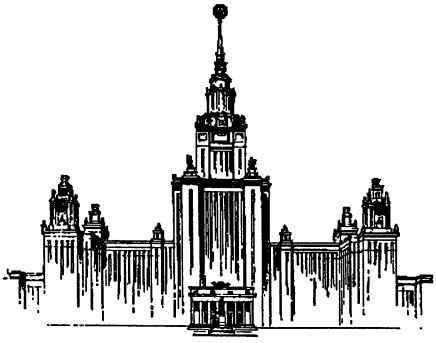
КЛАССИЧЕСКИЙ УНИВЕРСИТЕТСКИЙ УЧЕБНИК

основана в 2002 году по инициативе ректора
МГУ им. М.В. Ломоносова
академика РАН В.А. Садовничего
и посвящена

250-летию Московского университета



КЛАССИЧЕСКИЙ УНИВЕРСИТЕТСКИЙ УЧЕБНИК



Московский государственный университет имени М.В. Ломоносова

А.Н. Колмогоров, А.Г. Драгалин

МАТЕМАТИЧЕСКАЯ ЛОГИКА

Допущено Министерством высшего и среднего специального образования СССР в качестве учебного пособия для студентов математических специальностей вузов

Издание третье, стереотипное

ББК 22.12 87.4

Колмогоров Андрей Николаевич, Драгалин Альберт Григорьевич

Математическая логика. Изд. 3-е, стереотипное. — М.: КомКнига, 2006. 240 с. (Классический университетский учебник.)

ISBN 5–484–00520–5

А. Н. Колмогоров (1903–1987) и А. Г. Драгалин (1941–1998) — выдающиеся отечественные логики и математики, оказавшие глубокое воздействие на стиль и направление мировых исследований по логике и философии математики.

В настоящее издание включены учебники А. Н. Колмогорова и А. Г. Драгалина «Введение в математическую логику» и «Математическая логика. Дополнительные главы», содержащие классическое изложение понятий и результатов математической логики с элементами теории множеств, теории алгоритмов и оснований математики. Учебники написаны на основании курса математической логики, читавшегося обоими авторами на механико-математическом факультете МГУ им. М. В. Ломоносова.

Изложение фундаментальных фактов современной логики (основ логики высказываний и логики предикатов, начал аксиоматической теории множеств, теории алгоритмов, теоремы Гёделя о неполноте, программы Гильберта обоснования математики) не предполагает специальной подготовки и рассчитано на широкий круг читателей, интересующихся математической логикой и философскими проблемами современной математики.

Печатается по решению Ученого совета Московского университета

Издательство «КомКнига». 117312, г. Москва, пр-т 60-летия Октября, 9.
Подписано к печати 09.03.2006 г. Формат 60×90/16. Печ. л. 15. Зак. № 2330.
Отпечатано в типографии ООО ПФ «Полиграфист». 160001, г. Вологда, ул. Челюскинцев, 3.

ISBN 5–484–00520–5

Предисловие к серии

Уважаемый читатель!

Вы открыли одну из замечательных книг, изданных в серии «Классический университетский учебник», посвященной 250-летию Московского университета. Серия включает свыше 150 учебников и учебных пособий, рекомендованных к изданию Учеными советами факультетов, редакционным советом серии и издаваемых к юбилею по решению Ученого совета МГУ.

Московский университет всегда славился своими профессорами и преподавателями, воспитавшими не одно поколение студентов, впоследствии внесших заметный вклад в развитие нашей страны, составивших гордость отечественной и мировой науки, культуры и образования.

Высокий уровень образования, которое дает Московский университет, в первую очередь обеспечивается высоким уровнем написанных выдающимися учеными и педагогами учебников и учебных пособий, в которых сочетаются как глубина, так и доступность излагаемого материала. В этих книгах аккумулируется бесценный опыт методики и методологии преподавания, который становится достоянием не только Московского университета, но и других университетов России и всего мира.

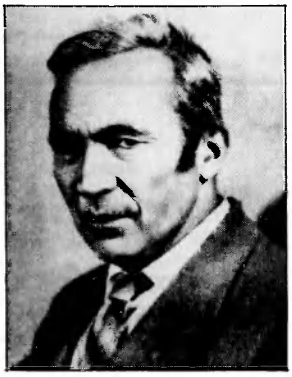
Издание серии «Классический университетский учебник» наглядно демонстрирует тот вклад, который вносит Московский университет в классическое университетское образование в нашей стране и, несомненно, служит его развитию.

Решение этой благородной задачи было бы невозможным без активной помощи со стороны издательств, принявших участие в издании книг серии «Классический университетский учебник». Мы расцениваем это как поддержку ими позиции, которую занимает Московский университет в вопросах науки и образования. Это служит также свидетельством того, что 250-летний юбилей Московского университета — выдающееся событие в жизни всей нашей страны, мирового образовательного сообщества.

Ректор Московского университета
академик РАН, профессор *В. А. Садовничий*

Андрей Николаевич Колмогоров

(1903–1987)



Выдающийся российский математик, академик. Родился в 1903 году в Тамбове. В 1925 году окончил Московский университет, профессором которого работал с 1931 года. Заведовал различными кафедрами, был деканом механико-математического факультета МГУ. Автор классических работ по теории функций действительного переменного, теории множеств, топологии, конструктивной логике, функциональному анализу, механике, теории алгоритмов, теории информации. Основополагающее значение имеют результаты А. Н. Колмогорова в области теории вероятности. Широко известна его деятельность по разработке методики и организации математического образования. А. Н. Колмогоров был председателем Московского математического общества, почетным доктором зарубежных университетов, иностранным членом многих академий и научных обществ, лауреатом международных премий и кавалером правительственных наград. Умер в Москве в 1987 году.

Альберт Григорьевич Драгалин

(1941–1998)

Видный представитель российской школы математического конструктивизма. Родился 10 апреля 1941 года на острове Моржевец Архангельской области. Окончил механико-математический факультет МГУ, где работал с 1966 года. С 1983 года жил в Венгрии, заведовал кафедрой вычислительной математики университета им. Л. Кошута (г. Дебрецен). В 1988 году Венгерской Академией наук ему была присвоена степень доктора наук. Автор фундаментальных трудов по теоретико-модельным и теоретико-доказательственным основаниям интуиционистской логики, конструктивным методам нестандартного анализа. Умер 18 декабря 1998 года в г. Дебрецене.

Колмогоров А. Н., Драгалин А. Г.

ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ

Предисловие*

Эта книга задумана как первоначальный курс математической логики. Она возникла в результате обработки конспектов лекций (читавшихся обоими авторами) семестрового курса математической логики для студентов первого курса механико-математического факультета Московского университета. Авторы стремились познакомить читателя с основными понятиями математической логики, полезными в работе математика любой специальности. Большое внимание уделено правильному использованию точных обозначений математической логики для записи математических суждений, логическим законам, началам теории множеств и теории алгорифмов.

Настоящая книга представляет собой первую часть задуманного авторами учебника и содержит три главы. Первая глава сама по себе является некоторым минимальным ознакомительным курсом математической логики. К этой же главе примыкают два небольших приложения, помещенные в конце книги, посвященные применениям математической логики в теории контактных схем и в теории кодирования. Во второй главе в уточненной форме излагаются основы семантики логико-математических языков. Третья глава посвящена изложению выводимости в логике предикатов и теориям первого порядка. Уже здесь мы стремились обсудить некоторые важные результаты математической логики, отложив полные доказательства до второй части, в которой излагаются начала теории множеств и теории алгорифмов, теорема Гёделя о полноте исчисления предикатов, обсуждается программа Гильберта обоснования математики.

Изучение курса логики предполагает выполнение упражнений на семинарских занятиях. С этой целью следует использовать специальные задачники, например [9]. Все упражнения в тексте легкие, обязательны для выполнения, предназначены для самоконтроля и не могут заменить такого рода задачника.

В книге используются следующие обозначения. Знак $\triangleright$ в тексте отмечает начало доказательства, а знак $\triangleleft$ — его окончание. Знаки $\leftrightharpoons$, $\Rightarrow$, $\Leftrightarrow$ заменяют словесные обороты «есть по определению», «если..., то», «тогда и только тогда, когда» соответственно. Звездочкой отмечены пункты и параграфы, не обязательные при первом чтении.

Мы предприняли попытку концентрического изложения предмета, когда важнейшие темы обсуждаются в процессе обучения несколько раз, постепенно приобретая полную ясность. Учебник разбит на две книги. Во второй книге большее внимание уделяется фундаментальным результатам математической логики. Мы вновь вернемся к рассмотрению понятия множества, но уже на базе формальной аксиоматической теории Цермело—Френкеля. Таким образом, мы

* Учебник А. Н. Колмогорова и А. Г. Драгалина «Введение в математическую логику» впервые опубликован издательством Московского университета (М., 1982, 120 с.).

надеемся дать неспециалисту представление о классических результатах математической логики и подготовить будущего специалиста к изучению более подробных руководств.

Авторы

Введение

1. Логика — наука очень старая. Она возникла тогда, когда развитие специальных наук и вообще человеческого мышления сделало актуальным вопрос о том, как надо рассуждать, чтобы получить правильные выводы. Несомненен интерес к логике среди математиков и философов эпохи расцвета греческой культуры в VI–IV вв. до н. э. Но первое дошедшее до нас большое сочинение, посвященное специально логике («Аналитики» Аристотеля, 384–322 гг. до н. э.), принадлежит уже позднегреческой эпохе. Независимо возникла буддистская логика, но дальнейшее развитие логики в Европе имеет своим исходным пунктом изучение Аристотеля.

Математическая логика с внешней стороны отличается от «обычной» тем, что она широко пользуется языком математических и логических знаков, исходя из того, что в принципе они могут совсем заменить слова обычного языка и принятые в обычных живых языках способы объединения слов в предложения. Довольно рано возникла идея о том, что, записав все исходные допущения на языке специальных знаков, похожих на математические, можно заменять рассуждение вычислением. Точно же сформулированные правила таких логических вычислений можно перевести на язык вычислительной машины, которая тогда будет способна автоматически выдавать интересующие нас следствия из введенных в нее исходных допущений. Своего рода «логическую машину» сконструировал еще в средние века Раймунд Луллий (1235–1315), дав ей, впрочем, лишь совершенно фантастические применения. Более определенный и близкий к реально осуществленному впоследствии замысел универсального логического исчисления развивал Лейбниц (1646–1716). Лейбниц надеялся даже, что в будущем философы вместо того, чтобы бесплодно спорить, будут брать бумагу и вычислять, кто из них прав.

Начало созданию того аппарата математической логики, который теперь мы называем логикой высказываний, положил Джордж Буль (1815–1864). Логико-математические языки и теория их смысла были затем значительно развиты в работах Фреге (1848–1925). Широко задуманное изложение больших разделов математики на языке математической логики было предпринято в работах Пеано (1858–1932) и особенно в фундаментальной трехтомной монографии Рассела и Уайтхеда, изданной в 1910–1913 гг.

В двадцатых годах XX века с программой обоснования математики на базе математической логики выступил знаменитый математик Гильберт (1862–1943). С этого времени и начинается современный этап развития математической логики, характеризующийся применением точных математических методов при изучении формальных аксиоматических теорий.

Заметим, что роль логического исчисления как средства открытия новых истин даже в области математики долго оставалась более чем скромной. Зато символический язык математической логики оказался на границе девятнадцато-

го и двадцатого веков очень важным подспорьем в изучении логических основ математики, поскольку он позволял избегать всякой неточности мысли, которая легко проскальзывает при использовании слов обычного языка, смысл которых дается не точным определением, а созданием привычки к принятому словоупотреблению.

Подъем широкого интереса к математической логике не только среди математиков, но и среди техников произошел тогда, когда обнаружилось, что в рамках математической логики уже создан аппарат для расчета действия самых различных вычислительных и управляющих дискретных устройств.

2. В математической логике предметом исследования часто оказываются математические теории, такие как математический анализ, алгебра, элементарная геометрия, арифметика и др. В логике математические теории изучаются в целом — и это одна из особенностей математической логики по сравнению с другими математическими дисциплинами.

Прежде всего, изучаемую математическую теорию уточняют и описывают на базе строгого логико-математического языка. Этот этап называется формализацией теории и составляет важную, хотя и предварительную, часть исследования теории. После формализации полученную формальную аксиоматическую теорию уже можно подвергнуть точному математическому изучению, можно ставить точные проблемы, получать математические результаты.

Какие же вопросы можно ставить относительно теории в целом?

Можно интересоваться непротиворечивостью теории, т. е. интересоваться вопросом, не выводится ли в данной теории некоторое утверждение и его отрицание. Так, с помощью метода интерпретаций Кэли и Клейн показали, что геометрия Лобачевского непротиворечива, если непротиворечива обычная евклидова геометрия.

Большое впечатление на современников произвело открытие в начале XX века Кантором и Расселом парадоксов в теории множеств. Это открытие свидетельствовало о том, что широко используемая и популярная (и в настоящее время) теория множеств в ее наивном изложении является противоречивой теорией. Изучение этого явления в значительной мере способствовало развитию современных методов математической логики. Была сформулирована аксиоматическая теория Цермело—Френкеля, в которой обычные способы вывода парадоксов уже не получаются. Программа Гильберта обоснования математики финитными средствами также в значительной степени связана с открытием парадоксов.

Знаменитая вторая теорема Гёделя, полученная в тридцатых годах XX века, утверждает, коротко говоря, что непротиворечивость достаточно богатой теории не может быть установлена средствами самой теории. Этот факт побуждает специалистов по основаниям математики изыскивать математические методы, с одной стороны, убедительные (с той или иной точки зрения) и, с другой стороны, не входящие в теорию, непротиворечивость которой изучается. Очень многие исследования по неклассическим, модальным и интуиционистским логикам стимулированы этой идеей.

Можно сказать, что к настоящему времени непротиворечивость таких теорий, как элементарная геометрия, арифметика, анализ, хорошо изучена и достаточно надежно обоснована. Непротиворечивость мощных аксиоматических теорий множеств, таких как система Цермело—Френкеля или теория Куайна, гораздо более проблематична.

Большой интерес представляет изучение полноты той или иной теории. Во многих математических теориях время от времени возникают конкретные

проблемы, которые не удается ни доказать, ни опровергнуть. Иногда это бывает в силу технической сложности самой проблемы, и, спустя определенное время, проблему все же удается разрешить. Однако в некоторых случаях ситуация совершенно иная: проблему просто невозможно ни доказать, ни опровергнуть в рамках исследуемой теории. Так, было показано, что подобными проблемами в теории множеств Цермело—Френкеля являются континуум-проблема Кантора и многие другие важные теоретико-множественные проблемы. Подчеркнем, что дано было точное доказательство того факта, что, например, аксиома выбора не может быть ни доказана, ни опровергнута в теории Цермело—Френкеля. Теорема Гёделя о неполноте утверждает, что всякая достаточно богатая теория необходимо содержит утверждения, которые нельзя ни доказать, ни опровергнуть в рамках теории.

Тем не менее некоторые важные теории оказываются полными. Таковы, например, элементарная геометрия, теория векторных пространств.

3. Существенно бывает исследовать разрешимость той или иной теории. Так, Тарский в 1948 г. построил конкретный алгорифм, позволяющий по всякому утверждению элементарной геометрии выяснить, является ли это утверждение истинным или ложным. Каждый, кто в школьные годы трудился над задачами геометрии, может оценить это открытие.

В то же время логики умеют доказывать, что многие теории, например, арифметика, анализ, теория множеств неразрешимы, т. е. что не существует алгорифма, позволяющего по всякому суждению теории узнавать, истинно оно или ложно.

Вопрос о существовании тех или иных алгорифмов занимает важное место в исследованиях логиков. Так, доказано, что не существует алгорифма, позволяющего решать вопрос о существовании решения у системы полиномиальных уравнений в целых числах.

В последнее время большое внимание уделяется изучению сложности алгорифмов. Так, например, недавно было показано, что арифметика сложения натуральных чисел, являющаяся разрешимой теорией, может иметь только очень сложные разрешающие алгорифмы.

Вопросы построения оптимальных по сложности и по времени работы вычислительных устройств занимают важное место в теоретической кибернетике — науке, тесно связанной с математической логикой.

Глава I

Начальные понятия математической логики и теории множеств

§ 1. Синтаксис языка математических и логических знаков

Некоторым знакам и комбинациям знаков мы приписываем самостоятельный смысл. Таковы следующие знаки и комбинации знаков:

$$5$$
$$2+2$$
$$2+2=5$$

(с которыми читатель, несомненно, встречался). Но таким отдельно взятым знакам, как $+$, $=$ или таким комбинациям знаков, как

$$2+$$
$$2+2=$$

мы не придаем самостоятельного смысла. Среди имеющих самостоятельный смысл знаков и комбинаций знаков выделяются прежде всего

1. Имена предметов. Таковы 1, 2, 2/3, 4/2, e (как обозначение числа e), 5–3, $\lim\limits_{x\to 0}\dfrac{e^x-1}{x}$.

Здесь написаны семь имен четырех предметов, так как

$$1=\lim_{x\to 0}\frac{e^x-1}{x},\quad 2=4/2=5-3,$$

т. е., например, 2 и 5–3 являются именами одного и того же предмета. Заметим, что такая комбинация знаков, как sin, тоже является именем, а именно именем функции «синус». Из имени функции sin и имени числа 5 можно образовать имя действительного числа $\sin 5$. Но что такое комбинация знаков

$$\frac{e^x-1}{x}\ ?$$

Это не имя предмета, а

2. Именная форма. Именной формой называется выражение (комбинация знаков), содержащее знаки «переменных», которое превращается в имя предмета, если вместо «переменных» поставить надлежащим образом выбранные имена предметов (в нашем примере вместо x можно подставлять имя любого числа, отличного от нуля). Данное общее представление об именных формах делается совершенно отчетливым только после дополнительных пояснений о подстановке вместо переменных их частных «значений». К этому мы будем еще неоднократно возвращаться.

Заметьте, что

$$\lim_{x\to 0}\frac{e^x-1}{x}$$

есть имя, а не именная форма с переменным x.

В этом выражении вместо x нельзя подставить имя какого-либо определенного числа: запись

$$\lim_{15\to 0}\frac{e^{15}-1}{15}$$

бессмысленна. Можно лишь изменить обозначение переменной x на переменную y. Полученная запись

$$\lim_{y\to 0}\frac{e^y-1}{y}$$

является именем того же числа 1.

Приведем еще несколько примеров именных форм:

$$x^2+2,\quad \sin(\alpha+\beta),\quad \lim_{x\to 0}\frac{\sin(xy)}{x}.$$

В последнем из этих примеров «свободной переменной», вместо которой можно что-либо «подставлять», является только буква y.

Соединяя два имени чисел знаками равенства или неравенства, получаем записи некоторых утверждений:

$$2+2=4,\quad 2^{10}>3^6,\quad 2+2=5.$$

Первые два из записанных утверждений верны, а третье ложно. Но все это

3. Высказывания. Более сложный пример высказывания:

$$\lim_{x\to 0}\frac{e^x-1}{x}=1.$$

Но что такое запись

$$x=|x|?$$

Здесь нельзя поставить вопрос об истинности или ложности. Не содержится никакого утверждения. Подставляя вместо x обозначения неотрицательных чисел, будем получать верные высказывания

$$0=|0|,\quad 2=|2|,\quad 1000=|1000|,\quad \ldots,$$

подставляя же обозначения отрицательных чисел — ложные:

$$-1 = |-1|, \quad -1000 = |-1000|.$$

Запись $x = |x|$ есть

4. Высказывательная форма. Так называют комбинации знаков, содержащие знаки переменных, которые превращаются в высказывания при замене переменных именами предметов.

Имена предметов и именные формы называют *термами*, высказывания и высказывательные формы — *формулами*.

Термами и формулами исчерпываются комбинации знаков, которым приписывается самостоятельный смысл. Иногда в математической логике термины «терм» и «формула» понимаются более узким образом, как комбинации знаков в некоторых точных логико-математических языках, например в так называемых языках первого порядка (см. гл. II, § 1).

Мы уже видели, что из термов можно сооружать новые термы и формулы. Рассмотрим в качестве примера «родословную» формулы

$$\lim_{x\to 0} \frac{e^x - 1}{x} = 1 \quad \text{(см. рис. 1)}.$$

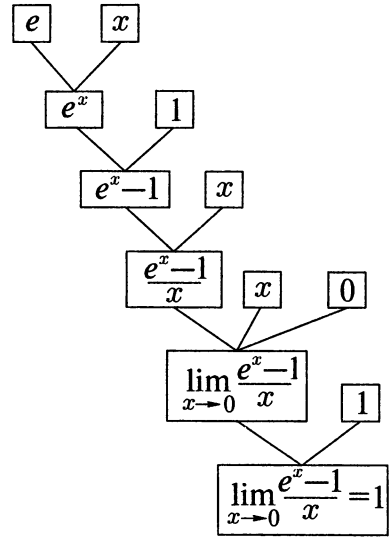


Рис. 1

Родословная начинается с простых термов

$$e,\ x,\ 1,\ 0,$$

которые ни из чего не «составлены». Дальнейшие термы и заключительная формула получаются при помощи следующих порождающих конструкций:

1. Из термов T_1 и T_2 образуется терм $T_1^{T_2}$.
2. Из термов T_1 и T_2 образуется терм T_1/T_2.
3. Из термов T_1 и T_2 образуется терм $T_1 - T_2$.
4. Из термов T_1, T_2 и T_3 образуется $\lim\limits_{T_1\to T_2} T_3$.
5. Из термов T_1 и T_2 образуется формула $T_1 = T_2$.

Первые четыре из встретившихся здесь порождающих конструкций служат для формирования из термов новых термов. Применяя пятую, мы получаем из двух термов формулу. Вскоре нам встретятся конструкции, создающие из формул формулы, из формул — терм и т. д. Несмотря

на краткость предыдущего изложения авторы рекомендуют читателю уже сейчас попробовать проанализировать строение термов и формул, встречающихся в специальных математических курсах. Что за переменные мы имеем, например, в формуле дифференцирования произведения

$$(uv)' = uv' + u'v? \tag{1}$$

Легко понять, что (1) есть высказывательная форма, которая превращается в истинное высказывание, если вместо u и v поставить имена двух дифференцируемых функций. Несколько труднее объяснить строение формулы

$$(x^2)' = 2x. \tag{2}$$

Сначала кажется, что здесь x — числовая переменная. Но, подставив вместо x значение 3, получим не имеющую смысла запись

$$(3^2)' = 2 \cdot 3.$$

Запись (2) является одной из тех «вольностей», которые на практике математики себе часто позволяют. Можно исправить допущенную неточность, например, так: определить *функцию* f равенством

$$f(x) = x$$

и тогда уже законно написать

$$(f^2)' = 2f.$$

Занимаясь таким разбором, следует иметь в виду, что *переменная* есть просто знак (иногда говорят — «буква»), характеризующийся правилами его употребления. В математических книгах часто встречаются, например, указания такого типа: «далее m и n — натуральные числа, а x, y, z — действительные». Конечно, даже при подстановке вместо переменных их числовых значений в рациональные выражения могут получаться выражения, лишенные смысла. Обратим еще внимание на встретившуюся нам порождающую конструкцию образования из трех термов x, T_1 и T_2 терма T, равного

$$\lim_{x \to T_1} T_2.$$

Для того чтобы терм T имел смысл, необходимо, чтобы терм T_1 не содержал переменной x. В терме T переменная x — «связанная».

В терм

$$\lim_{y \to 2} y^2$$

можно подставить вместо y новую переменную x, но получившийся терм

$$\lim_{x \to 2} x^2$$

является именем того же числа 4.

Одной из наших задач в дальнейшем будет в некоторых случаях довести правила обращения с переменными до полной отчетливости.

Разберем еще несколько примеров, относящихся к употреблению специальных логических знаков. Как, например, записать без употребления слов обычного языка известное вам определение предела функции: пределом функции $f(x)$ в точке a называется такое число B, что для любого $\varepsilon > 0$ существует такое $\delta > 0$, что разность $f(x) - B$ делается по модулю меньше ε, если только $|a - x| < \delta$, $x \neq a$? Чисто символическая запись этого определения требует введения обозначений для так называемых *кванторов общности и существования* и знаков логического следования и равносильности по определению. Символическая запись этого определения может выглядеть так:

$$\lim_{x \to a} f(x) = B \leftrightharpoons (\forall \varepsilon > 0)(\exists \delta > 0)(0 < |x - a| < \delta \Rightarrow |f(x) - B| < \varepsilon).$$

Здесь

$\forall$ — квантор общности, «для всех»,

$\exists$ — квантор существования, «существует».

Считается, что $x, a, \varepsilon, \delta$ суть переменные для действительных чисел.

Во введении уже было объяснено, почему возможность излагать все математические определения и результаты на таком чисто символическом языке имеет принципиальное значение.

Полезно уже сейчас поупражняться в чисто символической записи математических предложений. При этом можно пользоваться кроме кванторов знаками логических связок $\neg$, $\wedge$, $\vee$, $\Rightarrow$. Здесь $\neg A$ означает, что «A неверно», $A \wedge B$ означает: «A и B», $A \vee B$ означает: «хотя бы одно из предложений A или B верно», $A \Rightarrow B$ означает: «если A, то B». Логические связки имеют названия $\neg$ — *отрицание*, $\wedge$ — *конъюнкция*, $\vee$ — *дизъюнкция*, $\Rightarrow$ — *импликация*.

Часто употребляется также логическая связка $\Leftrightarrow$ «тогда и только тогда», *эквиваленция*. Она может быть выражена через остальные логические связки следующим образом:

$$A \Leftrightarrow B \leftrightharpoons (A \Rightarrow B) \wedge (B \Rightarrow A).$$

§ 2. О классификации суждений и теории силлогизмов по Аристотелю

1. В качестве первого упражнения в употреблении понятий и обозначений математической логики и теории множеств изложим на современном языке фрагмент традиционной логики Аристотеля.

Традиционная логика имеет дело с *понятиями*. Понятия делятся на *единичные* и *общие*. Единичное понятие — это просто имя определенного предмета. Общее понятие по содержанию определяется указанием

совокупности свойств, характеризующих подпадающие под него предметы. Класс предметов, обладающих этой характеристической совокупностью свойств, образует *объем* понятия.

Свойства предметов в математической логике называются *одноместными предикатами*. В этом параграфе мы будем иметь дело только с одноместными предикатами и называть их просто предикатами, обозначая буквами F, G, H. Высказывательную форму «предмет x обладает свойством F» будем записывать в виде $F(x)$. Например, если F есть свойство «быть четным числом», то высказывания $F(10)$ и $F(1000)$ истинны, а высказывание $F(1001)$ ложно.

Совокупность свойств $F_1, \ldots, F_n$ можно заменить свойством «обладать всеми свойствами F_k, $k = 1, 2, \ldots, n$». Поэтому с точки зрения содержания общее «понятие» традиционной логики есть не что иное, как одноместный предикат.

Имея предикат F, можно образовать *класс*

$$M = \{x \mid F(x)\} \tag{1}$$

всех предметов, обладающих свойством F. Этот класс и характеризует *объем* понятия.

При условии (1) для любого x имеет место *эквивалентность*

$$F(x) \Leftrightarrow x \in M.$$

Воспользовавшись квантором общности, напишем

$$\forall x(F(x) \Leftrightarrow x \in M),$$

«для всякого x имеет место $x \in M$ тогда и только тогда, когда $F(x)$». Содержательное употребление переменных предполагает, что мы *заранее* фиксировали некоторый непустой *класс* D предметов, объектов исследования, которые можно подставлять вместо переменной. И выражение «для всякого x» следует понимать как «для всякого предмета x из класса D».

Класс D в такой ситуации называется *областью изменения* переменной x. При употреблении выражений с переменными следует четко фиксировать область изменения соответствующих переменных. Например, в качестве D может выступать класс всех натуральных чисел, класс всех действительных чисел или даже класс всех множеств.

Заметьте также, что D и M мы назвали классами, а не *множествами*. Как мы увидим позднее, не всякое свойство определяет множество объектов, хотя можно считать, что всякое свойство (записанное в некотором логико-математическом языке) определяет класс. Множества суть частные виды классов.

Область изменения переменной может быть именно классом, но не множеством. В теории силлогизмов Аристотеля могут фигурировать произвольные классы.

Аристотель рассматривает четыре типа суждений (в нашей терминологии — высказываний):

$A(S, P)$ — общеутвердительное: «все S суть P»;

$E(S, P)$ — общеотрицательное: «ни одно S не есть P»;

$I(S, P)$ — частноутвердительное: «некоторые S суть P»;

$O(S, P)$ — частноотрицательное: «некоторые S не суть P».

Подходя к понятиям с точки зрения их объема, можно считать, что мы фиксировали некоторый непустой класс D предметов в качестве области изменения переменных. В наших словесных формулировках S и P суть классы, составленные из предметов класса D. По содержанию классам S и P соответствуют предикаты F и G:

$$\forall x(F(x) \Leftrightarrow x \in S), \quad \forall x(G(x) \Leftrightarrow x \in P),$$

переменная x пробегает класс D.

В обозначениях математической логики и теории множеств получаем такие формы записи указанных выше типов суждений:

$A(S, P)$	$S \subseteq P$ или $S \setminus P = \varnothing$	$\forall x(F(x) \Rightarrow G(x))$
$E(S, P)$	$S \cap P = \varnothing$	$\forall x(F(x) \Rightarrow \neg G(x))$ или $\forall x \neg(F(x) \wedge G(x))$
$I(S, P)$	$S \cap P \neq \varnothing$	$\exists x(F(x) \wedge G(x))$
$O(S, P)$	$S \setminus P \neq \varnothing$. или $\neg(S \subseteq P)$	$\exists x(F(x) \wedge \neg G(x))$

Здесь $S \cap P$ — *пересечение* классов S и P,

$$\forall x(x \in S \cap P \Leftrightarrow x \in S \wedge x \in P);$$

$S \setminus P$ — *разность* классов S и P,

$$\forall x(x \in S \setminus P \Leftrightarrow x \in S \wedge \neg x \in P);$$

$S \subseteq P$ означает: $\forall x(x \in S \Rightarrow x \in P)$; $\neg(S \subseteq P)$ означает: «неверно, что $S \subseteq P$»; $\varnothing$ — *пустое множество*, $\forall x \neg(x \in \varnothing)$.

С помощью этих обозначений можно формулировать общие логические законы, справедливые при любом выборе соответствующих классов. Так, для любых трех множеств S, M и P

$$(M \subseteq P) \wedge (S \subseteq M) \Rightarrow (S \subseteq P).$$

В традиционных обозначениях это высказывание можно записать в виде

$$\frac{A(M,P)}{\underline{A(S,M)}}\,.$$
$$A(S,P)$$

Это так называемый *модус силлогизма bArbArA*.

2. Какие еще существуют аналогичные правила вывода? Имеются ввиду правила вывода, позволяющие выводить суждения одного из видов $A(S,P)$, $E(S,P)$, $I(S,P)$ или $O(S,P)$ из двух суждений типов A, E, I или O, из которых первое связывает понятие P с третьим понятием M, а второе — понятие S с тем же третьим понятием M. Возможны четыре схемы такого рода правил (в традиционной терминологии — четыре *фигуры силлогизма*):

I	II	III	IV
$\cdot\ (M,P)$	$\cdot\ (P,M)$	$\cdot\ (M,P)$	$\cdot\ (P,M)$
$\underline{\cdot\ (S,M)}$	$\underline{\cdot\ (S,M)}$	$\underline{\cdot\ (M,S)}$	$\underline{\cdot\ (M,S)}$
$\cdot\ (S,P)$	$\cdot\ (S,P)$	$\cdot\ (S,P)$	$\cdot\ (S,P)$

В каждой из этих схем вместо точек можно $4^3 = 64$ способами расставить буквы A, E, I и O. Получается 256 возможных правил вывода (в традиционной терминологии — возможных *модусов силлогизма*). Однако не все эти правила будут состоятельны. Применение некоторых из них приводит к ошибкам. Модусы силлогизма, следуя которым из истинных посылок всегда получаются лишь истинные следствия, называются *правильными*. В аристотелевой логике таких правильных модусов всего девятнадцать. Им даны следующие названия:

1-я фигура	2-я фигура	3-я фигура	4-я фигура
bArbArA	cEsArE	dAtIsI	cAmEnEs
cElArEnt	cAmEstrEs	fErIsOn	frEsIsOn
dArII	fEstInO	dIsAmIs	dImArIs
fErIO	bArOcO	bOcAdO	*brAmAntIp
		*dArAptI	*fEsApO
		*fElAptOn	

Гласные буквы в этих названиях указывают на выбор букв A, E, I или O. Например, модус fElAptOn имеет вид

$$\frac{E(M,P)}{\underline{A(M,S)}}\,,$$
$$O(S,P)$$

т. е.

$$(M \cap P = \varnothing) \wedge (M \subseteq S) \Rightarrow \neg(S \subseteq P).$$

Эта формула превращается в ошибочное высказывание при $P = M = S = \varnothing$. Но легко понять, что при *непустых* множествах P, M и S наша импликация верна. Аристотель и его последователи вплоть до двадцатого века не признавали понятий с пустым объемом. Со своей точки зрения, они были правы, признавая наличие девятнадцати правильных модусов. Но для математиков такая позиция крайне неудобна. Например, в течение тысячелетий не удалось установить, пуст или нет объем понятия «нечетное совершенное число» (совершенным называется натуральное число, у которого сумма отличных от него делителей равна самому числу).

При допущении понятий с пустым объемом правильных модусов остается только пятнадцать (выпадают модусы, отмеченные выше звездочками).

§ 3. О понятии множества

1. В математических руководствах и работах, как правило, имеют дело не с произвольными классами, а с *множествами*. Поясним смысл этого различия.

Предположим вначале, что мы не делаем различия между классами и множествами и свободно вводим в рассмотрение множества по схеме

$$M = \{x \mid F(x)\},$$

где переменная x рассматривается как пробегающая множества (так называемая *схема свертывания*). Если формула F не содержит других свободных переменных кроме x, то терм $\{x \mid F(x)\}$ по самому замыслу этого обозначения должен быть именем определенного множества (переменная x при его образовании «связана»).

Например, если y есть числовая переменная, пробегающая множество всех действительных чисел, то $\{y \mid y^2 = 1\}$ есть имя множества $\{-1, 1\}$.

Рассмотрим терм $\{x \mid x \notin x\}$, где x — переменная для множеств. Он является именем для множества R всех тех множеств, которые не являются своими собственными элементами. Но свойства множества R должны были бы быть странными.

В самом деле, по смыслу его определения для любого множества M имеем

$$M \in R \Leftrightarrow M \notin M.$$

В частности, в качестве M можно взять и само R, так как мы считаем, что R — также полноправное множество. Мы получим

$$R \in R \Leftrightarrow R \notin R.$$

Но это противоречие. В самом деле, что можно сказать о высказывании $R \in R$? Если $R \in R$, то $R \notin R$, и, наоборот, если $R \notin R$, то $R \in R$!

Мы изложили «парадокс Рассела», открытый в 1902 году. Немного ранее были открыты другие парадоксы, в частности, связанные со свойствами «множества всех вещей» и «множества всех множеств».

Математики были поставлены перед необходимостью наложить запрет на способы рассуждения, приводящие к противоречиям. В случае парадокса Рассела надо было либо: а) признать незаконным само определение множества R при помощи схемы свертывания, либо же: б) опротестовать какое-либо звено дальнейших наших рассуждений. Отказаться от этих совершенно элементарных приемов рассуждения о множествах было бы затруднительно. Они часто применяются в более элементарных случаях и там не приводят к противоречиям. Поэтому достаточно единодушно в математике принято считать незаконным неограниченное определение с помощью схемы свертывания. Вообще было решено считать законным введение в рассмотрение новых множеств лишь в строго оговоренных случаях.

2. В общем случае считается, что схема $\{x \mid F(x)\}$ определяет некоторый *класс* M, который, вообще говоря, может оказаться и *не множеством*. Важно, что переменная x пробегает по-прежнему множества, так что M — класс, элементы которого суть множества. Для M по-прежнему выполняется определяющее соотношение

$$\forall x(x \in M \Leftrightarrow F(x)).$$

В обычной теории множеств запрещено образование классов, элементами которых были бы собственно классы, не множества; если x и M — классы и имеет место $x \in M$, то класс x необходимо есть множество.

При таком понимании классов рассуждения в парадоксе Рассела уже не ведут к противоречиям; R есть класс всех множеств x таких, что $x \notin x$, и наше рассуждение доказывает только, что класс R не является сам множеством!

3. Пусть F и G — два предиката и x — переменная, пробегающая некоторый класс D объектов. Будем говорить, что предикаты F и G *эквивалентны*, если при любых x из $F(x)$ вытекает $G(x)$ и из $G(x)$ вытекает $F(x)$:

$$\forall x(F(x) \Leftrightarrow G(x)).$$

Мы считаем, что два эквивалентных предиката определяют один и тот же класс:

$$\{x \mid F(x)\} = \{x \mid G(x)\}.$$

Это означает, что мы к понятию класса подходим с точки зрения его объема и изучаем классы с точностью до равносильности определяющих эти классы предикатов. Отсюда, если M и N — два класса, то

$$M = N \Leftrightarrow \forall x(x \in M \Leftrightarrow x \in N).$$

Это и есть так называемый *принцип объемности* (*экстенсиональности*). Его можно сформулировать также следующим образом: два класса равны в том и только в том случае, когда каждый элемент одного из них принадлежит второму и, наоборот, каждый элемент второго принадлежит первому.

4. В каких же случаях классы оказываются множествами? Сейчас мы перечислим лишь некоторые важнейшие правила образования множеств.

1) *Пустой класс* $\varnothing$ является множеством. Это множество характеризуется тем, что ему не принадлежит ни один предмет:

$$\forall x(x \notin \varnothing).$$

2) Для любого множества M существует множество $\{M\}$, состоящее только из элемента M:

$$\forall y(y \in \{M\} \Leftrightarrow y = M).$$

3) Для любых двух множеств M_1 и M_2 можно образовать их *объединение*, *пересечение* и *разность*. Это — вновь множества, характеризуемые эквивалентностями:

$$y \in M_1 \cup M_2 \Leftrightarrow y \in M_1 \vee y \in M_2,$$
$$y \in M_1 \cap M_2 \Leftrightarrow y \in M_1 \wedge y \in M_2,$$
$$y \in M_1 \setminus M_2 \Leftrightarrow y \in M_1 \wedge y \notin M_2.$$

Правила 2) и 3) позволяют ввести в рассмотрение все конечные семейства множеств. Кроме того, постулируется и существование некоторых бесконечных множеств.

4) Существует множество ω всех натуральных чисел, множество $\mathbf{R}$ всех действительных чисел, множество $\mathbf{Z}$ всех комплексных чисел и т. д. Фактически существование множеств $\mathbf{R}$ и $\mathbf{Z}$ можно уже доказать исходя из существования множества ω натуральных чисел, но мы не будем этим заниматься.

5) Для всякого множества M существует множество $P(M)$ всех подмножеств M:

$$x \in P(M) \Leftrightarrow x \subseteq M,$$

здесь

$$x \subseteq M \rightleftharpoons \forall z(z \in x \Rightarrow z \in M).$$

Для любых множеств M_1, M_2 существует множество $(M_1 \to M_2)$ всех отображений из M_1 в M_2. Его обозначают также через $M_2^{M_1}$ и называют *множеством-степенью* M_2 и M_1. Вместо $f \in (M_1 \to M_2)$ часто пишут $f\colon M_1 \to M_2$.

Упражнение. Пусть M, M_1, M_2 — конечные множества, содержащие соответственно m, m_1 и m_2 элементов. Докажите, что $P(M)$ содержит 2^m элементов, а $(M_1 \to M_2)$ содержит $m_2^{m_1}$ элементов.

6) Если M — множество и $F(x)$ — произвольный предикат теории множеств, то можно образовать множество M' с помощью следующего частного случая схемы свертывания:

$$M' = \{x \mid (x \in M) \wedge F(x)\}.$$

Мы вводим обозначение

$$M' = \{x \in M \mid F(x)\}$$

и говорим, что M' получено по *схеме выделения* из множества M. Определяющее свойство M' таково:

$$x \in M' \Leftrightarrow (x \in M) \wedge F(x).$$

В частности, если переменная z пробегает *множество* K, то можно образовать множество по схеме свертывания $\{z \mid F(z)\}$, так как она в этом случае сводится к схеме выделения

$$\{z \mid z \in K \wedge F(z)\}.$$

Заметим, что *класс всех множеств* V, характеризующийся утверждением $\forall x(x \in V)$, сам множеством не является. Действительно, иначе множеством оказался бы и класс Рассела. Его можно было бы определить по схеме выделения $\{x \in V \mid x \notin x\}$.

Некоторые дальнейшие способы образования множеств мы рассмотрим в следующем параграфе. Заметим, что семейство множеств образует столь мощную и гибкую структуру, что в математике практически нет необходимости использовать собственные классы.

Обычно в математике собственные классы используются лишь как способ выражения. Вместо того чтобы говорить о конкретном условии или предикате $F(x)$, говорят о классе $\{x \mid F(x)\}$ объектов, определяемых этим предикатом, причем упоминания о классах можно избежать, вновь вернувшись к условию, определяющему рассматриваемый класс. Именно в таком стиле говорят о классе всех групп или классе всех линейных пространств и т. п.

§ 4. Отношения и функции

1. Существуют различные способы введения «упорядоченной пары» двух предметов. Мы считаем, что для всяких множеств a и b существует множество $\langle a, b\rangle$ — упорядоченная пара a и b.

Основное свойство этого множества таково: для любых x, y, x', y' имеем

$$\langle x, y\rangle = \langle x', y'\rangle \Leftrightarrow (x = x') \wedge (y = y').$$

Множество всех таких пар $\langle x, y\rangle$, что $x \in M$ и $y \in N$, где M и N — множества, называется *декартовым*, или *прямым*, *произведением* множеств M и N и обозначается через $M \times N$.

То обстоятельство, что $M \times N$ есть именно множество, равно как и то, что упорядоченная пара есть множество, следует рассматривать сейчас как правила образования новых множеств. В следующей книге мы докажем, что эти правила выводятся из остальных.

Упражнение. Пусть M_1 и M_2 — конечные множества, содержащие соответственно m_1 и m_2 элементов. Докажите, что $M_1 \times M_2$ содержит ровно $m_1 \cdot m_2$ элементов.

Кроме того, допускают, что для любого множества M существуют множества

$$\mathrm{dom}(M) = \{x \mid \exists y(\langle x, y\rangle \in M)\},$$
$$\mathrm{rng}(M) = \{y \mid \exists x(\langle x, y\rangle \in M)\}$$

всех первых элементов пар из M и всех вторых элементов пар из M.

Ясно, что если M — множество пар, то

$$M \subseteq \mathrm{dom}(M) \times \mathrm{rng}(M).$$

2. Понятие *отношения* между двумя предметами широко употребляется в математике и за ее пределами. Говорят об отношении параллельности и перпендикулярности между прямыми, строгого и нестрогого неравенства между числами и т. д. (обозначения $a \parallel b$, $a \perp b$, $x < y$, $x \leqslant y$).

К отношениям в этом первоначальном, еще строго не определенном смысле слова можно, как и к понятиям, подойти с точки зрения *объема* и с точки зрения *содержания*.

С точки зрения содержания отношение определяется указанием высказывательной формы, указывающей на связь предметов в отношении:

$a \parallel b \leftrightharpoons$ «a и b суть прямые, лежащие в одной плоскости и не имеющие общей точки».

$$x \subseteq y \leftrightharpoons \forall z(z \in x \Rightarrow z \in y).$$

Можно образовать класс пар, связанных данным отношением как высказывательной формой, например, $\{\langle x, y\rangle \mid x \subseteq y\}$, но этот класс может и не быть множеством.

С точки зрения объема высказывательная форма полностью характеризуется указанием класса пар объектов, связанных соответствующим отношением.

Мы примем по определению, что отношением называется любое *множество* пар. Если R — отношение (т. е. просто множество пар), то говорят, что предметы x и y *связаны отношением* R, если пара $\langle x, y\rangle$ есть элемент R.

Высказывание «предметы x и y связаны отношением R» записывают: xRy. Таким образом,

$$xRy \leftrightharpoons \langle x, y\rangle \in R.$$

Если

$$R \subseteq M \times N,$$

то говорят, что отношение R есть отношение, определенное между элементами множеств M и N. Если

$$R \subseteq M \times M,$$

то говорят, что отношение R *определено* на множестве M. Ясно, что каждое отношение R есть отношение, определенное между $\mathrm{dom}R$ и $\mathrm{rng}R$, и является отношением на $\mathrm{dom}R \cup \mathrm{rng}R$.

Иногда говорят об отношениях принадлежности и включения одного множества в другое, считая знаки $\in$ и $\subseteq$ знаками этих отношений. Следует иметь в виду, что здесь мы *не имеем* отношения в смысле нашего определения именно потому, что соответствующий класс пар не является множеством. Если бы существовало множество E всех пар множеств $\langle x, y\rangle$, для которых $x \in y$, то существовало бы и множество $\mathrm{dom}E$. Но легко видеть, что оно было бы запретным множеством «всех множеств».

Любое свойство пары предметов будем называть *двуместным предикатом*. Например, знак $\in$ есть знак двуместного предиката «быть элементом множества». Высказывательная форма, выражающая применимость предиката F к паре предметов $\langle x, y\rangle$, стандартно пишется $F(x, y)$. При такой системе записи вместо $x \in M$ пишут $\in (x, M)$.

Если существует множество

$$R = \{\langle x, y\rangle \mid F(x, y)\},$$

то

$$F(x, y) \Leftrightarrow xRy.$$

В этом случае говорят, что предикат F имеет *график* R. Мы видели, что не всякий предикат имеет график.

Иногда, следуя Бурбаки, отношением называют тройку $\langle M_1, M_2, R\rangle$, где $R \subseteq M_1 \times M_2$, и говорят, что это — отношение между элементами множеств M_1 и M_2. Таким образом, в само понятие отношения включаются области, откуда берутся элементы пар. Нам такое определение представляется неудобным, и мы всюду далее ему не следуем.

3. Отношение R называется *функциональным отношением*, короче *функцией*, если для любого x в R содержится не более одной пары $\langle x, y\rangle$ с первым элементом x. В логической записи R есть функция, если

$$\langle x, y_1\rangle \in R \wedge \langle x, y_2\rangle \in R \Rightarrow y_1 = y_2.$$

Записанное здесь условие называется *условием униформности* (по второй координате). Таким образом, функция есть отношение, униформное по второй координате.

Как для любого отношения, для функции f определяются множества $\mathrm{dom}(f)$ и $\mathrm{rng}(f)$. Множество $\mathrm{dom}(f)$ называется *областью определения* функции f, а множество $\mathrm{rng}(f)$ — *множеством значений* функции f.

Функции иначе называются еще отображениями. Отображение f есть

1) отображение M *на* N, если $M = \mathrm{dom}(f)$, $N = \mathrm{rng}(f)$;

2) отображение M *в* N, если $M = \mathrm{dom}(f)$, $\mathrm{rng}(f) \subseteq N$;

3) отображение *из* M *на* N, если $\mathrm{dom}(f) \subseteq M$, $\mathrm{rng}(f) = N$;

4) отображение *из* M *в* N, если $\mathrm{dom}(f) \subseteq M$, $\mathrm{rng}(f) \subseteq N$.

Отображение типа 1) называется также *сюръекцией* M на N. Единственный предмет y, для которого при данном $x \in \mathrm{dom}(f)$ имеет место $\langle x, y\rangle \in f$, обозначается $f(x)$.

Для любых двух отношений R и S определяется их «композиция»

$$S \circ R \rightleftharpoons \{\langle x, z\rangle \mid \exists y((\langle x, y\rangle \in R) \wedge (\langle y, z\rangle \in S))\}.$$

Упражнение. Докажите, что композиция двух функций есть функция.

Заметьте, что пустое множество также есть функция, «нигде не определенная функция».

Отношение $S^{-1} = \{\langle x, y\rangle \mid \langle y, x\rangle \in S\}$ называется, отношением, *обратным* к отношению S. Отношение, обратное к функции, не всегда является функцией. Если f^{-1} — функция, то функция f называется *обратимой*, или *биекцией*. Называя функции отображениями, говорят в этом случае о *взаимно однозначном* отображении $\mathrm{dom}(f)$ на $\mathrm{rng}(f)$.

Фиксируем натуральное число m. Функцию, область определения которой состоит из упорядоченных последовательностей $\langle x_1, \ldots, x_m\rangle$, называют функцией m переменных и вместо $f(\langle x_1, \ldots, x_m\rangle)$ пишут $f(x_1, \ldots, x_m)$.

Рассмотрим *операции* над множествами, такие как Px, $x \cup y$, $x \cap y$. Нельзя рассматривать знак P в выражении Px (множество всех подмножеств множества x) как знак функции, так же и знак $\cup$ в выражении $x \cup y$ нельзя рассматривать как знак функции двух переменных. Дело в том, что, например, $\{\langle x, y\rangle \mid Px = y\}$ есть уже собственный класс, а не множество. Функция же по определению есть всегда множество.

Однако если ограничить область определения операции множествами, то ограниченная таким образом операция уже является функцией. Так, если M — множество, то $\{\langle x, y\rangle \mid x \in M, Px = y\}$ также есть множество. Это — один из фундаментальных принципов образования множеств, *принцип подстановки*.

4. Замечание. На практике используются иногда термы, не определенные при некоторых значениях переменных. Например, в терме T вида $1/(x^5 + 1982x + 1)$ можно заранее условиться, что x — числовая переменная, но в случае $x^5 + 1982x + 1 = 0$ выражение T не имеет смысла. Для того чтобы решить, при каких x это случится, надо решить уравнение пятой степени.

Если желать, чтобы правила, по которым термы отличаются от «не термов», были просты и эффективно применимы, приходится либо: а) признать существование «бессмысленных» термов, либо: б) приписать подобным термам искусственно какой-либо смысл.

В теории множеств удобно идти именно по второму пути, хотя на первый взгляд он расходится с практикой элементарной алгебры и школьной математикой. А именно, считают, что терм T *всегда* имеет значение, но для $x^5 + 1982x + 1 = 0$ это есть некоторое отдельное, специально выделенное значение, например некоторый формальный символ «бессмысленно». При таком подходе $1/0 = 15$ ложно (так как число 15 не равно символу «бессмысленно»), а формула $\neg(1/0 = 15)$ уже истинна.

§ 5. Математические структуры

1. С конца XIX – начала XX века укоренился обычай излагать концепции каждой специальной математической теории на языке теории множеств.

Например, теория групп изучает *группы*, а каждая группа есть пара $\langle A, * \rangle$, где A есть непустое множество (*элементов* группы), а $*$ есть функция, сопоставляющая каждой паре $\langle a, b \rangle$ элементов множества A некоторый элемент множества A, обозначаемый через $a * b$. При этом операция $*$ удовлетворяет хорошо известным аксиомам группы:

$G1$. $(a * b) * c = a * (b * c)$.

$G2$. Существует элемент $e \in A$, такой, что для всех $a \in A$,

$$a * e = e * a = a.$$

$G3$. Для всякого элемента a существует элемент b такой, что

$$a * b = b * a = e.$$

Аналогично, *кольцо* — это тройка $\langle R, +, \cdot \rangle$, состоящая из непустого множества R и двух функций $+$ и $\cdot$ от двух переменных, отображающих $R \times R$ в R. При этом выполняются следующие требования (здесь $a \cdot b$ мы коротко записываем как ab):

$R1$. $a + b = b + a$.

$R2$. $a + (b + c) = (a + b) + c$.

$R3$. $\forall a \forall b \exists! c(a + c = b)$.

$R4$. $a(bc) = (ab)c$.

$R5$. $a(b + c) = ab + ac$.

$R6$. $(a + b)c = ac + bc$.

Аксиома $R3$ гарантирует нам возможность и единственность вычитания. Знак $\exists!$ заменяет фразу: «существует и единственный». При желании мы могли бы обойтись и знаком $\exists$, например, аксиому $R3$ можно было бы записать в таком виде:

$$\forall a \forall b((0 \exists c(a + c = b)) \wedge \forall c_1 \forall c_2(((a + c_1 = b) \wedge (a + c_2 = b)) \Rightarrow (c_1 = c_2))).$$

Два закона дистрибутивности умножения относительно сложения появились из-за того, что в общем определении кольца не предполагается коммутативность умножения. Примеры некоммутативных колец известны из курса линейной алгебры: таковы кольца квадратных матриц порядка $\geqslant 2$. Интересующие нас далее булевы кольца, впрочем, коммутативны.

Нетрудно вывести из аксиом $R1-R6$, что в кольце существует единственный элемент o (*нуль кольца*), такой что

$$\forall a(a+o=a), \quad \forall a(oa=ao=o).$$

В кольце имеется не более одного элемента e, такого, что

$$\forall a(ae=ea=a).$$

Элемент e называют *единицей* кольца. Бывают кольца и без единицы: например, кольцо всех четных чисел относительно обычного сложения и умножения.

Кольцо называется *полем*, если умножение коммутативно и обладает свойствами группы на множестве элементов, отличных от o.

Приведем некоторые примеры колец.

1) Кольцо **D** из двух элементов $\{0, 1\}$, где операции сложения и умножения выполняются по mod 2:

$$0+0=1+1=0, \quad 0+1=1+0=1, \quad 0\cdot 0=0\cdot 1=1\cdot 0=0, \quad 1\cdot 1=1.$$

Это кольцо является полем.

2) $R=\{0, 1, 2, 3\}$. Операции задаются таблицами

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Из таблицы сложения видно, что операция $+$ коммутативна ($R1$), и поскольку в любом столбце и любой строке каждый элемент встречается ровно один раз, то выполнена аксиома R3. Справедливость остальных аксиом вытекает из того, что элементы нашего кольца складываются и умножаются как остатки от деления на 4 и, следовательно, на них переносятся свойства ассоциативности и дистрибутивности, верные для целых чисел (проверьте!).

3) $R=\{0, 1, i, 1+i\}$. Операции сложения и умножения задаются таблицами

$+$	0	1	i	$1+i$
0	0	1	i	$1+i$
1	1	0	$1+i$	i
i	i	$1+i$	0	1
$1+i$	$1+i$	i	1	0

$\cdot$	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$1+i$
i	0	i	$1+i$	1
$1+i$	0	$1+i$	1	i

Опять-таки видно, что аксиома $R3$ выполнена. Далее, так как в таблице умножения элементов $1, i, l+i$ в каждой строке и столбце встречается по одному разу каждый из этих элементов, то выполнима операция деления на ненулевой элемент. Для проверки остальных аксиом представим

каждый элемент нашего кольца в виде $a + bi$, где a и b равны 0 или 1, имея в виду, что

$$0 + 0 \cdot i = 0, \quad 0 + 1 \cdot i = i, \quad 1 + 0 \cdot i = 1, \quad 1 + 1 \cdot i = 1 + i.$$

Тогда операция сложения получает простое описание; чтобы сложить $a+bi$ и $c + di$, надо совершить сложение по mod 2 коэффициентов

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

Чтобы перемножить $a+bi$ и $c+di$, надо совершить почленное умножение, воспользоваться соотношением $i^2 = 1 + i$, а затем привести подобные члены

$$(a + bi)(c + di) = ac + (bc + ad)i + bdi^2 = (ac + bd) + (bc + ad + bd)i.$$

Упражнение. Пользуясь этими замечаниями, проведите самостоятельно проверку выполнения оставшихся аксиом.

Другой путь проверки выполнения аксиом кольца вытекает из следующего замечания: элементы $0, 1, i, 1 + i$ могут рассматриваться как остатки от деления многочленов от переменной i на многочлен $i^2 + i + 1$, при этом сложение и умножение остатков в точности отвечают нашим операциям в кольце.

Отметим, что полученное кольцо является полем.

4) $R = \{\langle 0, 0\rangle, \langle 1, 0\rangle, \langle 1, 0\rangle, \langle 1, 1\rangle\}$.

Операции сложения и умножения выполняются почленно в соответствии с правилами

$$0 + 0 = 1 + 1 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1,$$

т. е. члены пары $\langle a, b\rangle$ рассматриваются как элементы кольца **D**. В соответствии с этим кольцо R обозначают $\mathbf{D}^2$.

Пример 4) является частным случаем такой общей конструкции новых колец. Пусть дано кольцо $\langle R, +, \cdot\rangle$. Образуем множество R^m всех упорядоченных последовательностей

$$\langle x_1, x_2 \ldots, x_m\rangle$$

длины m элементов из R (сокращенно — «m-ок элементов из R»). Операции сложения и умножения в R^m будем выполнять почленно:

$$\langle x_1, \ldots, x_m\rangle + \langle y_1, \ldots, y_m\rangle = \langle x_1 + y_1, \ldots, x_m + y_m\rangle,$$
$$\langle x_1, \ldots, x_m\rangle \cdot \langle y_1, \ldots, y_m\rangle = \langle x_1 \cdot y_1, \ldots, x_m \cdot y_m\rangle.$$

Легко понять, что получается новое кольцо, которое также обозначается через R^m.

2. Группы и кольца являются примерами *математических структур*. В качестве следующего примера рассмотрим структуру *упорядоченного поля*. Так называется структура вида $\langle R, +, \cdot, <\rangle$, где $\langle R, +, \cdot\rangle$ является полем, а $<$ есть отношение на множестве R, удовлетворяющее следующим *аксиомам строгого упорядочения*:

1) $\neg(a < a)$;
2) $a < b \wedge b < c \Rightarrow a < c$;
3) $a < b \vee a = b \vee b < a$;
4) $a < b \Rightarrow a + c < b + c$;
5) $o < a \wedge b < c \Rightarrow ab < ac$.

Например, множество действительных чисел с естественными операциями и упорядочением образуют структуру упорядоченного поля.

3. Общее определение математической структуры достаточно громоздко.Ограничимся определением *математической структуры первого порядка*. Такая структура представляет собой набор объектов, состоящий:

1) из некоторого конечного запаса основных множеств

$$M_1, \ldots, M_l,$$

причем каждое из множеств M_i непусто;

2) конечного запаса отображений из декартовых произведений M_i в M_j, т. е. отображений вида

$$f\colon M_{i_1} \times \ldots \times M_{i_k} \to M_j;$$

3) конечного запаса отношений на M_i, т. е. конечного запаса подмножеств

$$R \subseteq M_{i_1} \times \ldots \times M_{i_k}.$$

Таким образом, структура первого порядка S имеет вид

$$\langle M_1, \ldots, M_l; f_1, \ldots, f_m; R_1, \ldots, R_n \rangle,$$

где $M_1, \ldots, M_l$ — *основные множества* S; $f_1, \ldots, f_m$ — *операции* S и $R_1, \ldots, R_n$ — отношения S.

Обычно рассматривают целый класс структур, удовлетворяющих одним и тем же условиям. Такой класс образует *род структур*. Например, кольца — это один род структур, группы — другой род структур.

В математической логике условия, определяющие род структур, записывают в виде формул в точных логико-математических языках. Для структур первого порядка с этой целью используются *языки первого порядка*. Математические структуры играют роль *интерпретаций*, *моделей* таких языков.

4. В качестве примера структуры, не являющейся структурой первого порядка, рассмотрим определение *топологического пространства*. Топологическим пространством называется пара $\langle X, T \rangle$, где X — непустое множество, элементы которого называются *точками* топологического пространства. T есть семейство подмножеств X, $T \subseteq P(X)$, элементы которого называются *открытыми подмножествами* X. Само семейство T называется *топологией* пространства $\langle X, T \rangle$. При этом должны выполняться следующие требования:

1) $\varnothing \in T$, $X \in T$;
2) $U_1, U_2 \in S \Rightarrow U_1 \cap U_2 \in S$;
3) для произвольного семейства $\{U_i \mid i \in I\}$ открытых множеств их объединение $\bigcup_i U_i$ также открыто.

Типичным примером топологического пространства является множество действительных чисел, если открытыми множествами считать все возможные объединения открытых интервалов.

§ 6. Булева алгебра

1. Для математической логики особое значение имеют структуры, называемые *булевыми кольцами* и *булевыми решетками*. Эти структуры тесно связаны между собой.

Булевы кольца выделяются из всех других колец двумя дополнительными аксиомами:

$$R7. \quad \exists e \forall a(ae = ea = a),$$

$$BR8. \quad \forall a(aa = a).$$

Аксиома $R7$ есть аксиома существования единицы. Из аксиом $R1$–$R7$ легко выводится, что единица в кольце только одна. Более специфична аксиома $BR8$.

Упражнение. а) Проверьте, что новые аксиомы $R7$ и $BR8$ выполнены в кольце $\mathbf{D}$, так что кольцо $\mathbf{D}$ — булево.

б) Докажите, что если B — булево кольцо, то B^m — также булево кольцо для всякого натурального $m > 0$.

в) Докажите, что булево кольцо $\mathbf{D}^m$ имеет 2^m элементов. Его единица есть m-ка $\langle 1, 1, \ldots, 1\rangle$, а нуль $\langle 0, 0, \ldots, 0\rangle$.

Мы увидим вскоре, что каждое конечное булево кольцо изоморфно какому-либо из колец $\mathbf{D}^m$.

2. С каждым множеством E, состоящим из m элементов, связаны два кольца, изоморфные $\mathbf{D}^m$:

1) кольцо $\mathbf{D}^E$ определенных на E функций со значениями из $\mathbf{D}$;
2) кольцо $P(E)$ всех подмножеств множества E с операциями

$$A + B = (A \cup B) \setminus (A \cap B), \quad A \cdot B = A \cap B.$$

Естественное изоморфное отображение $P(E)$ на $\mathbf{D}^E$ устанавливается, если подмножеству $A \subseteq E$ поставить в соответствие его *характеристическую функцию*

$$\chi_A(x) = \begin{cases} 1, & \text{если} \quad x \in A, \\ 0, & \text{если} \quad x \notin A. \end{cases}$$

Чтобы получить изоморфное отображение $\mathbf{D}^E$ на $\mathbf{D}^m$, расположим элементы E в определенном порядке:

$$e_1, e_2, \ldots, e_m.$$

Функции χ из $\mathbf{D}^E$ поставим в соответствие набор

$$\langle \chi(e_1), \chi(e_2), \ldots, \chi(e_m) \rangle \in \mathbf{D}^m.$$

В кольце $P(E)$ рассматривается унарная операция *взятия дополнения*

$$\overline{A} = E \setminus A = E + A.$$

Очевидно,

$$\overline{\overline{A}} = A, \quad A \cdot \overline{A} = \varnothing.$$

Операцию *объединения* множеств в $P(E)$ можно определить через операции кольца:

$$A \cup B = (A + B) + AB.$$

Свойство $A \subseteq B$ можно записать в виде

$$A \cdot B = A \quad \text{или} \quad A \cup B = B.$$

Отношение включения обладает следующими свойствами:

$$A \subseteq C \wedge B \subseteq C \Rightarrow A + B \subseteq C.$$

Сделаем еще одно замечание. Всякое непустое подмножество A может быть получено как объединение одноэлементных подмножеств множества E. Поскольку объединение непересекающихся множеств совпадает с их суммой

$$\bigcup_{i=1}^{k} A_i = A_1 \cup \ldots \cup A_k = \sum_{i=1}^{k} A_i = A_1 + \ldots + A_k,$$

получаем

$$A = \sum_{a \in A} \{a\}.$$

Заметим, что одноэлементные подмножества $\{a\}$ могут быть определены как минимальные элементы отношения $\subseteq$, т. е. такие подмножества A, что $A \neq \varnothing$ и, кроме того,

$$B \subseteq A \Rightarrow (B = \varnothing) \vee (B = A).$$

3. Описанные нами выше свойства булева кольца подмножеств тривиальны и непосредственно следуют из содержательного смысла введенных операций сложения и умножения. Замечательно то, что все приведенные выше построения можно произвести в любом конечном булевом кольце, опираясь на аксиомы булева кольца. Результатом таких построений явится теорема о том, что всякое конечное булево кольцо устроено как булево кольцо всех подмножеств некоторого конечного множества.

Лемма. *В любом булевом кольце имеют место свойства*

(1) $a + a = o$;

(2) $a + b = o \Rightarrow a = b$;

(3) $a \cdot b = b \cdot a$.

▷ Подставим в $BR8$ вместо a сумму $e+a$ и в левой части раскроем скобки

$$(e+a)\cdot(e+a) = e\cdot e + a\cdot e + e\cdot a + a\cdot a = \\ = e + a + a + a = (e+a) + (a+a) = e + a.$$

Из единственности вычитания $(R3)$ получаем $a + a = o$. Из единственности вычитания из (1) получаем (2). Докажем (3). По $BR8$ имеем

$$(a+b)(a+b) = a + b.$$

Преобразовав левую часть, получим

$$(a+b)(a+b) = a + ba + ab + b = (a+b) + (ba + ab) = a + b,$$

откуда $ba + ab = o$, т. е. в силу (2) $ab = ba$. ◁

Элемент $a+e$ называется *дополнением* к элементу a и обозначается $\bar{a}$. Для дополнений имеем

(4) $\bar{\bar{a}} = a$;

(5) $a + \bar{a} = e$;

(6) $a\bar{a} = o$.

▷
$$a = (\bar{\bar{a}} + e) + e = a + (e + e) = a;$$
$$a + \bar{a} = a + (a + e) = (a + a) + e = e;$$
$$a\bar{a} = a(a + e) = a + a = o.$$ ◁

Введем отношение $\leqslant$, положив

$$a \leqslant b \leftrightharpoons ab = a.$$

Скажем, что $a < b$, если $a \leqslant b$ и $a \neq b$.

(7) $a \leqslant b \wedge b \leqslant c \Rightarrow a \leqslant c$.

▷ Действительно, если $ab = a$, $bc = b$, то

$$ac = (ab)c = a(bc) = ab = a.$$ ◁

Свойство (7) транзитивности отношения $\leqslant$ означает, что отношение $\leqslant$ устанавливает в B «частичный порядок». Легко проверить, что отношение $<$ также транзитивно. Специфическим свойством этого отношения частичного порядка является следующее:

(8) $a \leqslant c \wedge b \leqslant c \Rightarrow a + b \leqslant c$;

(9) $ab \leqslant a$.

▷ Проверим (8). Дано $ac = a$, $bc = b$, тогда $ac + bc = a + b$, т. е. $(a+b)c = a + b$.

Проверим (9). Имеем $(ab)a = (aa)b = ab$. ◁

Минимальные элементы по отношению $\leqslant$ называются *атомами*. Иными словами, элемент $a \in B$, $a \neq o$ называется атомом, если $b \leqslant a \Rightarrow (b = o \vee b = a)$.

Лемма. *Если B — конечное булево кольцо и $b \in B$, $b \neq o$, то существует атом a, $a \leqslant b$.*

▷ Если b — атом, то положим $a = b$. Если b — не атом, то найдется элемент b_1, $b_1 \leqslant b$, $b_1 \neq b$, $b_1 \neq o$, т. е. $o < b_1 < b$.

Если b_1 — атом, то все доказано, если нет, то найдется элемент b_2 такой, что $o < b_2 < b_1$, и т. д. ... Цепочка

$$\ldots b_3 < b_2 < b_1 < b$$

состоит из попарно различных элементов, и так как B конечно, то на некотором шаге последовательность

$$b_k < b_{k-1} < \ldots < b_1 < b$$

обрывается, и элемент $b_k < b$ является атомом. ◁

(10) *Если a_1, a_2 — различные атомы, то*

$$a_1 a_2 = o.$$

▷ Из (9) следует, что $a_1 a_2 \leqslant a_1$, $a_1 a_2 \leqslant a_2$. Если $a_1 a_2 \neq o$, то, поскольку a_1, a_2 — атомы, необходимо $a_1 a_2 = a_1$ и $a_1 a_2 = a_2$, т. е. $a_1 = a_2$, чего не может быть, так как $a_1 \neq a_2$. ◁

4. Теорема. *Всякое конечное булево кольцо изоморфно стандартному булеву кольцу $\mathbf{D}^m$ при подходящем m.*

▷ Пусть B — конечное булево кольцо. Так как множество B конечно, то число всех атомов конечно. Расположим их в определенной последовательности: $a_1, a_2, \ldots, a_m$.

Докажем, что для каждого элемента $b \in B$, $b \neq o$ имеет место представление

$$b = \sum_{a_i \leqslant b} a_i,$$

где сумма берется по всем $i \leqslant m$ таким, что $a_i \leqslant b$. Положим пока $b' = \sum_{a_i \leqslant b} a_i$. Так как $a_i \leqslant b$ для всех членов в сумме b', то согласно (8) $b' \leqslant b$. Пусть $b' \neq b$. По свойству кольца тогда найдется и единственный элемент $d \neq o$ $b' + d = b$. Умножая это равенство на b' и замечая, что $b' \leqslant b$ (что означает $b'b = b'$), получим $b' + b'd = b'$, откуда $b'd = o$. Далее, $bd = (b' + d)d = b'd + dd = d$, т. е. $d \leqslant b$. Так как $d \neq o$, то найдется атом $a \leqslant d$. Ввиду $d \leqslant b$ отсюда следует, что $a \leqslant b$ и, значит, атом a фигурирует в сумме $b' = \sum_{a_i \leqslant b} a_i$. Отсюда $ab' = \sum_{a_i \leqslant b} aa_i = a$ (см. (10)), т. е. $ab' \neq o$. С другой стороны, ввиду того, что $a \leqslant d$, $ab' = (ad)b' = a(db') = ao = o$, и мы приходим к противоречию. Таким образом, $b' = b$, и наше представление установлено.

Заметим теперь, что для каждого элемента $b \in B$ найдутся $\mu_1, \ldots, \mu_m$, где $\mu_i = e$ или $\mu_i = o$ такие, что

$$b = \mu_1 a_1 + \mu_2 a_2 + \ldots + \mu_m a_m.$$

В самом деле, по доказанному $b = \sum_{a_i \leqslant b} a_i$, и достаточно положить $\mu_i = e$ для всех a_i, для которых $a_i \leqslant b$ и $\mu_i = o$ — для остальных a_i.

Теперь отметим, что указанные $\mu_1, \ldots, \mu_m$ находятся по элементу b единственным образом. Действительно, пусть имеем представления

$$b = \mu_1 a_1 + \ldots + \mu_m a_m,$$
$$b = \mu_1' a_1 + \ldots + \mu_m' a_m.$$

Складывая эти равенства, получаем (см. (1))

$$o = (\mu_1 + \mu_1') a_1 + \ldots + (\mu_m + \mu_m') a_m.$$

Далее, умножая на a_i, имеем

$$o = (\mu_i + \mu_i') a_i,$$

откуда $\mu_i + \mu_i' = 0$ или $\mu_i = \mu_i'$ (см. (2)).

Если $b = \mu_1 a_1 + \ldots + \mu_m a_m$ и $b' = \mu_1' a_1 + \ldots + \mu_m' a_m$, то, очевидно,

$$b + b' = (\mu_1 + \mu_1') a_1 + \ldots + (\mu_m + \mu_m') a_m,$$
$$bb' = (\mu_1 \mu_1') a_1 + \ldots + (\mu_m \mu_m') a_m.$$

Определим функцию

$$f(\mu) = \begin{cases} 1, & \text{если} \quad \mu = e, \\ 0, & \text{если} \quad \mu = o, \end{cases}$$

и поставим в соответствие каждому элементу $b = \mu_1 a_1 + \ldots + \mu_m a_m$ кольца B m-ку $\langle f(\mu_1), \ldots, f(\mu_m) \rangle \in \mathbf{D}^m$.

Описанные выше свойства этого соответствия показывают, что оно есть изоморфизм кольца B в $\mathbf{D}^m$. ◁

5. Полученное нами представление конечных булевых колец не обобщается непосредственно на бесконечные кольца. Неверно, что всякое булево кольцо изоморфно кольцу всех подмножеств некоторого множества. Однако верно, что для каждого булева кольца можно подобрать некоторую систему подмножеств (не всех) некоторого множества, которая относительно обычных теоретико-множественных операций образует кольцо, изоморфное исходному. Мы ограничимся схематичным рассмотрением интересного примера такого булева кольца.

Возьмем канторовское множество на отрезке $[0, 1]$ — множество, остающееся от отрезка, если из него выбросить систему интервалов

$$\left(\frac{1}{3}, \frac{2}{3}\right), \quad \left(\frac{1}{9}, \frac{2}{9}\right), \quad \left(\frac{7}{9}, \frac{8}{9}\right), \quad \left(\frac{1}{27}, \frac{2}{27}\right), \quad \left(\frac{7}{27}, \frac{8}{27}\right), \quad \ldots$$

и т. д. Полученное множество, которое мы обозначим K, обладает рядом замечательных свойств. Среди них отметим два: множество K — замкнутое множество действительной прямой (дополнение к открытому множеству, состоящему из объединения описанных выше интервалов и $(-\infty, 0)$, $(1, +\infty)$); множество K имеет мощность континуума.

Выделим в K систему R всех подмножеств, являющихся одновременно открытыми и замкнутыми относительно K. Такие подмножества в K существуют. Например, часть K, лежащая на отрезке $[0, 1/2]$, с одной стороны, замкнута относительно действительной прямой и, следовательно, относительно K. С другой стороны, дополнение к этой части относительно K снова замкнуто в K, так как это есть часть K, лежащая на отрезке $[1/2, 1]$. Следовательно, выделенная часть K является, как говорят, *открыто-замкнутым* подмножеством K. Итак, система R состоит из подмножеств K, которые замкнуты и дополнение относительно которых также замкнуто. Нетрудно проверить, что операции пересечения и симметрической разности не выводят нас из системы R и, следовательно, порождают в R структуру булева кольца.

Понятно, что система R не совпадает с системой всех подмножеств K: например, подмножество, состоящее из одного числа 0, не принадлежит R, так как дополнение этого подмножества в K не замкнуто (справа от 0 в любой близости к 0 имеются точки из K).

В нашем кольце R вообще не существует атомов; ими могли бы быть лишь одноэлементные подмножества K — точки, но они не принадлежат R.

6. С булевыми кольцами тесно связаны *булевы решетки*. По существу, теория булевых колец и теория булевых решеток являются лишь двумя формами изложения одних и тех же математических идей.

Булевой решеткой мы называем множество с тремя операциями

$$\langle B, \cap, \cup, {}^{-} \rangle,$$

где $\cap$ и $\cup$ — бинарные (двуместные) операции, называемые *пересечением* и *объединением* в решетке, $^{-}$ есть унарная (одноместная) операция — *дополнение*. B — непустое множество элементов решетки. При этом выполняются следующие требования:

$A1$. $a \cap b = b \cap a$, $\quad a \cup b = b \cup a$.

$A2$. $a \cap (b \cap c) = (a \cap b) \cap c$, $\quad a \cup (b \cup c) = (a \cup b) \cup c$.

$A3$. $(a \cap b) \cup b = b$, $\quad (a \cup b) \cap b = b$.

$A4$. $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$, $\quad a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$.

$A5$. $(a \cap \bar{a}) \cup b = b$, $\quad (a \cup \bar{a}) \cap b = b$.

Типичным примером булевой решетки является система $P(E)$ всех подмножеств какого-либо множества E с операциями $a \cap b$, $a \cup b$, $\bar{a}$, понимаемыми теоретико-множественно (как теоретико-множественное пересечение, объединение и дополнение соответственно).

Более общо, на некотором множестве E может быть выделено некоторое семейство $S \subseteq P(E)$ (не обязательно всех) подмножеств, замкнутое относительно теоретико-множественных операций пересечения, объединения и дополнения. Последнее означает, что из a, $b \in S$ следует $a \cap b \in S$ и аналогично для других операций. В этом случае S также

является булевой решеткой, ее называют *полем множеств* на E. Так, в п. 5 открыто-замкнутые подмножества составляют поле множеств на K.

Определим булеву решетку из двух элементов $\{0, 1\}$, задав операции следующим образом:

$$a \cap b = \min\{a, b\}, \quad a \cup b = \max\{a, b\}, \quad \bar{a} = 1 - a.$$

Наконец, если дана булева решетка B, то можно образовать решетку B^m, элементы которой суть наборы $\langle a_1, \ldots, a_m \rangle$ с почленными операциями.

7. Приведем некоторые простейшие следствия аксиом булевой решетки. Как легко видеть, система аксиом $A1$–$A5$ симметрична относительно операций $a \cap b$ и $a \cup b$: вместе с каждой аксиомой содержится двойственная аксиома, в которой операции $\cap$ и $\cup$ заменены друг на друга. Такая двойственная система аксиом позволяет доказывать утверждения парами: если мы доказали некоторое утверждение, то совершенно симметрично можно доказать и двойственное утверждение. Практически мы часто будем ограничиваться доказательством лишь одного из двойственных утверждений, оставляя второе читателю.

В любой булевой решетке верно следующее:

(1) $a \cup a = a$;

(2) $a \cap a = a$.

▷ (1) $a \underset{A3}{=} a \cup (a \cap b) \underset{A4}{=} (a \cup a) \cap (a \cup b) \underset{A4}{=}$

$$= (a \cap (a \cap b)) \cup (a \cap (a \cup b)) \underset{A3}{=} a \cup a.$$

Здесь под каждым равенством написано, на основании какой аксиомы оно получено. (2) доказывается симметрично. ◁

(3) $a \cap b = a \Leftrightarrow a \cup b = b$.

▷ Пусть $a \cap b = a$. Ввиду $A3$ и $A1$ имеем $(a \cap b) \cup b = b$. По допущению отсюда следует, что $a \cup b = b$. В обратную сторону доказательство проводится симметрично. ◁

Положим по определению

$$a \leqslant b \leftrightharpoons a \cap b = a,$$

что ввиду (3) равносильно $a \cup b = b$. Следующие три свойства означают, что $\leqslant$ есть *частичный порядок* на булевой решетке

(4) $a \leqslant a$;

(5) $a \leqslant b \wedge b \leqslant c \Rightarrow a \leqslant c$;

(6) $a \leqslant b \wedge b \leqslant a \Rightarrow a = b$.

▷ (4) см. (1).

(5) Дано $a \cap b = a$, и $b \cap c = b$, необходимо показать, что $a \cap c = a$. Но $a \cap c = (a \cap b) \cap c = a \cap b = a$. Мы использовали $A2$.

(6) Ввиду $a \leqslant b$ и $b \leqslant a$ имеем $a = a \cup b$ и $a = a \cap b$. Подставляя в первое из этих равенств вместо a выражение $a \cap b$, получим $a = (a \cap b) \cup b = b$ ввиду $A3$. ◁

Свойства (7)–(12), перечисленные ниже, называются *решеточными свойствами* объединения и пересечения.

(7) $a \leqslant a \cup b$;

(8) $b \leqslant a \cup b$;

(9) $a \leqslant c \wedge b \leqslant c \Rightarrow a \cup b \leqslant c$;

(10) $a \cap b \leqslant a$;

(11) $a \cap b \leqslant b$;

(12) $c \leqslant a \wedge c \leqslant b \Rightarrow c \leqslant a \cap b$.

▷ (7) $a \leqslant a \cup b$ означает, что $a \cap (a \cup b) = a$, и следует из $A3$ и $A1$.

(9) Дано: $a \cup c = c$ и $b \cup c = c$. Поэтому

$$(a \cup c) \cup (b \cup c) = c \cup c = c$$

(см. (1)). Используя $A1$ и $A2$, отсюда имеем $(a \cup b) \cup (c \cup c) = c$, т. е. $(a \cup b) \cup c = c$, что означает $a \cup b \leqslant c$. ◁

(13) $a \cap \bar{a} = b \cap \bar{b}$;

(14) $a \cup \bar{a} = b \cup \bar{b}$.

▷ (13) Аксиома $A5$ имеет вид $a \cap \bar{a} \leqslant b$. Заменяя b на $b \cap \bar{b}$, получим $a \cap \bar{a} \leqslant b \cap \bar{b}$. Так как a и b произвольны, то $a \cap \bar{a} = b \cap \bar{b}$. ◁

Ввиду (13) и (14) элементы $a \cap \bar{a}$ и $a \cup \bar{a}$ не зависят от выбора a. Определим «нуль» решетки $o = a \cap \bar{a}$ и «единицу» решетки $e = a \cup \bar{a}$. Из определения и ввиду $A5$:

(15) $o = a \cap \bar{a}$;

(16) $e = a \cup \bar{a}$;

(17) $o \leqslant a$;

(18) $a \leqslant e$.

Таким образом, o — наименьший, а e — наибольший элементы в решетке. Далее,

(19) $a \cup o = a, \quad a \cap o = o$;

(20) $a \cup e = e, \quad a \cap e = a$.

Важная характеристика дополнения определяется следующим свойством:

(21) $a \cap c = o \wedge a \cup c = e \Rightarrow c = \bar{a}$.

▷ $c = o \cup c \underset{(19)}{=} (a \cap \bar{a}) \cup c \underset{(15)}{=} (a \cup c) \cap (\bar{a} \cup c) \underset{A4}{=} e \cap (\bar{a} \cup c) \underset{(20)}{=} \bar{a} \cup c,$

т. е. $\bar{a} \leqslant c$.

$c = e \cap c \underset{(20)}{=} (a \cup \bar{a}) \cap c \underset{A4}{=} (a \cap c) \cup (\bar{a} \cap c) = o \cup (\bar{a} \cap c) \underset{(19)}{=} \bar{a} \cap c,$

т. е. $c \leqslant \bar{a}$. ◁

(22) $a = \bar{\bar{a}}$.

▷ Подставим в (21) вместо a элемент $\bar{a}$ и вместо c элемент a. Тогда ввиду (15) и (16) имеем $a = \bar{\bar{a}}$. ◁

Следующие два равенства называются *законами де Моргана*:

(23) $\overline{a \cup b} = \bar{a} \cap \bar{b}$;

(24) $\overline{a \cap b} = \bar{a} \cup \bar{b}$.

▷ (23) Используем (21). Пусть $c = \bar{a} \cap \bar{b}$, тогда $(a \cup b) \cap c = (a \cup b) \cap (\bar{a} \cap \bar{b}) = (a \cap \bar{a} \cap \bar{b}) \cup (b \cap \bar{a} \cap \bar{b}) = o \cup o = o$. Далее, $(a \cup b) \cup c = (a \cup b) \cup (\bar{a} \cap \bar{b}) = (a \cup b \cup \bar{a}) \cap (a \cup b \cup \bar{b}) = e \cap e = e$. ◁

Следующая эквивалентность называется *законом контрапозиции*:

(25) $a \leqslant b \Leftrightarrow \bar{b} \leqslant \bar{a}$.

▷ Пусть $a \leqslant b$, т. е. $a \cup b = b$, тогда $\overline{a \cup b} = \bar{b}$, т. е. (см. (23)) $\bar{a} \cap \bar{b} = \bar{b}$, что означает $\bar{b} \leqslant \bar{a}$. Обратно, если $\bar{b} \leqslant \bar{a}$, то $\bar{a} \cap \bar{b} = \bar{b}$, тогда $\overline{\bar{a} \cap \bar{b}} = \bar{b}$ и ввиду (24) и (22) $a \cup b = b$, т. е. $a \leqslant b$. ◁

(26) $\bar{o} = e$, $\bar{e} = o$.

▷ $\bar{o} \underset{(15)}{=} \overline{a \cap \bar{a}} \underset{(24)}{=} \bar{a} \cup \bar{\bar{a}} \underset{(22)}{=} a \cup \bar{a} = e.$ ◁

Определим *разность* двух элементов

$$a \setminus b \leftrightharpoons a \cap \bar{b}.$$

Упражнение. Докажите, что $a \leqslant b \Leftrightarrow a \setminus b = o$.

8. Укажем теперь на связь между булевыми кольцами и булевыми решетками.

Если дано булево кольцо $\langle B, +, \cdot \rangle$ то можно определить булеву решетку $\langle B, \cap, \cup, \bar{} \rangle$, положив $a \cap b = ab$, $a \cup b = a + b + ab$, $\bar{a} = a + e$. Следует, конечно, проверить, что это действительно булева решетка, т. е. что выполняются аксиомы $A1$–$A5$. Проверим, например, $A4$:

$a \cup (b \cap c) = a + bc + abc$;

$(a \cup b) \cap (a \cup c) = (a + b + ab)(a + c + ac) =$

$= a + ab + ab + ac + bc + abc + ac + abc + abc = a + bc + abc.$

Обратно, если дана булева решетка $\langle B, \cup, \cap, \bar{} \rangle$, то можно определить булево кольцо $\langle B, +, \cdot \rangle$, положив $a + b = (a \cup b) \setminus (a \cap b)$, $ab = a \cap b$.

Например, аксиома $BR8$ в п. 1 следует из (2) п. 7. Проверка остальных аксиом предоставляется читателю.

Важно отметить, что описанное соответствие между кольцами и решетками взаимно-обратно. Так, если по данной булевой решетке образовать кольцо, а затем по кольцу вновь образовать решетку, то мы получим не что иное, как первоначальную решетку.

Таким образом, между булевыми кольцами и булевыми решетками имеется каноническое взаимно однозначное соответствие. Мы имеем, по сути дела, одну теорию — *булеву алгебру.*

9. Рассмотрим булево кольцо $\mathbf{F}_n$ функций

$$f(x_1, \ldots, x_n)$$

от n переменных $x_1, \ldots, x_n \in \mathbf{D}$ со значениями из $\mathbf{D}$, так называемых *булевых функций.*

Упражнение. Сколько элементов в $\mathbf{F}_n$?

Пользуясь операциями сложения и умножения в кольце $\mathbf{D}$, можно представить такую функцию по *формуле Лагранжа* в виде

$$f(x_1, \ldots, x_n) = \sum_{a_1, a_2, \ldots, a_n} f(a_1, \ldots, a_n) \prod_{k=1}^{n} (x_k + a_k + 1), \qquad (1)$$

где суммирование ведется по всем наборам $a_1, \ldots, a_n$ из нулей и единиц, т. е. по всем элементам кольца $\mathbf{D}^n$. Для доказательства достаточно заметить, что произведение

$$\delta_{a_1, \ldots, a_n}(x_1, \ldots, x_n) = \prod_{k=1}^{n} (x_k + a_k + 1), \qquad (2)$$

рассматриваемое как функция от $x_1, \ldots, x_n$, равно единице только при $x_1 = a_1$, $x_2 = a_2$, $\ldots$, $x_n = a_n$. В остальных же случаях это произведение равно нулю.

Положив

$$x^a = x \quad \text{при } a = 1, \quad x^a = \bar{x} = x + 1 \quad \text{при } a = 0,$$

запишем произведение (2) в виде

$$\delta'_{a_1, \ldots, a_n}(x_1, \ldots, x_n) = x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}.$$

На языке булевых решеток $\delta_{a_1, \ldots, a_n}$ есть конъюнкция, в которую каждое x_k входит либо само, либо в виде $\bar{x}_k$ ровно один раз.

Так как различные произведения δ и δ' таковы, что $\delta\delta' = 0$, то в формуле (1) кольцевую сумму Σ можно заменить на булево объединение $\cup$. Мы получаем представление произвольной булевой функции в так называемой *совершенной дизъюнктивной нормальной форме*

$$f(x_1, \ldots, x_n) = \bigcup_{a_1, \ldots, a_n} f(a_1, \ldots, a_n) x_1^{a_1} \ldots x_n^{a_n}.$$

Если f не равна тождественно нулю, то это выражение можно записать в виде

$$f(x_1, \ldots, x_n) = \bigcup_{f(a_1,\ldots,a_n)=1} x_1^{a_1} \ldots x_n^{a_n},$$

где суммирование распространяется на все наборы $a_1, \ldots, a_n$, для которых $f(a_1, \ldots, a_n) = 1$.

Имеет место и двойственное представление в булевой решетке произвольной булевой функции в *совершенной конъюнктивной нормальной форме*. Если функция не равна тождественно единице, то

$$f(x_1, \ldots, x_n) = \bigcap_{f(a_1,\ldots,a_n)=0} (x_1^{\bar{a}_1} \cup \ldots \cup x_n^{\bar{a}_n}).$$

§ 7. Логика высказываний

1. Будем считать, что большие латинские буквы обозначают высказывания. Нам уже знакомы операции, которые, будучи применены к одному или двум высказываниям, доставляют новые высказывания. Из высказывания A можно образовать отрицание этого высказывания

$$\neg A.$$

Из двух высказываний A и B — их конъюнкцию $A \wedge B$ и их дизъюнкцию $A \vee B$ и т. д. Нас будут занимать только такие операции над высказываниями F, для которых истинностное значение $F(A_1, \ldots, A_n)$ полностью определяется истинностными значениями $A_1, \ldots, A_n$:

$$|F(A_1, \ldots, A_n)| = f(|A_1|, \ldots, |A_n|).$$

Операции F с одной и той же булевой функцией f равносильны. Операции над высказываниями нас интересуют лишь «с точностью до равносильности». Поэтому классификация операций над высказываниями «с точностью до равносильности» совпадает с классификацией соответствующих булевых функций $f(a_1, \ldots, a_n)$, отображающих $\mathbf{D}^n$ в $\mathbf{D}$.

Имеется четыре попарно не равносильных операции над одним высказыванием:

$$F_1(A) \Leftrightarrow A \wedge \neg A, \qquad F_2(A) \Leftrightarrow A,$$
$$F_3(A) \Leftrightarrow \neg A, \qquad F_4(A) \Leftrightarrow A \vee \neg A$$

и шестнадцать попарно не равносильных операций над двумя высказываниями:

$F_5(A, B) \Leftrightarrow A \wedge \neg A$, $F_6(A, B) \Leftrightarrow A \wedge B$,
$F_7 \Leftrightarrow A \wedge \neg B$, $F_8 \Leftrightarrow \neg A \wedge B$,
$F_9 \Leftrightarrow \neg A \wedge \neg B$, $F_{10} \Leftrightarrow A$,
$F_{11} \Leftrightarrow B$, $F_{12} \Leftrightarrow \neg A$,
$F_{13} \Leftrightarrow \neg B$, $F_{14} \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$,
$F_{15} \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge \neg B)$, $F_{16} \Leftrightarrow A \vee B$,
$F_{17} \Leftrightarrow A \vee \neg B$, $F_{18} \Leftrightarrow \neg A \vee B$,
$F_{19} \Leftrightarrow \neg A \vee \neg B$, $F_{20} \Leftrightarrow A \vee \neg A$.

Все перечисленные операции мы выразили через три: отрицание, конъюнкцию и дизъюнкцию. Через эти три операции выражаются и все n-местные операции над высказываниями при любом n (например, в дизъюнктивной нормальной форме, которая соответствует указанной в § 6 форме записи булевых функций).

Так как

$$A \wedge B \Leftrightarrow \neg(\neg A \vee \neg B), \quad A \vee B \Leftrightarrow \neg(\neg A \wedge \neg B),$$

можно было бы пользоваться только наборами операций $\neg$, $\vee$ или $\neg$, $\wedge$. Это примеры *базисов* для системы операций логики высказываний. Любопытно, что существуют базисы, состоящие только из одной двуместной операции. Для этого пригодны операция

$$A \uparrow B \leftrightharpoons \neg A \wedge \neg B \Leftrightarrow F_9(A, B)$$

или двойственная ей операция

$$A \mid B \leftrightharpoons \neg A \vee \neg B \Leftrightarrow F_{19}(A, B).$$

Например, через $\uparrow$ отрицание и конъюнкция выражаются так:

$$\neg A \Leftrightarrow A \uparrow A, \quad A \wedge B \Leftrightarrow (A \uparrow A) \uparrow (B \uparrow B).$$

Представляет интерес еще базис $\neg$, $\Rightarrow$, где известная вам операция $\Rightarrow$ импликации есть

$$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B) \Leftrightarrow F_{18}(A, B).$$

В этом базисе конъюнкция и дизъюнкция выражаются так:

$$A \vee B \Leftrightarrow (\neg A \Rightarrow B), \quad A \wedge B \Leftrightarrow \neg(A \Rightarrow \neg B).$$

2. Будем считать буквы $P, Q, R, \ldots$ переменными, область значений которых состоит из всевозможных высказываний. Такие переменные называются *пропозициональными*.

Формулы *логики высказываний* (*пропозициональные формулы*) строятся из пропозициональных переменных с помощью формальных символов — скобок и знаков, обозначающих операции над высказываниями. Мы используем следующие знаки:

$\wedge$ — «конъюнкция», операция F_6, «и»;

$\vee$ — «дизъюнкция», F_{16}, «или»;

$\supset$ — «импликация», F_{18}, «если..., то»;

$\neg$ — «отрицание», одноместная операция F_3, «не».

Пропозициональные формулы строятся начиная с пропозициональных переменных с помощью следующего порождающего правила: если A и B суть уже построенные формулы логики высказываний, то можно построить новые формулы

$$(A \wedge B), \quad (A \vee B), \quad (A \supset B), \quad \neg A.$$

Применяя последовательно это правило, можно строить различные строчки символов — формулы. Например, формулами логики высказываний являются выражения

$$((P \supset Q) \supset ((P \supset (Q \supset R)) \supset (P \supset R))), \quad (P \supset (Q \supset (P \wedge Q))).$$

Заметим, что в формулах знаки $\vee$ $\supset$ $\wedge$ и т. п. суть просто символы, а не обозначения результата действия соответствующих операций. Чтобы подчеркнуть это, мы используем формальный знак $\supset$ вместо $\Rightarrow$. Знак $\supset$ следует воспринимать как букву, символ, а $A \Rightarrow B$ есть сокращенное обозначение для выражения на русском языке «если верно A, то B». Остальные логические знаки мы используем и формально, и для содержательных сообщений, но это не должно вести к недоразумениям.

Подобным образом, $(A \equiv B)$ есть сокращенное обозначение для формулы $((A \supset B) \wedge (B \supset A))$, в то время как $A \Leftrightarrow B$ есть сокращение для высказывания на русском языке «A тогда и только тогда, когда B».

Сама по себе пропозициональная формула не истинна и не ложна, это просто строчка символов, но если вместо ее пропозициональных переменных подставить конкретные высказывания, то естественно определяется конкретное высказывание, получающееся, если выполнить над высказываниями указанные операции.

Таким образом, каждой формуле логики высказываний $F(P_1, \ldots, P_n)$ от пропозициональных переменных $P_1, \ldots, P_n$ соответствует булева функция $f(x_1, \ldots, x_n)$ кольца $\mathbf{F}_n$.

Упражнение. Каким из двуместных операций F_5–F_{20} соответствуют формулы

a) $((P \wedge Q) \supset (P \vee Q))$,

b) $((\neg P \vee Q) \supset \neg Q)$?

Формула $F(P_1, \ldots, P_n)$ называется *тавтологией* (*пропозициональной тавтологией*, *общезначимой формулой*, *логическим законом*), если она становится истинной при подстановке любых конкретных высказываний вместо $P_1, \ldots, P_n$, т. е. если этой формуле соответствует булева функция из $\mathbf{F}_n$, тождественно равная единице.

Примеры тавтологий:

$A \vee \neg A$ (закон исключенного третьего),

$\neg\neg A \equiv A$ (закон двойного отрицания),

$\neg(A \wedge \neg A)$ (закон противоречия),

$(\neg A \supset B) \wedge (\neg A \supset \neg B) \supset A$.

Последняя из тавтологий служит основанием для проведения доказательств от противного: если отрицание A приводит к противоречию, то A верно.

Чтобы убедиться, что формула $F(P_1, \ldots, P_n)$ является тавтологией, достаточно проделать довольно громоздкую, но всегда выполнимую процедуру вычисления соответствующей функции $f(x_1, \ldots, x_n)$ для всевозможных наборов значений переменных. Таким образом, всегда можно эффективно установить, является ли данная формула тавтологией или нет.

Две формулы F и G *равносильны* или *логически эквивалентны*, если формула $(F \equiv G)$ является тавтологией. Иными словами, если F и G рассматривать как задающие булевы функции от одних и тех же переменных, то F и G задают одну и ту же функцию.

Существует несколько «нормальных форм» формул логики высказываний. Упомянем о *совершенной дизъюнктивной нормальной форме*, которая вполне аналогична установленной в § 6 для булевых функций.

Для пропозициональных переменных $P_1, \ldots, P_n$ будем называть *совершенным конъюнктивным членом* конъюнкцию $A_1 \wedge \ldots \wedge A_n$, в которой A_i есть P_i или $\neg P_i$. Формула $F(P_1, \ldots, P_n)$ имеет дизъюнктивную совершенную нормальную форму, если она имеет вид дизъюнкции $G_1 \vee \ldots \vee G_m$, где каждое G_j является совершенным конъюнктивным членом переменных $P_1, \ldots, P_n$.

Имеет место

Теорема. *Любая не тождественно ложная формула логики высказываний равносильна формуле в совершенной дизъюнктивной нормальной форме.*

▷ Для доказательства следует, например, рассмотреть булеву функцию, соответствующую данной формуле. Затем булеву функцию привести к совершенной дизъюнктивной нормальной форме согласно п. 9 § 6 и написать формулу по полученному представлению. ◁

§ 8. Исчисление высказываний

1. На примере логики высказываний познакомимся с приемами строгой формализации математических теорий.

При формализации математической теории полностью отвлекаются от ее содержания. Теоремы воспринимаются просто как формулы, которые могут быть выведены по определенным правилам. Поэтому формальные теории иначе называют *исчислениями*. О знаках и формулах исчисления приходится, однако, рассуждать содержательно: рядом

с формальной теорией возникает *метатеория*, которая тоже пользуется некоторыми обозначениями. Эти обозначения метатеории следует строго отличать от знаков и формул, относящихся к собственно формальной теории. Формализация логики высказываний, превращение ее в «исчисление высказываний» сама по себе не очень интересна, так как после сведения логики высказываний к вычислениям с истинностными значениями мы и так находимся в сфере рассуждений о конечных объектах весьма простой природы. Однако с ней полезно познакомиться, как с первым важным примером формальной аксиоматической теории.

Существует много вариантов формализации логики высказываний. Мы опишем один из них; назовем его «теория L».

Формализация всякой содержательной теории начинается с выбора символов формальной теории, *языка теории*. Основные символы теории L суть:

1) пропозициональные буквы $P_1, \ldots, P_n, \ldots$,
2) логические связки $\wedge$, $\vee$, $\supset$, $\neg$,
3) скобки $($, $)$.

Как уже было сказано, кроме знаков самой теории L, мы будем пользоваться символами, относящимися к метатеории.

Для обозначения произвольной пропозициональной буквы мы будем употреблять знаки $P, Q, R, P_1, Q_1, \ldots$. Дальнейшие соглашения и обозначения метатеории будут появляться по мере необходимости.

После того как выбраны основные символы теории, выделяют некоторые их комбинации, которые называют *формулами*. Формулы определяются индуктивно с помощью следующих ниже двух пунктов. Первый из этих пунктов является базисом индукции. В нем непосредственно сообщается, какие комбинации символов следует считать формулами. Второй пункт представляет собой порождающее правило. Предполагается, что все формулы L построены из формул пункта 1) с помощью последовательного применения правила 2). Итак:

1) Пропозициональные буквы суть формулы L.
2) Если A и B — формулы, то формулами являются и следующие комбинации символов:

$$(A \wedge B), \quad (A \vee B), \quad (A \supset B), \quad \neg A.$$

Некоторые из формул теории называются *аксиомами*. В теории L их десять:

1) $(P_1 \supset (P_2 \supset P_1))$,
2) $((P_1 \supset (P_2 \supset P_3)) \supset ((P_1 \supset P_2) \supset (P_1 \supset P_3)))$,
3) $((P_1 \wedge P_2) \supset P_1)$,
4) $((P_1 \wedge P_2) \supset P_2)$,
5) $(P_1 \supset (P_2 \supset (P_1 \wedge P_2)))$,
6) $(P_1 \supset (P_1 \vee P_2))$,

7) $(P_2 \supset (P_1 \vee P_2))$,
8) $((P_1 \supset P_3) \supset ((P_2 \supset P_3) \supset ((P_1 \vee P_2) \supset P_3)))$,
9) $((P_1 \supset P_2) \supset ((P_1 \supset \neg P_2) \supset \neg P_1))$,
10) $(\neg\neg P_1 \supset P_1)$.

Здесь P_1, P_2, P_3 — конкретные пропозициональные переменные, так что 1)–10) есть список из десяти конкретных формул языка L.

Далее принимаются правила вывода, применяя которые можно из уже установленных теорем получать новые. В теории L — два таких правила вывода.

Первое правило имеет вид

$$(MP)\frac{A,\ A \supset B}{B}.$$

Это правило, называемое modus ponens, утверждает, что если формулы A и $A \supset B$ установлены как теоремы, то формула B также является теоремой.

Второе правило имеет вид

$$(S)\frac{A}{A(Q_1, \ldots, Q_m \parallel B_1, \ldots, B_m)}.$$

Здесь $A, B_1, \ldots, B_m$ суть формулы, $Q_1, \ldots, Q_m$ — попарно различные пропозициональные буквы. Через $A(Q_1, \ldots, Q_m \parallel B_1, \ldots, B_m)$ мы обозначим результат одновременного замещения всех вхождений букв $Q_1, \ldots, Q_m$ в A на формулы $B_1, \ldots, B_m$ соответственно. Следует заметить, что это *правило подстановки* (S) можно применять и к пропозициональным буквам Q_i, которые вовсе не входят в A. В этом случае соответствующее B_i никуда не подставляется и просто не играет никакой роли.

2. Перейдем теперь к описанию того, что есть *теорема*, или иначе, *выводимая формула* теории L.

Выводом назовем любую конечную последовательность формул

$$A_1, A_2, \ldots, A_n,$$

такую, что каждая формула этой последовательности есть либо аксиома, либо совпадает с какой-либо предыдущей, либо получается из каких-то предыдущих с помощью одного из правил вывода. Скажем, что вывод $A_1, \ldots, A_n$ является выводом своей последней формулы A_n и формулу A_n назовем *выводимой*, или, что то же самое, *теоремой* теории. Будем записывать это в виде:

$$L \vdash A \quad \text{или просто} \quad \vdash A.$$

В дальнейшем мы будем употреблять сокращенный вывод, когда в качестве A_i могут стоять теоремы теории L, полученные раньше, имея

в виду, что мы всегда можем дополнить вывод, вставляя недостающие его отрезки.

Рассмотрим для примера вывод в теории L теоремы $(A \supset A)$.

Возьмем в качестве первой формулы A_1 вывода аксиому 2). Применим к ней правило подстановки в виде

$$(P_1, P_2, P_3 \parallel A, (A \supset A), A).$$

Получим

(а) $\vdash ((A \supset ((A \supset A) \supset A)) \supset ((A \supset (A \supset A)) \supset (A \supset A)))$.

Из аксиомы 1) подстановкой $(P_1, P_2 \parallel A, (A \supset A))$ получаем

(б) $\vdash (A \supset ((A \supset A) \supset A))$.

Применим правило (MP) к (а) и (б):

(в) $\vdash ((A \supset (A \supset A)) \supset (A \supset A))$.

Из аксиомы 1) подстановкой $(P_1, P_2 \parallel A, A)$ получаем

(г) $\vdash (A \supset (A \supset A))$.

Применяя MP к (в) и (г), окончательно получим

(д) $\vdash (A \supset A)$.

3. Напомним, что теорию L мы строили как формальный аналог содержательного исчисления высказываний. В соответствии с этим нам хотелось бы, чтобы все теоремы теории L при содержательном толковании давали «истинные» утверждения логики высказываний, т. е. тавтологии. Это действительно так. Покажем сначала, что всякая выводимая формула теории L при нашей интерпретации есть тавтология. Для этого надо проверить, что аксиомы 1)–10) — тавтологии; такая проверка проводится элементарно построением таблиц истинности. Далее, всякая выводимая формула A является конечной формулой некоторого вывода

$$A_1, \ldots, A_n (= A).$$

Вспомнив определение вывода, убеждаемся, что достаточно проверить, что правила вывода (MP) и (S), примененные к тавтологиям, снова дают тавтологии. Такая проверка также тривиальна. Таким образом, всякая выводимая формула — тавтология.

Замечательно, что имеет место и обратное утверждение: всякая тавтология выводится в теории L. Мы не будем здесь останавливаться на доказательстве этого утверждения. В следующей нашей книге будет доказана гораздо более глубокая теорема о полноте исчисления предикатов. Метод доказательства этой теоремы непосредственно приложим и к теории L, которая является частью исчисления предикатов.

Из изложенных результатов вытекает, что формальная теория L *непротиворечива* в следующем смысле: не найдется формулы такой, что и она сама и ее отрицание выводимы. В самом деле, если A выводима, то она является тавтологией, то же верно для $\neg A$. С другой стороны, если одна из формул A или $\neg A$ — тавтология, то вторая необходимо является противоречием, что и доказывает наше утверждение. Наша теория L

также оказывается *полной* в следующем смысле: если к числу аксиом теории L присоединить какую-либо невыводимую формулу, то теория станет противоречивой (в описанном выше смысле). Докажем это.

Пусть $F(P_1, \ldots, P_n)$ — невыводимая в L формула. Тогда F — не тавтология, и, следовательно, существует набор $\varepsilon_1, \ldots, \varepsilon_n$ нулей и единиц, такой, что на этом наборе F имеет значение нуль. Для каждого ε_i выберем формулу B_i следующим образом: если $\varepsilon_i = 1$, то B_i есть $C \vee \neg C$, если же $\varepsilon_i = 0$, то B_i есть $C \wedge \neg C$. Здесь C — некоторая фиксированная формула. Формула $F(B_1, \ldots, B_n)$ принимает значение 0 уже при любых значениях переменных, и, значит, формула $\neg F(B_1, \ldots, B_n)$ есть тавтология и, следовательно, $\vdash \neg F(B_1, \ldots, B_n)$. Если же к L присоединить в качестве аксиомы формулу $F(P_1, \ldots, P_n)$, то по правилу подстановки S из нее можно вывести формулу $F(B_1, \ldots, B_n)$ и получить, таким образом, противоречие в расширенной теории.

§ 9. О логике предикатов

1. Язык логики предикатов является расширением языка логики высказываний. Теперь мы употребляем два набора исходных символов. Это, прежде всего, *индивидные* (или *предметные*) переменные $u_1, u_2, \ldots$, которые мы обозначаем через $x, y, z, \ldots$, и, кроме того, *предикатные буквы* вида P_j^i, где $i, j = 0, 1, 2, \ldots$. Буква P_j^i называется i-местной (i-арной) предикатной буквой. Нульместные предикатные буквы назовем *пропозициональными*. Предикатные буквы обозначаем через $P, Q, R, \ldots$.

Формулы логики предикатов определяются индуктивно с помощью следующих ниже трех пунктов. Первый пункт — базис этой индукции, а остальные — порождающие правила.

1) Всякая пропозициональная буква есть формула; если P есть n-местная предикатная буква, $n > 0$, и $x_1, \ldots, x_n$ — индивидные переменные, то $P(x_1, \ldots, x_n)$ есть формула.
2) Если A и B — формулы, то формулами являются и следующие комбинации символов:
$$(A \wedge B), \quad (A \vee B), \quad (A \supset B), \quad \neg A.$$
3) Если A — формула и x — индивидная переменная, то $\forall x A$ и $\exists x A$ суть формулы.

Все формулы строятся из формул вида 1) с помощью последовательного применения правил 2) и 3). Например, формулой является выражение
$$(\exists u_1 P_1^2(u_1, u_2) \supset P_1^1(u_2)),$$
которое, используя метаобозначения, будем записывать (опуская также внешние скобки) как
$$\exists x P(x, y) \supset Q(y).$$

Вхождение предметной переменной x в формулу A может быть *свободным* или *связанным*.

1) В формулу $P(x_1, \ldots, x_n)$ переменные $x_1, \ldots, x_n$ входят свободным образом.
2) Свободное вхождение переменной x в формулы A и B остается свободным и в формулах $(A \wedge B)$, $(A \vee B)$, $(A \supset B)$, $\neg A$, $\forall y A$, $\exists y A$, если переменная y отлична от x.
3) Свободное вхождение переменной x в формулу A делается связанным в формулах $\forall x A$, $\exists x A$.
4) Связанные вхождения в A и B остаются связанными в формулах

$$(A \wedge B), \quad (A \vee B), \quad (A \supset B), \quad \neg A, \quad \forall x A, \quad \exists x A.$$

Формула называется *замкнутой*, или *предложением*, если в ней нет свободных вхождений предметных переменных.

Одна и та же переменная может входить в формулу в разных местах и свободно, и связанно. Если переменная входит свободно (хоть один раз) в формулу, она называется *параметром* формулы. Предложения суть формулы, не содержащие параметров.

2. Формула логики предикатов получает определенную *интерпретацию*, если указано непустое множество M и заданы истинностные значения каждого из входящих в формулу предикатных символов как функций (со значениями 0 и 1) от элементов M:

$$|P(y_1, \ldots, y_n)| = f(y_1, \ldots, y_n),$$

где $f\colon M^n \to \mathbf{D}$.

Если задана интерпретация формулы, то можно вычислить и ее истинностное значение как функцию от параметров индукцией по построению формулы. При этом значения кванторов вычисляются следующим образом:

$$|\forall x A(x, y_1, \ldots, y_n)| = \min_{x \in M} |A(x, y_1, \ldots, y_n)|,$$

$$|\exists x A(x, y_1, \ldots, y_n)| = \max_{x \in M} |A(x, y_1, \ldots, y_n)|.$$

При данной интерпретации замкнутая формула имеет определенное истинностное значение.

Как и в логике высказываний, особый интерес представляют *общезначимые формулы* (*тождества*, *логические законы*), истинностное значение которых равно единице в любой интерпретации (в случае незамкнутых формул надо еще добавить: при подстановке любых значений свободно входящих переменных из множества M).

Читатель должен владеть достаточно богатым запасом тождеств логики предикатов и уметь их обосновывать при помощи содержательных теоретико-множественных соображений. Ряд таких формул появится в гл. II.

Формула, ложная в любой интерпретации, называется *противоречием*. Если формула не является противоречием, то она *выполнима*: ее истинностное значение равно единице хотя бы при одной интерпретации (и, для незамкнутых формул, при каком-либо наборе значений свободных переменных).

Рассмотрим в виде примера такую формулу:

$$\forall x \neg P(x, x) \wedge \forall x \forall y \forall z \big(P(x, y) \wedge P(y, z) \supset P(x, z)\big) \wedge \forall x \exists y P(x, y).$$

Эта формула выполнима, так как она истинна в интерпретации, где множество M есть множество натуральных чисел, а предикат $P(x, y)$ интерпретируется как $x < y$.

Вместе с тем эта формула не может быть выполнима ни на каком конечном множестве M. В самом деле, из истинности формулы в M следует существование последовательности $a_1, a_2, \ldots, a_n, \ldots$ элементов M, для которых $P(a_i, a_j)$ при $i < j$, но $\neg P(a_i, a_j)$, если $a_i = a_j$, так что все элементы a_i различны.

Можно показать, что из выполнимости формулы в некоторой интерпретации следует ее выполнимость и в счетной интерпретации, так что для решения вопросов об общезначимости или выполнимости формул исчисления предикатов нет необходимости выходить за пределы интерпретаций с конечными или счетными множествами M.

3. Можно формализовать теорию общезначимых формул логики предикатов и получить *исчисление предикатов*, аналогичное исчислению высказываний. Оказывается, что такое исчисление также будет полным: всякая общезначимая формула будет в нем выводима. Аккуратному изложению этого круга вопросов посвящены следующие главы.

Глава II

Логико-математические языки. Логические законы

§ 1. Язык первого порядка. Формулы и термы

Теперь мы дадим точные определения ряда понятий, о которых шла речь в первой части.

При исследовании некоторой математической теории общий подход состоит в том, что следует, прежде всего, фиксировать *логико-математический язык*, формулы которого будут выражать суждения и отношения рассматриваемой теории. Начнем с изучения самого распространенного вида логико-математических языков — *языков первого порядка* (*языков первой ступени*).

1. Язык первого порядка задается набором из четырех множеств

$$\Omega = \langle \mathrm{Srt}, \mathrm{Cnst}, \mathrm{Fn}, \mathrm{Pr} \rangle$$

(этот набор из четырех множеств иногда называется *сигнатурой* языка Ω, мы будем отождествлять язык с его сигнатурой).

Здесь

1) Srt — непустое множество, элементы которого называются *сортами объектов* (*сортами индивидов*, или просто *сортами*). Для каждого сорта $\pi \in \mathrm{Srt}$ мы фиксируем счетный набор символов $u_1^\pi, u_2^\pi, \ldots, u_n^\pi, \ldots$. Эти символы называются *переменными сорта* π, или *предметными* (*индивидными*) *переменными сорта* π. Переменные (произвольного сорта) мы будем обозначать через $x, y, z, \ldots$, иногда указывая их сорт $x^\pi, y^\pi, z^\pi, \ldots$. Разумеется, мы считаем, что переменные как символы отличаются от других символов языка. В частности, любые две переменные различных сортов различны. С каждой переменной x языка фиксированным образом связан определенный сорт языка.

Наиболее часто встречаются языки с одним-единственным сортом, *односортные* языки. В этом случае множество Srt состоит из единственного элемента.

2) Cnst — множество (может быть, и пустое) *констант* языка Ω (в другой терминологии — *предметных констант*, *индивидных констант*,

индивидных символов). Каждой константе $c \in \mathrm{Cnst}$ языка приписан определенный сорт $\pi \in \mathrm{Srt}$. Константы различных сортов различны.

3) Fn — множество (может быть, и пустое), элементы которого называются *функциональными символами* языка Ω (*функциональными буквами*). С каждой функциональной буквой $f \in \mathrm{Fn}$ однозначно связан некоторый объект — *вид* данной функциональной буквы. Вид функциональной буквы f есть выражение

$$(\pi_1, \ldots, \pi_k \to \pi),$$

где π_i, π суть сорта языка, $k > 0$. Число k называется *количеством аргументных мест* f (арностью символа f). Сорт π_i называется *сортом i-го аргументного места* символа f, а сорт π называется сортом самого символа f (или *сортом значений* символа f). Как всегда, символы различных видов различны.

В наиболее популярном случае односортного языка для задания вида функционального символа достаточно указать количество его аргументов.

4) Pr — непустое множество, элементы которого называются *предикатными символами* (*предикатными буквами*) языка Ω. С каждой предикатной буквой $P \in \mathrm{Pr}$ связан некоторый объект — *вид* данной предикатной буквы. Вид предикатной буквы P есть выражение $(\pi_1, \ldots, \pi_k)$, где π_i суть сорта языка, $k \geqslant 0$. Число k называется *количеством аргументных мест* символа P (арностью символа P). Сорт π_i, называется *сортом i-го аргументного места символа P*. В отличие от случая функциональных символов, здесь мы не исключаем возможности $k = 0$. Нульместные предикатные символы называются *пропозициональными переменными* (*пропозициональными буквами* или *символами*).

2. Если задан язык Ω, то можно определить некоторые правильно построенные тексты, составленные из символов Ω, скобок, запятых и некоторых дополнительных символов (*логических символов*). Эти тексты называются *выражениями* языка Ω и подразделяются на *термы* и *формулы*.

Начнем с определения *термов* языка Ω. Это определение индуктивное и содержит три пункта. Первые два пункта являются базисом индукции: в них непосредственно указано, какие из объектов языка следует считать термами. Третий пункт представляет собой шаг индукции — он задает *порождающие правила*: если уже построены некоторые термы, то разрешается построить из них новый терм по указанному правилу. Каждый терм имеет либо вид, указанный в первых двух пунктах определения, либо получен по порождающему правилу третьего пункта из термов, построенных на более раннем этапе.

Каждому терму в силу определения будет однозначно приписан некоторый сорт языка — *сорт данного терма* (в другой терминологии — *сорт значений* данного терма). Итак, приведем индуктивное определение терма данного сорта языка Ω:

1) каждая переменная x сорта π языка Ω есть терм сорта π;
2) константа c сорта π языка Ω есть терм сорта π;
3) если f — функциональный символ вида $(\pi_1, \ldots, \pi_k \to \pi)$ языка Ω и t_1 — терм сорта π_1, t_2 — терм сорта $\pi_2, \ldots, t_k$ — терм сорта π_k, то выражение $f(t_1, \ldots, t_k)$ есть терм сорта π; коротко этот пункт запишем в виде правила вывода

$$\frac{t_1, t_2, \ldots, t_k}{f(t_1, \ldots, t_k)}.$$

Множество всех термов сорта π языка Ω обозначим через $\mathrm{Tm}^{\pi}_{\Omega}$, множество всех термов всевозможных сортов — через Tm_{Ω}.

Таким образом, каждый терм имеет один и только один из следующих двух видов.

А. Константа или переменная языка Ω;

Б. $f(t_1, \ldots, t_k)$, где f — функциональный символ языка Ω и $t_1, \ldots, t_k$ суть термы соответствующих сортов.

Например, термом некоторого языка может быть выражение

$$g(h(c, x), g(x, h(c, y))),$$

где g и h — двумерные функциональные символы, c — константа, x и y — переменные. При этом сорта выражений должны быть надлежащим образом согласованы.

Роль термов в языке состоит в том, чтобы описывать именные формы и имена предметов. Так, в некотором языке переменные могут рассматриваться как пробегающие множество $0, 1, 2, \ldots$ натуральных чисел, $g(x, y)$ описывает сумму $x+y$, а $h(x, y)$ — произведение $x \cdot y$ натуральных чисел. Константа c обозначает натуральное число 0. Тогда вышеприведенный терм задает именную форму

$$0 \cdot x + (x + 0 \cdot y).$$

Подчеркнем, однако, что сами по себе термы — просто строчки символов и ничего не выражают. Чтобы узнать, какую именную форму задает терм, необходимо дополнительно объяснить, что обозначают символы, встречающиеся в терме, т. е., как говорят логики, задать *семантику* языка, задать *интерпретацию* языка. Одной из наших дальнейших задач и будет точное оформление этой идеи.

Индуктивный характер определения множества Tm_{Ω} предполагает возможность использовать следующий способ рассуждения: *принцип индукции по построению множества термов* (языка Ω). А именно, пусть мы желаем доказать, что некоторое свойство X выполняется для всех термов языка Ω. С этой целью достаточно установить, что:

1) каждая переменная языка Ω обладает свойством X;
2) каждая константа языка Ω обладает свойством X;
3) если $t_1, \ldots, t_m$ суть термы, обладающие свойством X, $f(t_1, \ldots, t_m)$ — терм, то $f(t_1, \ldots, t_m)$ также обладает свойством X.

В такой ситуации в силу индуктивного определения множества Tm_Ω можно быть уверенным, что всякий терм языка Ω обладает свойством X.

Этот принцип индукции естественно обобщает известный школьный принцип полной математической индукции. Действительно, натуральные числа можно трактовать как индуктивно порождаемые объекты: они порождаются из объекта 0 последовательным применением операции прибавления единицы. Поэтому если мы установим, что:

1) 0 обладает свойством X,
2) если n есть натуральное число, обладающее свойством X, то $n+1$ также обладает свойством X, то можно быть уверенным, что *всякое* натуральное число обладает свойством X.

С этой точки зрения множество термов образует *арифметику со многими операциями следования*, которые могут быть и *многоместными*. Подобные индуктивные определения играют важную роль в математической логике.

Докажем, например, что всякий терм языка содержит одинаковое количество вхождений левых и правых скобок. В самом деле, это верно по отношению к переменным и константам языка (ни те, ни другие вовсе не содержат скобок). Далее, если термы $t_1, \ldots, t_m$ таковы, что каждый терм t_i содержит одинаковое количество левых и правых скобок, то терм $f(t_1, \ldots, t_m)$, очевидно, тоже таков (в нем добавилось ровно одно вхождение левой скобки и одно вхождение правой скобки). Наше утверждение следует теперь из принципа индукции по построению термов языка.

Упражнение. Индукцией по построению термов докажите, что количество запятых в терме равно $m - k$, где m — сумма арностей всех вхождений функциональных символов, а k — количество вхождений функциональных символов в терм.

Аналогично, индуктивный характер определения Tm_Ω дает возможность *задавать функции*, определенные на множестве Tm_Ω индукцией по построению множества термов языка Ω (иногда в таких случаях говорят о возможности задавать функции *рекурсией* (*примитивной рекурсией*) по построению множества термов). А именно:

1) пусть с каждой переменной x языка Ω мы связали некоторый объект $F(x)$,
2) с каждой константой c языка Ω мы связали некоторый объект $F(c)$,
3) пусть задано правило, в соответствии с которым если термам $t_1, \ldots, t_m$ уже приписаны объекты $F(t_1), \ldots, F(t_m)$, то правило позволяет отыскать объект $F(f(t_1, \ldots, t_m))$ для терма $f(t_1, \ldots, t_m)$.

В такой ситуации для всякого терма t языка однозначно определен объект $F(t)$.

Определим, например, функцию $\widetilde{l}$ на множестве всех термов языка Ω рекурсией:

1) если x — переменная языка, то положим $\widetilde{l}(x) = 0$,
2) если c — константа языка, то положим $\widetilde{l}(c) = 0$,
3) если терм имеет вид $f(t_1, \ldots, t_k)$, то определим:

$$\widetilde{l}(f(t_1, \ldots, t_k)) = \widetilde{l}(t_1) + \ldots + \widetilde{l}(t_k) + 1.$$

На последнее равенство следует смотреть как на правило, в силу которого можно вычислить $\widetilde{l}(f(t_1, \ldots, t_k))$, если уже известны значения $\widetilde{l}(t_1), \ldots, \widetilde{l}(t_k)$. Указанное определение дает рецепт для вычисления $\widetilde{l}$ от любого терма. Например,

$$\widetilde{l}(f(g(x, y), c, z, x)) = 2.$$

Значение $\widetilde{l}(t)$ называется *функциональной сложностью* терма t.

Упражнение. Индукцией по построению термов докажите, что для всякого терма t значение $\widetilde{l}(t)$ равно количеству вхождений функциональных символов в терм t.

Таким образом, можно было бы дать и не индуктивное, *явное* определение функции $\widetilde{l}$. Оба определения математически эквивалентны: приняв одно из них, второе можно доказать как математическую теорему. Такая ситуация еще не раз у нас встретится.

Заметим, что множество Tm_Ω^π всегда бесконечно, так как содержит переменные сорта π (даже если в языке отсутствуют функциональные символы и константы).

3. *Атомарные формулы* языка Ω (в другой терминологии — *элементарные формулы* языка Ω) определяются следующим образом. Если P — предикатный символ языка Ω вида $(\pi_1, \ldots, \pi_k)$, а $t_1, \ldots, t_k$ суть термы, причем терм t_i имеет сорт π_i, то выражение $P(t_1, \ldots, t_k)$ есть атомарная формула.

В частности, если P — пропозициональная буква (т. е. нульместная буква), то P сама по себе является атомарной формулой.

Множества всех атомарных формул языка Ω обозначим через AtFm_Ω.

4. *Формулы* языка Ω определяются индуктивно с помощью следующих ниже семи пунктов. Первый пункт представляет собой базис индукции, а остальные шесть пунктов суть порождающие правила, позволяющие строить новые формулы из уже построенных.

При построении формул используются новые символы, которые называются *логическими символами*. Они делятся на две категории — *логические связки* и *кванторы*.

Мы употребляем следующие четыре логические связки:

$\wedge$ — «конъюнкция», «и»;
$\vee$ — «дизъюнкция», «или»;
$\supset$ — «импликация», «если..., то», «влечет»;
$\neg$ — «отрицание», «не».

Мы используем два квантора:

$\forall$ — всеобщность (генерализация), «для всех»;
$\exists$ — существование (экзистенция), «существует».

Итак, приведем индуктивное определение формулы языка Ω:

1) каждая атомарная формула есть формула;
2) $\dfrac{A, B}{(A \wedge B)}$, т. е. если уже построены формулы A и B, то разрешается построить новую формулу $(A \wedge B)$.

Подобным образом следует трактовать и следующие три пункта:

3) $\dfrac{A, B}{(A \vee B)}$;
4) $\dfrac{A, B}{(A \supset B)}$;
5) $\dfrac{A}{\neg A}$;
6) $\dfrac{A, x}{\forall x A}$, т. е. если уже построена формула A и x — произвольная переменная языка Ω, то разрешается построить новую формулу $\forall x A$.

Подобным образом следует трактовать и следующий пункт:

7) $\dfrac{A, x}{\exists x A}$.

Множество всех формул языка Ω обозначим через Fm_Ω. Таким образом, каждая формула имеет один и только один из следующих трех видов:

А. атомарная формула языка Ω;
Б. $(A \Delta B)$, где A, B суть формулы языка Ω, а Δ — логическая связка, один из символов $\wedge$, $\vee$, $\supset$; или $\neg A$, где A — формула языка Ω;
В. QxA, где A — формула языка Ω, x — переменная языка Ω и Q — квантор, один из символов $\forall, \exists$.

Например, формулой некоторого языка может быть выражение

$$\forall x \exists z((P(f(x, y)) \wedge \exists x Q(x, z)) \supset \exists y Q(x, y)).$$

Читая логические связки и кванторы, мы можем «прочесть» эту формулу: «для всякого x существует z такое, что если $P(f(x, y))$ и существует x, для которого $Q(x, z)$, то существует y, для которого $Q(x, y)$».

Выражением языка Ω мы назовем формулу языка Ω или терм языка Ω. Множество всех выражений языка Ω обозначим Exp_Ω. По определению $\mathrm{Exp}_\Omega = \mathrm{Fm}_\Omega \cup \mathrm{Tm}_\Omega$.

5. Индуктивный характер определения множества Fm_Ω предполагает возможность использовать следующий способ рассуждения — *индукцию по построению множества формул* (языка Ω). А именно если мы желаем доказать, что некоторое свойство X выполняется для всех формул языка Ω, то достаточно установить, что:

А. каждая атомарная формула языка Ω обладает свойством X;

Б. если формулы A и B обладают свойством X, то формулы $(A \wedge B)$, $(A \vee B)$, $(A \supset B)$, $\neg A$ также обладают свойством X;

В. если формула A обладает свойством X, то свойством X обладают и формулы $\forall x A$, $\exists x A$.

Если факты А, Б, В установлены, то можно быть уверенным, что свойство X имеет место для любой формулы языка.

Докажем, например, что всякая формула языка содержит одинаковое количество вхождений левых и правых скобок. В самом деле:

А. атомарная формула $(Pt_1, \ldots, t_m)$ такова, так как каждый терм t_i содержит одинаковое число вхождений левых и правых скобок;

Б. если формулы A, B содержат одинаковое количество левых и правых скобок, то, очевидно, таковы же и формулы

$$(A \wedge B), \quad (A \vee B), \quad (A \supset B), \quad \neg A;$$

В. если формула A содержит одинаковое количество левых и правых скобок, то, очевидно, таковы же формулы $\forall x A$, $\exists x A$.

Аналогично, индуктивный характер определения Fm_Ω дает возможность задавать функции, определенные на множестве Fm_Ω индукцией по определению множества Fm_Ω (задавать функции *рекурсией* (примитивной рекурсией) по построению множества Fm_Ω). А именно:

А. пусть с каждой атомарной формулой A языка Ω мы связали некоторый объект $F(A)$;

Б. пусть задано правило, в соответствии с которым, если формулам A и B уже приписаны некоторые значения $F(A)$ и $F(B)$, можно отыскать и объекты $F(A \wedge B)$, $F(A \vee B)$, $F(A \supset B)$, $F(\neg A)$;

В. пусть задано правило, в соответствии с которым, если формуле A уже приписан объект $F(A)$, для любой переменной x можно отыскать объекты $F(\forall x A)$ и $F(\exists x A)$.

В такой ситуации для всякой формулы A языка Ω определен объект $F(A)$.

6. Свяжем, например, с каждой формулой $A \in \mathrm{Fm}_\Omega$ натуральное число $l(A)$, называемое *логической сложностью* формулы A, следующим образом:

1) $l(A) = 0$, если A — атомарна;

2) $l(A \Delta B) = l(A) + l(B) + 1$; $\quad l(\neg A) = l(A) + 1$;

3) $l(Qx A) = l(A) + 1$.

Упражнение. Проверьте, что

$$l(\forall x\, \exists z((P(f(x, y)) \wedge \exists x Q(x, z)) \supset \exists y Q(x, y))) = 6.$$

Упражнение. Индукцией по построению множества формул докажите, что $l(A)$ равно количеству вхождений логических символов в A.

7. Практически записывая формулы, удобно экономить скобки, пользуясь некоторыми традициями и приемами. Эти «экономные» записи следует рассматривать как неформальные обозначения для формул в нашей записи. Вся точная теория у нас будет относиться лишь к формулам в точном определении.

Прежде всего, мы опускаем внешние скобки. Кроме того, ниже мы расположим связки и кванторы в определенном порядке, считая, что те символы, которые в этом порядке находятся правее, «связывают сильнее», т. е. их следует выполнять «в первую очередь»:

$$\begin{matrix} & \vee & & \forall \\ \supset & & \neg & \\ & \wedge & & \exists \end{matrix}.$$

Таким образом, дизъюнкция и конъюнкция связывают сильнее, чем импликация, а сами они равноправны в отношении связывания. Аналогично, равноправны и кванторы. Они связывают сильнее, чем любые логические связки.

Так, формулу

$$(P \supset ((Q \vee R) \supset (\neg R \supset \neg P)))$$

можно сокращенно записать в виде

$$P \supset (Q \vee R \supset (\neg R \supset \neg P)).$$

Формулу

$$(\forall x(P(x, y) \supset (\forall z Q(z) \wedge R)) \vee Q(x))$$

сокращенно запишем в виде

$$\forall x(P(x, y) \supset \forall z Q(z) \wedge R) \vee Q(x).$$

Дальнейшая экономия скобок достигается употреблением точки. Если внутри скобок выполняется несколько однородных (по силе связывания) логических символов, то точкой мы отмечаем тот логический символ, который выполняется *в последнюю очередь* в пределах своих скобок. Рассмотрим примеры:

1) формулу

$$P \supset (Q \vee R \supset (\neg R \supset \neg P))$$

можно записать в виде

$$P \supset (Q \vee R \supset .\, \neg R \supset \neg P);$$

2) формулу

$$(((P \supset Q) \supset R) \supset (P \supset (Q \supset R)))$$

можно записать в виде

$$(P \supset Q .\supset R) \supset (P \supset . Q \supset R);$$

3) формулу

$$(P \supset (Q \supset R)) \supset ((P \supset Q) \supset (P \supset R))$$

можно записать в виде

$$P \supset (Q \supset R) \supset . (P \supset Q) \supset (P \supset R)$$

или в виде

$$(P \supset . Q \supset R) \supset (P \supset Q .\supset P \supset R);$$

4) формулу

$$(((P \supset Q) \supset R) \vee P) \supset Q$$

можно записать в виде

$$((P \supset Q \supset . R) \vee P) \supset Q;$$

5) формулу

$$P \supset \forall x (Q(x) \vee R(x))$$

можно записать в виде

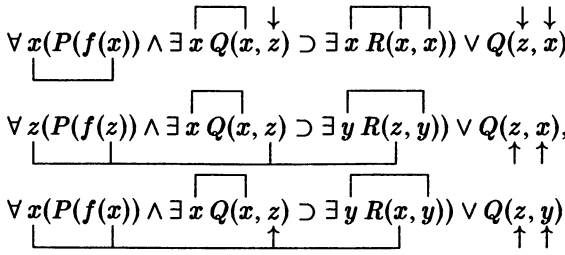
$$P \supset \forall x . Q(x) \vee R(x).$$

8. В формулах вида $\forall x A$, $\exists x A$ выражение $\forall x$ или $\exists x$ называется *кванторной приставкой*, x — *переменной кванторной приставки*, а формула A — *областью действия кванторной приставки*.

Каждое вхождение переменной в формулу мы будем называть *свободным* или *связанным*. А именно, вхождение переменной x в формулу A называется *связанным*, если в A входит формула вида QxB, причем рассматриваемое вхождение x в A является вхождением x в эту формулу QxB. Кратко говорят, что вхождение x в A связано, если оно попадает в область действия квантора по x или в саму кванторную приставку с переменной x. Вхождение переменной, не являющееся связанным, называется *свободным*. Таким образом, каждое связанное вхождение переменной происходит из-за некоторой кванторной приставки, которая «связывает» переменную.

В примерах, приводимых ниже, мы указываем, какие переменные являются связанными и от каких кванторов это происходит (стрелками

отмечены свободные вхождения переменных):



Заметим, что одна и та же переменная может иметь и свободные, и связанные вхождения в одну и ту же формулу. Вхождение переменной может быть связано во всей формуле и в то же время свободно в некоторой ее подформуле. Здесь *подформулой* мы называем вхождение формулы в данную формулу, т. е. часть формулы, которая сама является формулой. В аналогичном смысле используется термин *подтерм* и т. п.

В атомарную формулу всякая переменная по определению входит свободно. Удобно также считать по определению, что все переменные, входящие в терм, входят в него свободно.

9. Выше мы дали явное определение свободных и связанных вхождений переменных в формулу, но нетрудно дать и индуктивный рецепт, позволяющий отыскать свободные и связанные вхождения переменных.

А. Если рассматриваемая формула атомарна, то всякая переменная, входящая в нее, свободна.

Б. Если формула имеет вид $(A\Delta B)$, то следует посмотреть, куда именно входит переменная x, в A или в B. Допустим, например, что в A. Тогда x свободна (связана) в $(A\Delta B) \Leftrightarrow x$ свободна (связана) в A. Кратко это правило можно выразить так: логические связки переменных «не связывают».

В. Если формула имеет вид QyA, и мы интересуемся вхождением переменной x в эту формулу, то следует разобрать два случая.

1) y совпадает с x. Тогда x автоматически входит связанно в QyA.
2) y отлично от x. Тогда x свободна (связана) в $QyA \Leftrightarrow x$ свободна (связана) в A.

10. Переменная x называется *свободной переменной формулы* A, или *параметром* A, если x входит (хотя бы один раз) свободно в A. Разумеется, при этом x может входить в A и связанно.

Множество всех параметров A обозначим через $\mathrm{Fv}(A)$. Это — конечное множество переменных, может быть, и пустое. Формулу, не содержащую параметров, назовем *замкнутой* формулой, или *предложением*. Множество всех предложений языка Ω обозначим через St_Ω.

Например, следующая формула есть предложение:

$$\forall x.P(x) \wedge \exists x Q(x, x) \supset \exists y R(x, y).$$

Аналогично, *параметром* терма назовем всякую переменную, в него входящую. Терм назовем *замкнутым*, если он не содержит переменных (т. е. построен, исходя лишь из констант языка Ω).

Нетрудно дать и индуктивный рецепт для вычисления множества $\mathrm{Fv}(A)$:

А. $\mathrm{Fv}(P(t_1, \ldots, t_k)) = \mathrm{Fv}(t_1) \cup \ldots \cup \mathrm{Fv}(t_k)$;

Б. $\mathrm{Fv}(A \Delta B) = \mathrm{Fv}(A) \cup \mathrm{Fv}(B)$;
$\mathrm{Fv}(\neg A) = \mathrm{Fv}(A)$;

В. $\mathrm{Fv}(QxA) = \mathrm{Fv}(A) \backslash \{x\}$.

Здесь $\cup$ обозначает объединение множеств, $\backslash$ обозначает разность множеств и $\{x\}$ — одноэлементное множество, единственным элементом которого является переменная x.

11. Роль формул в языке состоит в том, чтобы описывать высказывания и высказывательные формы в языке. При этом высказывательная форма зависит от переменных — параметров формулы (а не от связанных переменных формулы). Каждая высказывательная форма, в свою очередь, задает некоторый предикат от своих параметров. Под предикатом мы понимаем функцию от переменных, пробегающих некоторую область, причем эта функция принимает лишь два значения: 1 — «истина» и 0 — «ложь».

Например, в некотором языке атомарная формула $P(x, y, z)$ может выражать высказывательную форму

$$x + y = z,$$

где x, y, z обозначают натуральные числа $0, 1, 2, 3, \ldots$. Таким образом, $P(x, y, z)$ задает трехместную функцию — предикат:

$$P(3, 5, 3) = 0, \quad P(3, 5, 8) = 1, \quad P(0, 4, 2) = 0, \ldots$$

Формула $\exists y P(x, y, z)$ задает уже предикат лишь от двух переменных x и z. Переменная y оказывается связанной. Например:

$$\exists y P(2, y, 3) = 1,$$
$$\exists y P(0, y, 0) = 1,$$
$$\exists y P(5, y, 2) = 0.$$

Нетрудно понять, что формула $\exists y P(x, y, z)$ задает форму $x \leqslant z$.

На этом примере можно понять, почему свободные и связанные переменные играют различную роль в формуле.

Во-первых, вместо связанной переменной нельзя подставить конкретное значение — получится бессмысленное выражение. Так, например,

$\exists\, yP(0, y, 3)$ — вполне осмысленное истинное утверждение, а $\exists\, 3P(2, 3, 3)$ не имеет разумного смысла.

Во-вторых, связанная переменная не имеет самостоятельного значения, ее можно заменить на другую переменную и смысл формулы от этого не изменится. Все формулы

$$\exists\, yP(x, y, z), \quad \exists\, uP(x, u, z), \quad \exists\, vP(x, v, z)$$

выражают один и тот же предикат, одну и ту же функцию от x, z. Такая операция называется *переименованием связанной переменной.*

При переименовании связанной переменной смысл формулы не меняется, если при этом соблюдать одну существенную предосторожность: никакая свободная переменная в любой подформуле данной формулы не должна после переименования оказаться связанной.

Например, если в формуле $\exists\, yP(x, y, z)$ мы решим заменить переменную y на переменную x, то получится формула $\exists\, xP(x, x, z)$, которая имеет совершенно иной смысл, чем исходная формула. Прежде всего, $\exists\, xP(x, x, z)$ зависит уже лишь от одного параметра z, а не от двух, и задает всегда истинный предикат от z. Причина неприятности состоит в том, что после неудачного переименования связанной переменной y первое вхождение переменной x, которое раньше было свободным, стало связанным.

Указанное явление мы назовем *коллизией переменных* при переименовании связанных переменных. Коллизия переменных недопустима.

По существу, эта ситуация хорошо известна и в обыденной математике. В сумме

$$\sum_{i=1}^{10} a_{ij}$$

переменная i связана «квантором суммы» $\sum$, а переменная j остается свободной — параметром суммы. Вместо j можно подставить конкретное значение и рассмотреть сумму, например, $\sum_{i=1}^{10} a_{i3}$, в то время как вместо i бессмысленно подставлять конкретные значения. Переменную i можно заменить на другую, например, $\sum_{k=1}^{10} a_{kj}$, — это будет, в сущности, та же самая сумма (иногда говорят, что индекс i *«немой»* и допускает переименование). Однако если вместо i подставить j, то произойдет коллизия переменных — сумма $\sum_{j=1}^{10} a_{jj}$ имеет уже совсем другой смысл (говорят, что переменная j «уже занята» и нельзя вместо i подставить j). Аналогично, в интеграле

$$\int_0^y x^2 y\, dx$$

переменная y во всех вхождениях свободна, а переменная x связана «кванторной приставкой» dx. Переменную x можно заменить на переменную z — интеграл от этого не изменится, но отнюдь не на переменную y!

12. Уточним теперь, что именно означает ситуация, когда две формулы A и A' отличаются друг от друга лишь правильным (т. е. без коллизий переменных) переименованием связанных переменных. В этом случае мы будем говорить, что формулы A и A' *конгруэнтны*, или что формула A' является *вариантом* формулы A, и писать $A \approx A'$.

Рассмотрим некоторую формулу, например,

$$\forall x(P(f(x)) \wedge \exists x Q(x, z) \supset \exists y R(x, y)) \vee Q(z, y).$$

Отметим линиями связанные переменные этой формулы и кванторы, от которых происходит связывание:

$$\forall x(P(f(x)) \wedge \exists x Q(x, z) \supset \exists y R(x, y)) \vee Q(z, y).$$

Сотрем теперь все связанные переменные, оставляя линии

$$\forall\ (P(f(\ )) \wedge \exists\ Q(\ , z) \supset \exists\ R(\ ,\ )) \vee Q(z, y).$$

Полученную фигуру можно назвать скелетом исходной формулы.

Две формулы конгруэнтны тогда и только тогда, когда их скелеты совпадают.

Упражнение. Укажите несколько вариантов формулы

$$\forall z(P(z) \wedge \exists z Q(x, z) \supset \exists y R(z, y)) \vee Q(z, x).$$

Какие переименования связанных переменных ведут к коллизии?

Можно дать и аккуратное математическое определение отношения $A \approx A'$ индукцией по логической сложности $l(A)$ формулы A. А именно:

А) единственным вариантом атомарной формулы является она сама;

Б) если A имеет вид $(B \Delta C)$, то всякий вариант A' формулы A имеет вид $(B' \Delta C')$, где $B \approx B'$ и $C \approx C'$;
если A имеет вид $\neg B$, то всякий вариант A' формулы A имеет вид $\neg B'$, где $B \approx B'$;

В) если A имеет вид QxB, то всякий вариант A' формулы A имеет вид QyC, где y и C таковы, что для всякой новой переменной z (т. е. не входящей ни свободно, ни связанно в формулы QxB и QyC) имеем $B_z^x \approx C_z^y$.

Здесь через B_z^x обозначен результат замещения всех свободных вхождений переменной x в B на переменную z. Аналогично понимается C_z^y. Предполагается еще, конечно, что все три переменные x, y, z имеют один и тот же сорт.

Приведенное определение дает возможность точно доказывать различные свойства вариантов формулы A индукцией по логической сложности $l(A)$ формулы A. Например, нетрудно доказать, что если $A \approx A'$,

то $l(A) = l(A')$, $\mathrm{Fv}(A) = \mathrm{Fv}(A')$ и A и A' имеют один и тот же *главный* (т. е. последний в построении) логический символ.

Отношение $\approx$ является отношением эквивалентности между формулами рассматриваемого языка, и с точки зрения смысла формул конгруэнтные формулы можно считать «несущественно отличающимися друг от друга». Можно сказать, что математическая логика изучает скорее не отдельные формулы, а классы конгруэнтных между собой формул.

§ 2. О правильной подстановке термов в формулы

1. *Формальной подстановкой* (или просто *подстановкой*) назовем функцию θ, определенную на конечном (может быть, и пустом) множестве переменных языка Ω и перерабатывающую каждую переменную x из области определения θ в некоторый терм $\theta(x)$ языка, причем x и $\theta(x)$ имеют один и тот же сорт.

Формальную подстановку можно изображать в виде двумерной таблицы

$$\begin{pmatrix} x_1, & x_2, & \ldots, & x_k \\ t_1, & t_2, & \ldots, & t_k \end{pmatrix},$$

где в верхней строке указана область определения функции θ:

$$\mathrm{dom}\,\theta = \{x_1, \ldots, x_k\}$$

и, кроме того, $\theta(x_i) = t_i$. Здесь x_i и t_i имеют один и тот же сорт. Порядок столбцов в двумерной таблице несущественен. Таблица может быть и пустой, если функция θ имеет пустую область определения.

2. Пусть T — выражение языка Ω (т. е. формула или терм) и θ — формальная подстановка $\begin{pmatrix} x_1, \ldots, x_k \\ t_1, \ldots, t_k \end{pmatrix}$. Через $(T\theta)$ мы обозначим результат одновременного замещения всех *свободных* вхождений переменных $x_1, \ldots, x_k$ в T на термы $t_1, \ldots, t_k$ соответственно. Конечно, при этом некоторые x_i могут и не входить свободно в T. Тогда соответствующие t_i никуда не подставляются и просто не играют никакой роли. Подчеркнем, что замещаются только *свободные* вхождения x_i в T.

Вместо $(T\theta)$ будем иногда употреблять одно из следующих обозначений:

$$T\theta, \quad T\begin{pmatrix} x_1, \ldots, x_k \\ t_1, \ldots, t_k \end{pmatrix}, \quad T\begin{matrix} x_1, \ldots, x_k \\ t_1, \ldots, t_k \end{matrix}.$$

Дадим теперь индуктивный рецепт для вычисления подстановки в формулу. Этот рецепт можно рассматривать и как самостоятельное индуктивное определение подстановки. Можно убедиться с помощью индукции, что оно эквивалентно данному ранее определению.

А. $(P(t_1, \ldots, t_m)\theta) = P(t_1\theta, \ldots, t_m\theta)$.

Б. $(A \Delta B)\theta = (A\theta \Delta B\theta)$,
$(\neg A\theta) = \neg(A\theta)$.

В. $(QzB\theta) = Qz(B(\theta - \{z\}))$.

Здесь через $\theta - \{z\}$ обозначен результат «выбрасывания» переменной z из области определения θ, т. е. $\theta - \{z\}$ есть такая подстановка θ', что $\operatorname{dom}\theta' = \operatorname{dom}\theta \backslash \{z\}$ и $\theta'(x) = \theta(x)$ для всякой переменной $x \in \operatorname{dom}\theta'$.

3. *Упражнение.* Вычислите результаты подстановок:

1) $\left(\exists y P(x, y, z)\left(\begin{smallmatrix} x \\ f(x, y) \end{smallmatrix}\right)\right)$;

2) $\left(\exists y P(x, y, z)\left(\begin{smallmatrix} y \\ f(x, y) \end{smallmatrix}\right)\right)$;

3) $(\exists y P(x, y, z))\begin{smallmatrix} x \\ f(x, z) \end{smallmatrix}$;

4) $(\exists z \forall y P(x, y) \supset Q(x))\begin{smallmatrix} x \\ f(x, z) \end{smallmatrix}$;

5) $(\forall y P(x, y) \supset Q(x))\begin{smallmatrix} x \\ f(x, z) \end{smallmatrix}$;

6) $(P(x, y) \supset \forall y Q(y))\begin{smallmatrix} x, y \\ f(x, y), z \end{smallmatrix}$;

7) $(\forall y P(y, z) \vee \exists y R(x, y))\begin{smallmatrix} x, y \\ f(x, y), z \end{smallmatrix}$.

4. Заметим теперь, что не все подстановки одинаково пригодны с точки зрения логики.

Пусть, например, в некотором языке атомарная формула $P(x, y, z)$ выражает предикат $x + y = z$, где переменные пробегают натуральные числа $0, 1, 2, \ldots$. Формула $\exists y P(x, y, z)$ выражает уже предикат от переменных x и z, а именно $x \leqslant z$.

Пусть в этом же языке терм $f(x, y)$ задает операцию умножения натуральных чисел $x \cdot y$. Теперь мы желали бы подставить $f(x, y)$ в $\exists y P(x, y, z)$ вместо свободной переменной x с целью выразить предикат от трех переменных $x \cdot y \leqslant z$.

Однако ошибочно было бы рассмотреть с этой целью формулу $\left(\exists y P(x, y, z)\left(\begin{smallmatrix} x \\ f(x, y) \end{smallmatrix}\right)\right)$, т. е. формулу $\exists y P(f(x, y), y, z)$. Эта последняя формула выражает совсем иную мысль (в частности, зависимость от двух параметров x и z, а не от трех).

Причина затруднения состоит в том, что переменная y была свободна в терме $f(x, y)$, а оказалась связанной в результирующей формуле. Как говорят, произошла *коллизия переменных при подстановке*.

Правильный выход из положения состоит в том, что сначала следует переименовать связанную переменную y, например, образовать формулу $\exists u P(x, u, z)$, которая выражает тот же предикат, а уже затем произве-

сти подстановку, так что в результате получим формулу $\exists u P(f(x, y), u, z)$, которая и выражает нужный предикат.

5. Выделим теперь класс подстановок, которые заведомо не приводят к коллизии переменных.

Подстановка θ называется *свободной для выражения* T (или *допустимой для выражения* T), если для всякой переменной $x \in \mathrm{dom}\theta$ любое свободное вхождение x в T не попадает в область действия кванторов по переменным, свободно входящим в терм $\theta(x)$.

Упражнение. Выясните, какие из подстановок п. 3 свободны.

Как всегда, мы укажем и индуктивное определение свободной подстановки.

А. Если T — терм или атомарная формула, то всякая подстановка является допустимой для T.

Б. θ свободна для $(A \Delta B) \Leftrightarrow \theta$ свободна для A и θ свободна для B.
θ свободна для $\neg A \Leftrightarrow \theta$ свободна для A.

В. θ свободна для $QzB \Leftrightarrow$ подстановка $\theta - \{z\}$ свободна для B, и, кроме того, для всякой переменной $x \in \mathrm{dom}\,\theta \cap \mathrm{Fv}(QzB)$ терм $\theta(x)$ не содержит свободно переменной z.

6. Если для всех $x \in \mathrm{dom}\,\theta$ выражение T вовсе не содержит кванторов по параметрам терма $\theta(x)$, то θ допустима для T.

Просто обстоит дело и в том случае, если для всякой переменной $x \in \mathrm{dom}\theta$ терм $\theta(x)$ является замкнутым. Такая подстановка называется *константной*. Константная подстановка свободна для всякого выражения.

Если подстановка θ свободна для выражения T, то нетрудно описать множество параметров выражения $T\theta$. А именно, пусть θ' получается из θ выбрасыванием из области определения θ всех переменных, не входящих свободно в T. Пусть θ' есть

$$\begin{pmatrix} x_1, \ldots, x_k \\ t_1, \ldots, t_k \end{pmatrix},$$

тогда

$$\mathrm{Fv}(T\theta) = (\mathrm{Fv}(T) \backslash \{x_1, \ldots, x_k\}) \cup \mathrm{Fv}(t_1) \cup \ldots \cup \mathrm{Fv}(t_k),$$

т. е. из $\mathrm{Fv}(T)$ следует выбросить параметры, вместо которых подставляют термы, и добавить параметры подставляемых термов.

Упражнение. Приведите пример нарушения этого равенства в случае, когда θ не допустима для T.

7. Пусть A — формула и θ — подстановка, необязательно допустимая для A. Как мы уже говорили, в этом случае $A\theta$, вообще говоря, непригодна с точки зрения предполагаемого смысла подстановки. Правильный способ действий в этой ситуации таков. Следует найти

вариант A', $A' \approx A$, такой, что θ допустима для A', и рассмотреть формулу $A'\theta$. Мы назовем $A'\theta$ результатом *правильной подстановки* θ в A и обозначим $A'\theta$ через $[A\theta]$.

Формула $[A\theta]$ определена неоднозначно, она зависит от выбора варианта A'. Однако если $A' \approx A''$ и θ — подстановка, свободная для A' и для A'', то $A'\theta \approx A''\theta$. Таким образом, правильная подстановка определена однозначно с точностью до конгруэнтности.

То обстоятельство, что нужный вариант A', для которого θ допустима, найдется, вытекает, например, из следующей леммы.

Будем говорить, что формула A обладает *свойством чистоты переменных*, если, во-первых, все ее связанные переменные отличны от свободных и, во-вторых, любые два различные вхождения кванторных приставок связывают различные переменные.

Лемма (о чистоте переменных). *Пусть A — формула и S — конечное множество переменных. Тогда может быть построена формула B со свойством чистоты переменных такая, что $A \approx B$ и всякая связанная переменная B отлична от переменных из множества S.*

▷ Доказательство проведем индукцией по $l(A)$. Если A атомарна, то в качестве B достаточно взять A. Пусть A есть $(C\Delta D)$ и задано множество переменных S. Пусть S_1 — множество всех переменных D (и свободных, и связанных). Найдем по индуктивному предположению формулу C' со свойством чистоты переменных, $C' \approx C$, такую, что связанные переменные C' отличны от всех переменных из $S \cup S_1$. Пусть теперь S_2 — множество всех переменных C'. Найдем вариант $D' \approx D$ со свойством чистоты переменных, так что связанные переменные D' отличны от переменных из $S \cup S_1 \cup S_2$. Положим $B = (C'\Delta D')$.

Пусть A есть QzC. Выберем новую переменную u и определим формулу C', $C' \approx C'^{z}_{u}$, так что C' обладает свойством чистоты переменных и связанные переменные C' отличны от элементов множества $S \cup \{u\}$. Положим $B = QuC'$. ◁

Дадим теперь индуктивное определение результата правильной подстановки.

Пусть A — формула, θ — формальная подстановка. Определим формулу $[A\theta]$ индукцией по $l(A)$.

А. Если A атомарная формула, то $[A\theta] \leftrightharpoons (A\theta)$.

Б. Если A есть $(B\Delta C)$, то

$$[A\theta] \leftrightharpoons ([B\theta]\Delta[C\theta]).$$

Если A есть $\neg B$, то

$$[A\theta] \leftrightharpoons \neg[B\theta].$$

В. Пусть A имеет вид $Qx B$. Тогда рассмотрим два случая.

1. «Простой случай». Какую переменную $y \in \operatorname{dom}\theta \cap \operatorname{Fv}(A)$ ни взять, все параметры соответствующего терма $\theta(y)$ отличны от x. Тогда определим
$$[A\theta] \leftrightharpoons Qx[B(\theta - \{x\})].$$
2. «Сложный случай». Найдется переменная $y \in \operatorname{dom}\theta \cap \operatorname{Fv}(A)$ такая, что соответствующий терм $\theta(y)$ содержит свободно x. Выберем тогда новую переменную u, не входящую в QxB ни свободно, ни связанно и не фигурирующую в подстановке θ. Положим
$$[A\theta] \leftrightharpoons Qu[(B_u^x)(\theta - \{x\})].$$

Мы говорим, что $[A\theta]$ есть *результат правильной подстановки* θ в A.

8. Если θ есть $\begin{pmatrix} x_1, \ldots, x_k \\ t_1, \ldots, t_k \end{pmatrix}$, то вместо $[A\theta]$ мы часто будем писать $(A(x_1, \ldots, x_k \parallel t_1, \ldots, t_k))$. Если не возникает разночтений, эту запись сокращаем до $A(x_1, \ldots, x_k \parallel t_1, \ldots, t_k)$ или даже до $A(t_1, \ldots, t_k)$, если упоминание о переменных $x_1, \ldots, x_k$ несущественно.

Последнее обозначение, конечно, двусмысленно (неясно, вместо каких переменных подставляют термы!), но компактно и практически часто употребляется.

Например, если мы интересуемся параметрами x и y формулы A, то можно формулу A обозначить через $A(x, y)$. Если затем в контексте имеется формула $A(t, r)$, то следует, конечно, иметь в виду именно правильную подстановку $A(x, y \parallel t, r)$.

Упражнение. Произведите правильную подстановку:

1) $(\exists y P(z, y, x))(x, y, z \parallel z, z, y))$;
2) $(\exists z \forall y Q(x, y) \supset P(x))(x \parallel f(x, z))$.

§ 3. Семантика языка. Истинность в модели

1. Чтобы определить, что выражают формулы языка, следует, прежде всего, указать, какие множества пробегают переменные этого языка. Точно соответствующее понятие вводится следующим образом.

Пусть дан язык первого порядка:
$$\Omega = \langle \mathrm{Srt}, \mathrm{Cnst}, \mathrm{Fn}, \mathrm{Pr} \rangle.$$

Носителем для языка Ω, или *объектной областью* для языка Ω, мы назовем функцию D, сопоставляющую каждому сорту $\pi \in \mathrm{Srt}$ непустое множество D_π, D: $\pi \to D_\pi$.

Множество D_π называется *носителем сорта* π, или *объектной областью сорта* π. В наиболее популярном случае односортного языка носитель D полностью определяется заданием множества D_π.

Далее, мы желали бы изучать формулы и термы, в которые вместо параметров подставлены объекты носителя. По замыслу каждая такая «оцененная» формула задает в модели конкретное высказывание. Так, в нестрогих рассмотрениях п. 11 § 1 фигурировали выражения $P(3, 5, 3)$, $P(3, 5, 8)$, $\exists\, y P(2, y, 3)$ и т. д. Весьма желательно, чтобы выражения такого типа сами были бы формулами некоторого языка. С этой целью можно попытаться расширить исходный язык Ω объектами носителя, используя их в качестве новых констант языка. Но это неудобно по ряду причин. Во-первых, выражение языка есть строка из символов, а не объектов «произвольной природы», и нельзя замещать переменные выражения любыми объектами. Еще более серьезная причина состоит в том, что после подстановки объектов сложной природы может нарушаться однозначность чтения выражений. Так, элементы области D_π могут сами случайно оказаться выражениями языка Ω, и может оказаться, что после подстановки по полученному выражению уже невозможно определить, где именно находятся в нем объекты носителя.

Мы обойдем эту формальную трудность, сопоставив взаимно однозначным образом каждому объекту a сорта π из носителя новый символ $\underline{a}$ и образовав язык, полученный добавлением именно этих новых символов.

2. Итак, если задан носитель D для языка Ω, то можно определить новый язык $\Omega(D)$:

$$\Omega(D) = \langle \mathrm{Srt}, \mathrm{Cnst}(D), \mathrm{Fn}, \mathrm{Pr} \rangle,$$

отличающийся от Ω только наличием новых констант $\mathrm{Cnst} \subseteq \mathrm{Cnst}(D)$. А именно каждому элементу $a \in D_\pi$ и сорту π мы сопоставим новую константу $\underline{a}$ сорта π и добавим эту константу в множество $\mathrm{Cnst}(D)$. Каждая область D_π взаимно однозначно сопоставлена с множеством констант $\{\underline{a} \mid a \in D_\pi\}$. Кроме того, мы считаем, что константы различных сортов различны и, конечно, отличны от всех символов старого языка Ω.

Замкнутое выражение языка $\Omega(D)$ мы назовем *оцененным выражением* языка Ω. Можно представлять, что оцененное выражение получается из некоторого выражения языка Ω, если в последнем заместить все параметры новыми константами языка $\Omega(D)$. В частности, замкнутое выражение самого языка Ω является оцененным выражением.

Формальная подстановка языка $\Omega(D)$ вида $\begin{pmatrix} x_1, \ldots, x_k \\ \underline{a}_1, \ldots, \underline{a}_k \end{pmatrix}$, т. е. подстановка, принимающая в качестве значений новые константы, называется *оценкой* языка Ω (в носителе D). Заметим, что всякая оценка является константной подстановкой и потому свободна для всякого выражения.

Будем говорить, что оценка θ есть оценка *для выражения* T, если $\mathrm{Fv}(T) \subseteq \mathrm{dom}\,\theta$. В этом случае $T\theta$ есть всегда оцененное выражение.

Впрочем, на практике мы будем иногда смешивать a и $\underline{a}$. Необязательно следовать всем канонам строгости, достаточно понимать, как их достичь!

3. Введем фундаментальное в математической логике понятие — понятие *интерпретации* языка Ω (в другой терминологии — понятие *алгебраической структуры* языка Ω, *модели* языка Ω).

Чтобы определить интерпретацию M для языка Ω, необходимо задать несколько функций.

А именно:

1. Следует задать носитель D для языка Ω:

$$D\colon \pi \mapsto D_\pi \quad (\pi \in \mathrm{Srt}).$$

Мы говорим, что переменные сорта π *пробегают* область D_π. Таким образом, нужно задать область пробегания переменных каждого сорта.

2. Каждой константе $c \in \mathrm{Cnst}$ сорта π следует сопоставить объект $\widetilde{c} \in D_\pi$, т. е. следует задать функцию

$$\widehat{\mathrm{Cnst}}\colon c \mapsto \widetilde{c}.$$

3. Каждому функциональному символу $f \in \mathrm{Fn}$ вида $(\pi_1, \ldots, \pi_k \to \pi)$ следует сопоставить функцию $\widetilde{f}$ вида $D_{\pi_1} \times \ldots \times D_{\pi_k} \to D_\pi$, т. е. k-местную функцию, перерабатывающую наборы $a_1, \ldots, a_k$ объектов соответствующих сортов в объекты сорта π.

Все это соответствие задается, таким образом, функцией

$$\widehat{\mathrm{Fn}}\colon f \mapsto \widetilde{f}.$$

4. Каждому предикатному символу $P \in \mathrm{Pr}$ вида $(\pi_1, \ldots, \pi_k)$ следует сопоставить предикат $\widetilde{P}$ вида $D_{\pi_1} \times \ldots \times D_{\pi_k} \to \{0, 1\}$, т. е. k-местную функцию, перерабатывающую наборы $a_1, \ldots, a_k$ объектов из соответствующих областей $D_{\pi_1}, \ldots, D_{\pi_k}$ в истинностные значения 0 или 1 (0 — «ложь», 1 — «истина»).

В частном случае $k = 0$ пропозициональной букве P сопоставляется просто истинностное значение $\widetilde{P}$ (т. е. $\widetilde{P}$ есть 0 или 1).

Это соответствие задается функцией

$$\widehat{\mathrm{Pr}}\colon P \mapsto \widetilde{P}.$$

Таким образом, *модель* M для языка Ω определяется четверкой функций

$$M = \langle D, \widehat{\mathrm{Cnst}}, \widehat{\mathrm{Fn}}, \widehat{\mathrm{Pr}} \rangle$$

указанного выше вида.

Интуитивно говоря, модель языка есть предписание, сопоставляющее символам языка «настоящие» объекты: функциональным символам — функции, предикатным символам — предикаты и т. п. Если угодно, модель наполняет содержанием, смыслом символические выражения языка. Логики говорят, что модель определяет *семантику* языка (точнее, *классическую семантику первого порядка*).

4. Если дана модель M для языка Ω, то носитель D модели M определяет согласно п. 1 оцененные формулы и термы языка Ω.

Определим *значение* оцененного терма в модели M. Если t — терм сорта π, то его значение $|t|_M$ есть объект области D_π. Значение определяется индукцией по построению термов:

1) если $c \in \mathrm{Cnst}$, то $|c|_M = \widetilde{c}$;
2) если t имеет вид $\underline{a}$ для $a \in D_\pi$, то $|t|_M = a$;
3) $|f(t_1, \ldots, t_k)|_M = \widetilde{f}(|t_1|_M, \ldots, |t_k|_M)$.

Пусть теперь $t \in \mathrm{Tm}_\Omega$ — терм, быть может, содержащий параметры. Тогда для всякой оценки θ для t выражение $t\theta$ есть уже оцененный терм, и, следовательно, определено значение $|t\theta|_M$. Таким образом, терм с параметрами определяет *функцию* от своей оценки. Значение терма *зависит* от значений его параметров.

В частности, замкнутый терм $t \in \mathrm{Tm}_\Omega^\pi$ сам по себе является оцененным термом и определяет в M некоторый объект $|t|_M$.

5. Оцененные в модели M формулы языка Ω будем подразделять на *истинные* или *ложные* в M. Запись $M \models A$ будет означать: «оцененная формула A истинна в модели M». Определим $M \models A$ индукцией по логической сложности $l(A)$ формулы A:

1) $M \models P(t_1, \ldots, t_k) \leftrightharpoons \widetilde{P}(|t_1|_M, \ldots, |t_k|_M) = 1$;
2) $M \models A \wedge B \leftrightharpoons M \models A$ и $M \models B$;
3) $M \models A \vee B \leftrightharpoons M \models A$ или $M \models B$;
4) $M \models A \supset B \leftrightharpoons$ если $M \models A$, то $M \models B$;
5) $M \models \neg A \leftrightharpoons$ неверно, что $M \models A$;
6) $M \models \forall x A \leftrightharpoons$ для всякого $a \in D_\pi$, $M \models A^x_{\underline{a}}$;
7) $M \models \exists x A \leftrightharpoons$ существует $a \in D_\pi$, $M \models A^x_{\underline{a}}$,

в пунктах 6), 7) x — переменная сорта π.

Это определение является уточнением идеи истинности формулы, если:

— ее связки и кванторы понимать «естественным образом, как они читаются»,
— считать, что переменные сорта π пробегают объекты области D_π,
— функциональные символы и предикатные символы «понимаются» как функции и предикаты, указанные в модели M.

На первый взгляд определение истинности вообще может показаться бессодержательным (слева и справа написано одно и то же!). Это обманчивое впечатление.

Следует ясно понимать, что формула сама по себе ничего не означает, и нужно точно указать, как именно определять истинность формул в связи с моделью M. Чтение логических связок по-русски само по себе

не придает значения формуле, необходимо точное определение истинности. Заметим, что приведенное выше определение $M \models A$ является законным математическим определением индукцией по величине логической сложности формулы A. В самом деле, справа в определении фигурируют лишь формулы меньшей логической сложности, чем слева. Важной особенностью определения истинности по сравнению с другими индуктивными определениями, до сих пор у нас встречавшимися, является то, что для выяснения истинности некоторой формулы необходимо исследовать *бесконечное* количество формул меньшей сложности. Так, для установления $M \models \forall x A$ следует убедиться, что имеет место $M = A_a^x$ *для всех* $a \in D_\pi$, в то время как область D_π может быть (и обыкновенно бывает) бесконечной. Аналогично, для установления $M \models \exists x A$ следует показать существование $a \in D_\pi$ такого, что $M \models A_{\underline{a}}^x$. Если D_π бесконечна, то этого нельзя сделать, просто перебирая все объекты из D_π. Приходится провести некоторое теоретическое исследование. Это одна из причин особой сложности предиката истинности, источник многих замечательных свойств этого понятия.

Если формула содержит параметры, то истинность или ложность ее зависят от оценки ее параметров. При одной оценке параметров формула будет истинной в модели, при другой — ложной. Таким образом, в данной модели формула с параметрами задает *предикат* от своих параметров в соответствии с нашим замыслом.

В частном случае, когда формула замкнута, она определяет в M некоторое истинностное значение. Таким образом, замкнутая формула задает конкретное истинное или ложное *высказывание.*

6. Уточним теперь наше понимание логических связок $\wedge$, $\vee$, $\supset$, $\neg$. Пусть, как и ранее, 1 означает «истина», 0 — «ложь». Логические связки $\wedge$, $\vee$, $\neg$ ведут себя как операции в простейшей булевой решетке из двух элементов $\{0, 1\}$. Удобно ввести также производную логическую связку — *эквиваленцию* — с помощью знакомого нам сокращения:

$$A \equiv B \leftrightharpoons (A \supset B) \wedge (B \supset A).$$

A	B	$A \wedge B$	$A \vee B$	$A \supset B$	$A \equiv B$	$\neg A$
1	1	1	1	1	1	0
1	0	0	1	0	0	0
0	1	0	1	1	0	1
0	0	0	0	1	1	1

Таким образом, если A и B истинны, то высказывание $A \vee B$ также истинно, т. е. мы понимаем $A \vee B$ как «по крайней мере A или B». Это так называемое «неразделительное или». В обыденном языке чаще употребляется «разделительное или» — «A или B, но не оба вместе», что в наших связках может быть записано примерно так: $(A \vee B) \wedge \neg(A \wedge B)$.

Особую проблему составляет понимание импликации. Как понимать импликацию, если ее посылка ложна? Попутно заметим, что в импликации $A \supset B$ формула A называется *посылкой* (иногда — *антецедентом*), формула B — *заключением* (иногда — *сукцедентом*, или *консеквентом*). В обыденной жизни сообщение $A \supset B$, если заведомо *известно*, что A ложно, не считается ни истинным, ни ложным; такое сообщение просто не имеет ценности, бессодержательно. Какое значение может иметь сообщение «если A, то B», если A ложно и, следовательно, вышеуказанное сообщение не может быть использовано для отыскания B? Если мы желаем иметь логику только с двумя истинностными значениями 0 и 1, то с этой точки зрения последние две строчки в таблице для импликации можно заполнить произвольным образом.

В целях лучшего соответствия с практикой обычных математических рассуждений, где часто приходится использовать импликацию как раз в ситуации, когда истинностное значение посылки *неизвестно*, в последних двух строках имликации ставят истину. Так понимаемая импликация называется *материальной*, именно она и используется в математике.

Эквивалентность истинна тогда и только тогда, когда оба ее члена имеют одинаковые истинностные значения: оба истинны или оба ложны.

7. Пусть формула A языка Ω составлена из формул $A_1, \ldots, A_k$ с помощью логических связок $\wedge$, $\vee$, $\supset$, $\neg$ без использования кванторов. Кванторы могут входить лишь в состав самих формул A_i. Тогда мы говорим, что формула A есть *булева комбинация* формул $A_1, \ldots, A_k$.

Мы хотели бы полностью проанализировать, как зависит истинность формулы A от истинности формул $A_1, \ldots, A_k$. Такой анализ дает построение *таблицы Куайна* для формулы A.

Построение таблицы начинается с того, что под каждой из формул $A_1, \ldots, A_k$ мы выписываем всевозможные комбинации нулей и единиц. Возникает k столбцов из нулей и единиц, каждый столбец высотой 2^k. Затем выполняем почленно все операции формулы, пока не получаем последний главный столбец таблицы. Операции выполняются над столбцами.

Вот пример составления таблицы Куайна для формулы — булевой комбинации формул A, B, C (главный столбец выделен):

A	$\supset$	$(B$	$\vee$	C	$\supset .$	C	$\supset$	$\neg$	$A)$
1	0	1	1	1	0	1	0	0	1
1	1	1	1	0	1	0	1	0	1
1	0	0	1	1	0	1	0	0	1
1	1	0	0	0	1	0	1	0	1
0	1	1	1	1	1	1	1	1	0
0	1	1	1	0	1	0	1	1	0
0	1	0	1	1	1	1	1	1	0
0	1	0	0	0	1	0	1	1	0

Из таблицы видно, что наша формула может быть ложна лишь в двух случаях:

A	B	C
1	1	1
1	0	1

Дальнейший анализ зависит уже от строения формул A, B, C и от рассматриваемой модели. Может оказаться, например, что в рассматриваемой модели оба случая не реализуются и, следовательно, наша формула истинна.

Особенно интересен случай, когда главный столбец таблицы состоит лишь из единиц. Это означает, что независимо от истинности составляющих формул $A_1, \ldots, A_k$ рассматриваемая формула будет истинной (при любой оценке, в любой модели). Такую формулу мы назовем *пропозициональной тавтологией.*

Упражнение. Убедитесь, что следующая формула является пропозициональной тавтологией:

$$A \equiv B \supset . A \vee C \equiv B \vee C.$$

§ 4. Примеры языков и моделей

1. Рассмотрим язык элементарной арифметики Ar. Язык Ar содержит лишь один сорт объектов и, следовательно, один сорт переменных $x, y, z, \ldots$. Ar содержит единственную константу, которую мы обозначим 0, и три функциональных символа f, g, h, причем f — одноместный функциональный символ, g, h — двуместные функциональные символы.

Пример терма Ar:

$$g(h(x, 0), g(f(y), f(f(0)))).$$

Специально для языка Ar удобно ввести обозначения:

$$(t + r) \leftrightharpoons g(t, r),$$
$$(t \cdot r) \leftrightharpoons h(t, r),$$
$$\mathrm{St} \leftrightharpoons f(t).$$

В этих обозначениях (с обычной экономией скобок) предыдущий терм запишется в виде

$$x \cdot 0 + (Sy + SS0).$$

Наконец, язык Ar содержит единственную двуместную предикатную букву P. Вместо $P(t, r)$ мы будем писать $(t = r)$. Атомарные формулы языка Ar мы будем называть *формальными равенствами.*

Описание языка Ar закончено.

Рассмотрим модель для Ar, которую мы назовем ω. Носитель ω есть множество натуральных чисел (это множество мы также обозначим через ω).

Константе 0 припишем значение $0 \in \omega$.

Функциональным символам $x + y$, $x \cdot y$, Sx припишем функции сложения, умножения и прибавления единицы в области натуральных чисел.

Атомарная формула $x = y$ выражает в ω совпадение натуральных чисел, т. е. $\omega \models (\underline{n} = \underline{m}) \Leftrightarrow n$ и m есть одно и то же натуральное число.

Описание модели ω закончено.

Примеры. Терм $(x + y) \cdot z + Sx$, оцененный посредством

$$\begin{pmatrix} x & y & z \\ \underline{1} & \underline{5} & \underline{3} \end{pmatrix},$$

задает оцененный терм $(\underline{1} + \underline{5}) \cdot \underline{3} + S\underline{1}$ и имеет в ω значение 20. Этот же терм при оценке

$$\begin{pmatrix} x & y & z \\ \underline{2} & \underline{6} & \underline{4} \end{pmatrix}$$

имеет вид $(\underline{2} + \underline{6}) \cdot \underline{4} + S\underline{2}$ и имеет значение 35.

Формула $\exists y(x + y = z)$ при оценке

$$\begin{pmatrix} x & z \\ \underline{3} & \underline{5} \end{pmatrix}$$

превращается в оцененную формулу

$$\exists y(\underline{3} + y = \underline{5}),$$

которая истинна. При оценке

$$\begin{pmatrix} x & z \\ \underline{5} & \underline{3} \end{pmatrix}$$

получим ложную формулу $\exists y(\underline{5} + y = \underline{3})$.

Некоторые формулы Ar истинны в ω при любой оценке. Такие формулы назовем *арифметическими законами* (языка Ar). Например, таковы

$$\begin{aligned} &x + y = y + x, \\ &\neg x = 0 \supset \exists z(Sz = x), \\ &Sx = Sy \supset x = y. \end{aligned}$$

Можно ввести сокращенные обозначения для формул Ar, естественные с точки зрения интерпретации ω:

$$\begin{aligned} x \leqslant y &\leftrightharpoons \exists z(x + z = y), \\ x < y &\leftrightharpoons x \leqslant y \wedge \neg x = y, \\ (x \text{ — четно}) &\leftrightharpoons \exists y(x = y + y), \\ (x \mid y) &\leftrightharpoons \neg x = 0 \wedge \exists z(x \cdot z = y), \\ (x \text{ — простое}) &\leftrightharpoons \neg x = 0 \wedge \neg x = S0 \wedge \forall z((z \mid x) \supset z = S0 \vee z = x). \end{aligned}$$

Можно выразить некоторые высказывания в языке Ar.

1) $\forall x((x$ — простое $) \supset \exists y((x < y) \wedge (y$ — простое $)))$ «количество простых чисел бесконечно».
2) $\forall x \exists y(x \leqslant y \wedge (y$ — простое$) \wedge (y + SS0$ — простое $))$ «количество простых чисел-близнецов бесконечно». Истинно или ложно это последнее высказывание — неизвестно в настоящее время.
3) Принцип полной математической индукции также можно выразить в Ar. А именно, для каждой формулы A в ω истинна формула

$$A(0) \wedge \forall x(A(x) \supset A(Sx)) \supset \forall x A(x).$$

Более аккуратно, не употребляя неформального обозначения $A(x)$, этот принцип можно записать в виде

$$A_0^x \wedge \forall x(A \supset A_{Sx}^x) \supset \forall x A.$$

Заметим, что в языке Ar для каждой формулы A формулируется свой принцип индукции, в языке нет возможности сказать: «для всякой формулы A». Индукция формулируется в виде бесконечной серии формул — *схемы аксиом индукции*.

2. Рассмотрим другую модель для Ar, которую мы обозначим через R. Носитель этой модели есть множество R действительных чисел. Константе 0 соответствует 0, символам $+$, $\cdot$, S опять-таки соответствуют сложение, умножение и прибавление единицы, но уже в области действительных чисел. Формула $x = y$ выражает совпадение действительных чисел.

Формулы Ar, истинные при любой оценке в R, назовем *законами действительных чисел* (языка Ar). Таковы, например, формулы

$$x + y = y + x,$$
$$Sx = Sy \supset x = y,$$
$$\forall x \exists z(x + z = 0),$$
$$\neg x = 0 \supset \exists y(x \cdot y = S0).$$

Заметим, что здесь фигурируют и формулы, не являющиеся арифметическими законами. Понятие закона языка зависит от его интерпретации, его модели. Как говорят логики, это *семантическое понятие*.

В модели R естественны уже другие сокращенные обозначения для формул. Например, с точки зрения R естественно ввести обозначение

$$x \leqslant y \leftrightharpoons \exists z(x + z \cdot z = y).$$

Упражнение. Определите естественным образом модель Z целых чисел для языка Ar. Как в этой модели определить $x \leqslant y$? (Указание: по известной теореме Лагранжа каждое натуральное число представимо в виде суммы четырех квадратов).

Часто язык рассматривают вместе с какой-либо одной выделенной моделью, которую называют *подразумеваемой интерпретацией* (*естественной моделью*, *стандартной моделью*) языка. Для языка Ar стандартной моделью мы будем считать модель ω.

Все выразительные возможности языка Ar, может быть, и не видны с первого взгляда. Например, может показаться стеснительным, что в Ar есть сложение и умножение, но нет обозначения для функции 2^x. В действительности функция 2^x (и весьма многие другие) может быть выражена в Ar в виде формулы, т. е. может быть построена формула $A(x, y)$ с двумя параметрами x и y такая, что

$$\omega \models A(\underline{m}, \underline{n}) \Leftrightarrow m = 2^n.$$

О теории определения числовых функций можно прочесть в более подробных курсах математической логики (см. список литературы).

3. Рассмотрим язык *линейного порядка* Lin. Этот язык содержит лишь один сорт переменных $x, y, z, \ldots$ и не содержит ни констант, ни функциональных символов. Язык Lin содержит два двуместных предикатных символа P и Q. Мы обозначим

$$x = y \leftrightharpoons P(x, y),$$
$$x < y \leftrightharpoons Q(x, y).$$

Вот формулы языка Lin:

$$\forall x \forall y(x < y \supset \exists z(x < z \wedge z < y)),$$
$$x < y \vee (x = y \vee y < x).$$

Важнейшей моделью Lin является Q (здесь через Q мы обозначаем также множество рациональных чисел). Носитель модели Q есть множество Q.

$\underline{a} = \underline{b}$ означает, что a и b равны как рациональные числа;

$\underline{a} < \underline{b}$ означает, что $a < b$ в области рациональных чисел.

Приведенные выше формулы суть законы рациональных чисел языка Lin.

Упражнение. Убедитесь, что следующая формула не является законом рациональных чисел:

$$\exists x \forall y(x = y \vee x < y).$$

Упражнение. Определите модель ω для Lin, где $x < y$ означает отношение «меньше» на множестве ω. Какие из вышеуказанных формул Lin являются законами ω?

4. Определим еще язык *векторного пространства* Vect. Этот язык содержит два сорта переменных: переменные для действительных чисел $x, y, z, \ldots$ (сорт 0) и переменные для векторов $a, b, c, \ldots$ (сорт 1).

Язык Vect содержит две константы:

0_0 — «нуль-действительное число», это константа сорта действительных чисел;

0_1 — «нуль-вектор», это константа сорта векторов.

Язык Vect содержит пять функциональных символов:

$$\begin{aligned} f &\ — \text{ одноместный вида } 0 \to 0,\\ g, h &\ — \text{ двуместные вида } (0, 0 \to 0),\\ p &\ — \text{ двуместный вида } (1, 1 \to 1),\\ q &\ — \text{ двуместный вида } (0, 1 \to 1). \end{aligned}$$

Обозначим

$$\begin{aligned} Sx &\leftrightharpoons f(x),\\ (x + y) &\leftrightharpoons g(x, y),\\ (x \cdot y) &\leftrightharpoons h(x, y),\\ (a + b) &\leftrightharpoons p(a, b),\\ (x \cdot a) &\leftrightharpoons q(x, a). \end{aligned}$$

Наконец, наш язык содержит два двуместных предикатных символа: P вида $(0, 0)$ и Q вида $(1, 1)$. Введем обозначение:

$$\begin{aligned} (x = y) &\leftrightharpoons P(x, y),\\ (a = b) &\leftrightharpoons Q(a, b). \end{aligned}$$

Вот несколько формул языка Vect:

$$\begin{gathered} x \cdot (a + b) = x \cdot a + x \cdot b,\\ x \cdot (y \cdot a) = (x \cdot y) \cdot a,\\ \forall a \exists b (a + b = 0_1),\\ 0_0 \cdot a = 0_1,\\ \exists a \exists b \forall x \forall y (x \cdot a + y \cdot b = 0_1 \supset x = 0_0 \wedge y = 0_0). \end{gathered}$$

Типичной структурой языка Vect является *n-мерное векторное линейное пространство* E_n над полем действительных чисел.

Упражнение. Определите подробнее модель E_n для Vect. Какие из вышеприведенных формул есть законы E_1, E_2?

Формулу Vect назовем *законом векторного пространства*, если она является законом E_n при всяком n.

Упражнение. Какие из вышеприведенных формул Vect суть законы векторного пространства?

5. В практике математического рассуждения часто вместе с основными объектами исследования используются и более сложные теоретико-множественные образования — множества объектов, множества множеств объектов и т. д. Например, в рассуждениях о натуральных числах используется понятие идеала, а идеал — это особым образом устроенное множество целых чисел. Чтобы иметь возможность естественно записывать такие рассуждения в точном языке, язык Ar элементарной

арифметики следует пополнить переменными для множеств натуральных чисел, а также, если это необходимо, переменными для множеств множеств натуральных чисел. Таким образом, возникает расширяющаяся иерархия языков: *арифметика второго порядка*, *арифметика третьего порядка* и т. д. — *теоретико-множественные надстройки* элементарного языка. Объединение всех таких языков конечного порядка образует язык *простой теории типов* Рассела и Уайтхеда, играющий важную роль в основаниях математики.

В качестве примера опишем подробнее язык Ar2 арифметики второго порядка. Этот язык содержит два сорта переменных: переменные для натуральных чисел $x, y, z, \ldots$ (сорт 0) и переменные для подмножеств множества ω натуральных чисел $X, Y, Z, \ldots$ (сорт 1). Далее, язык Ar2 содержит те же функциональные и предикатные символы, что и язык Ar, и, кроме того, новый предикатный символ Q вида $(0, 1)$.

Обозначение

$$t \in X \leftrightharpoons Q(t, X).$$

Подразумеваемой моделью языка Ar2 является модель, которую мы будем обозначать через ω, как и в случае элементарного языка Ar. В этой модели переменные сорта 0 пробегают натуральные числа. Функциональные и предикатные символы языка Ar2 интерпретируются в этой модели так же, как они интерпретировались в стандартной модели ω для языка Ar. Далее, переменные $X, Y, Z, \ldots$ сорта 1 рассматриваются как пробегающие *произвольные* подмножества множества ω. Наконец, если U есть подмножество ω и n — натуральное число, то по определению

$$\omega \models Q(\underline{n}, \underline{U}) \Leftrightarrow n \in U.$$

Некоторые обозначения языка Ar2:

$$X \subseteq Y \leftrightharpoons \forall x(x \in X \supset x \in Y),$$
$$X = Y \leftrightharpoons (X \subseteq Y) \wedge (Y \subseteq X),$$
$$X \subset Y \leftrightharpoons (X \subseteq Y) \wedge \neg(X = Y),$$
$$(X \text{ — бесконечно}) \leftrightharpoons \forall x \exists y(x \leqslant y \wedge y \in X).$$

Для каждой формулы $A(x)$ языка Ar2 можно образовать множество всех натуральных чисел x, удовлетворяющих условию $A(x)$ в стандартной модели ω. Утверждение о существовании этого множества называется *аксиомой свертывания* и выражается следующей формулой Ar2, истинной в ω:

$$\exists X \forall x(x \in X \equiv A(x)),$$

где X не входит свободно в $A(x)$.

Аналогичным образом можно определить теоретико-множественные надстройки и для других из рассмотренных нами языков.

§ 5. Логические законы

1. Сделаем несколько замечаний о сокращенных способах рассуждений с оцененными формулами.

Пусть фиксирована модель M языка Ω.

Тогда вместо $M \models A$ говорят просто «истинно A», не упоминая M, или «пусть A» или даже просто «A» (это так называемое *утвердительное* употребление формулы A).

Если нас интересует формула A при произвольной оценке, то мы употребляем *сами параметры* A, чтобы обозначать эту произвольную оценку. При этом говорят примерно так: «фиксируем параметры A таким образом, что...».

Приведем два примера.

1) Покажем, что формула

$$\exists y((x + Sy) = z) \supset \exists u((Sx + u) = z)$$

есть арифметический закон.

Подробное рассуждение может выглядеть следующим образом.

Возьмем произвольную оценку $\begin{pmatrix} x & z \\ \underline{m} & \underline{n} \end{pmatrix}$, $m, n \in \omega$ и докажем

$$\omega \models \exists y(\underline{m} + Sy = \underline{n}) \supset \exists u(S\underline{m} + u = \underline{n}).$$

С этой целью допустим

$$\omega \models \exists y(\underline{m} + Sy = \underline{n})$$

и установим

$$\omega \models \exists u(S\underline{m} + u = \underline{n}).$$

Так как $\omega \models \exists y(\underline{m} + Sy = \underline{n})$, то существует $k \in \omega$ такое, что $\omega \models \underline{m} + S\underline{k} = \underline{n}$. Но, очевидно,

$$|\underline{m} + S\underline{k}|_\omega = |S\underline{m} + \underline{k}|_\omega.$$

Тогда из $\omega \models \underline{m} + S\underline{k} = \underline{n}$ следует

$$\omega \models S\underline{m} + \underline{k} = \underline{n},$$

что и дает

$$\omega \models \exists u(S\underline{m} + u = \underline{n}).$$

В сокращенной форме это же рассуждение может выглядеть таким образом.

Фиксируем x и z и докажем, что

$$\exists y(x + Sy = z) \supset \exists u(Sx + u = z).$$

Пусть $\exists y(x + Sy = z)$, установим $\exists u(Sx + u = z)$. Если $\exists y(x + Sy = z)$, то для некоторого y имеем $x + Sy = z$. Но для натуральных чисел, очевидно,

$$x + Sy = Sx + y,$$

так что $Sx + y = z$, а, значит, $\exists u(Sx + u = z)$ (достаточно в качестве u взять y).

2) Пусть $A \in \mathrm{Fm}_\Omega$. Покажем, что в любой модели M языка Ω и при любой оценке θ для A будет иметь место

$$M \models (\neg\forall x A \supset \exists x \neg A)\theta.$$

Подробное рассуждение. Переменная x не входит свободно в рассматриваемую формулу, поэтому можно считать, что $\mathrm{dom}\,\theta = \mathrm{Fv}(A)\backslash\{x\}$.

Ввиду п. 2 § 2 необходимо показать, что

$$M \models \neg\forall x(A\theta) \supset \exists x \neg(A\theta).$$

С этой целью допустим $M \models \neg\forall x(A\theta)$ и докажем, что $M \models \exists x \neg(A\theta)$. Так как $M \models \neg\forall x(A\theta)$, то неверно, что $M \models \forall x(A\theta)$. Таким образом, неверно, что для всякого объекта a из области соответствующего сорта

$$M \models (A\theta)^x_{\underline{a}}.$$

(Кстати, заметим, что

$$(A\theta)^x_{\underline{a}} = A\left(\theta\left(\tfrac{x}{\underline{a}}\right)\right).)$$

Следовательно, существует a такое, что неверно $M \models (A\theta)^x_{\underline{a}}$, что означает $M \models \neg(A\theta)^x_{\underline{a}}$.

По определению истинности это дает

$$M \models \exists x \neg(A\theta),$$

что и требовалось.

Сокращенное рассуждение. Возьмем произвольную модель и фиксируем параметры нашей формулы. Докажем

$$\neg\forall x A \supset \exists x \neg A.$$

Пусть $\neg\forall x A$, установим $\exists x \neg A$. Так как $\neg\forall x A$, то не для всех x имеет место A, и, следовательно, найдется x, для которого $\neg A$. Таким образом, $\exists x \neg A$.

Следует развивать навыки такого сокращенного рассуждения (*дедуктивноподобный способ рассуждения*), но, разумеется, в случае необходимости нужно уметь восстановить и все детали.

2. Формула A языка Ω называется *логическим законом* (другие термины — *общезначимой формулой*, *тавтологией*), если A истинна во всякой модели языка Ω при любой оценке. Запись $\models A$ означает: «A есть логический закон». Покажем, например, что

$$\models \neg A \vee B \supset \neg(A \wedge \neg B).$$

С этой целью рассмотрим произвольную модель M языка Ω и произвольную оценку θ для нашей формулы. Необходимо доказать, что

$$M \models (\neg A \vee B \supset \neg(A \wedge \neg B))\theta.$$

Для этого достаточно показать

$$M \models \neg(A\theta) \vee (B\theta) \supset \neg((A\theta) \wedge \neg(B\theta)).$$

Допустим $M \models \neg(A\theta) \vee (B\theta)$ и установим

$$M \models \neg((A\theta) \wedge \neg(B\theta)),$$

т. е. установим, что неверно $M \models (A\theta) \wedge \neg(B\theta)$. А для этого мы допустим еще, что

$$M \models (A\theta) \wedge \neg(B\theta),$$

и получим противоречие.

Но действительно, из первого допущения следует, что имеет место одно из двух:

a) $M \models \neg(A\theta)$,

b) $M \models (B\theta)$.

Мы видим, что обе возможности противоречат второму допущению, так как из второго допущения следует, что $M \models A\theta$, $M \models \neg(B\theta)$.

Утверждение доказано.

Сокращенное дедуктивноподобное доказательство этого же факта может выглядеть следующим образом. Пусть $\neg A \vee B$, установим $\neg(A \wedge \neg B)$. Допустим еще, что $A \wedge \neg B$, и получим противоречие. Из первого допущения следует, что а) $\neg A$ или b) B, а из второго — что A и $\neg B$. В случае а) имеем противоречие A и $\neg A$, а в случае b) — противоречие B и $\neg B$.

Наконец, есть еще способ установить наш логический закон. Достаточно формально проверить, что наша формула как булева комбинация A и B является пропозициональной тавтологией:

¬	A	∨	B	⊃	¬	(A	∧	¬	B)
0	1	1	1	1	1	1	0	0	1
0	1	0	0	1	0	1	1	1	0
1	0	1	1	1	1	0	0	0	1
1	0	1	0	1	1	0	0	1	0

Покажем теперь

$$\models \neg\exists x \neg A \supset \forall x A.$$

Нашу формулу можно рассматривать как булеву комбинацию формул $\exists x \neg A$, $\forall x A$, но она не является пропозициональной тавтологией:

¬	$\exists x \neg A$	⊃	$\forall x A$
0	1	1	1
0	1	1	0
1	0	1	1
1	0	0	0

Тем не менее, это — логический закон, что мы и установим, учитывая кванторную структуру формулы.

Итак, пусть M — произвольная модель языка, а θ — произвольная оценка для нашей формулы. Переменная x не входит свободно в нашу формулу, так что можно считать

$$\operatorname{dom}\theta = \operatorname{Fv}(A)\backslash\{x\}.$$

Проделав подстановку по правилам п. 2 § 2, можно считать, что необходимо доказать

$$M \models \neg\exists x\neg(A\theta) \supset \forall x(A\theta).$$

Допустим

$$M \models \neg\exists x\neg(A\theta)$$

и докажем $M \models \forall x(A\theta)$, т. е. что для всякого объекта $a \in D_\pi$, $M \models (A\theta)^x_{\underline{a}}$. Предположим противное, т. е. что для некоторого $a \in D_\pi$ неверно, что $M \models (A\theta)^x_{\underline{a}}$. Тогда для этого a имеем $M \models \neg(A\theta)^x_{\underline{a}}$ и, значит, $M \models \exists\neg(A\theta)$, что, однако, противоречит первому допущению.

Пусть P — двуместная атомарная буква некоторого языка. Докажем, что формула

$$\forall x\exists y P(x,y) \supset \exists y\forall x P(x,y)$$

не является логическим законом.

С этой целью нужно подобрать модель и оценку, в которой эта формула ложна. Об оценке можно пока не беспокоиться, так как наша формула замкнута, является предположением и сама по себе, как известно, является оцененной формулой (строго говоря, можно взять пустую оценку). Модель же должна быть такова, чтобы посылка была истинной, а заключение — ложным (тогда и вся импликация будет ложной).

Пусть x и y пробегают натуральные числа, а $P(x,y)$ интерпретируется как $x < y$. Тогда, очевидно,

$$\omega \models \forall x\exists y P(x,y)$$

и неверно, что

$$\omega \models \exists y\forall x P(x,y).$$

Упражнение. Покажите, что следующие формулы не являются логическими законами. Здесь $P, Q, P(x,y)$ суть атомарные формулы.

1. $P \supset Q \supset .Q \supset P$.
2. $\exists x P(x) \supset \forall x P(x)$.
3. $\forall x\exists y P(x,y) \supset \exists y\forall x P(x,y)$.
4. $\exists x P(x) \wedge \exists x Q(x) \supset \exists x(P(x) \wedge Q(x))$.
5. $\forall x(P(x) \vee Q(x)) \supset \forall x P(x) \vee \forall x Q(x)$.
6. $\forall x P(x,x) \supset \forall x\forall y P(x,y)$.
7. $\exists x\exists y P(x,y) \supset \exists x P(x,x)$.
8. $P(x) \supset \forall x P(x)$.
9. $\exists x P(x) \supset P(x)$.
10. $\forall x P(x,y) \equiv \forall y P(y,y)$.
11. $\exists x P(x,y) \equiv \exists y P(y,y)$.

3. Две формулы A и B называются *логически эквивалентными*, если $A \equiv B$ есть логический закон. Мы будем писать $A \sim B$ вместо «A логически эквивалентно B», т. е. вместо $\models A \equiv B$.

Как доказать $A \sim B$? Следует установить два факта: $\models A \supset B$, $\models B \supset A$, т. е. для произвольной модели M и оценки θ для формулы $A \supset B$ следует, допустив $M \models A\theta$, доказать $M \models B\theta$, а затем, допустив $M \models B\theta$, доказать $M \models A\theta$.

4. Упомянем о некоторых логических законах. Вывод их предоставляется читателю.

Законы де Моргана:

1. $\neg(A \vee B) \sim \neg A \wedge \neg B$.
2. $\neg(A \wedge B) \sim \neg A \vee \neg B$.
3. $\neg \forall x A \sim \exists x \neg A$.
4. $\neg \exists x A \sim \forall x \neg A$.

Закон контрапозиции:

5. $A \supset B \sim \neg B \supset \neg A$.

Формула $\neg B \supset \neg A$ называется *контрапозицией* формулы $A \supset B$.

Закон двойного отрицания:

6. $\neg\neg A \sim A$.

В следующих восьми эквивалентностях формула A не содержит свободно переменной x. Одностороннее пронесение кванторов:

7. $A \wedge \forall x B(x) \sim \forall x(A \wedge B(x))$.
8. $A \vee \forall x B(x) \sim \forall x(A \vee B(x))$.
9. $A \wedge \exists x B(x) \sim \exists x(A \wedge B(x))$.
10. $A \vee \exists x B(x) \sim \exists x(A \vee B(x))$.
11. $A \supset \exists x B(x) \sim \exists x(A \supset B(x))$.
12. $A \supset \forall x B(x) \sim \forall x(A \supset B(x))$.
13. $\forall x B(x) \supset A \sim \exists x(B(x) \supset A)$.
14. $\exists x B(x) \supset A \sim \forall x(B(x) \supset A)$.

Если допустить, что формула A может содержать свободно переменную x, то законы пронесения кванторов уже не имеют столь совершенного вида:

15. $\forall x A(x) \wedge \forall x B(x) \sim \forall x(A(x) \wedge B(x))$.
16. $\exists x A(x) \vee \exists x B(x) \sim \exists x(A(x) \vee B(x))$.
17. $\models \exists x(A(x) \wedge B(x)) \supset \exists x A(x) \wedge \exists x B(x)$.
18. $\models \forall x A(x) \vee \forall x B(x) \supset \forall x(A(x) \vee B(x))$.

Пусть теперь A — формула, x, y — различные переменные одного сорта, причем y не входит свободно в A. Тогда имеют место следующие законы переименования кванторов:

19. $\forall x A \sim \forall y(A(x \parallel y))$.
20. $\exists x A \sim \exists y(A(x \parallel y))$.

Сокращенно такого рода законы записывают просто как

$$\forall x A(x) \sim \forall y A(y).$$

Не следует, однако, забывать, что такая эквивалентность верна лишь при соблюдении сделанных выше оговорок.

5. Имеется также несколько важных, простых и интуитивно очевидных правил, позволяющих преобразовывать эквивалентным образом формулы. Они могут быть, конечно, точно доказаны, исходя из точных определений, но мы не будем здесь на этом останавливаться.

21. Если $A \approx B$, то $A \sim B$.

22. Если $A \sim B$, то $A(x_1, \ldots, x_k \parallel t_1, \ldots, t_k) \sim B(x_1, \ldots, x_k \parallel t_1, \ldots, t_k)$.

Далее, мы хотели бы получить аналогичный результат для замены внутри формулы некоторой подформулы на эквивалентную. Например, кажется, что следующие две формулы эквивалентны:

$$R(x) \vee \forall z \underline{\neg \forall x Q(x, z)}; \quad R(x) \vee \forall z \underline{\exists x \neg Q(x, z)},$$

так как они получаются заменой подчеркнутой формулы по закону де Моргана. Естественно считать, что, например, первая из рассматриваемых формул получена из формулы $R(x) \vee \forall z P(z)$ путем подстановки вместо предикатной буквы P формулы $\neg \forall x Q(x, z)$, причем параметр z играет роль аргумента при подстановке. В общем случае подставляемые формулы могут содержать и другие параметры, остающиеся фиксированными при подстановке, и следует обычным образом избегать коллизии переменных. Дадим точное индуктивное определение подстановки вместо предикатной буквы.

Пусть A — формула и $x_1, \ldots, x_k$ — список различных переменных сортов $\pi_1, \ldots, \pi_k$ соответственно. *Формальным предикатом* вида $(\pi_1, \ldots, \pi_k)$ назовем выражение

$$x_1 \ldots x_k A.$$

Переменные x_i назовем аргументными переменными формального предиката и будем рассматривать как *связанные* переменные. Здесь не исключается и случай $k = 0$, т. е. всякая формула сама по себе является формальным предикатом вида ( ) без аргументных мест.

Пусть B — формула, $U = x_1 \ldots x_k A$ — формальный предикат вида $(\pi_1, \ldots, \pi_k)$, P — предикатная буква вида $(\pi_1, \ldots, \pi_k)$. Индукцией по логической сложности $l(B)$ определим формулу $B(P \parallel U)$ — результат *правильной подстановки* (*замены*) P в формуле B на формальный предикат U.

A. Пусть B есть атомарная формула $Q(r_1, \ldots, r_m)$. Если Q отлична от P, то $B(P \parallel U) = B$. Если же Q есть P, то $B(P \parallel U) = A(x_1, \ldots, x_k \parallel r_1, \ldots, r_m)$.

В этом случае, конечно, $k = m$.

Б. B есть $(C \Delta D)$, тогда

$$B(P \parallel U) = C(P \parallel U) \Delta D(P \parallel U).$$

B есть $\neg C$, тогда $B(P \parallel U) = \neg(C(P \parallel U))$.

В. B имеет вид QzC. Здесь следует рассмотреть два случая.

1. U не содержит свободно z, или P не входит в C. Напомним, что все вхождения $x_1, \ldots, x_k$ в U считаются связанными. В рассматриваемом случае
$$B(P \parallel U) = Qz(C(P \parallel U)).$$
2. U содержит свободно z, и P входит в C. Выберем тогда новую переменную u и положим
$$B(P \parallel U) = Qu((C_u^z)(P \parallel U)).$$

В соответствии с этим определением нетрудно увидеть, что формула $R(x) \vee \forall z \neg \forall x Q(x, z)$ представима как результат правильной подстановки

$$(R(x) \vee \forall z P(z))(P \parallel z \neg \forall x Q(x, z)).$$

Теперь мы можем продолжить описание логических законов

23. $\models \forall x_1 \ldots x_k (A \equiv B) \supset . C(P \parallel x_1 \ldots x_k A) \equiv C(P \parallel x_1 \ldots x_k B)$.

24. Если $A \sim B$, то $C(P \parallel x_1 \ldots x_k A) \sim C(P \parallel x_1 \ldots x_k B)$.

Именно это правило и решает задачу, поставленную в начале п. 5. Логические законы можно использовать, заменяя эквивалентные подформулы внутри формулы.

Формулу вида $C(P \parallel x_1 \ldots x_k A)$ часто называют *подстановочным примером*, или *частным случаем* формулы C. Мы видим, в частности, что если C есть логический закон, то всякий подстановочный пример формулы C также является логическим законом.

§ 6. Приложения теории логико-математических языков. Предваренная форма. Дизъюнктивная и конъюнктивная нормальная форма. Язык логики высказываний и логики предикатов

1. *Предваренной* (или *пренексной*) формулой называется формула вида

$$Q_1 x_1 \ldots Q_n x_n A,$$

где Q_i суть кванторы, а формула A (называемая *матрицей* предваренной формулы) уже кванторов не содержит. Таким образом, в предваренной формуле все кванторы находятся в начале формулы. В частности, мы не исключаем и случая $n = 0$, бескванторная формула также считается предваренной.

Если $A \sim B$ и B — предваренная формула, то B называют *предваренной формой* формулы A.

Теорема о предваренной форме. *Для всякой формулы A существует предваренная формула B, $A \sim B$.*

▷ По лемме п. 7 § 2 найдется формула C со свойством чистоты переменных $A \approx C$, и, следовательно, $A \sim C$ (см. п. 5 § 5). Затем, используя одностороннее пронесение кванторов (п. 4 § 5, законы 7–14), приводим C к предваренной форме. При этом мы пользуемся тем, что можно *внутри* формулы C заменять эквивалентные формулы, т. е. пользуемся эквивалентностью при замене. Возможность одностороннего вынесения кванторов обеспечивается именно свойством чистоты переменных.

Например, пусть дана формула

$$\forall x \neg \exists y P(x, y) \supset \forall x (Q(x) \supset \neg \exists y P(x, y)).$$

Соответствующая формула со свойством чистоты переменных такова:

$$\forall x \neg \exists y P(x, y) \supset \forall u (Q(u) \supset \neg \exists v P(u, v)).$$

Применяя логические законы, получим последовательно

$$\forall x \forall y \neg P(x, y) \supset \forall u \forall v (Q(u) \supset \neg P(u, v)),$$
$$\exists x \exists y \forall u \forall v (\neg P(x, y) \supset (Q(u) \supset \neg P(u, v))).$$

Обратите внимание на два момента:

1) в матрице результирующей формулы логические связки расположены в том же порядке, что и в первоначальной формуле;
2) кванторы можно выносить в разном порядке (сначала из посылки, а потом из заключения или наоборот), так что вид кванторной приставки зависит от способа получения предваренной формы. ◁

2. Можно производить и иные упрощения формул. Например, можно избавиться от импликаций, выражая $\supset$ через $\wedge$, $\vee$, $\neg$. Затем, применяя законы де Моргана (законы 1–4), добиваемся, чтобы отрицание относилось только к атомарным формулам. Например, формулу

$$\neg(\neg \forall x P(x, y) \supset . \exists y Q(x, y) \wedge R(x))$$

сначала приводим к виду

$$\neg \forall x P(x, y) \wedge \neg(\exists y Q(x, y) \wedge R(x))$$

и затем к виду

$$\exists x \neg P(x, y) \wedge (\forall y \neg Q(x, y) \vee R(x)).$$

3. Применение логических законов дает способ приведения формул к конъюнктивной и дизъюнктивной нормальным формам.

Бескванторная формула называется *простой конъюнкцией*, если она имеет вид $B_1 \wedge \ldots \wedge B_k$, где каждое B_i есть атомарная формула или отрицание атомарной формулы ($k \geqslant 1$, расстановка скобок в серии конъюнкций или дизъюнкций несущественна с точностью до логической эквивалентности ввиду ассоциативности, так же как несущественен ввиду коммутативности порядок сомножителей).

Аналогично, *простая дизъюнкция* есть бескванторная формула вида $B_1 \vee \ldots \vee B_k$, где B_i — атомарная формула или отрицание атомарной формулы.

Дизъюнктивная нормальная форма (*д. н. ф.*) есть бескванторная формула вида $D_1 \vee \ldots \vee D_m$, где D_i суть простые конъюнкции. Аналогично, *конъюнктивная нормальная форма* (*к. н. ф.*) есть бескванторная формула вида $D_1 \wedge \ldots \wedge D_m$, где D_i суть простые дизъюнкции. Заметим, что название определяется главными (последними в построении) логическими связками. В частности, атомарные формулы и их отрицания суть одновременно и д. н. ф. и к. н. ф.

Теорема. *Всякая бескванторная формула логически эквивалентна некоторой д. н. ф. и некоторой к. н. ф.*

▷ Доказательство основано на применении некоторых логических законов. Покажем, как привести бескванторную формулу к д. н. ф. Сначала согласно п. 2 преобразуем формулу так, чтобы она не содержала импликаций и отрицания в ней относились лишь к атомарным формулам. С помощью логического закона двойного отрицания

$$\neg\neg A \sim A$$

можно добиться, чтобы при атомарных формулах стояло не более одного отрицания. С помощью логических законов дистрибутивности

$$A \wedge (B \vee C) \sim (A \wedge B) \vee (A \wedge C),$$
$$A \vee (B \wedge C) \sim (A \vee B) \wedge (A \vee C)$$

можно затем преобразовать формулу таким образом, чтобы в ней сначала применялись конъюнкции, а уже затем — дизъюнкции. Это и будет искомая д. н. ф.

Впрочем, ее, как правило, можно еще значительно упростить с помощью различных логических законов.

Рассмотрим, например, формулу

$$\neg(P \supset (Q \supset \neg P)) \wedge (Q \supset \neg P).$$

Используя законы

$$A \supset B \sim \neg A \vee B,$$
$$\neg(A \supset B) \sim A \wedge \neg B,$$

избавимся от импликации

$$P \wedge \neg(Q \supset \neg P) \wedge (\neg Q \vee \neg P),$$
$$P \wedge Q \wedge P \wedge (\neg Q \vee \neg P).$$

Это уже к. н. ф., но нам нужна д. н. ф.!

С помощью дистрибутивности, умножая конъюнкцию на дизъюнкцию, получим

$$(P \wedge Q \wedge P \wedge \neg Q) \vee (P \wedge Q \wedge P \wedge \neg P).$$

Это есть искомая д. н. ф.

Можно указать и более простую форму

$$Q \wedge \neg Q. \qquad \triangleleft$$

4. Для изучения булевых комбинаций формул естественно рассмотреть язык, в котором присутствуют только нульместные предикатные буквы (пропозициональные буквы). Кванторы в таком языке роли не играют, всякая формула эквивалентна бескванторной. Это вытекает из того, что имеют место следующие логические законы:

$$\forall x A \sim A,$$
$$\exists x A \sim A$$

в случае, когда переменная x не входит свободно в формулу A.

Язык логики высказываний (в другой терминологии — *пропозициональный язык*) получается, если, исходя из счетного набора нульместных предикатных букв $p, q, r, \ldots$, образовывать формулы с помощью только логических связок, без кванторов. Такие формулы называются *пропозициональными*.

Делая подстановочные примеры, можно из логических законов пропозионального языка получать логические законы в иных языках.

Аналогично, для изучения кванторной структуры формул можно рассмотреть *язык логики предикатов*, не содержащий ни функциональных символов, ни констант, а лишь счетный набор предикатных букв с различными аргументными местами. Такой язык мы уже рассматривали в первой главе. Можно сказать, что *логика предикатов* состоит в изучении истинности формул в языке логики предикатов.

Глава III

Формальные аксиоматические теории

§ 1. Исчисление предикатов

1. В предыдущих главах мы широко обсуждали, каким образом следует записывать математические утверждения в точных логико-математических языках. В то же время способы доказательства этих утверждений оставались неформализованными, они основывались на неуточненных семантических представлениях о свойствах моделей и множеств.

В этой части мы займемся как раз уточнением способов доказательства математических утверждений.

Фиксируем логико-математический язык Ω. *Аксиомами исчисления предикатов* (в языке Ω) называются формулы этого языка, имеющие один из следующих видов:

1) $A \supset . B \supset A$;
2) $(A \supset . B \supset C) \supset . (A \supset B) \supset (A \supset C)$;
3) $A \supset . B \supset A \wedge B$;
4) $A \wedge B \supset A$;
5) $A \wedge B \supset B$;
6) $(A \supset C) \supset . (B \supset C) \supset (A \vee B \supset C)$;
7) $A \supset A \vee B$;
8) $B \supset A \vee B$;
9) $(A \supset B) \supset . (A \supset \neg B) \supset \neg A$;
10) $\neg\neg A \supset A$;
11) $\forall x A \supset A(x||t)$;
12) $\forall x(C \supset A(x)) \supset . C \supset \forall x A(x)$;
13) $A(x||t) \supset \exists x A$;
14) $\forall x(A(x) \supset C) \supset . \exists x A(x) \supset C$.

Здесь A, B, C — произвольные формулы Ω, так что каждая строка вышеприведенного списка задает *схему аксиом* исчисления предикатов. Фиксируя A, B, C, из каждой из четырнадцати схем аксиом можно получить бесконечное семейство конкретных аксиом. Далее, $A(x||t)$ означает правильную подстановку терма вместо переменной с необходимыми переименованиями связанных переменных. Вместо $A(x||t)$ будем иногда

несколько неточно писать $A(t)$ (см. п. 8 § 4 гл. II). В схемах 12) и 14) формула C не содержит свободной переменной x.

С помощью методов второй части нетрудно убедиться, что все аксиомы исчисления предикатов суть логические законы, общезначимые формулы.

Фигуры следующих двух видов называются *правилами вывода* исчисления предикатов:

$$\frac{A,\ A \supset B}{B}, \qquad \frac{A}{\forall x A}.$$

Здесь A и B — произвольные формулы, а x — произвольная переменная.

Первое правило вывода носит уже знакомое нам традиционное латинское название — *модус поненс* (modus ponens). Второе правило называется *правилом обобщения*.

Правило модус поненс сохраняет истинность формул при фиксированной оценке. Это означает, что если M — интерпретация языка Ω и θ — оценка для $A \supset B$, то из $M \models A\theta$ и $M \models (A \supset B)\theta$ следует $M \models B\theta$.

Правило обобщения также сохраняет истинность формул, но в некотором более слабом смысле — при *интерпретации всеобщности*: если θ — оценка для $\forall x A$ и для всякого объекта a имеем $M \models (A_a^x)\theta$, то $M \models (\forall x A)\theta$.

Мы видим, что все правила сохраняют логические законы: если выше черты стоят общезначимые формулы, то формула ниже черты также общезначима.

2. *Дерево формул* (в исчислении предикатов) есть по определению некоторая двумерная фигура, составленная из формул языка по следующим индуктивным правилам:

1) каждая формула A сама по себе является деревом формул, нижней формулой этого дерева формул считается по определению формула A;
2) если D_1 и D_2 суть деревья формул с нижними формулами вида A и $A \supset B$ соответственно, то фигура

$$\frac{D_1,\ D_2}{B}$$

есть дерево формул; мы говорим, что формула B *получена* в этом дереве из A и $A \supset B$ по правилу модус поненс; нижней формулой результирующего дерева формул является по определению B;
3) есть D_1 — дерево формул с нижней формулой A и x — переменная, то фигура

$$\frac{D_1}{\forall x A}$$

есть также дерево формул; мы говорим, что нижняя формула $\forall x A$ этого дерева *получена* из A по правилу обобщения; нижней формулой этого дерева является, конечно, формула $\forall x A$.

Определение дерева формул закончено.

Последовательность вхождений формул в дерево формул, начинающаяся с нижней формулы дерева и продолжающаяся без пропусков до одной из самых верхних формул дерева, называется *ветвью* дерева формул. Количество формул в самой длинной ветви дерева называется *высотой* дерева формул. Верхние формулы дерева формул, не имеющие вида аксиом исчисления предикатов, называются *гипотезами*, или *открытыми посылками*, дерева формул. Мы говорим, что формула B, входящая в вывод, расположена *выше* формулы A, если существует ветвь вывода, содержащая A и B, причем B в этой ветви встречается позже, чем A.

Вот пример дерева формул высоты три:

$$\dfrac{\dfrac{P \supset Q(x)}{\forall x(P \supset Q(x))} \quad \forall x(P \supset Q(x)) \supset . P \supset \forall x Q(x)}{P \supset \forall x Q(x)}.$$

Самая длинная ветвь этого дерева формул — это

$$P \supset \forall x Q(x);\ \forall x(P \supset Q(x));\ P \supset Q(x).$$

Единственная открытая посылка этого дерева — $P \supset Q(x)$. Здесь формула $P \supset Q(x)$ расположена выше формулы $\forall x(P \supset Q(x))$. В то же время формула $P \supset Q(x)$ не расположена выше формулы

$$\forall x(P \supset Q(x)) \supset . P \supset \forall x Q(x).$$

Деревом вывода, или просто *выводом*, в исчислении предикатов называется дерево формул, удовлетворяющее некоторому дополнительному *структурному требованию*. А именно, если формула $\forall x A$ получена в выводе из формулы A по правилу обобщения, то переменная x не входит свободно в гипотезы, расположенные выше рассматриваемого вхождения формулы $\forall x A$.

Приведенный выше пример дерева формул не является, таким образом, выводом. «Запрещен» переход

$$\dfrac{P \supset Q(x)}{\forall x(P \supset Q(x))},$$

так как гипотеза $P \supset Q(x)$ содержит свободно переменную x.

Если формула $\forall x A$ получена в дереве формул из формулы A по правилу обобщения, а формула B расположена в дереве формул выше рассматриваемого вхождения $\forall x A$ и содержит свободно x, то говорят, что переменная x *варьируется* в формуле B. Наше структурное требование можно выразить следующим образом: в выводе параметры гипотез *не варьируются*, *остаются фиксированными*.

Структурное требование выполняется тривиально, если дерево формул не содержит вовсе правил обобщения, или если все гипотезы дерева формул суть замкнутые формулы, или если дерево формул вовсе не содержит гипотез.

Пусть Γ — конечный список формул и A — формула. Будем говорить, что формула A *выводима* в исчислении предикатов *из списка формул* Γ, и писать $\Gamma \vdash A$, если существует вывод D с нижней формулой A и такой, что всякая гипотеза D является членом списка Γ. При этом, конечно, некоторые формулы Γ могут и не быть гипотезами D. Мы говорим, что вывод D формулы A *не зависит* от таких членов Γ.

Список Γ может быть и пуст. Тогда $\Gamma \vdash A$ означает, что существует вывод A *без гипотез*; мы пишем в этом случае $\vdash A$ и говорим, что формула A *выводима* в исчислении предикатов.

Саму фигуру $\Gamma \vdash A$ мы будем называть иногда *выводимостью* (или, в другой терминологии, *секвенцией*). Таким образом, чтобы обосновать секвенцию $\Gamma \vdash A$, следует построить вывод в исчислении предикатов с нижней формулой A, все гипотезы которого находятся среди членов списка Γ.

3. Следующая лемма описывает семантические свойства выводимости.

Лемма. *Пусть* $\Gamma \vdash A$, *где* Γ *есть список формул* $B_1, \ldots, B_m$. *Пусть* M *— интерпретация языка* Ω *и* θ *— оценка для* $B_1, \ldots, B_m, A$. *Тогда если* $M \models B_1\theta, \ldots, M \models B_m\theta$, *то* $M \models A\theta$.

▷ Доказательство проведем индукцией по высоте вывода для $\Gamma \vdash A$. Если этот вывод состоит из единственной формулы A, то A — либо гипотеза (и, следовательно, член Γ), либо аксиома исчисления предикатов. Если A — гипотеза, т. е. одна из формул B_i, то $M \models A\theta$ ввиду $M \models B_1\theta$. Если A — аксиома, то $M \models A\theta$, так как A — логический закон.

Если A в выводе получена по модус поненс, то $M \models A\theta$ следует из индуктивного предположения и того, что это правило сохраняет истинность формул при фиксированной оценке.

Пусть A имеет вид $\forall x C$ и получена в выводе из формулы C по правилу обобщения. Таким образом C выведена с помощью вывода меньшей высоты, чем вывод $\forall x C$, поэтому к выводу C можно применить индуктивное предположение. По структурному требованию x не есть параметр гипотез вывода формулы C. Чтобы показать $M \models (\forall x C)\theta$, достаточно установить, что для произвольного объекта a имеем $M \models (C_a^x)\theta$. Так как всякая гипотеза B_i вывода для C не содержит свободно x, то из $M \models B_i\theta$ следует $M \models (B_{ia}^{\,x})\theta$. По индуктивному предположению отсюда $M \models (C_a^x)\theta$. ◁

Следствие. *Если* $\Gamma \vdash A$ *и все члены* Γ *суть логические законы, то* A *— также логический закон. В частности, если* $\vdash A$, *то* A *— логический закон.*

Таким образом, на выводимость в исчислении предикатов можно смотреть, как на некоторый инструмент для получения логических законов.

4. Рассмотрим примеры выводов в исчислении предикатов. Для удобства выводы записываем в виде столбцов формул, а не деревьев.

1. $\vdash A \supset A$. В самом деле, можно построить следующий вывод:

1) $A \supset .(A \supset A) \supset A$,

это пример схемы аксиом 1) п. 1;

2) $(A \supset .(A \supset A) \supset A) \supset ((A \supset .A \supset A) \supset .A \supset A)$,

это пример схемы аксиом 2);

3) $(A \supset .A \supset A) \supset (A \supset A)$,

получается по модус поненс из 1 и 2;

4) $A \supset .A \supset A$,

это пример схемы аксиом 1);

5) $A \supset A$

получается из 3 и 4 по модус поненс.

2. Пусть A — формула, x и y — различные переменные, причем y не входит свободно в A. Тогда $\vdash \forall x A \supset \forall y(A(x\|y))$. В более традиционной (но менее точной) записи это высказывание имеет вид

$$\forall x A(x) \supset \forall y A(y).$$

Действительно, строим вывод

1) $\forall x A(x) \supset A(y)$,
это пример схемы аксиом 11) п. 1;
2) $\forall y(\forall x A(x) \supset A(y))$
по правилу обобщения из 1, структурное требование выполняется, так как 1 — не гипотеза (а аксиома исчисления предикатов);
3) $\forall y(\forall x A(x) \supset A(y)) \supset .\forall x A(x) \supset \forall y A(y)$,
это пример схемы аксиом 12) (существенно, что $\forall x A(x)$ не содержит свободно y);
4) $\forall x A(x) \supset \forall y A(y)$
вытекает из 2 и 3 по модус поненс.

Упражнение. Установите в тех же условиях, что и во втором примере, что

$$\vdash \exists y(A(x\|y)) \supset \exists x A.$$

§ 2. Теорема о дедукции. Техника естественного вывода

1. Непосредственно использовать выводы в исчислении предикатов для установления логических законов крайне неудобно. Выводы даже простых формул получаются очень громоздкими, а главное, весьма непохожими на обычные способы рассуждения, употребляемые математиками. Поэтому понятие вывода в исчислении предикатов, как мы

его сформулировали в § 1, используется главным образом в теоретических исследованиях, где существенно, чтобы выводы имели простую структуру.

Практически же выводимость формул и секвенций устанавливается с помощью серии специально подобранных допустимых вспомогательных правил вывода, относящихся непосредственно к секвенциям. С их помощью мы можем установить, что секвенция выводима, не строя для нее вывод в исчислении предикатов. Указанные правила уже близко соответствуют обычной практике математического рассуждения, что сильно облегчает доказательство выводимости. Набор этих правил и называется *техникой естественного вывода*.

2. Ключевым фактом здесь является так называемая *теорема о дедукции*.

Теорема. *Если* $\Gamma, A \vdash B$, *то* $\Gamma \vdash A \supset B$. *Этот факт записывается в виде вспомогательного правила вывода*:

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}.$$

▷ Воспользуемся индукцией по высоте вывода для $\Gamma, A \vdash B$. Если этот вывод состоит из единственной гипотезы B, то возможны два случая: B равно A или B есть член Γ. В первом случае $\Gamma \vdash A \supset B$ следует из $\vdash A \supset A$. Если B есть член Γ, то $\Gamma \vdash B$. Кроме того, очевидно $\vdash B \supset .A \supset B$ (это пример схемы аксиом исчисления предикатов). С помощью модус поненс отсюда получается, что $\Gamma \vdash A \supset B$.

Если B есть аксиома исчисления предикатов, то из $\vdash B \supset .A \supset B$ вновь получим $\vdash A \supset B$ и, значит, $\Gamma \vdash A \supset B$.

Теперь рассмотрим случай, когда B получена из $\Gamma, A \vdash C$ и $\Gamma, A \vdash C \supset B$ по правилу модус поненс. По индуктивному предположению тогда $\Gamma \vdash A \supset C$ и $\Gamma \vdash A \supset .C \supset B$. Далее, имеем

$$\vdash (A \supset .C \supset B) \supset .(A \supset C) \supset (A \supset B)$$

(это пример схемы аксиом 2 исчисления предикатов). Дважды применяя модус поненс, получим $\Gamma \vdash A \supset B$.

Пусть теперь формула B имеет вид $\forall x C$ и получена из формулы C по правилу обобщения. Таким образом, $\Gamma, A \vdash C$. Если вывод для $\Gamma, A \vdash C$ не зависит от A, то $\Gamma \vdash C$. По правилу обобщения в этом случае $\Gamma \vdash \forall x C$. Кроме того, очевидно, $\Gamma \vdash \forall x C \supset .A \supset \forall x C$ (это пример схемы 1). По модус поненс отсюда $\Gamma \vdash A \supset \forall x C$.

Если же A есть гипотеза вывода для $\Gamma, A \vdash C$, то по структурному требованию A не содержит свободно x. Пусть Γ_1 есть часть списка Γ, состоящая из всех гипотез вывода для $\Gamma, A \vdash C$, отличных от A. Ни один член F_1 не содержит x свободно (по структурному требованию) и $\Gamma_1, A \vdash C$. По индуктивному предположению $\Gamma_1 \vdash A \supset C$. Далее, по правилу обобщения $\Gamma_1 \vdash \forall x (A \supset C)$. Далее, $\Gamma_1 \vdash \forall x (A \supset C) \supset .A \supset \forall x C$ (это пример схемы аксиом 12)). По модус поненс отсюда $\Gamma_1 \vdash A \supset \forall x C$,

и, следовательно, добавляя формулы, от которых вывод не зависит (а они могут и содержать x свободно!), получим

$$\Gamma \vdash A \supset \forall x C. \qquad \triangleleft$$

Теорема о дедукции показывает, что для установления импликации $\Gamma \vdash A \supset B$ достаточно показать $\Gamma, A \vdash B$, что часто бывает гораздо проще. В математической практике этому соответствует следующий пример рассуждения. Если нужно в некоторой ситуации установить, что $A \supset B$, то *допустим* (*введем гипотезу*), что A верно, и докажем B, исходя из этой гипотезы.

3. Следующие правила называются *структурными правилами* техники естественного вывода:

1) закон тождества

$$A \vdash A;$$

2) правило добавления

$$\frac{\Gamma \vdash A}{\Gamma, B \vdash A};$$

3) правило перестановки

$$\frac{\Gamma, B, C, \Delta \vdash A}{\Gamma, C, B, \Delta \vdash A};$$

4) правило сокращения

$$\frac{\Gamma, B, B, \Delta \vdash A}{\Gamma, B, \Delta \vdash A};$$

5) правило сечения

$$\frac{\Gamma \vdash A;\ \Delta, A \vdash B}{\Gamma, \Delta \vdash B}.$$

Правила 2)–5) следует понимать как *допустимые правила вывода*. Это означает, что если дан вывод для секвенций, расположенных выше черты, то можно построить вывод и для секвенции, расположенной ниже черты.

▷ 1) Из гипотезы A и ввиду $\vdash A \supset A$ (п. 4 § 1) по модус поненс $A \vdash A$.

2)–4) Тривиально допустимы. Вывод, обосновывающий секвенцию выше черты, обосновывает и секвенцию ниже черты.

5) Из $\Delta, A \vdash B$ по теореме о дедукции $\Delta \vdash A \supset B$. Отсюда и из $\Gamma \vdash A$ по правилу добавления $\Gamma, \Delta \vdash A \supset B$: $\Gamma, \Delta \vdash A$. Применяя модус поненс, получим $\Gamma, \Delta \vdash B$. $\triangleleft$

В технике естественного вывода доказанные правила широко употребляются без явного упоминания.

4. Следующую группу образуют *логические правила* техники естественного вывода. Правила эти разбиваются на группы: для каждой логической связки и квантора — своя группа правил. Кроме того, внутри группы правила делятся на два вида: *правила введения*, указывающие, как

доказывать формулу с данным логическим символом, и *правила удаления*, указывающие, как использовать формулу с данным логическим символом для доказательства других формул.

1) Импликация:

введение $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}$; удаление $\dfrac{\Gamma \vdash A; \Gamma \vdash A \supset B}{\Gamma \vdash B}$.

2) Конъюнкция:

введение $\dfrac{\Gamma \vdash A; \Gamma \vdash B}{\Gamma \vdash A \wedge B}$; удаление $\dfrac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}$.

3) Дизъюнкция:

введение $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$; $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$; удаление $\dfrac{\Gamma, A \vdash C; \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$.

4) Отрицание:

введение $\dfrac{\Gamma, A \vdash B; \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$; удаление $\dfrac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$.

5) Общность:

введение $\dfrac{\Gamma \vdash A(y)}{\Gamma \vdash \forall x A(x)}$; удаление $\dfrac{\Gamma \vdash \forall x A}{\Gamma \vdash A(x\|t)}$.

(здесь y не входит свободно в Γ, и если x отлично от y, то x не входит свободно в $A(y)$);

6) Существование:

введение $\dfrac{\Gamma \vdash A(x\|t)}{\Gamma \vdash \exists x A}$; удаление $\dfrac{\Gamma, A(y) \vdash C}{\Gamma, \exists x A(x) \vdash C}$

(здесь y не входит свободно в Γ и C, и если x отлично от y, то x не входит свободно в $A(y)$, $A(x)$ есть $A(y\|x)$).

7) Эквивалентность:

введение удаление

$$\frac{\Gamma, A \vdash B; \Gamma, B \vdash A}{\Gamma \vdash A \equiv B}; \qquad \frac{\Gamma \vdash A; \Gamma \vdash A \equiv B}{\Gamma \vdash B}; \qquad \frac{\Gamma \vdash B; \Gamma \vdash A \equiv B}{\Gamma \vdash A}.$$

▷ Рассмотрим некоторые из правил. Доказательство допустимости остальных правил предоставляется читателю.

$\supset$-введение. Это есть в точности теорема о дедукции.

$\supset$-удаление. Из данных выводов $\Gamma \vdash A; \Gamma \vdash A \supset B$ вывод для $\Gamma \vdash B$ получим с помощью модус поненс.

$\vee$-введение. Имеем: $\Gamma \vdash A$. Кроме того, $\vdash A \supset A \vee B$ (это аксиома). По модус поненс $\Gamma \vdash A \vee B$.

$\vee$-удаление. Из данных $\Gamma, A \vdash C; \Gamma, B \vdash C$ по теореме о дедукции $\Gamma \vdash A \supset C$ и $\Gamma \vdash B \supset C$. Кроме того, $\vdash (A \supset C) \supset .(B \supset C) \supset (A \vee B \supset C)$ (это аксиома). Дважды применяя модус поненс, получаем: $\Gamma \vdash A \vee B \supset C$. По закону тождества (и правилу добавления) $\Gamma, A \vee B \vdash A \vee B$. По модус поненс $\Gamma, A \vee B \vdash C$.

$\exists$-удаление. Из $\Gamma, A(y) \vdash C$ по теореме о дедукции следует, что $\Gamma \vdash A(y) \supset C$. По правилу обобщения

$$\Gamma \vdash \forall y(A(y) \supset C),$$

здесь существенно, что y не входит свободно в Γ. Имеем аксиому $\forall y(A(y) \supset C) \supset .\exists y A(y) \supset C$. По модус поненс $\Gamma \vdash \exists y A(y) \supset C$. Ввиду п. 4 § 1 $\vdash \exists x A(x) \supset \exists y A(y)$. Отсюда $\Gamma, \exists x A(x) \vdash \exists y A(y)$. Следовательно, по модус поненс $\Gamma, \exists x A(x) \vdash C$.

$\equiv$-введение. Из $\Gamma, A \vdash B$ и $\Gamma, B \vdash A$ по теореме о дедукции $\Gamma \vdash A \supset B$, $\Gamma \vdash B \supset A$, $\Gamma \vdash (A \supset B) \wedge (B \supset A)$, что и означает по определению эквивалентности $\Gamma \vdash A \equiv B$.

◁

На практике логические правила применяются, так сказать, в обратном порядке; нужно установить секвенцию ниже черты, и мы замечаем, что для этого достаточно установить секвенции выше черты. В этом свете можно заметить, что все правила соответствуют довольно обычным приемам математического рассуждения.

Например, $\vee$-удаление соответствует *разбору случаев*. Если в некоторой ситуации из $A \vee B$ нужно вывести C, то мы рассуждаем так: если верно $A \vee B$, то либо A, либо B и поэтому достаточно разобрать случаи, вывести C из A и вывести C из B по отдельности.

$\exists$-удаление соответствует *правилу единичного выбора* (в другой терминологии, *правилу* C). Допустим, что $\exists x A(x)$, и выведем C. Раз существует x такое, что $A(x)$, то можно рассмотреть (выбрать) одно из таких x. Обозначим его через y. Для этого y верно $A(y)$. Таким образом, достаточно вывести формулу C из $A(y)$.

Правило $\neg$-введения соответствует *приведению к абсурду* (традиционное латинское название — *reductio ad absurdum*): чтобы установить $\neg A$, достаточно, допустив A, получить противоречие, т. е. вывести B и $\neg B$ одновременно для подходящего B.

5. Руководствуясь этими идеями, можно доказывать выводимость логических законов исходя из их содержательного смысла.

Докажем, например,

$$\vdash A \vee B \equiv \neg(\neg A \wedge \neg B).$$

Согласно $\equiv$-введению достаточно установить

$$A \vee B \vdash \neg(\neg A \wedge \neg B)$$

и

$$\neg(\neg A \wedge \neg B) \vdash A \vee B.$$

Начнем с первой секвенции. Слева у нее стоит дизъюнкция, поэтому, разбирая случаи согласно $\vee$-удалению, достаточно установить два факта:

$$A \vdash \neg(\neg A \wedge \neg B),$$
$$B \vdash \neg(\neg A \wedge \neg B).$$

Мы установим только первый, второй устанавливается симметрично. Для вывода отрицания $\neg(\neg A \wedge \neg B)$ достаточно допустить $\neg A \wedge \neg B$ и вывести противоречие, т. е. использовать $\neg$-введение. Противоречие будет состоять в выводе A и $\neg A$. Итак, для вывода $A \vdash \neg(\neg A \wedge \neg B)$ с помощью $\neg$-введения достаточно установить

$$A, \neg A \wedge \neg B \vdash A,$$
$$A, \neg A \wedge \neg B \vdash \neg A.$$

Первая секвенция выводима по закону тождества. Для вывода второй согласно $\wedge$-удалению достаточно показать

$$A, \neg A, \neg B \vdash \neg A,$$

что также следует из закона тождества.

Теперь установим

$$\neg(\neg A \wedge \neg B) \vdash A \vee B.$$

Здесь наше рассуждение будет косвенным. Согласно $\neg$-удалению достаточно установить

$$\neg(\neg A \wedge \neg B) \vdash \neg\neg(A \vee B).$$

А для этого согласно $\neg$-введению следует, допустив $\neg(A \vee B)$, вывести противоречие. Мы докажем

$$\neg(\neg A \wedge \neg B), \neg(A \vee B) \vdash \neg(\neg A \wedge \neg B)$$

и

$$\neg(A \vee B) \vdash \neg A \wedge \neg B.$$

Первая секвенция, очевидно, выводима по закону тождества. Вторую секвенцию получим по $\wedge$-введению. Достаточно вывести

$$\neg(A \vee B) \vdash \neg A$$

и

$$\neg(A \vee B) \vdash \neg B.$$

Мы выведем первую секвенцию, вторая выводится симметрично. Используя $\neg$-введение, достаточно вывести

$$\neg(A \vee B), A \vdash \neg(A \vee B)$$

и

$$\neg(A \vee B), A \vdash A \vee B.$$

Но первая из этих секвенций очевидна, а вторая получается с помощью $\vee$-введения из $\vdash (A \vee B), A \vdash A$.

6. Выведем $\vdash A \vee \neg A$. Согласно $\neg$-удалению достаточно вывести $\vdash \neg\neg(A \vee \neg A)$. С этой целью по $\neg$-введению допустим, что $\neg(A \vee \neg A)$, и получим противоречие:

$$\neg(A \vee \neg A) \vdash \neg A,$$
$$\neg(A \vee \neg A) \vdash \neg\neg A.$$

Для вывода первой секвенции ($\neg$-введение) допустим A и получим противоречие:

$$\neg(A \vee \neg A), A \vdash \neg(A \vee \neg A),$$
$$\neg(A \vee \neg A), A \vdash A \vee \neg A.$$

Первая из этих секвенций очевидна, а вторая получается $\vee$-введением. Аналогично, для получения секвенции

$$\neg(A \vee \neg A) \vdash \neg\neg A$$

достаточно вывести секвенции

$$\neg(A \vee \neg A), \neg A \vdash \neg(A \vee \neg A),$$
$$\neg(A \vee \neg A), \neg A \vdash A \vee \neg A,$$

которые доказываются аналогично.

7. Выведем $\vdash \exists x A(x) \supset \neg\forall x \neg A(x)$. С этой целью допустим $\exists x A(x)$ и выведем $\neg\forall x \neg A(x)$, т. е. выведем

$$\exists x A(x) \vdash \neg\forall x \neg A(x).$$

Для этого согласно $\exists$-удалению выберем новую переменную y и установим

$$A(y) \vdash \neg\forall x \neg A(x).$$

Это можно сделать с помощью $\neg$-введения:

$$A(y), \forall x \neg A(x) \vdash A(y)$$

и

$$A(y), \forall x \neg A(x) \vdash \neg A(y).$$

Первая секвенция есть закон тождества, а вторая получается $\forall$ -удалением.

8. Докажем $\vdash A \supset . \neg A \supset B$. Расположим теперь доказательство в технике естественного вывода прямым образом, «сверху вниз»:

1. $A, \neg A, \neg B \vdash A$,
2. $A, \neg A, \neg B \vdash \neg A$,
3. $A, \neg A \vdash \neg \neg B$ ($\neg$-введение из 1 и 2),
4. $A, \neg A \vdash B$ ($\neg$-удаление из 3),
5. $\vdash A \supset . \neg A \supset B$ ($\supset$-введение дважды).

9. Разумеется, в технике естественного вывода можно использовать и другие секвенции, выводимости которых уже установлены, или иные допустимые правила.

Например, с помощью техники естественного вывода можно установить, что если формула A конгруэнтна формуле B, то $\vdash A \equiv B$. Доказательство проводится довольно непосредственной индукцией по сложности формулы A.

Еще одно полезное правило — *правило подстановки*:

$$\frac{\Gamma \vdash A}{\Gamma(x_1, \ldots, x_k \| t_1, \ldots, t_k) \vdash A\,(x_1, \ldots, x_k \| t_1, \ldots, t_k)}.$$

▷ Пусть для простоты Γ есть список $B_1 B_2$. Из $B_1, B_2 \vdash A$ по $\wedge$-удалению $B_1 \wedge B_2 \vdash A$, а по $\supset$-введению $\vdash B_1 \wedge B_2 \supset A$. По правилу обобщения $\vdash \forall x_1 \ldots x_k (B_1 \wedge B_2 \supset A)$. Далее, $\forall x_1 \ldots x_k (B_1 \wedge B_2 \supset A) \supset (B_1 \wedge B_2 \supset A)'$ есть аксиома; штрихом здесь обозначена подстановка $(x_1, \ldots, x_k \| t_1, \ldots, t_k)$. По модус поненс $\vdash (B_1 \wedge B_2 \supset A)'$, или, что то же самое, $\vdash B_1' \wedge B_2' \supset A'$. Далее, по $\wedge$-введению $B_1', B_2' \vdash B_1' \wedge B_2'$. По модус поненс $B_1', B_2' \vdash A'$, что и требовалось. ◁

10. Приведенные рассмотрения должны убедить читателя, что исчисление предикатов — достаточно мощный аппарат для получения логических законов. Фактически, доказательство выводимости всех логических законов, упомянутых во второй части, с помощью техники естественного вывода, является длинным, но нетрудным упражнением.

Позже мы установим, что *всякий* логический закон выводится в исчислении предикатов. Это и есть содержание знаменитой теоремы Гёделя о полноте исчисления предикатов.

Заметим, что существуют и иные эквивалентные формулировки исчисления предикатов. Особенно интересны формулировки, где в основу положены именно правила типа правил техники естественного вывода. Это

так называемые *исчисления натурального вывода* и *исчисления секвенций*, изучение которых было начато Генценом в 1934 г. Такие исчисления играют важную роль и в современных исследованиях по теории доказательств.

Сделаем несколько предварительных замечаний, касающихся теории алгорифмов. Аккуратное изложение начал этой теории мы надеемся привести в нашей следующей книге.

Ясно, что выражения рассмотренных нами языков могут рассматриваться как слова (строчки символов) в некотором конечном алфавите Σ. Множество всех слов (строчек символов) в алфавите Σ обозначим через Σ^*.

Множество $M \subseteq \Sigma^*$ слов назовем *разрешимым*, или *рекурсивным*, если существует вычислимая функция (алгорифм) $f\colon \Sigma^* \to \{0, 1\}$, определенная на всем множестве Σ^*, такая, что для всякого слова $A \in \Sigma^*$ имеем $f(A) = 1 \Leftrightarrow A \in M$.

Неформально говоря, множество M разрешимо, если существует алгорифм, позволяющий выяснить по заданному слову, принадлежит это слово множеству M или нет.

Множество $M \subseteq \Sigma^*$ называется *рекурсивно-перечислимым*, или просто *перечислимым*, если существует вычислимая функция f, определенная на некотором подмножестве $V \subseteq \Sigma^*$, $f\colon V \to \{0, 1\}$, такая, что $M \subseteq \operatorname{dom} f$ и для всякого слова $A \in V$ имеем

$$f(A) = 1 \Leftrightarrow A \in M.$$

Очевидно, что всякое рекурсивно-перечислимое множество является и рекурсивным. Неформально говоря, множество M перечислимо, если мы умеем алгорифмически выяснять, когда $A \in M$, но не обязательно можем узнать, когда $A \notin M$.

Из известных результатов Гёделя и Чёрча следует, что множество всех логических законов в любом из рассмотренных нами языков первого порядка является рекурсивно-перечислимым, но не разрешимым.

§ 3. Формальные аксиоматические теории. Примеры формальных аксиоматических теорий

1. До сих пор мы интересовались способами доказательства логических законов. Теперь рассмотрим способы получения теорем в конкретных математических теориях типа арифметики, анализа или теории множеств.

Формальная аксиоматическая теория (мы будем часто опускать один или оба из этих эпитетов) определяется набором

$$T = \langle \Omega, X \rangle,$$

где Ω — логико-математический язык, X — некоторое множество предложений (т. е. замкнутых формул) языка Ω, называемое множеством *нелогических аксиом* теории T.

Будем говорить, что формула A языка Ω *выводима в теории* T, и писать $T \vdash A$, если существует конечный список Γ, составленный из нелогических аксиом теории T и такой, что $\Gamma \vdash A$ в исчислении предикатов.

Это определение уточняет, что значит вывести утверждение A в теории T с помощью законов логики. Описывая нелогические аксиомы теории, мы будем часто приводить незамкнутые формулы. В этом случае всегда имеется в виду, что следует взять замыкание рассматриваемых формул кванторами общности.

2. Модель M для языка Ω называется *моделью теории* $T = \langle \Omega, X \rangle$, если $M \models A$ для всякой нелогической аксиомы $A \in X$.

Теорема. *Если M — модель теории T и $T \vdash B$, то для всякой оценки θ для формулы B имеем $M \models B\theta$.*

▷ См. п. 3 § 1. ◁

Таким образом, если формула B выводится в теории T, то B истинна во всякой модели теории T. Из теоремы Гёделя о полноте исчисления предикатов вытекает и обратное: если формула B истинна во всякой модели теории T, то B выводится в теории T. Наш, казалось бы, чисто формальный аппарат выводимости оказывается *адекватным инструментом* установления истинности фактов в теории.

3. Приведем некоторые примеры формальных теорий.

Элементарная арифметика Ar есть формальная аксиоматическая теория в языке Ar (см. п. 1 § 4 гл. II). Нелогические аксиомы Ar суть формулы следующих видов.

Аксиомы равенства:

1) $x = x$;
2) $x = y \wedge x = z \supset y = z$.

Аксиомы Пеано:

3) $Sx \neq 0$;
4) $(Sx = Sy) \equiv x = y$;
5) $A(0) \wedge \forall x(A(x) \supset A(Sx)) \supset \forall x A(x)$ (принцип полной математической индукции; здесь $A(x)$ — произвольная формула Ar, так что 5) определяет бесконечную серию аксиом, *схему аксиом индукции*).

Определяющие аксиомы для сложения и умножения:

6) $x + 0 = x$;
7) $x + Sy = S(x + y)$;
8) $x \cdot 0 = 0$;
9) $x \cdot Sy = x \cdot y + x$.

Определение теории Ar закончено. Легко видеть, что модель ω языка Ar является моделью и формальной теории Ar.

Упражнение. Докажите, что аксиома 1) выводится из 2) и 6) и, таким образом, является излишней. (Тем не менее мы приводим ее в целях единообразного введения аксиом равенства в различных теориях. И в дальнейшем мы далеко не всегда будем приводить минимальный список аксиом.)

С помощью аксиом 1) и 2) докажите, что

$$\mathrm{Ar} \vdash x = y \supset y = x.$$

Аксиомы 1)–9) выбраны таким образом, чтобы все обычные факты, верные в ω и формулируемые на языке Ar, выводились бы в Ar. В этом отношении успех аксиоматики Ar впечатляет: привести пример истинного в ω, но не выводимого в Ar утверждения очень непросто. Впервые некоторый искусственный пример такого рода привел Гёдель в 1931 году, примеры же математически содержательных теорем, невыводимых в Ar, появились совсем недавно.

Если M — модель языка Ω, то через $\mathrm{Th}_\Omega(M)$ обозначим множество всех предложений языка Ω, истинных в M. Множество $\mathrm{Th}_\Omega(M)$ называется *теорией модели* M. С другой стороны, если T — теория в языке Ω, то через $[T]$ обозначим множество всех предложений, выводимых в T (так называемое *логическое замыкание* теории T). Теория T называется *полной по отношению к модели* M, если $[T] = \mathrm{Th}_\Omega(M)$. Теория T называется просто *полной*, если для всякого предложения A в языке Ω имеем $T \vdash A$ или $T \vdash \neg A$.

Упражнение. Докажите следующие утверждения.

1) Если теория T полна по отношению к некоторой модели M, то T является полной теорией.
2) Если T — полная теория, то T является полной по отношению ко всякой модели теории T.

Как мы отметили выше, $[\mathrm{Ar}] \subseteq \mathrm{Th}_{\mathrm{Ar}}(\omega)$, но $[\mathrm{Ar}] \neq \mathrm{Th}_{\mathrm{Ar}}(\omega)$, так что элементарная арифметика — неполная теория.

Далее, теория T называется *разрешимой*, если множество $[T]$ рекурсивно. Иными словами, T разрешима, если существует алгорифм, позволяющий по любому предложению A выяснить, верно ли $T \vdash A$ или нет.

Известно, что множество [Ar] рекурсивно-перечислимо, но не разрешимо, так что элементарная арифметика — неразрешимая теория. Что касается множества $\mathrm{Th}_{\mathrm{Ar}}(\omega)$, то оно даже не рекурсивно перечислимо.

Еще один замечательный факт, открытый Скулемом в 1920-х годах, состоит в том, что существуют модели элементарной арифметики (и даже модели $\mathrm{Th}_{\mathrm{Ar}}(\omega)$), существенно неизоморфные модели ω. Они называются *нестандартными моделями* арифметики. И хотя в такой модели выполняются все аксиомы арифметики 1)–9), в том числе и аксиомы Пеано, все же, например, существуют подмножества множества объектов модели, не имеющие первого элемента в смысле порядка, определимого естественной формулой арифметики! Как же быть тогда с утверждением, что аксиомы Пеано однозначно определяют натуральный ряд (категоричность натурального ряда)?

Следует ясно понимать, что здесь различаются постановки вопроса. Категоричность натурального ряда означает, что в рамках некоторой теоретико-множественной системы, например, системы Цермело—Френкеля (так сказать, внутри системы) можно доказать единственность натурального ряда (с точностью до изоморфизма), существенно пользуясь законами теории множеств. Модель же элементарной арифметики совсем не обязана быть натуральным рядом, это должна быть просто интерпретация языка Ar, удовлетворяющая аксиомам 1)–9). Принцип индукции (схема аксиом 5) должен выполняться не для всех теоретико-множественно понимаемых свойств $A(x)$, а только для свойств, *выразимых* в языке Ar. Такая структура может быть и не изоморфна обыкновенному ряду. Так, подмножество без первого элемента в нестандартной модели существует, но это подмножество невыразимо в языке Ar.

Кстати, если теория Цермело—Френкеля непротиворечива, то у нее *тоже* существуют неизоморфные модели. В каждой такой модели ввиду категоричности существует только один натуральный ряд, хотя натуральные ряды из разных моделей могут быть и неизоморфны!

Доказательство всех этих классических результатов читатель найдет в более подробных руководствах по математической логике (см. список литературы в конце книги).

4. Рассмотрим теперь *элементарную теорию действительных чисел* R. Эта теория, так же как и Ar, — в языке Ar. Нелогические аксиомы R суть формулы следующих видов.

Аксиомы равенства:

1) $x = x$;
2) $x = y \wedge x = z \supset y = z$;
3) $x = y \supset Sx = Sy$;
4) $x = y \supset x + z = y + z$;
5) $x = y \supset x \cdot z = y \cdot z$.

Эта группа аксиом подобрана таким образом, чтобы выводились следующие схемы, *определяющие схемы равенства*:

a) $x = y \supset . t(x) = t(y)$;
b) $x = y \supset . A(x) \equiv A(y)$;
c) $x = x$.

Здесь t — произвольный терм, а A — произвольная формула языка. Иногда в теории определяющие схемы равенства a)–c) сразу принимают в качестве аксиом, причем относят их к разряду логических аксиом. В таких случаях говорят, что теория рассматривается в *исчислении предикатов с равенством*. Мы все же в наших примерах будем явно описывать аксиомы, относящиеся к равенству, и считать их нелогическими аксиомами. Но при этом, конечно, схемы a)–c) будут выводиться.

Аксиомы поля:

6) $0 \neq S0$;
7) $x + 0 = x$;
8) $x + y = y + x$;
9) $(x + y) + z = x + (y + z)$;
10) $\exists y(x + y = 0)$;
11) $x \cdot S0 = x$;
12) $x \cdot y = y \cdot x$;
13) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
14) $x \neq 0 \supset \exists y(x \cdot y = S0)$;
15) $x \cdot (y + z) = x \cdot y + x \cdot z$.

Аксиомы порядка:

16) $\exists z(z^2 = x^2 + y^2)$;
17) $x + y = 0 \supset \exists z(x = z^2 \vee y = z^2)$.

Здесь, конечно, $x^2 \leftrightharpoons x \cdot x$. Если ввести естественное сокращение: $x \leqslant y \leftrightharpoons \exists z(x + z^2 = y)$, то написанные выше аксиомы порядка позволят вывести все обычные свойства порядка в области действительных чисел. Читателю в качестве упражнения рекомендуется убедиться в том, что из аксиом 1)–17) вытекают следующие свойства порядка:

d) $x \leqslant x$;
e) $x \leqslant y \wedge y \leqslant z \supset x \leqslant z$;
f) $x = y \equiv (x \leqslant y \wedge y \leqslant x)$;
g) $x \leqslant y \vee y \leqslant x$;
h) $0 \leqslant x \equiv \exists y(x = y^2)$;
i) $x \leqslant y \supset x + z \leqslant y + z$;
j) $0 \leqslant x \wedge y \leqslant z \supset x \cdot y \leqslant x \cdot z$;
k) $0 \leqslant S0$.

Определим, далее, $x < y \leftrightharpoons (x \leqslant y) \wedge x \neq y$. Пусть $t(x)$ — произвольный терм языка Ar. Следующая формула называется *аксиомой вещественной замкнутости*:

18) $x < y \wedge t(x) < 0 \wedge 0 < t(y) \supset \exists z(x < z \wedge z < y \wedge t(z) = 0)$.

Суть аксиомы состоит в том, что если многочлен с вещественными коэффициентами принимает на концах некоторого отрезка значения разных знаков, то внутри отрезка он обращается в нуль в некоторой точке.

Формулировка теории R закончена.

Сразу видно, что множество действительных чисел R является моделью теории R.

В отличие от Ar теория R является полной и разрешимой. Этот замечательный факт был обнаружен Тарским. Модели теории R называются

в алгебре вещественно замкнутыми упорядоченными полями. Хорошо известны модели теории R, неизоморфные множеству всех действительных чисел. Так, счетное множество алгебраических чисел составляет модель R. Известны и более экзотические модели, являющиеся неархимедовыми полями.

5. Рассмотрим теперь теорию Lin в языке Lin. Нелогические аксиомы Lin суть следующие.

Аксиомы равенства:

1) $x = x$;
2) $x = y \wedge x = z \supset y = z$;
3) $x = y \wedge x < z \supset y < z$;
4) $x = y \wedge z < x \supset z < y$.

Аксиомы порядка:

5) $\neg x < x$;
6) $x < y \wedge y < z \supset x < z$;
7) $x < y \supset \exists z(x < z \wedge z < y)$;
8) $\exists z(z < x)$;
9) $\exists z(x < z)$.

Формулировка теории Lin закончена. Множество Q рациональных чисел и множество R действительных чисел с естественным порядком являются, очевидно, моделями Lin. Вообще модели Lin называются плотными линейными упорядочениями без первого и последнего элементов.

Теория Lin полна и разрешима.

Примечательная особенность Lin состоит в том, что все *счетные* модели Lin изоморфны и, следовательно, изоморфны Q. Как говорят, теория Lin *категорична в счетной мощности*.

Заметим, что теория R выглядит более мощной по своим выразительным возможностям, чем теория Lin. В самом деле, в R можно определить некоторые, уже, быть может, и не атомарные формулы $x = y$, $x < y$, относительно которых все аксиомы Lin могут быть выведены в R. Мы говорим, что теория Lin *интерпретируется* (или *относительно интерпретируется*) в теории R.

Общее определение важного понятия относительной интерпретации одной теории в другой довольно громоздко, и мы не будем его давать. Коротко говоря, теория T_1 *относительно интерпретируется* в теории T_2, если все атомарные понятия теории T_1 могут быть выражены в виде формул и термов T_2 таким образом, что все нелогические аксиомы T_1 оказываются выводимыми в T_2, по крайней мере если объекты T_1 изображаются некоторой частью объектов T_2. Эта часть определяется формулой T_2.

Если формула выводима в T_1, то ее интерпретация выводима в T_2. В частности, если в T_1 выводимо противоречие $A \wedge \neg A$, то после интерпретации окажется, что в T_2 также выводимо некоторое противоречие.

А отсюда следует, что из непротиворечивости T_2 следует непротиворечивость T_1. Таким образом, можно устанавливать непротиворечивость теорий, не обращаясь к моделям.

В случае интерпретируемости T_1 в T_2 всякая модель T_2 порождает некоторую модель для T_1. Таким образом, теория моделей T_2 позволяет судить о моделях теории T_1.

6. Для каждого натурального $n > 0$ определим теорию E_n — *элементарную теорию векторного пространства размерности* n. Это теория в языке Vect. Нелогические аксиомы E_n распадаются на две группы. Первая группа — это просто аксиомы R, относящиеся к переменным $x, y, z, \ldots$, формулам и термам Sx, $x+y$, $x \cdot y$, 0_1, $x = y$. Вторая группа — знакомые аксиомы линейного пространства:

1) $a + 0_1 = a$;
2) $a + b = b + a$;
3) $(a + b) + c = a + (b + c)$;
4) $\exists b(a + b = 0_1)$;
5) $x \cdot (a + b) = x \cdot a + x \cdot b$; $(x + y) \cdot a = x \cdot a + y \cdot a$;
6) $x \cdot (y \cdot a) = (x \cdot y) \cdot a$;
7) $a \cdot S0 = a$;
8) $\exists a_1 \ldots a_n \forall x_1 \ldots x_n (x_1 \cdot a_1 + \ldots + x_n \cdot a_n = 0_1 \supset x_1 = 0_0 \wedge \ldots \wedge x_n = 0_0)$;
9) $\forall a_1 \ldots a_{n+1} \exists x_1 \ldots x_{n+1} ((x_1 \neq 0_0 \vee x_2 \neq 0_0 \vee \ldots \vee x_{n+1} \neq 0_0) \wedge x_1 \cdot a_1 + \ldots + x_{n+1} \cdot a_{n+1} = 0_1)$.

Последние, две аксиомы как раз выражают то обстоятельство, что размерность подразумеваемого пространства равна n.

Естественной моделью теории E_n является n-мерное линейное векторное пространство над полем вещественных чисел. Известно, что теория E_n полна и разрешима.

7. Теоретико-множественные надстройки элементарных теорий определяются однотипным образом. Например, арифметика второго порядка Ar2 есть теория в языке Ar2, содержащая те же нелогические аксиомы, что и Ar, с той, однако, разницей, что в схеме аксиом индукции в качестве формулы $A(x)$ можно брать теперь любую формулу полного языка Ar2. Кроме того, в число нелогических аксиом зачисляется схема аксиом свертывания:

$$\exists X \forall x (x \in X \equiv A(x)),$$

где X не входит свободно в $A(x)$.

Теоретико-множественная надстройка сразу сильно расширяет выразительные возможности теории. Так, в теории R2 интерпретируется теория Ar2. В отличие от R теория R2 уже неполна и неразрешима.

8. Читатель может попробовать свои силы в формализации математических теорий, самостоятельно определив формальную аксиоматическую теорию — *элементарную геометрию плоскости* в стиле аксиоматики Гильберта. При естественной формализации оказывается, что полученная теория будет полной и разрешимой.

Для облегчения этой работы наметим построение языка. В элементарной геометрии плоскости два сорта переменных:

$A, B, C, \ldots$ для точек,

$a, b, c, \ldots$ для прямых.

Атомарные формулы теории могут выглядеть следующим образом:

$A = B$ — «точка A совпадает с точкой B»,

$a = b$ — «прямая a совпадает с прямой b»,

$A \in a$ — «точка A лежит на прямой a»,

$[ABC]$ — «A, B, C — три различные точки, лежащие на одной прямой так, что точка B лежит между A и C»,

$P(A, B, C, D)$ — «$A \neq B, C \neq D$ и отрезки AB и CD конгруэнтны».

Наглядно эту формулу можно записывать в виде $AB \approx CD$.

$Q(A, B, C, A_1, B_1, C_1)$ — «A, B, C — три различные точки, не лежащие на одной прямой, равно как и A_1, B_1, C_1, причем угол ABC равен углу $A_1B_1C_1$».

Наглядно эту формулу записывают в виде $\angle ABC \approx \angle A_1B_1C_1$.

В этом языке можно естественно записать все аксиомы геометрии в аксиоматике Гильберта, кроме аксиомы Архимеда и аксиомы непрерывности. Рассмотрим, например, следующую *аксиому Паша*:

Пусть A, B, C — три точки, не лежащие на одной прямой, и a — прямая, не проходящая ни через одну из точек A, B, C; если при этом прямая a проходит через одну из точек отрезка AB, то она должна пройти через одну из точек отрезка AC или через одну из точек отрезка BC.

Ее символическая запись в нашем языке:

$$\neg\exists\, b(A \in b \wedge B \in b \wedge C \in b) \wedge A \notin a \wedge B \notin a \wedge C \notin a \wedge$$
$$\wedge\, \exists\, D(D \in a \wedge [ADB]) \supset \exists\, E(E \in a \wedge ([AEC] \vee [BEC])).$$

Именно соответствующая теория (без аксиомы Архимеда и аксиомы непрерывности) и называется элементарной геометрией плоскости. Для формулировки двух последних упомянутых аксиом уже требуется надстройка языка теоретико-множественными средствами и средствами арифметики. Возникающая при этом теория — теория второго порядка геометрии плоскости — уже не является ни полной, ни разрешимой, но обладает гораздо большими выразительными возможностями.

Кодирование с исправлением ошибок

Интересным применением булевых колец является составление кодов с исправлением ошибок. Здесь мы излагаем начала теории кодов Хемминга, позволяющих исправлять одну ошибку. Подлежащая передаче информация состоит из двоичных слов

$$y = y_1 y_2 \dots y_k$$

длины k. Они кодируются «кодовыми словами»

$$x = x_1 x_2 \dots x_n$$

длины $n \geqslant k$. Предполагается, что вместо поданного отправителем кодового слова x получатель может принять слово x', отличающееся от x не более чем в одном знаке. При каких k и n кодовые слова в числе 2^n могут быть выбраны так, что по x' можно будет безошибочно восстановить x (а значит, и y)?

Со словами длины n будем обращаться как с элементами кольца $\mathbf{D}^n$. Введем норму $\|x\|$, равную числу единиц в x, и будем считать величину

$$\|x + x'\|$$

расстоянием между элементами x и x'. Ясно, что наше требование будет выполнено, если расстояние между двумя кодовыми словами будет не менее трех, т. е. сферы радиуса единица с центрами в кодовых словах не будут пересекаться. Такие сферы в $\mathbf{D}^n$ имеют по $n + 1$ элементов. Поэтому должно быть

$$2^k(n + 1) \leqslant 2^n.$$

При

$$n = 2^m - 1, \quad k = 2^m - m - 1 = n - m$$

имеем равенство

$$2^k(n + 1) = 2^n.$$

Хемминг показал, что при этих k и n поставленные задачи разрешимы.

Индексы x_r, $1 \leqslant r < 2^m$, букв кодовых слов будем записывать по двоичной системе счисления

$$r = \overline{i_1 i_2 \dots i_m},$$

где хотя бы один знак i_l отличен от нуля.

Вместо x_r с $r = i_1 \dots i_m$ будем писать

$$x_{i_1 i_2 \dots i_m}.$$

Подчиним буквы кодовых слов x линейным условиям

$$z_l = \sum_{i_l=1} x_{i_1 \dots i_m} = 0, \quad l = 1, \dots, m. \qquad (*)$$

Из теории линейных уравнений (примененной к случаю поля **D**) вытекает, что $n - m$ переменным x_r можно с соблюдением этих условий придать произвольные значения. Таким образом, получим $2^{n-m} = 2^k$ кодовых слов, удовлетворяющих условиям $(*)$. Если слово x' отличается от x в знаке $x_{i_1 \dots i_m}$, то

$$z'_l = \begin{cases} 1 & \text{при } i_l = 1, \\ 0 & \text{при } i_l = 0. \end{cases}$$

Это позволяет получателю найти и исправить ошибочную букву. Эффективность простейших кодов Хемминга показывает табличка

m	2	3	4	5
k	1	4	11	27
n	3	7	15	31

При $n = 3$ можно выбрать два кодовых слова

$$000 \quad \text{и} \quad 111.$$

Для понимания механизма действия изложенной теории полезно выписать 16 кодовых слов длины 7.

Применения к контактным схемам

На рис. 2*а* изображена схема с шестью узлами и восемью контактами. Поступающие на схему сигналы x, y и z принимают значения 0 и 1. Если $u = 1$, то контакт, обозначенный u, замыкается (пропускает ток), а контакт, обозначенный $\bar{u}$, размыкается. Если $u = 0$, то, напротив, считается замкнутым контакт $\bar{u}$, контакт же u оказывается разомкнутым. Легко понять, что схема рис. 2*а* пропускает ток из узла 1 в узел 2 в том и только в том случае, если сигналы x, y, z удовлетворяют условию

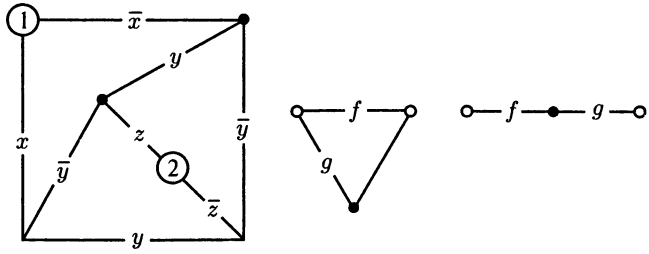
$$x\bar{y}z \cup \bar{x}yz \cup xy\bar{z} \cup \bar{x}\bar{y}\bar{z} = 1,$$

т. е.

$$x + y + z = 1.$$

Схемы такого типа с двумя выделенными узлами (на рис. 2*а* это узлы 1 и 2) называются *двухполюсными релейными схемами*, или просто *двухполюсниками*. Каждый двухполюсник, на который подается n сигналов $x_1, \ldots, x_n$, определяет некоторую булеву функцию $f(x_1, \ldots, x_n)$ от подаваемых сигналов. Эта функция называется *функцией проводимости* двухполюсника. Она описывает, при каких наборах входных сигналов ток проходит из одного выделенного узла в другой.

Из двухполюсников можно конструировать новые двухполюсники при помощи параллельных (рис. 2*б*) и последовательных (рис. 2*в*) соединений.



а) *б*) *в*)

Рис. 2

Так как всякая булева функция представима в конъюнктивной и дизъюнктивной нормальной формах, то отсюда следует, что этими двумя приемами можно построить двухполюсник с любой наперед заданной проводимостью.

Однако этот метод построения двухполюсников — далеко не всегда самый экономичный. Так, на рис. 2*а* указан двухполюсник с проводимостью $x + y + z$, содержащий восемь контактов. Мы воспользовались при этом «мостиковой» схемой, которую нельзя получить, итерируя последовательные и параллельные соединения элементов двухполюсников.

Пусть дан двухполюсник с m узлами. Если даны значения всех входных сигналов, то для каждой пары узлов i и j определено значение *непосредственной проводимости* a_{ij}, равное нулю или единице. А именно $a_{ij} = 1$, если i и j соединены контактом с проводимостью 1. Если i и j не соединены, то мы считаем $a_{ij} = 0$. Всегда $a_{ii} = 1$ и $a_{ij} = a_{ji}$.

Если заданы все непосредственные проводимости a_{ij}, то существует универсальный метод вычисления по ним *«окончательных проводимостей»* b_{ij}. Мы полагаем $b_{ij} = 1$ тогда и только тогда, когда ток проходит из узла i в узел j при данном наборе значений сигналов.

Для этого можно воспользоваться булевым умножением матриц:

$$\|c_{ij}\| = \|a_{ij}\| \cdot \|d_{ij}\|,$$

где

$$c_{ij} = a_{i1}d_{1j} \cup a_{i2}d_{2j} \cup \ldots \cup a_{im}d_{mj}.$$

Для такого умножения матриц справедлива теорема: для любой матрицы A порядка m ее степени начиная с $(m-1)$-й совпадают:

$$A^{m-1} = A^m = A^{m+1} = \ldots = A^\omega.$$

«Окончательная» степень A^ω матрицы непосредственных проводимостей и есть матрица окончательных проводимостей между узлами.

Литература

1. *Клини С. К.* Введение в метаматематику. М.: ИЛ, 1957.
2. *Клини С. К.* Математическая логика. М.: Мир, 1973.
3. *Мендельсон Э.* Введение в математическую логику. М.: Наука, 1971.
4. *Шенфилд Дж.* Математическая логика. М.: Наука, 1975.
5. *Гудстейн Р. Л.* Математическая логика. М.: ИЛ, 1961.
6. *Гильберт Д., Бернайс П.* Основания математики. Т. 1, 2. М.: Наука, 1979, 1982.
7. *Новиков П. С.* Элементы математической логики. М.: Физматгиз, 1959.
8. *Бурбаки Н.* Теория множеств. М.: Мир, 1965.
9. *Лавров И. А., Максимова Л. Л.* Задачи по теории множеств, математической логике и теории алгорифмов. М.: Наука, 1975.

Колмогоров А. Н., Драгалин А. Г.

МАТЕМАТИЧЕСКАЯ ЛОГИКА. ДОПОЛНИТЕЛЬНЫЕ ГЛАВЫ

Предисловие*

Книга представляет собой вторую часть первоначального курса математической логики [1], но может читаться и независимо, если читатель имеет некоторое предварительное знакомство с логико-математическими языками и теорией логического вывода. Необходимые предварительные сведения можно получить как в нашей книге [1], так и в первых главах любого из более подробных курсов математической логики, например [2–4]. Необходимый минимум сведений и терминологию мы напоминаем также во введении.

Книга возникла в результате обработки конспектов лекций семестрового курса математической логики для студентов первого курса механико-математического факультета Московского университета, читавшегося обоими авторами. В первой книге мы стремились познакомить читателя с основными понятиями математической логики, правильным обращением с логической символикой, логическими законами, техникой логического вывода, что составляет, на наш взгляд, минимум сведений, полезных в работе математика любой специальности. В настоящей второй части большее внимание уделяется изложению некоторых фундаментальных результатов математической логики, представляющих общематематический интерес. Предполагается, что при построении курса лектор может выбрать из предложенного материала ту или иную тему в зависимости от потребностей учебного плана или аудитории.

В первой главе излагается теория множеств в стиле аксиоматической системы Цермело—Френкеля. Мы стремились показать, как основные математические понятия и структуры могут быть введены на базе точного логико-математического языка теории множеств. Здесь же обсуждаются традиционные вопросы, относящиеся к основаниям теории множеств: парадоксы теории множеств, непротиворечивость системы Цермело—Френкеля, парадокс Скулема, содержательный аксиоматический метод и формальный аксиоматический метод в математике.

Во второй главе излагаются элементы теории алгорифмов. Здесь даны точные определения, касающиеся вычислимости по Тьюрингу, обсуждаются тезис Чёрча и понятия рекурсивного и рекурсивно-перечислимого множества. Эта часть главы может рассматриваться как обязательный минимум по теории алгорифмов. Далее приводятся основные теоремы общей теории алгорифмов относительно существования неразрешимых множеств и предикатов и излагается подготовительный материал по гёделевой нумерации конструктивных объектов и выводам свойств конструктивных объектов в формальной арифметике. Этот материал может рассматриваться как факультативный по отношению к обязательному курсу

* Учебник А. Н. Колмогорова и А. Г. Драгалина «Математическая логика. Дополнительные главы» впервые опубликован издательством Московского университета (М., 1984, 120 с.).

логики, лектор может использовать его выборочно или перенести часть материала на семинарские занятия.

Третья глава посвящена теории вывода. Здесь доказываются теорема Гёделя о полноте исчисления предикатов, теорема Лёвенгейма—Скулема, теорема о неполноте и неразрешимости всякой достаточно выразительной формальной аксиоматической теории. Доказываются также знаменитая вторая теорема Гёделя о невозможности доказательства непротиворечивости достаточно мощной формальной аксиоматической теории средствами самой этой теории и теорема Генцена об устранении сечения. Завершается глава обсуждением программы Гильберта обоснования математики. Материал третьей главы также может рассматриваться как факультативный. Например, лектор может ограничиться лишь формулировками некоторых фундаментальных теорем.

Сложность изложения многих важных результатов математической логики состоит в том, что они часто требуют для своего доказательства большого подготовительного аппарата для аккуратного проведения деталей доказательств. Так, необходимо убеждаться, что те или иные предикаты действительно вычислимы по Тьюрингу или примитивно-рекурсивны, что рассматриваемые формулы действительно выводимы в тех или иных формальных аксиоматических теориях. Такого рода утверждения доказываются обычно путем громоздкого, но в принципе нетрудного непосредственного построения соответствующих машин Тьюринга, примитивно-рекурсивных описаний, формальных выводов и т. п. Разумеется, в коротком курсе нецелесообразно тратить время на такие построения. Читателя, интересующегося деталями построений, мы в таких случаях отсылаем к более подробным руководствам, но все же стремимся к тщательному изложению всех принципиальных моментов доказательств.

Авторы

Введение

Напомним некоторые определения и понятия, нужные для дальнейшего. Подробное изложение имеется, например, в нашей книге [1], но может быть почерпнуто и из начальных глав более подробных учебников, предназначенных для лиц, специализирующихся по математической логике (см. [2–4]).

Математические суждения в логике записываются в виде формул в точно определенных логико-математических языках. Основными объектами данного логико-математического языка являются его *выражения*. Выражения подразделяются на *формулы* и *термы*. Язык Ω содержит несколько сортов переменных. Переменные каждого сорта рассматриваются как пробегающие некоторую область — множество объектов данного сорта. Вхождения переменных в выражения языка делятся на *свободные* и *связанные*. Переменные, входящие в выражение свободно, называются его *параметрами*. Выражение, не содержащее параметров, называется *замкнутым*.

Выражения логико-математического языка представляют собой строчки символов-букв из алфавита языка и строятся по некоторым строго определенным правилам. Так, каждая формула C данного языка Ω может иметь один и только один из следующих семи видов:

$(A \wedge B)$ — читается «A и B»,

$(A \vee B)$ — читается «A или B»,

$(A \supset B)$ — «из A следует B»,

$\neg A$ — «не A»,

$\forall x A$ — «для всякого x имеет место A»,

$\exists x A$ — «существует x такое, что A», атомарная формула.

Символы $\wedge$, $\vee$, $\supset$, $\neg$ называются *логическими связками* и имеют соответственно наименования: *конъюнкция*, *дизъюнкция*, *импликация* и *отрицание*. Символы $\forall, \exists$ называются *кванторами* (квантор общности и квантор существования). Как обычно, считается, что кванторные приставки $\forall x$, $\exists x$ связывают переменную x в последующей формуле, так что в формулу, начинающуюся с такой приставки, переменная x не входит свободно.

Строение атомарных формул зависит от рассматриваемого языка. Особенно просто устроены атомарные формулы у *языков первого порядка*, которые и составляют основной объект изучения в математической логике. А именно, атомарная формула языка первого порядка имеет вид $P(t_1, \ldots, t_n)$, где P — *предикатная буква* языка, а $t_1, \ldots, t_n$ — термы языка. Здесь возможен и случай $n = 0$, тогда 0-местная предикатная буква P сама по себе является атомарной формулой и называется в этом случае *пропозициональной буквой*, или *пропозициональной переменной*. n-местная предикатная буква изображает в языке *предикат* от n

переменных, в иной терминологии, *параметрическое суждение*, *высказывательную форму* от n переменных.

Термы также в разных языках устроены по-разному. И здесь самым простым и важным случаем является случай языков первого порядка. В языках первого порядка термы строятся из переменных и констант языка с помощью *функциональных символов*, т. е. каждый терм есть либо переменная, либо константа языка, либо имеет вид $f(t_1, \ldots, t_n)$, где f — функциональный символ, обозначающий в языке n-местную операцию. В языках первого порядка все переменные, входящие в терм, являются свободными, т. е. являются параметрами этого терма.

При практическом написании формул и термов мы экономим скобки, пользуясь хорошо известными соглашениями. Так, обычно опускаются внешние скобки. Кроме того, мы располагаем связки и кванторы в определенном порядке, считая, что те символы, которые в этом порядке находятся правее, «связывают сильнее», т. е. что их следует выполнять в первую очередь. Для конкретности мы придерживаемся следующего порядка выполнения операций:

$$\equiv \supset \begin{matrix} \vee & \forall \\ \wedge & \neg \quad \exists \end{matrix}.$$

Здесь $\equiv$ — производная логическая связка, $A \equiv B$ есть сокращенное обозначение формулы $((A \supset B) \wedge (B \supset A))$.

Например, формулу

$$(\forall x(P(x, y) \supset (\forall z Q(z) \wedge R)) \vee Q(x))$$

можно записать в виде

$$\forall x(P(x, y) \supset \forall z Q(z) \wedge R) \vee Q(x).$$

Иногда для дальнейшей экономии скобок мы используем точку. Если внутри скобок выполняется несколько однородных (по силе связывания) логических символов, то точкой внизу у символа мы отмечаем *главный логический символ*, т. е. тот, который выполняется в последнюю очередь. Например, формулу

$$P \supset (Q \vee R \equiv (\neg R \equiv \neg P))$$

можно записать в виде

$$P \supset (Q \vee R \equiv .\, \neg R \equiv \neg P).$$

Если T — выражение языка, $x_1, \ldots, x_n$ — различные переменные и $t_1, \ldots, t_n$ — термы соответствующих сортов, то через $(T(x_1, \ldots, x_n \parallel t_1, \ldots, t_n))$ мы обозначим результат *правильной подстановки* термов $t_1, \ldots, t_n$ вместо свободных вхождений переменных $x_1, \ldots, x_n$ в T. Для получения выражения $(T(x_1, \ldots, x_n \parallel t_1, \ldots, t_n))$ следует заместить одновременно все свободные вхождения переменных $x_1, \ldots, x_n$ на термы $t_1, \ldots, t_n$ соответственно. При этом, если необходимо, следует переименовать некоторые связанные переменные выражения T. А именно, если некоторая переменная x некоторого терма t_i, будучи свободной в t_i оказывается связанной после подстановки (в таких случаях говорят, что терм t_i *не свободен* для подстановки, или что происходит *коллизия* переменных), то следует в T предварительно переименовать некоторые связанные переменные на новые, чтобы при подстановке не происходило коллизий. Например, результатом правильной подстановки

$$(\exists x P(x, y)(y \parallel f(x, y)))$$

является формула

$$\exists u P(u, f(x, y))$$

с новой связанной переменной u.

Выражение $(T(x_1, \ldots, x_n \parallel t_1, \ldots, t_n))$ сокращаем до $T(x_1, \ldots, x_n \| t_1, \ldots, t_n)$ или даже до $T(t_1, \ldots, t_n)$, если упоминание о переменных $x_1, \ldots, x_n$ несущественно. Следует помнить, что в записях вида $A(t, r)$ всегда имеется в виду именно правильная подстановка с необходимым переименованием связанных переменных.

Мы предполагаем, что читатель знаком с обычными языками первого порядка, такими как язык арифметики, язык теории групп, язык логики предикатов. Впрочем, язык логики предикатов и язык арифметики мы напомним ниже.

Выражения языка суть просто строчки символов специального вида и сами по себе не имеют никакого смысла. Для придания смысла выражениям языка Ω необходимо задать *интерпретацию для языка* Ω (в другой терминологии, *структуру для языка* Ω). Задать интерпретацию M для языка Ω означает, в частности, задать *область пробегания* для каждого сорта переменных, фигурирующих в языке. Если в произвольном выражении языка заместить все его параметры объектами из соответствующих областей пробегания, то получится то, что называется *оцененным выражением* языка (точнее, выражением, оцененным в данной модели M). В частности, замкнутое выражение само по себе является оцененным в любой модели.

Каждая интерпретация M языка позволяет по естественным правилам подразделить все оцененные формулы на *истинные* в данной интерпретации и на *ложные* в данной интерпретации. Если A — формула, оцененная в M, то запись $M \models A$ будет означать, что A истинна в интерпретации M.

Понятие истинности оцененной формулы в структуре M согласовано со строением формулы. Например, $M \models A \wedge B$ тогда и только тогда, когда $M \models A$ и $M \models B$. Далее, $M \models A \vee B$ тогда и только тогда, когда $M \models A$ или $M \models B$. $M \models \neg A$ равносильно тому, что неверно $M \models A$. Утверждение $M \models A \supset B$ ложно лишь в одном случае, а именно когда $M \models A$ и $M \models \neg B$. При остальных комбинациях истинностных значений утверждение $M \models A \supset B$ считается истинным (так понимаемую логическую связку $\supset$ часто называют *материальной импликацией*). Далее, $M \models \forall x A$ тогда и только тогда, когда для всякого объекта a из области пробегания переменной x имеем $M \models A(x \parallel a)$. Аналогично $M \models \exists x A$ равносильно тому, что существует объект a из нужной области такой, что $M \models A(x \parallel a)$. Коротко можно сказать, что мы придерживаемся классической семантики, где логические связки трактуются по законам двузначной булевой алгебры.

Подобным образом интерпретация M позволяет приписать значение $|t|_m$ каждому оцененному терму языка. Значением $|t|_m$ является объект, который выражает терм t при данной оценке своих параметров. Значение терма зависит только от значений составляющих его подтермов. Это означает, что, если r — терм, в котором оценены все параметры, за исключением, может быть, x, и t — оцененный терм того же сорта, что и x, то $|(x \parallel t)|_M$ совпадает с $|r(x \parallel |t|_M)|_M$.

Аналогично, $M \models A(x \parallel t)$ тогда и только тогда, когда $M \models A(x \parallel |t|_m)$.

Таким образом, при фиксированной интерпретации M языка Ω формула A этого языка рассматривается как выражающая некоторое параметрическое суждение, зависящее от оценки параметров. Как говорят, формула задает в Ω *высказывательную форму*. В частности, если формула является предложением Ω, т. е. вовсе не содержит параметров, то в M такая формула определяет конкретное истинное или ложное высказывание. Аналогично терм t задает в M операцию от своих параметров. Замкнутый терм задает в интерпретации M некоторый конкретный объект.

С точки зрения логики особенно интересны формулы языка, истинные в любой интерпретации для Ω при любой оценке своих параметров. Такие формулы называются *логическими законами* языка (в другой терминологии — *общезначимыми формулами*, *тавтологиями* языка). Понятие логического закона является некоторым математическим уточнением идеи формулы, истинной «лишь в силу своей формы, независимо от содержания».

Далее, мы говорим, что формула A логически эквивалентна формуле B, и пишем $A \sim B$, если формула $A \equiv B$ является логическим законом. Читатель, несомненно, знаком с некоторыми логическими законами и логическими эквивалентностями, такими как выражение одних логических связок через другие, пронесение кванторов через логические связки и т. п. Логические законы позволяют преобразовывать формулы к нужному нам виду, например, всякую формулу, как известно, можно заменить логически эквивалентной формулой, имеющей уже предваренный вид, т. е. такой, у которой все кванторы находятся впереди формулы, а далее идет бескванторная формула.

Для каждого логико-математического языка Ω определяется *исчисление предикатов* в языке Ω. При описании исчисления предикатов задаются его аксиомы и правила вывода, при этом в различных учебниках можно найти несколько отличающиеся друг от друга формулировки (эти отличия, конечно, несущественны для развиваемой далее теории). Мы остановимся на следующей формулировке. *Аксиомами исчисления предикатов* в языке Ω называются формулы этого языка, имеющие один из следующих видов:

1) $A \supset . B \supset A$;
2) $(A \supset . B \supset C) \supset . (A \supset B) \supset (A \supset C)$;
3) $A \supset . B \supset A \wedge B$;
4) $A \wedge B \supset A$;
5) $A \wedge B \supset B$;
6) $(A \supset C) \supset . (B \supset C) \supset (A \vee B \supset C)$;
7) $A \supset A \vee B$;
8) $B \supset A \vee B$;
9) $(A \supset B) \supset . (A \supset . \neg B) \supset \neg A$;
10) $\neg\neg A \supset A$;
11) $\forall x A \supset A(x||t)$;
12) $\forall x(C \supset A(x)) \supset . C \supset \forall x A(x)$;
13) $A(x||t) \supset \exists x A$;
14) $\forall x(A(x) \supset C) \supset . \exists x A(x) \supset C$.

Здесь A, B, C — произвольные формулы Ω. В схемах 12), 14) формула C не содержит свободно переменной x. Нетрудно убедиться, что все аксиомы исчисления предикатов суть логические законы.

Правилами вывода исчисления предикатов являются фигуры следующих видов:

$$\frac{A,\ A \supset B}{B}, \qquad \frac{A}{\forall x A}.$$

Здесь A, B — произвольные формулы Ω, x — произвольная переменная. Первое правило носит традиционное латинское название — *модус поненс*, второе правило называется *правилом обобщения*.

Дерево формул есть по определению двумерная фигура, составленная из формул языка по следующим правилам:

1) каждая формула A является деревом формул, нижней формулой этого дерева называется сама формула A;
2) если D_1 и D_2 суть деревья формул с нижними формулами вида A и $A \supset B$ соответственно, то фигура $\dfrac{D_1, D_2}{B}$ есть дерево формул; мы говорим, что формула B получена в этом дереве из A и $A \supset B$ по правилу модус поненс; нижней формулой результирующего дерева формул является по определению формула B;
3) если D_1 — дерево формул с нижней формулой A и x — переменная, то формула $\dfrac{D_1}{\forall x A}$ есть также дерево формул; мы говорим, что нижняя формула $\forall x A$ этого дерева формул получена из A по правилу обобщения.

Коротко говоря, дерево формул есть конечное дерево, в вершинах которого расставлены формулы и переходы сверху вниз в котором совершаются по правилам вывода исчисления предикатов.

Верхние, начальные формулы в дереве формул, *которые не имеют вида аксиом исчисления предикатов*, называются *гипотезами*, или *открытыми посылками* рассматриваемого дерева формул. Ветвью дерева формул D мы назовем последовательность $A_1, \ldots, A_n$ вхождений формул в D такую, что для всякого $i < n$ формула A_{i+1} находится в D непосредственно выше формулы A_i, и A_1 — нижняя формула D, а A_n — верхняя формула D. Пусть A и B — различные вхождения формул в D. Мы говорим, что формула B *расположена выше* формулы A в D, если существует ветвь $A_1, \ldots, A_n$ дерева формул D такая, что A есть A_i и B есть A_j, причем $j > i$.

Деревом вывода, или просто *выводом*, в исчислении предикатов назовем дерево формул, удовлетворяющее следующему *структурному требованию*: если формула вида $\forall x A$ получена в выводе из формулы A по правилу обобщения, то переменная x не входит свободно в гипотезы, расположенные выше рассматриваемого вхождения формулы $\forall x A$.

Если формула вида $\forall x A$ получена по правилу обобщения из формулы A и формула B находится выше рассматриваемого вхождения $\forall x A$ и содержит свободно x, то говорят, что переменная x *варьируется* в формуле B. Наше структурное требование означает, таким образом, что в выводе параметры гипотез *не варьируются*, остаются *фиксированными*.

Если Γ — конечный список формул и A — формула языка Ω, то будем говорить, что формула A *выводима* в исчислении предикатов из списка формул Γ, и писать $\Gamma \vdash A$, если может быть построен вывод D с нижней формулой A такой, что всякая гипотеза D является членом списка Γ. Разумеется, некоторые формулы Γ могут при этом и не быть гипотезами D. Мы говорим, что вывод D формулы A не зависит от таких членов Γ.

Если список Γ пуст, то $\Gamma \vdash A$ означает, что существует вывод формулы A вообще без гипотез. В этом случае мы говорим, что формула A *выводима* в исчислении предикатов, и пишем $\vdash A$.

Саму фигуру $\Gamma \vdash A$ назовем *выводимостью*, или *секвенцией*. Таким образом, чтобы установить секвенцию $\Gamma \vdash A$, следует построить вывод в исчислении предикатов с нижней формулой A, все гипотезы которого находятся среди членов Γ.

Теорема о дедукции. *Если* $\Gamma, A \vdash B$, *то* $\Gamma \vdash A \supset B$.

Если $\vdash A$, то A является логическим законом. Таким образом, на исчисление предикатов можно смотреть как на некоторый формальный механизм для получения логических законов.

Для вывода формул в исчислении предикатов используется специально подобранная удобная система производных правил, называемая *техникой естественного вывода*. Читатель может познакомиться с этими правилами по нашей книге [1] или, например, по книге [3]. Мы будем предполагать некоторое умение выводить формулы в исчислении предикатов и иногда будем опускать доказательства того, что та или иная формула выводима. Начинающему при этом полезно по крайней мере убеждаться, что рассматриваемая формула является логическим законом.

Формальная аксиоматическая теория T задается двумя объектами: логико-математическим языком Ω и множеством Y предложений этого языка. Ω называется языком теории T, а элементы множества Y называются *нелогическими аксиомами* T. Подчеркнем, что все нелогические аксиомы суть предложения, т. е. замкнутые формулы языка Ω.

Мы говорим, что формула A языка Ω *выводима в теории* T, и пишем $T \vdash A$, если существует конечный список Γ членов Y такой, что $\Gamma \vdash A$ в исчислении предикатов.

Интерпретация M для языка Ω называется *моделью теории* T, если $M \models A$ для всякого предложения $A \in Y$, т. е. если всякая нелогическая аксиома теории T истинна в M. Если M — модель теории T и $T \vdash B$, где B — предложение, то $M \models B$. Таким образом, выводимое в T предложение оказывается истинным во всякой модели теории T.

Опишем кратко некоторые формальные аксиоматические теории.

Элементарная арифметика Ar. Язык этой теории содержит один сорт переменных $x, y, z, \ldots$, константу 0, один одноместный функциональный символ Sx и два двуместных функциональных символа $x + y$, $x \cdot y$. Атомарные формулы Ar имеют вид $(t = r)$, где t, r — произвольные термы языка.

Нелогические аксиомы Ar делятся на три группы: аксиомы равенства, аксиомы Пеано, определяющие аксиомы для сложения и умножения. При формулировке нелогических аксиом ниже мы будем опускать кванторы общности спереди. Предполагается, конечно, что каждая аксиома является предложением.

Аксиомы равенства:

1) $x = x$;
2) $x = y \wedge x = z \supset y = z$.

Аксиомы Пеано:

3) $Sx \neq 0$;
4) $(Sx = Sy) \equiv x = y$;
5) $A(0) \wedge \forall x(A(x) \supset A(Sx)) \supset \forall x A(x)$ (принцип полной математической индукции).

Определяющие аксиомы для сложения и умножения:

6) $x + 0 = x$;
7) $x + Sy = S(x + y)$;
8) $x \cdot 0 = 0$;
9) $x \cdot Sy = x \cdot y + x$.

Аксиоматика теории Ar подобрана таким образом, чтобы все обычные факты, выразимые в языке теории, были бы в ней выводимы. Стандартной моделью теории Ar является модель ω. В этой модели переменные рассматриваются как пробегающие множество всех натуральных чисел; это множество мы также обозначаем через ω, константа изображает натуральное число нуль, функциональные символы интерпретируются очевидным образом. Как мы увидим далее, существуют и другие модели теории Ar, не изоморфные ω. В то же время теория Ar является неполной: можно указать предложение, истинное в модели ω, но не выводимое в Ar; мы докажем это в гл. III, § 1.

Арифметика второго порядка Ar2. Язык этой теории содержит два сорта переменных. Переменные $x, y, z, \ldots$ рассматриваются как пробегающие натуральные числа, переменные $X, Y, Z, \ldots$ пробегают произвольные подмножества множества всех натуральных чисел. Константы и функциональные символы Ar2 те же, что и в языке Ar. Таким образом, язык Ar2 содержит термы двух сортов: термы для натуральных чисел и термы для множеств натуральных чисел, причем термами для множеств натуральных чисел являются лишь переменные $X, Y, Z, \ldots$. Атомарные формулы Ar2 имеют один из следующих двух видов: формальные равенства $(t = r)$, где t и r — термы для натуральных чисел, и $(t \in X)$, где t — терм для натуральных чисел и X — переменная для множеств натуральных чисел. Сложные формулы строятся обычным образом с помощью логических связок и кванторов, причем кванторы используются по обоим сортам переменных.

Нелогические аксиомы Ar2 имеют тот же вид, что и аксиомы Ar, но в схеме индукции 5) в качестве формулы $A(x)$ можно использовать произвольную формулу языка Ar2. Кроме того, добавляется новая схема аксиом, *аксиома свертывания*:

10) $\exists X \forall x (x \in X \equiv A(x))$,

где $A(x)$ — произвольная формула Ar2, не содержащая свободно переменной X.

Стандартной моделью Ar2 является модель, которую мы, так же как и в случае Ar, будем называть моделью ω. В этой модели переменные $x, y, z, \ldots$ пробегают множество ω всех натуральных чисел, а переменные $X, Y, Z, \ldots$ пробегают множество $P\omega$ всех подмножеств натуральных чисел. Эта теория также имеет много других интересных моделей, неизоморфных ω.

Исчисление предикатов в языке Ω также можно рассматривать как формальную аксиоматическую теорию в языке Ω с пустым множеством нелогических аксиом. Всякая интерпретация языка Ω является моделью этой теории.

Чистое исчисление предикатов есть по определению исчисление предикатов в специальном языке с одним сортом переменных, без констант и функциональных символов, со счетным набором предикатных символов для каждого числа аргументных мест.

Глава I

Теория множеств

§ 1. Язык наивной теории множеств, парадоксы наивной теории множеств

1. Теперь мы перейдем к изучению некоторого конкретного языка M^+, предназначенного для описания свойств множеств. Мы исходим из гипотезы, что имеется некоторая математическая структура — семейство множеств. Для каждых двух множеств a и b определено, когда $a \in b$ — a принадлежит b, а когда это неверно. Каковы дальнейшие свойства этой структуры $\mathcal{M}$ и в какой мере законно ее рассмотрение, мы обсудим позднее.

Язык M^+ содержит один сорт переменных $x, y, z, \ldots$, которые рассматриваются как пробегающие *множества* — элементы структуры $\mathcal{M}$.

Понятие *формулы* и *терма языка* M^+ формулируется в виде одновременного индуктивного определения. Пункт 1) — базис этого определения, а 2)–5) — индуктивные шаги:

1) переменная есть терм;
2) если t и r суть термы, то $(t \in r)$ есть формула;
3) если φ и ψ суть формулы, то

$$(\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \supset \psi), \neg\varphi$$

также суть формулы;

4) если x — переменная, а φ — формула, то $\forall x\varphi, \exists x\varphi$ суть формулы;
5) если x — переменная, φ — формула, то $\{x \mid \varphi\}$ есть терм.

Определение закончено.

Формула M^+ может быть, например, такой

$$\{x \mid x \in y \supset x \in z\} \in \{y \mid \neg y \in y\}.$$

Терм $\{x \mid \varphi\}$ читается так: «множество всех x, для которых $\varphi(x)$». Мы говорим, что этот терм определяет множество *свертыванием*, а сам терм называем *сверткой* по формуле φ. Формула φ может быть совершенно произвольной формулой языка. Говорят, что в языке M^+ имеется *неограниченное свертывание*.

Заметим, что язык M^+ не является языком первого порядка, именно в силу пункта 5) определения, позволяющего определять новые термы

с помощью формул. Такого эффекта нет в языках первого порядка, где термы определяются отдельно. Следует иметь в виду, что в терме $\{x \mid \varphi\}$ переменная x — связанная, так что $\{x \mid\}$ играет роль квантора. В языке M^+ термы могут содержать связанные переменные, так что теория переименования связанных переменных, коллизии переменных и т. п. должны теперь относиться и к термам.

2. Введем сокращенные обозначения:

x включено в y:	$x \subseteq y \leftrightharpoons \forall z(z \in x \supset z \in y)$;
x равно y:	$x = y \leftrightharpoons (x \subseteq y) \wedge (y \subseteq x)$;
x не равно y:	$x \neq y \leftrightharpoons \neg(x = y)$;
x не принадлежит y:	$x \notin y \leftrightharpoons \neg(x \in y)$;
x строго включено в y:	$x \subset y \leftrightharpoons (x \subseteq y) \vee (x \neq y)$.

Разумеется, эти обозначения можно использовать не только с переменными x и y, но и с другими термами. При этом $(t \subseteq r)$ следует трактовать, конечно, как $(x \subseteq y)(x, y \parallel t, r)$. Аналогичное замечание относится и к дальнейшим обозначениям.

Пользуясь законами логики, можно установить, что в $\mathcal{M}$ имеют место некоторые факты. Например, в $\mathcal{M}$ при любой оценке $x \subseteq x$, т. е. $x \subseteq x$ есть *закон теории множеств*. В самом деле, $x \subseteq x$ имеет вид $\forall z(z \in x \supset z \in x)$ и вытекает из логического закона тождества $z \in x \supset z \in x$.

Мы будем писать

$$.x \subseteq x,$$

где точка слева заменяет словесный оборот «следующая формула является законом теории множеств», т. е. истинна в $\mathcal{M}$ при любой оценке свободных переменных.

Упражнение. Докажите:

$$.x = x;$$
$$.x = y \supset y = x;$$
$$.x = y \wedge y = z \supset x = z.$$

3. Так как структура $\mathcal{M}$ должна отражать интуитивные свойства множеств, мы считаем, что в ней законами являются следующие два вида формул.

1) Аксиома объемности (экстенсиональности):

$$.x = y \wedge x \in z \supset y \in z.$$

2) Аксиома свертывания:

$$.z \in \{y \mid \varphi(y)\} \equiv \varphi(z).$$

Здесь $\varphi(z)$ есть, разумеется, $\varphi(y \parallel z)$.

Аксиома объемности имеет следствием, что определенное нами равенство $x = y$ действительно обладает свойствами равенства. А именно выполняются *свойства замены равного на равное*:

$$.x = y \supset (\varphi(x) \equiv \varphi(y));$$
$$.x = y \supset (t(x) = t(y)).$$

Нетрудно доказать эти два закона, исходя из аксиомы объемности, индукцией по определению п. 1, но мы не будем этим заниматься и свободно используем эти два последних закона в дальнейшем.

Аксиома свертывания описывает свойства выражения $\{x \mid \varphi\}$.

4. Введем понятие *неупорядоченной пары*:

$$\{x, y\} \leftrightharpoons \{z \mid z = x \vee z = y\}.$$

Основные свойства этого выражения:

1) $.u \in \{x, y\} \equiv (u = x \vee u = y)$;
2) $.x \in \{x, y\}$;
3) $.y \in \{x, y\}$;
4) $.\{x, y\} = \{y, x\}$.

▷ Свойство 1) следует из аксиомы свертывания. Докажем 2).

Из первого утверждения, в частности, следует

$$.x \in \{x, y\} \equiv (x = x \vee x = y),$$

но

$$.x = x \vee x = y,$$

так как $.x = x$ (см. п. 2). Следовательно, верна правая часть эквивалентности, а значит, и левая.

Докажем утверждение 4). Необходимо показать, что для всякого z

$$z \in \{x, y\} \equiv z \in \{y, x\}.$$

Но ввиду первого свойства

$$z \in \{x, y\} \equiv (z = x \vee z = y),$$
$$z \in \{y, x\} \equiv (z = y \vee z = x),$$

и правые части логически эквивалентны. ◁

5. Понятие *одноэлементного множества* (*синглетона*):

$$\{x\} \leftrightharpoons \{z \mid z = x\}.$$

Основные свойства:

1) $.u \in \{x\} \equiv (u = x)$;
2) $.x \in \{x\}$.

Доказательство предоставляется читателю в качестве упражнения.

Лемма.

1) $.\{x\} = \{y\} \equiv (x = y)$;
2) $.\{x, y\} = \{u, v\} \equiv ((x = u \wedge y = v) \vee (x = v \wedge y = u))$;
3) $.\{x, y\} = \{u\} \equiv (x = u \wedge y = u)$.

▷ Докажем 2). Импликация справа налево вытекает просто из общих законов равенства п. 3. Допустим $\{x, y\} = \{u, v\}$. По определению равенства это означает

$$\forall z(z \in \{x, y\} \equiv z \in \{u, v\}).$$

Имеем $x \in \{x, y\}$ и, значит, $x \in \{u, v\}$. Отсюда (п. 4) $x = u \vee x = v$. Разберем два случая и покажем, что в каждом из них верно

$$(x = u \wedge y = v) \vee (y = u \wedge x = v).$$

1) Пусть $x = u$. Ввиду $v \in \{u, v\}$ имеем $v \in \{x, y\}$, т. е. $v = x \vee v = y$. Если $v = y$, то $(x = u \wedge y = v)$, что и требовалось. Если же $v = x$, то ввиду $x = u$ имеем $u = v$. Далее $y \in \{x, y\}$ и, значит, $y \in \{u, v\}$, т. е. $y = u \vee y = v$. Ввиду $u = v$ всегда $y = v$. Таким образом, вновь имеем $(x = u \wedge y = v)$. 2) Пусть $x = v$. Рассматривается симметрично. ◁

6. Понятие *пустого множества*:

$$\varnothing \leftrightharpoons \{x \mid x \neq x\}.$$

Основные свойства:

1) $.\forall z(z \notin \varnothing)$;
2) $.\varnothing \neq \{\varnothing\}$;
3) $.\{\varnothing\} \neq \{\varnothing, \{\varnothing\}\}$.

▷ 1) $z \in \varnothing \equiv (z \neq z)$, но правая часть ложна в силу п. 2. Значит, $z \notin \varnothing$. 2) Имеем $\varnothing \notin \varnothing$ и $\varnothing \in \{\varnothing\}$ значит,

$$\neg\forall z(z \in \varnothing \equiv z \in \{\varnothing\}),$$

т. е. $\varnothing \neq \{\varnothing\}$. ◁

Упражнение. Докажите $.\varnothing \subseteq u$ и, в частности, $\varnothing \subseteq \varnothing$.

Приведите примеры конкретных множеств A, B, C, D (множества описываются замкнутыми термами M^+) таких, что

$$A \subseteq B, \quad \text{но } A \notin B \quad \text{и} \quad C \in D, \quad \neg(C \subseteq D).$$

7. *Пересечение, объединение и разность двух множеств*

$$x \cap y \leftrightharpoons \{z \mid z \in x \wedge z \in y\};$$
$$x \cup y \leftrightharpoons \{z \mid z \in x \vee z \in y\};$$
$$x \setminus y \leftrightharpoons \{z \mid z \in x \wedge z \notin y\}.$$

1) $.u \in x \cap y \equiv (u \in x \wedge u \in y)$;
2) $.u \in x \cup y \equiv (u \in x \vee u \in y)$;
3) $.u \in x \setminus y \equiv (u \in x \wedge u \notin y)$.

▷ Эти утверждения вытекают непосредственно из аксиомы свертывания. ◁

Упражнение. Докажите:

1) $.z \setminus (x \cap y) = (z \setminus x) \cup (z \setminus y)$;
2) $.(x \cup y) \cap z = (x \cap z) \cup (y \cap z)$.

8. Определим теперь *объединение* и *пересечение* семейства множеств.

$$\cup x \leftrightharpoons \{z \mid \exists u(u \in x \wedge z \in u)\};$$
$$\cap x \leftrightharpoons \{z \mid \forall u(u \in x \supset z \in u)\}.$$

Для формулировки свойств этих термов введем полезное общее определение *ограниченных кванторов*

$$(\forall x \in y)\varphi(x) \leftrightharpoons \forall x(x \in y \supset \varphi(x));$$
$$(\exists x \in y)\varphi(x) \leftrightharpoons \exists x(x \in y \wedge \varphi(x)).$$

Первое читается как «для всех x, принадлежащих y, имеет место $\varphi(x)$», а второе — как «существует x, принадлежащее y, такое, что имеет место $\varphi(x)$».

Обратите внимание, что для общности используется импликация, а для существования — конъюнкция. При таком определении законы де Моргана верны и для ограниченных кванторов.

Точнее,

$$.\neg(\forall x \in y)\varphi(x) \equiv (\exists x \in y)\neg\varphi(x);$$
$$.\neg(\exists x \in y)\varphi(x) \equiv (\forall x \in y)\neg\varphi(x).$$

В самом деле, $\neg(\forall x \in y)\varphi(x)$ означает $\neg\forall x(x \in y \supset \varphi(x))$ и по логическим законам эквивалентно $\exists x\neg(x \in y \supset \varphi(x))$ и далее, $\exists x(x \in y \wedge \neg\varphi(x))$.

Подобным образом можно определить

$$(\forall x \subseteq y)\varphi(x) \leftrightharpoons \forall (x \subseteq y \supset \varphi(x));$$
$$(\exists x \subseteq y)\varphi(x) \leftrightharpoons \exists (x \subseteq y \wedge \varphi(x))$$

с выполнением законов

$$.\neg(\forall x \subseteq y)\varphi(x) \equiv (\exists x \subseteq y)\neg\varphi(x);$$
$$.\neg(\exists x \subseteq y)\varphi(x) \equiv (\forall x \subseteq y)\neg\varphi(x).$$

В языке арифметики можно определить

$$(\forall x \leqslant y)A(x) \leftrightharpoons \forall x(x \leqslant y \supset A(x));$$
$$(\exists x \leqslant y)A(x) \leftrightharpoons \exists x(x \leqslant y \wedge A(x)).$$

И вновь будем иметь, например,

$$\omega \models \neg(\exists x \leqslant y)A(x) \equiv (\forall x \leqslant y)\neg A(x).$$

Заметьте, что знак неравенства в законах де Моргана «не переворачивается»! Студент иногда склонен ошибочно утверждать

$$\omega \models \neg(\exists x \leqslant y)A(x) \equiv (\forall x > y)\neg A(x)?$$

Основные свойства объединения и пересечения:

1) $.z \in \cup x \equiv (\exists u \in x)(z \in u)$;
2) $.z \in \cap x \equiv (\forall u \in x)(z \in u)$.

▷ Эти свойства имеют место по аксиоме свертывания и в силу определения. ◁

9. *Универсальное множество* (*универсум*, *множество всех множеств*) определяется как

$$V = \{z \mid z = z\}.$$

Имеем: $.\forall z(z \in V)$.

▷ По определению $z \in V \equiv (z = z)$, но правая часть верна (см. п. 2). ◁

Общее дополнение определяется следующим образом:

$$\tilde{x} \leftrightharpoons V \setminus x.$$

Упражнение.

$$.\overline{x \cup y} = \tilde{x} \cap \tilde{y};$$
$$.x \setminus y = x \cap \tilde{y}.$$

Лемма.

$$.\cup \varnothing = \varnothing; \quad .\cap \varnothing = V.$$

▷ $z \in \cup\varnothing \equiv (\exists u \in \varnothing)(z \in u)$ и правая часть ложна, так как $\forall u(u \notin \varnothing)$. Следовательно, $z \notin \cup\varnothing$ для всякого z и, значит, $\cup \varnothing = \varnothing$. $z \in \cap\varnothing \equiv (\forall u \in \varnothing)(z \in u)$ и правая часть истинна (в силу ложности посылки импликации). Следовательно, $z \in \cap\varnothing$ для всякого z и, значит, $\cap \varnothing = V$. ◁

10. *Множество всех подмножеств* (*множество-степень*)

$$Px \leftrightharpoons \{z \mid z \subseteq x\}; \quad .u \in Px \equiv (u \subseteq x).$$

11. Дадим определение некоторого стандартного бесконечного множества.

Введем теоретико-множественную *операцию следования*:

$$Sx \leftrightharpoons x \cup \{x\}.$$

Назовем множество x *прогрессивным*, если оно содержит $\varnothing$ и замкнуто относительно S. Формально

$$\mathrm{Prog}(x) \leftrightharpoons (\varnothing \in x) \wedge \forall z(z \in x \supset Sz \in x).$$

Теперь в качестве стандартного бесконечного множества возьмем пересечение семейства всех прогрессивных множеств:

$$\omega \leftrightharpoons \cap \{x \mid \mathrm{Prog}(x)\}.$$

Интуитивно ω состоит из последовательности элементов:

$$\varnothing, \quad \{\varnothing\}, \quad \{\varnothing, \{\varnothing\}\}, \quad \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \quad \ldots .$$

Каждый член этой последовательности получается операцией S из предыдущего члена. Все члены различны, так что ω бесконечно. Член последовательности с номером n (если считать с нуля) является n-элементным множеством. Эти интуитивные идеи можно подтвердить в виде точных фактов:

1) $.\varnothing \in \omega$;
2) $.z \in \omega \supset Sz \in \omega$;
3) $.\mathrm{Prog}(x) \supset (\omega \subseteq x)$.

▷ По определению $u \in \omega \equiv \forall x(\mathrm{Prog}(x) \supset u \in x)$. Если сюда вместо u подставить $\varnothing$, то правая часть верна (по определению $\mathrm{Prog}(x)$). Следовательно, $\varnothing \in \omega$. Далее, если $z \in \omega$, то $z \in x$ для всех x, $\mathrm{Prog}(x)$. Но тогда и $Sz \in x$ для всех x, $\mathrm{Prog}(x)$, т. е. $Sz \in \omega$. Наконец, докажем 3). Пусть $\mathrm{Prog}(x)$, необходимо установить $\omega \subseteq x$, т. е. $z \in \omega \supset z \in x$ для всех z. Но если $z \in \omega$, то, конечно, $z \in x$ ввиду $\mathrm{Prog}(x)$. ◁

12. Введем теперь два специальных обозначения для некоторых термов вида свертки.

Определение множества выделением:

$$\{x \in y \mid \varphi(x)\} \leftrightharpoons \{x \mid x \in y \wedge \varphi(x)\}.$$

Выражение слева читается как «множество всех x, принадлежащих y, такое, что $\varphi(x)$». Здесь переменная x — связанная, а y — свободная. Мы считаем, что x отлично от y. На общих основаниях вместо y можно, разумеется, правильно подставлять термы (переименовывая связанное x, если нужно).

Основное свойство этого обозначения:

$$.u \in \{x \in y \mid \varphi(x)\} \equiv (u \in y \wedge \varphi(u)).$$

Определение множества подстановкой:

$$\{y \mid x \in u, \ (x \mapsto y), \ \varphi(x, y)\} \leftrightharpoons$$
$$\leftrightharpoons \{y \mid (\exists\, x \in u)(\varphi(x, y) \wedge \forall\, z(\varphi(x, z) \supset y = z))\}.$$

Здесь x, y, u — различные переменные, причем x и y — связанные, а u — свободная.

Таким образом, слева обозначено некоторое множество Q такое, что $y \in Q \Leftrightarrow$ найдется $x \in u$ такое, что для этого x верно $\varphi(x, y)$, причем указанное y *единственно*. Иными словами, будем просматривать различные $x \in u$. Для некоторых $x \in u$ не найдется вовсе y такого, что $\varphi(x, y)$. Для некоторых $x \in u$ существует много y таких, что $\varphi(x, y)$. А вот для некоторых $x \in u$ существует ровно одно y такое, что $\varphi(x, y)$. В точности все такие y мы и зачисляем в множество Q.

Эти интуитивные идеи можно оформить в виде точных фактов.

Пусть далее Q обозначает терм

$$\{y \mid x \in u, \quad (x \mapsto y), \quad \varphi(x, y)\},$$
$$.z \in Q \equiv (\exists\, x \in u)(\varphi(x, z) \wedge \forall\, v(\varphi(x, v) \supset z = v)).$$

▷ Утверждение следует непосредственно из определения. ◁

Введем сокращение (читается «существует и только одно x такое, что $\varphi(x)$»):

$$\exists! x\, \varphi(x) \leftrightharpoons \exists\, x\, \varphi(x) \wedge \forall\, y\, z(\varphi(y) \wedge \varphi(z) \supset y = z).$$

Упражнение. $x \in u \wedge \exists! v\, \varphi(x, v) \wedge \varphi(x, y) \supset y \in Q$.

13. Рассмотрим *множество Рассела*

$$R \leftrightharpoons \{x \mid x \notin x\}.$$

Это — конкретное множество, описанное замкнутым термом языка M^+.

По аксиоме свертывания для любого u имеем

$$.u \in R \equiv u \notin u.$$

В частности, подставляя вместо u множество R, получим

$$.R \in R \equiv R \notin R.$$

С другой стороны, очевидно, имеем $\neg(R \in R \equiv R \notin R)$.

Мы пришли к противоречию.

Это короткое рассуждение и является *парадоксом Рассела* в нашем языке.

Обсудим кратко природу парадоксов, к которым относится и парадокс Рассела.

Рассмотрим следующее высказывание:

«Высказывание, написанное в этой строке, ложно».

Истинно или ложно высказывание, написанное в кавычках? Исходя из его смысла, можно заключить, что оно истинно тогда и только тогда, когда оно ложно, и мы приходим к противоречию. Причину парадокса можно усматривать в структуре высказывания, написанного в кавычках; оно ссылается само на себя. Здесь проявляется *абстракция отчуждения*, в силу которой исследователь сам процесс своего исследования, свои мысли, делает объектом исследования. Мы видим, что если это делать неосторожно, то получаются внутренне противоречивые высказывания.

В несколько иной форме этот парадокс известен как *парадокс Эвбулида* (IV век до н. э.). Пусть некто говорит: «Я лгу». Истинно или ложно это его высказывание?

Конечно, можно устранить парадоксы, считая приведенные высказывания неосмысленными (или неправильно построенными). Но возникает трудная проблема, а какие высказывания осмыслены? Не окажется ли, что, казалось бы, надежные утверждения в математике или физике

внутренне противоречивы? Каковы критерии, отличающие осмысленные высказывания от неосмысленных?

Внимательный анализ показывает, что в теории множеств возникает аналогичная ситуация при использовании аксиомы свертывания (п. 3). Сначала исследователь формулирует свойство $\varphi(y)$, а затем образует объект исследования — множество $\{y \mid \varphi(y)\}$. Свойство $\varphi(y)$ может сообщать нечто обо всех множествах, в том числе и о вновь образуемом $\{y \mid \varphi(y)\}$. Так происходит ссылка на себя. Например, $\varphi(y)$ может содержать кванторы по переменным, которые, естественно, мыслятся как пробегающие все множества, в том числе и множество $\{y \mid \varphi(y)\}$. В определенном смысле множество $\{y \mid \varphi(y)\}$ нельзя считать вновь образованным: о нем уже идет речь в формулировке свойства $\varphi(y)$! Это явление называется *непредикативностью* теории множеств.

Полный отказ от непредикативных определений требует значительной перестройки существующей математики, и поэтому обычно используется компромиссный подход. В необходимых случаях используется непредикативная аксиома свертывания, но ее применение ограничивается, чтобы избежать возникновения парадоксов.

Рассмотрим теперь еще одну парадоксальную ситуацию. Деревенский парикмахер бреет тех и только тех в своей деревне, кто сам не бреется. Бреет ли он сам себя? Несложное рассуждение показывает, что он бреет сам себя тогда и только тогда, когда не бреет сам себя.

Как следует реагировать на такую ситуацию? Очень просто. Такого парикмахера просто не существует. Условие, которому должен подчиняться наш гипотетический парикмахер, внутренне противоречиво, его нельзя выполнить (хотя это сразу и незаметно). Конечно, не следует полагать, что тем самым снимаются все вопросы, которые вызывает вышеприведенный очень тонкий пример. Главный вопрос — какие же условия в таком случае внутренне противоречивы, а какие — нет? Можно ли уверенно выделить широкий класс заведомо непротиворечивых условий?

Аналогично естественно считать, что множество R не существует. Однако в таком случае необходимо подвергнуть пересмотру наши представления о структуре $\mathcal{M}$ теории множеств и изменить строение языка M^+. До сих пор мы полагали, что *всякий замкнутый терм* M^+ *определяет множество*, т. е. мы считали, что любое условие $\varphi(x)$ определяет объект $\{x \mid \varphi(x)\}$. Оказалось, однако, что такая точка зрения внутренне противоречива. Нужно выделить класс условий, которые заведомо определяют множества, и таких множеств должно быть достаточно для обслуживания обычных математических рассуждений. В то же время следует признать, что некоторые условия множеств не определяют.

Современная математическая логика еще очень далека от полного решения этой задачи. Имеется несколько практически удобных решений. Из них самым популярным, по-видимому, является подход, предложенный Цермело и усовершенствованный Френкелем. Основная его идея состоит в том, что мы отказываемся от «слишком обширных» множеств неопределенной мощности, таких, как например, универсальное множество.

§ 2. Язык теории множеств Цермело—Френкеля

1. Мы вновь исходим из гипотезы, что имеется математическая структура $\mathscr{M}_0$ — семейство множеств с отношением $a \in b$. Ее свойства определяются *семантическими соглашениями*, которые мы (несколько неточно) будем, называть аксиомами теории множеств Цермело—Френкеля.

Язык ZF^+ содержит один сорт переменных $x, y, z, \ldots$, которые рассматриваются как пробегающие множества.

Понятие *формулы* и *терма* ZF^+ определяется одновременной индукцией:

1) переменная есть терм;
2) если t, r — термы, то $(t \in r)$ есть формула;
3) если φ и ψ суть формулы, то

$$(\varphi \wedge \psi), \quad (\varphi \vee \psi), \quad (\varphi \supset \psi), \quad \neg\varphi$$

также суть формулы;

4) если x — переменная, а φ — формула, то $\forall x\varphi$, $\exists x\varphi$ суть формулы;
5) символы $\varnothing$ и ω суть термы;
6) если t, r — термы, то $\{t, r\}$ есть терм;
7) если t — терм, то Pt и $\cup t$ суть термы;
8) если φ — формула, t — терм, не содержащий свободно переменной x, то $\{x \in t \mid \varphi\}$ есть терм;
9) если φ — формула, x, y — различные переменные и t — терм, не содержащий свободно переменных x и y, то

$$\{y \mid x \in t,\ (x \mapsto y),\ \varphi\}$$

есть терм.

Определение формулы и терма закончено.

Идея языка ZF^+ состоит в том, что в него мы включаем лишь часть конструкций из M^+, избегая известных парадоксов. Теперь $\varnothing$, ω, $\cup$, P уже не определяются, а являются самостоятельными значками. Вместо неограниченной аксиомы свертывания мы имеем лишь ее частные случаи, в том числе определение выделением и определение подстановкой.

2. Мы считаем, что законами структуры $\mathscr{M}_0$ являются следующие формулы:

1) *Аксиома объемности*:

$$.x = y \wedge x \in z \supset y \in z.$$

Существенным для нас является то, что из этой аксиомы (с помощью остальных аксиом) выводятся свойства равенства:

$$.x = y \supset (\varphi(x) \equiv \varphi(y));$$
$$.x = y \supset (t(x) = t(y))$$

(ср. п. 3 § 1). Здесь $x \subseteq y$ и $x = y$ определяются, как и раньше (п. 2 § 1).

2) *Аксиома пустого множества*:

$$.\forall z(z \notin \varnothing);$$

в M^+ это свойство доказывается, а знак $\varnothing$ определяется особым образом. В языке ZF^+ знак $\varnothing$ является самостоятельным, и его свойства следует специально определить. Это замечание относится и к другим конструкциям ZF^+.

3) *Аксиома пары*:

$$.\forall z(z \in \{x, y\} \equiv (z = x \vee z = y)).$$

Свойства пары п. 4 и п. 5 § 1 доказываются и в ZF^+, так как все они выводятся только из п. 4 § 1, 1), а это свойство пары выполняется и в ZF^+. Далее, определим теперь

$$\{x\} \leftrightharpoons \{x, x\},$$

тогда основное свойство п. 5 § 1, 1) $\{x\}$ также выполняется в ZF^+.

4) *Аксиома суммы*:

$$.\forall z(z \in \cup x \equiv (\exists u \in x)(z \in u)).$$

Основное свойство объединения п. 8 § 1, 1) тогда выполняется и в ZF^+.

5) *Аксиома множества подмножеств*:

$$.\forall z(z \in \boldsymbol{P}x \equiv (z \subseteq x))$$

(ср. п. 10 § 1).

6) *Аксиомы стандартного бесконечного множества*:

$$.\varnothing \in \omega;$$
$$.(\forall z \in \omega)(Sz \in \omega);$$
$$.\forall x(\mathrm{Prog}(x) \supset (\omega \subseteq x))$$

(ср. п. 11 § 1).

7) *Аксиома выделения*:

$$.\forall z(z \in \{x \in t \mid \varphi(x)\} \equiv (z \in t \wedge \varphi(z)))$$

(ср. п. 12 § 1).

8) *Аксиома подстановки*:

$$.\forall z\big(z \in \{y \mid x \in u,\ (x \mapsto y),\ \varphi(x, y)\} \equiv$$
$$\equiv (\exists x \in u)(\varphi(x, z) \wedge \forall v(\varphi(x, v) \supset z = v))\big)$$

(ср. п. 12 § 1).

На этом формулировка семантических соглашений ZF^+ заканчивается. Заметьте, что в естественном смысле ZF^+ есть часть языка наивной теории множеств M^+.

В языке ZF^+ уже нет никакой возможности образовать универсальное множество $V = \{x \mid x = x\}$ или множество Рассела $R = \{x \mid x \notin x\}$, для этого просто нет подходящих языковых средств. Мы считаем, что эти множества отсутствуют в структуре $\mathcal{M}_0$.

3. Далее нам следует убедиться, что обычные множества, употребляемые в математике, выражаются в ZF^+. Мы начнем с рассмотрения тех конструкций, которые уже встречались в § 1.

Пересечение, объединение и дополнение двух множеств можно определить в ZF^+:

$$x \cup y \leftrightharpoons \cup \{x, y\};$$
$$x \cap y \leftrightharpoons \{z \in (x \cup y) \mid z \in x \wedge z \in y\};$$
$$x \setminus y \leftrightharpoons \{z \in x \mid z \notin y\}.$$

Упражнение. Убедитесь, что свойства п. 7 § 1 этих понятий выполняются и в новом определении.

Чуть сложнее обстоит дело с определением пересечения семейства множеств. Определить $\cap x$ так, чтобы выполнялось определяющее свойство п. 8 § 1

$$z \in \cap x \equiv (\forall u \in x)(z \in u),$$

не представляется возможным, так как тогда согласно лемме п. 9 § 1 было бы $\cap \varnothing = V$. Однако в ZF^+ можно определить очень похожее понятие:

$$\cap x \leftrightharpoons \{z \in \cup x \mid (\forall u \in x)(z \in u)\}.$$

Лемма. *Имеем*:

1) $x \neq \varnothing \supset \forall z(z \in \cap x \equiv (\forall u \in x)(z \in u))$;
2) $\cap \varnothing = \varnothing$.

▷ Если $x \neq \varnothing$, то существует $u_0 \in x$. Тогда из $(\forall u \in x)(z \in u)$ следует $z \in u_0$ и, значит, $z \in \cup x$, так что ограничение в аксиоме выделения становится фиктивным. Далее, $\cap \varnothing = \varnothing$, так как $\cup \varnothing = \varnothing$. ◁

Разумеется, в ZF^+ нам придется отказаться от общего дополнения, так как тогда было бы $\overline{\varnothing} = V$. Множества V такого, что $\forall z(z \in V)$, существовать не может, так как иначе мы выделением могли бы определить и множество Рассела

$$R = \{z \in V \mid z \notin z\}.$$

§ 3. Отношения и функция в языке теории множеств

1. *Упорядоченная пара* (по Куратовскому) определяется следующим образом:

$$\langle x, y\rangle \leftrightharpoons \{\{x\},\ \{x, y\}\}.$$

Основное свойство этого множества выражается следующей леммой:

Лемма. $\langle x, y\rangle = \langle u, v\rangle \equiv (x = u \wedge y = v)$.

▷ Импликация справа налево следует из свойств равенства. Допустим $\langle x, y\rangle = \langle u, v\rangle$ и докажем $x = u \wedge y = v$.

По допущению $\{\{x\},\ \{x, y\}\} = \{\{u\},\ \{u, v\}\}$. Согласно лемме п. 5 § 2, 2) тогда

$$\{x\} = \{u\} \wedge \{x, y\} = \{u, v\}$$

или

$$\{x\} = \{u, v\} \wedge \{x, y\} = \{u\}.$$

Соответственно разберем два случая.

a. $\{x\} = \{u, v\}$, $\{x, y\} = \{u\}$. Ввиду п. 5 § 2 тогда $x = y = u = v$, так что, очевидно, $x = u \wedge y = v$.

b. $\{x\} = \{u\}$, $\{x, y\} = \{u, v\}$. Ввиду п. 5 § 2 тогда $x = u$.

Далее, имеем два случая:

$$x = u \wedge y = v \quad \text{или} \quad x = v \wedge y = u.$$

В первом случае мы уже имеем искомое. Во втором же случае ввиду $x = u$ получаем $x = u = y = v$, т. е. вновь $x = u \wedge y = v$. ◁

Далее можно определить *упорядоченные тройки*, *четверки* и т. п.

$$\langle x\rangle \leftrightharpoons x;$$

$$\langle x_1, \ldots, x_n, x_{n+1}\rangle \leftrightharpoons \langle\langle x_1, \ldots, x_n\rangle, x_{n+1}\rangle.$$

Из леммы будет следовать и более общее утверждение

$$.\langle x_1, \ldots, x_n\rangle = \langle u_1, \ldots, u_n\rangle \equiv (x_1 = u_1 \wedge \ldots \wedge x_n = u_n).$$

Заметим, что упорядоченная n-ка при $n > 0$ в нашем определении есть одновременно и упорядоченная пара.

2. *Отношение* есть по определению множество, каждый элемент которого есть упорядоченная пара. На нашем языке «быть отношением» записывается как

$$\mathrm{Rel}(x) \leftrightharpoons (\forall z \in x)\ \exists uv(z = \langle u, v\rangle).$$

Мы говорим, что u и v *находятся в отношении* x, если $\langle u, v\rangle \in x$. Последнее записывается также в виде uxv.

Полем отношения x называется множество всех u таких, что u входит в x в качестве левого члена некоторой пары или в качестве правого члена некоторой пары.

Оказывается, что в нашем языке поле отношения может быть определено следующим образом:

$$\mathrm{Fld}(x) \leftrightharpoons \cup\cup x.$$

То, что это действительно подходящее определение, видно из следующей леммы:

Лемма.

1) $.\langle u, v\rangle \in x \supset u \in \mathrm{Fld}(x) \wedge v \in \mathrm{Fld}(x)$;

2) $.\mathrm{Rel}(x) \wedge u \in \mathrm{Fld}(x) \supset \exists v(\langle u, v\rangle \in x \vee \langle v, u\rangle \in x)$.

▷ 1) Имеем $\{u, v\} \in \langle u, v\rangle \in x$, что означает $\{u, v\} \in \cup x$. Далее, $u \in \{u, v\} \in \cup x$, что влечет $u \in \cup\cup x$, т. е. $u \in \mathrm{Fld}(x)$. Симметрично, $v \in \mathrm{Fld}(x)$.

2) Пусть $\mathrm{Rel}(x)$, $u \in \mathrm{Fld}(x)$. Таким образом, найдется v, $u \in v \in \cup x$. А значит, найдется z такое, что $u \in v \in z \in x$. Так как $\mathrm{Rel}(x)$, то найдутся v_1, v_2, $z = \langle v_1, v_2\rangle$. Ввиду $v \in \langle v_1, v_2\rangle$ имеем $v = \{v_1\}$ или $v = \{v_1, v_2\}$. Так как $u \in v$, то необходимо $u = v_1$ или $u = v_2$. ◁

Область определения отношения x есть множество всех левых членов пар из x.

$$\mathrm{dom}(x) \leftrightharpoons \{u \in \mathrm{Fld}(x) \mid \exists v(\langle u, v\rangle \in x)\}.$$

Это типичное определение в ZF^+ выделением.

Заметим, что ввиду леммы ограничение $u \in \mathrm{Fld}(x)$ в определении несущественно:

$$.\exists v(\langle u, v\rangle \in x) \supset u \in \mathrm{Fld}(x).$$

В обыденной математике дают более простое определение:

$$\mathrm{dom}(x) = \{u \mid \exists v(\langle u, v\rangle \in x)\}.$$

Но в нашем языке последняя конструкция просто невозможна, и нам приходиться предложить некоторое, хотя бы и несущественное, ограничение.

Такое *фиктивное ограничение* в аксиоме выделения — особенность ZF^+ — есть плата за устранение парадоксов.

Основные свойства области определения:

1) $.\langle u, v\rangle \in x \supset u \in \mathrm{dom}(x)$;

2) $.\mathrm{Rel}(x) \wedge u \in \mathrm{dom}(x) \supset \exists v(\langle u, v\rangle \in x)$.

▷ 2) Пусть $\mathrm{Rel}(x)$ и $u \in \mathrm{dom}(x)$. Тогда по аксиоме выделения непосредственно $\exists v(\langle u, v\rangle \in x)$. ◁

$$.\mathrm{Rel}(x) \supset \mathrm{dom}(x) \subseteq \mathrm{Fld}(x).$$

Область значений отношения x есть множество всех правых членов пар из x.

$$\mathrm{rng}(x) \leftrightharpoons \{v \in \mathrm{Fld}(x) \mid \exists u(\langle u, v\rangle \in x)\}.$$

1) $.\langle u, v\rangle \in x \supset v \in \mathrm{rng}(x)$;
2) $.\mathrm{Rel}(x) \wedge v \in \mathrm{rng}(x) \supset \exists\, u(\langle u, v\rangle \in x)$;
3) $.\mathrm{Rel}(x) \supset \mathrm{rng}(x) \cup \mathrm{dom}(x) = \mathrm{Fld}(x)$.

▷ Для доказательства используйте лемму. ◁

3. *Декартово произведение двух множеств* x и y есть некоторое отношение. А именно это есть множество всех пар $\langle u, v\rangle$ таких, что $u \in x$, $v \in y$.

В языке M^+ декартово произведение можно было бы определить следующим образом:

$$x \times y \rightleftharpoons \{z \mid \exists\, uv(z = \langle u, v\rangle \wedge u \in x \wedge v \in y)\}.$$

В языке ZF^+ нам придется подобрать некоторое (фиктивное) ограничивающее условие для определения выделением. Оказывается, что можно определить

$$x \times y \rightleftharpoons \{z \in PP(x \cup y) \mid \exists\, uv(z = \langle u, v\rangle \wedge u \in x \wedge v \in y)\}.$$

В самом деле, покажем, что из условия справа от черты следует $z \in PP(x \cup y)$. Итак, пусть для некоторых u, v имеем $z = \langle u, v\rangle$, $u \in x$, $v \in y$.

Тогда $u \in x \cup y$ и $v \in x \cup y$. Отсюда

$$\{u\} \subseteq x \cup y, \quad \{v\} \subseteq x \cup y, \quad \{u, v\} \subseteq x \cup y.$$

Это дает $\{u\} \in P(x \cup y)$, $\{u, v\} \in P(x \cup y)$. В свою очередь, отсюда

$$\{\{u\}\},\ \{u, v\}\} \subseteq P(x \cup y),$$

т. е. $\langle u, v\rangle \subseteq P(x \cup y)$ и, значит, $\langle u, v\rangle \in PP(x \cup y)$, т. е. $z \in PP(x \cup y)$.

Итак, в аксиоме выделения условие слева от черты выполняется, если выполняется условие справа от черты.

Основные свойства декартова произведения предлагается доказать в качестве упражнения:

1) $.u \in x \wedge v \in y \supset \langle u, v\rangle \in x \times y$;
2) $.z \in x \times y \supset \exists\, uv(z = \langle u, v\rangle \wedge u \in x \wedge v \in y)$.

Мы говорим, что отношение R *задано на множестве* z, если $R \subseteq z \times z$. Следующая лемма указывает, откуда берется множество z.

Лемма. $\mathrm{Rel}(R) \supset R \subseteq \mathrm{dom}(R) \times \mathrm{rng}(R)$.
Отсюда $R \subseteq z \times z$, *где* $z = \mathrm{dom}(R) \cup \mathrm{rng}(R)$.

▷ Пусть $\mathrm{Rel}(R)$ и $y \in R$. Тогда $y = \langle u, v\rangle$ и из определений $u \in \mathrm{dom}(R)$, $v \in \mathrm{rng}(R)$, что ввиду 1) дает $y = \langle u, v\rangle \in \mathrm{dom}(R) \times \mathrm{rng}(R)$. ◁

4. Для каждого отношения R может быть определено *обратное отношение*, состоящее из пар, расположенных в обратном порядке. Оно обозначается R^{-1}, $\breve{R}$ или $\mathrm{nv}(R)$. Точное определение таково:

$$\mathrm{Conv}(R) \leftrightharpoons \{z \in \mathrm{rng}(R) \times \mathrm{dom}(R) \mid \exists uv(z = \langle u, v\rangle \wedge \langle v, u\rangle \in R)\}.$$

Заметим, что ограничение здесь — фиктивное.

1) $.\mathrm{Rel}(\mathrm{Conv}(R))$;
2) $.\langle u, v\rangle \in \mathrm{Conv}(R) \equiv \langle v, u\rangle \in R$.

5. Если даны два отношения, то может быть определена их *композиция*

$$R \circ S \leftrightharpoons \{z \in \mathrm{dom}(S) \times \mathrm{rng}(R) \mid \exists uv\omega(z = \langle u, \omega\rangle \wedge \langle u, v\rangle \in S \wedge \langle v, \omega\rangle \in R)\}.$$

Основные свойства композиции:

1) $.\mathrm{Rel}(R \circ S)$;
2) $.\langle u, v\rangle \in S \wedge \langle v, \omega\rangle \in R \supset \langle u, \omega\rangle \in R \circ S$;
3) $.\langle u, \omega\rangle \in R \circ S \supset \exists v(\langle u, v\rangle \in S \wedge \langle v, \omega\rangle \in R)$.

▷ Докажем 3), доказательства остальных свойств предоставим читателю.

Если $\langle u, \omega\rangle \in R \circ S$, то по определению $\langle u, \omega\rangle \in \mathrm{dom}(S) \times \mathrm{rng}(R)$ и, кроме того, существуют u', v', ω', $\langle u, \omega\rangle = \langle u', \omega'\rangle$, $\langle u', v'\rangle \in S$, $\langle v', \omega'\rangle \in R$. Ввиду п. 1 тогда $u = u'$, $\omega = \omega'$. Если определить $v = v'$, то мы видим, что $\langle u, v\rangle \in S$, $\langle v, \omega\rangle \in R$. ◁

6. Введем понятия *рефлексивного, симметричного и транзитивного отношений*.

Напомним, что $xRy \leftrightharpoons \langle x, y\rangle \in R$.

$$\mathrm{Ref}(R) \leftrightharpoons (\forall x \in \mathrm{Fld}(R))(xRx);$$
$$\mathrm{Sym}(R) \leftrightharpoons \forall xy(xRy \supset yRx);$$
$$\mathrm{Trans}(R) \leftrightharpoons \forall xyz(xRy \wedge yRz \supset xRz).$$

Отношение называется *отношением эквивалентности*, если оно одновременно рефлексивно, симметрично и транзитивно. Точное определение

$$\mathrm{Eq}(R) \leftrightharpoons \mathrm{Rel}(R) \wedge \mathrm{Ref}(R) \wedge \mathrm{Sym}(R) \wedge \mathrm{Trans}(R).$$

Упражнение. Докажите:

$$.\mathrm{Rel}(R) \wedge \mathrm{Ref}(R) \supset \mathrm{Fld}(R) = \mathrm{dom}(R) = \mathrm{rng}(R).$$

7. *Ограничение отношения R множеством x* есть по определению множество таких пар $\langle u, v\rangle$ из R, что $u \in x$. Точное определение $R \restriction x \leftrightharpoons R \cap (x \times \mathrm{rng}(R))$.

$$.\langle u, v\rangle \in (R \restriction x) \equiv (\langle u, v\rangle \in R \wedge u \in x).$$

Образ множества x по отношению к R — это множество всех тех v, для которых найдется u, принадлежащее x и $\langle u, v\rangle \in R$.

$$R\text{“}x \leftrightharpoons R[x] \leftrightharpoons \{v \in \operatorname{rng}(R) \mid (\exists u \in x)(\langle u, v\rangle \in R)\}.$$

Упражнение. Докажите:

$$.R\text{“}x = \operatorname{rng}(R \restriction x).$$

Симметричное понятие — *прообраз множества x по отношению к R* — это множество всех тех u, для которых найдется v принадлежащее x, и такое, что $\langle u, v\rangle \in R$. Точное определение

$$R_{-1}x \leftrightharpoons \{u \in \operatorname{dom}(R) \mid (\exists v \in x)(\langle u, v\rangle \in R)\}.$$

Упражнение. Докажите:

$$.\operatorname{Rel}(R) \supset R_{-1} = (R^{-1})\text{“}x.$$

Подобным образом можно было бы развивать и теорию многоместных отношений. Например, трехместное отношение есть по определению множество, все элементы которого суть упорядоченные тройки.

8. *Функция* (от одной переменной) есть по определению отношение, которое удовлетворяет следующему условию: если $\langle u, v_1\rangle \in R$ и $\langle u, v_2\rangle \in R$, то $v_1 = v_2$, т. е. для каждого u из области определения R существует только одно v, находящееся с этим u в отношении R. Точное определение:

$$\operatorname{Fnc}(R) \leftrightharpoons \operatorname{Rel}(R) \wedge \forall uv_1v_2(uRv_1 \wedge uRv_2 \supset v_1 = v_2).$$

Второй конъюнктивный член здесь называют иногда *условием униформности* (по второй координате). Таким образом, функция есть отношение, униформное по второй координате.

Мы говорим, что функция f *отображает* множество X в множество Y, и пишем

$$f\colon X \to Y,$$

если область определения f есть X, а область значений f включена в Y:

$$f\colon X \to Y \leftrightharpoons \operatorname{Fnc}(f) \wedge \operatorname{dom}(f) = X \wedge \operatorname{rng}(f) \subseteq Y.$$

Мы говорим, что функция f *переводит x в y*, если $\langle x, y\rangle \in f$:

$$f\colon x \mapsto y \leftrightharpoons \operatorname{Fnc}(f) \wedge \langle x, y\rangle \in f.$$

Если $x \in \operatorname{dom}(f)$ и f — функция, то существует и только одно y такое, что $\langle x, y\rangle \in f$. Это y называется *значением функции f на x*. Можно дать и явное определение значения функции в нашем языке:

$$f\text{‘}x \leftrightharpoons f(x) \leftrightharpoons \cup \{y \in \operatorname{rng}(f) \mid \langle x, y\rangle \in f\}.$$

Основное свойство этого обозначения:

$$.\operatorname{Fnc}(f) \wedge x \in \operatorname{dom}(f) \supset ((z = f\text{‘}x) \equiv (\langle x, z\rangle \in f)).$$

▷ Пусть $\mathrm{Fnc}(f)$ и $x \in \mathrm{dom}(f)$. Так как $x \in \mathrm{dom}(f)$, то найдется u такое, что $\langle x, u\rangle \in f$. Пусть $Q = \{y \in \mathrm{rng}(f) \mid \langle x, y\rangle \in f\}$. По определению $y \in Q \equiv \langle x, y\rangle \in f$. Но по условию униформности $\langle x, y\rangle \in f \wedge \langle x, y\rangle \in f \supset y = u$. Таким образом, $y \in Q \equiv (y = u)$. Отсюда следует $Q = \{u\}$. А тогда $\cup Q = \cup \{u\} = u$. Но $\cup Q$ есть $f`x$, так что $f`x = u$. Если $z = f`x$, то $z = u$ и, значит, $\langle x, z\rangle \in f$. Обратно, если $\langle x, z\rangle \in f$, то ввиду $\langle x, u\rangle \in f$ и условия униформности $z = u$, т.е. $z = f`x$. ◁

Не следует путать два обозначения, имеющие совсем разный смысл:

$f(x) \leftrightharpoons f`x$ — значение функции f в x.

$f[\mathrm{x}] \leftrightharpoons f``x$ — образ множества x по отношению к функции f.

Аналогично, различный смысл имеют и формулы:

$f\colon X \to Y$ — функция f отображает множество X в множество Y.

$f\colon x \mapsto y$ — функция f переводит x в y.

Заметим, что всякая функция есть в то же время и отношение, так что все определения, предназначенные для изучения отношений, могут быть использованы и для функций. Таким образом, задаются область определения функций, область значений, ограничение функции множеством, композиция функций.

Лемма. *Композиция двух функций есть функция*:

$$.\mathrm{Fnc}(f) \wedge \mathrm{Fnc}(g) \supset \mathrm{Fnc}(f \circ g).$$

▷ Пусть $\mathrm{Fnc}(f)$, $\mathrm{Fnc}(g)$, проверим условие униформности для $f \circ g$. Пусть $\langle u, v_1\rangle \in f \circ g$, $\langle u, v_2\rangle \in f \circ g$, покажем $v_1 = v_2$. По определению композиции найдутся ω_1 и ω_2 такие, что

$$\langle u, \omega_1\rangle \in g, \quad \langle \omega_1, v_1\rangle \in f$$

и

$$\langle u, \omega_2\rangle \in g, \quad \langle \omega_2, v_2\rangle \in f.$$

Из условия униформности для g имеем $\omega_1 = \omega_2$. Но тогда $v_1 = v_2$ из условия униформности для f. ◁

Лемма. *Значение композиции равно последовательному вычислению значений составляющих функций*:

$$.\mathrm{Fnc}(f) \wedge \mathrm{Fnc}(g) \wedge x \in \mathrm{dom}(g) \wedge (g`x) \in \mathrm{dom}(f) \supset (f \circ g)`x = f`(g`x).$$

Обратите внимание, что сначала вычисляется значение функции g (правой в композиции).

▷ Пусть $v = (f \circ g)`x$. Тогда $\langle x, v\rangle \in (f \circ g)$ и значит, найдется $\omega$, $\langle x, \omega\rangle \in g$, $\langle \omega, v\rangle \in f$ по определению композиции. Но тогда $\omega = g`x$ и $v = f`\omega$, т.е. $v = f`(g`x)$. ◁

Для данной функции f обратное отношение $f^{-1} = \mathrm{Conv}(f)$ может и не быть функцией. Функция f называется *взаимно однозначной функцией*, или *биекцией*, если обратное отношение также является функцией:

$$(1-1)(f) \leftrightharpoons \mathrm{Fnc}(f) \wedge \mathrm{Fnc}(\mathrm{Conv}(f)).$$

Множество *всех функций* из множества X в множество обозначим через $(X \to Y)$. Таким образом,

$$.f \in (X \to Y) \equiv f\colon X \to Y.$$

Точное определение выделением:

$$(X \to Y) \leftrightharpoons \{f \in P(X \times Y) \mid f\colon X \to Y\}.$$

Упражнение. Убедитесь, что ограничение $f \in P(X \times Y)$ фиктивно и следует из условия $f\colon X \to Y$.

Можно было бы естественно развивать и теорию функций нескольких переменных. Так, функция от двух переменных есть по определению трехместное отношение, униформное по последней координате.

9. Пусть $t(i)$ — терм языка ZF^+ с выделенной переменной i. Мы будем писать иногда t_i вместо $t(i)$, чтобы подчеркнуть особую роль переменной i. Пусть I — произвольный терм, не содержащий свободно переменную i.

Можно ввести обозначение

$$\{t_i \mid i \in I\}$$

таким образом, что

$$.u \in \{t_i \mid i \in I\} \equiv (\exists\, i \in I)(u = t_i).$$

Это обозначение мы читаем так: «семейство всех t_i для $i \in I$».

Аналогично для терма $t(i, j)$ с двумя выделенными переменными определяется семейство $\{t_{ij} \mid i \in I, j \in J\}$ так, что

$$.u \in \{t_{ij} \mid i \in I, j \in J\} \equiv (\exists\, i \in I)(\exists\, j \in J)(u = t_{ij}).$$

Подобным образом можно определить семейства множеств по термам с большим количеством выделенных переменных.

▷ Эти обозначения вводятся с помощью определения подстановкой. Пусть, например, $t(i, j)$ — терм, i, j — две различные переменные, а I, J — произвольные термы, не содержащие свободно переменных i и j. Определим

$$\{t_{ij} \mid i \in I,\ j \in J\} \leftrightharpoons \{y \mid x \in I \times J,\ (x \mapsto y),\ \exists\, ij(x = \langle i, j\rangle \wedge y = t_{ij})\}.$$

Тогда согласно п. 12 § 1 $u \in \{t_{ij} \mid i \in I, j \in J\} \Leftrightarrow$ существует $x \in I \times J$ такое, что в точности для одного u имеем

$$\exists\, ij(x = \langle i, j\rangle \wedge u = t_{ij}).$$

Но для всякого $x \in I \times J$ такое u всегда существует и единственно. В самом деле, по $x \in I \times J$ однозначно определяются i и j, $x = \langle i, j \rangle$, а тогда u однозначно определяется из равенства $u = t_{ij}$. Таким образом, $u \in \{t_{ij} \mid i \in I, j \in J\}$ тогда и только тогда, когда существуют $i \in I$, $j \in J$, $u = t_{ij}$. ◁

Эти обозначения позволяют компактно и наглядно выразить в языке ZF^+ многие популярные конструкции обыденной математики.

Например,

$$U \times V = \{\langle u, v \rangle \mid u \in U, v \in V\},$$

здесь u и v — выделенные переменные.

Заметьте, что выделенные переменные связаны в нашем обозначении.

Определим *объединение семейства множеств*

$$\bigcup_{i \in I} t_i \rightleftharpoons \bigcup \{t_i \mid i \in I\}.$$

Основное свойство:

$$.z \in \bigcup_{i \in I} t_i \equiv (\exists\, i \in I)(z \in t_i).$$

▷ $$z \in \bigcup_{i \in I} t_i \equiv z \in \bigcup \{t_i \mid i \in I\} \equiv (\exists\, u \in \{t_i \mid i \in I\})(z \in u) \equiv$$

$$\equiv \exists\, u(\exists\, i \in I)(u = t_i \wedge z = u) \equiv (\exists\, i \in I)(z \in t_i).$$ ◁

Определим *пересечение семейства множеств*

$$\bigcap_{i \in I} t_i \rightleftharpoons \bigcap \{t_i \mid i \in I\}.$$

1) $I \neq \varnothing \supset .z \in \bigcap\limits_{i \in I} t_i \equiv (\forall\, i \in I)(z \in t_i)$;

2) $\bigcap\limits_{i \in \varnothing} t_i = \varnothing$.

▷ См. п. 3 § 2. ◁

Декартово произведение семейства множеств определяется следующим образом:

$$. \quad \prod_{i \in I} t_i \rightleftharpoons \{f \in (I \to \bigcup_{i \in I} t_i) \mid (\forall\, i \in I)((f\text{`}i) \in t_i)\}.$$

10. В обычной математике под функцией иногда понимают аналитическое выражение, зависящее от переменной. Например, говорят о «функции» $x^2 + x + 1$. В точном языке такого рода выражениям соответствуют **не функции, а термы**. Терм описывает не функцию, а ее значения.

Если по терму $t(x)$ мы желаем образовать функцию с областью определения z, то она (функция) будет определяться уже другим термом

$$f = \{\langle x, t(x)\rangle \mid x \in z\}.$$

Для всех $x \in z$ будет

$$.f\colon\ x \mapsto t(x).$$

§ 4. Натуральные числа в теории множеств. Запись математических утверждений в языке теории множеств

1. Рассмотрим последовательность множеств:

$$\varnothing, \quad \{\varnothing\}, \quad \{\varnothing, \{\varnothing\}\}, \quad \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}, \quad \ldots .$$

Эта последовательность получается, если начиная с пустого множества последовательно применять операцию $Sx = x \cup \{x\}$:

$$\{\varnothing\} = S(\varnothing), \quad \{\varnothing, \{\varnothing\}\} = S(\{\varnothing\}) \quad \text{и т. д.}$$

Первый член нашей последовательности вовсе не содержит элементов, второй содержит один элемент, третий — два и т. д.

Обратите внимание на важную особенность нашей последовательности: каждый член в ней равен в точности множеству всех предыдущих членов последовательности. Например, члену $\{\varnothing, \{\varnothing\}\}$ предшествуют в точности члены $\varnothing$ и $\{\varnothing\}$. Если упорядочить члены нашей последовательности, считая, что $a < b \Leftrightarrow a$ появилось в последовательности раньше, чем b, то для членов нашей последовательности

$$a < b \Leftrightarrow a \in b.$$

Таким образом, отношение принадлежности задает линейный порядок на нашей последовательности.

Фон Нейман предложил определить *натуральные числа* в теории множеств как члены вышеуказанной последовательности:

$$0 \rightleftharpoons \varnothing, \quad 1 \rightleftharpoons \{\varnothing\}, \quad 2 \rightleftharpoons \{\varnothing, \{\varnothing\}\}, \quad \ldots,$$

и вообще, если задано натуральное число n, то следующее число есть Sn.

Аксиомы бесконечности (п. 2 § 2) как раз и утверждают, что ω есть в точности множество всех натуральных чисел по фон Нейману. В самом деле, первые два утверждения

$$\varnothing \in \omega, \quad (\forall x \in \omega)(Sx \in \omega)$$

гласят, что ω во всяком случае содержит все натуральные числа, а третье утверждение

$$\forall x(\mathrm{Prog}(x) \supset (\omega \subseteq x))$$

гласит, что ω — «самое маленькое» из множеств, содержащих все натуральные числа, т. е., интуитивно говоря, состоит только из натуральных чисел.

Основные свойства натуральных чисел выражаются следующими тремя утверждениями:

1) $.(\forall x \in \omega)(Sx \neq 0)$;
2) $.(\forall xy \in \omega)(Sx = Sy \equiv x = y)$;
3) для всякой формулы $\varphi(x)$ выполняется следующее утверждение, называемое *принципом полной математической индукции*:

$$.\varphi(0) \wedge (\forall x \in \omega)(\varphi(x) \supset \varphi(Sx)) \supset (\forall x \in \omega)\varphi(x).$$

▷ 1) Очевидно, $x \in Sx = x \cup \{x\}$. Если было бы $Sx = 0$, то $x \in \varnothing$, что невозможно.

3) Допустим $\varphi(0)$ и

$$(\forall x \in \omega)(\varphi(x) \supset \varphi(Sx))$$

и докажем $(\forall x \in \omega)\varphi(x)$. С этой целью рассмотрим множество $u = \{x \in \omega \mid \varphi(x)\}$. Из допущений следует, что $\mathrm{Prog}(u)$. А тогда по аксиомам бесконечности имеем $\omega \subseteq u$, что и означает $(\forall x \in \omega)\varphi(x)$.

2) Для установления этого факта нам понадобится доказать два вспомогательных утверждения с помощью принципа полной математической индукции.

Первое утверждение:

$$(\forall x \in \omega)\,\forall yz(y \in z \wedge z \in x \supset y \in x).$$

Для $x = 0$ это утверждение:

$$\forall yz(y \in z \wedge z \in \varnothing \supset y \in \varnothing)$$

тривиально в силу ложности посылки $z \in \varnothing$. Рассмотрим произвольное число $x \in \omega$ и, допустив

$$\forall yz(y \in z \wedge z \in x \supset y \in x),$$

докажем

$$\forall yz(y \in z \wedge z \in Sx \supset y \in Sx).$$

Итак, пусть $y \in z$, $z \in Sx$. Из $z \in Sx$ следует $z \in x$ или $z = x$. В первом случае $y \in z$, $z \in x$, и, значит, $y \in x$ по индуктивному предположению. Отсюда $y \in Sx$.

Во втором случае $y \in Sx$ ввиду $z \in Sx$.

Первое утверждение доказано.

Второе утверждение:

$$\forall x(x \notin x).$$

Очевидно, $\varnothing \notin \varnothing$. Допустим для $x \in \omega$, что $x \notin x$, и докажем $Sx \notin Sx$. Предположим противное, и пусть $Sx \in Sx$. Тогда $Sx \in x$ или $Sx = x$. В первом случае ввиду $x \in Sx$ первого утверждения имеем

$x \in x$, что противоречит индуктивному предположению. Во втором случае ввиду $x \in Sx$ непосредственно заключаем $x \in x$, что вновь противоречит индуктивному предположению. Второе утверждение доказано.

Установим теперь 2). Пусть $Sx = Sy$, докажем $x = y$ (обратная импликация следует из общих законов равенства). Так как $x \in Sx$, то $x \in Sy$ и, значит, $x \in y$ или $x = y$. Во втором случае утверждение доказано, так что достаточно показать, что случай $x \in y$ невозможен. Из $y \in Sy$ заключаем $y \in Sx$, т. е. $y \in x$ или $y = x$. Но если $x \in y$ и $y \in x$, то по первому вспомогательному утверждению тогда $x \in x$, что противоречит второму утверждению. ◁

Оказывается, все, что требуется в математике от натуральных чисел, вытекает уже только из указанных трех утверждений, называемых *аксиомами Пеано*. Можно определять натуральные числа в теории множеств и по-иному, не обязательно по фон Нейману, важно лишь, чтобы выполнялись утверждения 1)–3).

Например, из аксиом Пеано средствами ZF^+ можно уже доказать существование функций сложения, умножения, возведения в степень для натуральных чисел и вывести все обычные свойства этих функций.

Более того, оказывается, что аксиомы Пеано фактически однозначно определяют натуральный ряд в ZF^+. Точнее, если имеется некоторое множество ω^*, элемент $0^* \in \omega^*$ и функция, определенная на ω^*, $S^*\colon \omega^* \to \omega^*$, причем так, что для 0^*, ω^*, S^*, выполняются аксиомы Пеано, то существует естественный изоморфизм между ω и ω^*, т. е. существует взаимно однозначная функция $f\colon \omega \to \omega^*$ на все множество ω^* такая, что $f`0 = 0^*$ и $f`(Sx) = S^*(f`x)$. Кроме того, такая функция f единственна. Как говорят, аксиомы Пеано *категоричны в теории множеств*, т. е. фактически однозначно определяют натуральный ряд, если позволить себе пользоваться средствами теории множеств.

Основные свойства натуральных чисел, действительных чисел изучаются в учебниках по числовым системам и по математическому анализу, и мы не будем здесь этого повторять, но все же наметим коротко определение множества R всех действительных чисел в стиле Дедекинда.

Сначала определим множество Rat_0 *канонических обозначений для рациональных чисел*. А именно,

$$x \in \mathrm{Rat}_0 \equiv \exists\, uvw(x = \langle u, v, w\rangle \wedge (u = 0 \vee u = 1) \wedge v \in \omega \wedge w \in \omega \wedge \omega \neq 0).$$

Если $x = \langle u, v, w\rangle$, то u назовем знаком x, v — числителем x и w — знаменателем x. Тройку вида $\langle 0, v, w\rangle$ будем обозначать через v/w или $+v/w$, а тройку вида $\langle 1, v, w\rangle$ будем обозначать через $-v/w$.

Определим далее *естественное отношение эквивалентности* между каноническими обозначениями для рациональных чисел таким образом, что

$$\langle u, v, w\rangle =_r \langle u, v_1, w_1\rangle \leftrightharpoons v \cdot w_1 = v_1 \cdot w,$$
$$\langle 0, v, w\rangle =_r \langle 1, v_1, w_1\rangle \leftrightharpoons v = v_1 = 0,$$

здесь умножение справа есть обычное умножение натуральных чисел.

Множество Rat всех *рациональных чисел* определяется как множество всех классов эквивалентности Rat_0 по этому отношению эквивалентности. Более формально,

$$\mathrm{Rat} \rightleftharpoons \{y \in P(\mathrm{Rat}_0) \mid (\exists z \in \mathrm{Rat}_0)\, \forall x (x \in y \equiv (x =_r z))\}.$$

Далее, на множестве Rat обычным образом вводятся все основные действия над рациональными числами. Например, умножение рациональных чисел описывается следующим образом, отражающим известное школьное правило «умножения дроби на дробь»:

$$x_1 \cdot_r x_2 \rightleftharpoons \{z \in \mathrm{Rat}_0 \mid \exists u u_1 v_1 w_1 u_2 v_2 w_2 ((\langle u_1, v_1, w_1\rangle \in x_1) \wedge$$
$$\wedge (\langle u_2, v_2, w_2\rangle \in x_2) \wedge (z =_r \langle u, v_1 \cdot v_2, w_1 \cdot w_2\rangle) \wedge$$
$$\wedge (u = 0 \vee u = 1) \wedge (u = 1 \equiv (u_1 \neq u_2)))\}.$$

Разумеется, следует проверить, что эта операция действительно по рациональным числам x_1 и x_2 выдает рациональное число и удовлетворяет обычным свойствам умножения рациональных чисел. При желании можно определить и константу, функцию от двух аргументов — *умножение рациональных чисел*:

$$\cdot_r \rightleftharpoons \{z \in \mathrm{Rat}^3 \mid (\exists x_1 x_2 x_3 \in \mathrm{Rat})(z = \langle x_1, x_2, x_3\rangle \wedge x_3 = x_1 \cdot_r x_2)\}.$$

Тогда будем иметь

$$.(\forall x_1 x_2 \in \mathrm{Rat})(\,\cdot_r\,\langle x_1, x_2\rangle = x_1 \cdot_r x_2).$$

В таком же стиле можно ввести операции сложения $x +_r y$, вычитания $x -_r y$, взятия модуля $|x|_r$ для рациональных чисел, а также отношение $x <_r y$ строгого неравенства между рациональными числами.

Сечением в области рациональных чисел называется, как известно, разбиение множества Rat рациональных чисел на два непустых подмножества X и Y таким образом, что X вместе с каждым числом содержит и все меньшие, а Y вместе с каждым числом содержит и все большие. Определение сечения в нашем языке:

$$\mathrm{Ct}(x) \rightleftharpoons (\exists X \subseteq \mathrm{Rat})(\exists Y \subseteq \mathrm{Rat})(x = \langle X, Y\rangle \wedge X \neq \varnothing \wedge$$
$$\wedge Y \neq \varnothing \wedge X \cup Y = \mathrm{Rat} \wedge X \cap Y = \varnothing \wedge$$
$$\wedge (\forall uv \in \mathrm{Rat})(u <_r v \supset (v \in X \supset u \in X) \wedge (u \in Y \supset v \in Y))).$$

Сечение $\langle X, Y\rangle$ назовем *правильным*, если в нижнем классе X этого сечения отсутствует наибольшее число. В нашем языке понятие правильного сечения можно записать в виде следующей формулы:

$$\mathrm{CorCt}(x) \rightleftharpoons \mathrm{Ct}(x) \wedge \forall XY (x = \langle X, Y\rangle \supset (\forall u \in X)(\exists v \in X)(u <_r v)).$$

Теперь, следуя знакомой схеме, мы отождествим множество R всех действительных чисел со множеством всех правильных сечений:

$$\mathrm{R} \rightleftharpoons \{x \in P(\mathrm{Rat}) \times P(\mathrm{Rat}) \mid \mathrm{CorCt}(x)\}.$$

Это типичное определение по схеме выделения, где слева от черты стоит фиктивное ограничение.

Далее следует определить на множестве R все обычные действия над действительными числами. Отношение строгого неравенства, например, можно ввести следующим образом:

$$\langle X_1, Y_1\rangle < \langle X_2, Y_2\rangle \leftrightharpoons Y_1 \cap X_2 \neq \varnothing.$$

2. Мы не будем заниматься далее развитием теории действительных чисел и примем, что в ZF^+ могут быть определены множество R всех действительных чисел и все обычные операции над действительными числами: сложение, умножение, взятие модуля действительных чисел и т. п.

Напомним определение ограниченных кванторов (см. п. 8 § 1):

$$(\forall\, x \in y)\varphi(x) \leftrightharpoons \forall\, x(x \in y \supset \varphi(x));$$
$$(\exists\, x \in y)\varphi(x) \leftrightharpoons \exists\, x(x \in y \wedge \varphi(x)).$$

Ценность этого определения помимо его компактности состоит еще и в том, что ограниченные кванторы во многом ведут себя аналогично обычным, особенно если $y \neq \varnothing$. Так, для ограниченных кванторов имеет место аналог законов де Моргана. Далее,

$$.y \neq \varnothing \supset ((\forall\, x \in y)\varphi(x) \supset (\exists\, x \in y)\varphi(x)).$$

Можно пойти еще немного далее в употреблении сокращений. А именно, фиксируем некоторое множество u, $u \neq \varnothing$. В языке ZF^+ это множество может изображаться, в частности, некоторым замкнутым термом. Фиксируем теперь некоторый набор F переменных: $a, b, c, \ldots$, которые условимся считать *пробегающими элементы множества* u. Более формально это означает, что:

1) во всяком доказательстве, рассматривая элемент a, изображаемый переменной из набора $\boldsymbol{F}$, мы автоматически считаем верным $.a \in u$;
2) во всех формулах кванторы
$$\forall\, a\varphi(a), \quad \exists\, a\varphi(a)$$
следует понимать как ограниченные
$$(\forall\, a \in u)\varphi(a), \quad (\exists\, a \in u)\varphi(a);$$
3) термы вида $\{a \mid \varphi(a)\}$ следует рассматривать как $\{a \in u \mid \varphi(a)\}$.

Коротко говоря, мы всюду опускаем ограничение $\in u$, если речь идет о переменных набора $\boldsymbol{F}$. При аккуратной полной записи это ограничение следует, конечно, восстанавливать. Указанием на то, что следует добавлять ограничение, служит то обстоятельство, что переменная берется из набора $\boldsymbol{F}$.

Такой способ употребления переменных называется *введением подчиненных переменных*. Мы говорим, что переменные из списка $\boldsymbol{F}$ *подчинены условию* $\in u$.

Например, мы согласимся употреблять буквы $m, n, k, \ldots$, быть может с индексами, для обозначения *натуральных чисел*, т. е. переменные набора $m, n, k, \ldots$ подчиним условию $\in \omega$.

В этих обозначениях принцип полной математической индукции запишется в виде

$$\varphi(0) \wedge \forall m(\varphi(m) \supset \varphi(Sm)) \supset \forall m\varphi(m).$$

Его более развернутая запись имеет вид

$$\varphi(0) \wedge (\forall m \in \omega)(\varphi(m) \supset \varphi(Sm)) \supset (\forall m \in \omega)\varphi(m).$$

Упражнение. Обдумайте следующие определения:

1) a есть последовательность действительных чисел:

$$(a\colon \omega \to R).$$

2) b есть подпоследовательность последовательности a:

$$(a\colon \omega \to R) \wedge (b\colon \omega \to R) \wedge \\ \wedge (\exists f \in (\omega \to \omega))\forall m((f`m < f`Sm) \wedge (b`m = a`(f`m))).$$

Согласимся, далее, употреблять буквы $\alpha, \beta, \gamma, \delta, \varepsilon, \ldots$, быть может с индексами, для обозначения действительных чисел, т. е. переменные этого набора подчиним условию $\in R$.

Отрезок $[\alpha, \beta]$ действительных чисел:

$$[\alpha, \beta] \leftrightharpoons \{\gamma \mid \alpha \leqslant \gamma \wedge \gamma \leqslant \beta\}.$$

Функция f непрерывна в точке α отрезка $[0, 1]$:

$$(f\colon [0, 1] \to R) \wedge \alpha \in [0, 1] \wedge (\forall \varepsilon > 0)(\exists \delta > 0) \\ (\forall \beta \in [0, 1])(|\alpha - \beta| < \delta \supset |f`\alpha - f`\beta| < \varepsilon).$$

Функция f непрерывна в каждой точке отрезка $[0, 1]$:

$$(f\colon [0, 1] \to R) \wedge (\forall \varepsilon > 0)(\forall \alpha \in [0, 1])(\exists \delta > 0) \\ (\forall \beta \in [0, 1])(|\alpha - \beta| < \delta \supset |f`\alpha - f`\beta| < \varepsilon).$$

Функция f равномерно непрерывна на отрезке $[0, 1]$:

$$(f\colon [0, 1] \to R) \wedge (\forall \varepsilon > 0)(\exists \delta > 0)(\forall \alpha \in [0, 1]) \\ (\forall \beta \in [0, 1])(|\alpha - \beta| < \delta \supset |f`\alpha - f`\beta| < \varepsilon).$$

Обратите внимание на различие в порядке кванторов по δ и по α в определении непрерывности и равномерной непрерывности. В этой перестановке кванторов — важное различие между непрерывностью и равномерной непрерывностью.

Знание логических законов позволяет теперь быстро преобразовать формулы к нужному нам виду. Сформулируем, например, утверждение, что функция f на отрезке $[0, 1]$ неравномерно непрерывна, причем так, чтобы отрицание не фигурировало в этом утверждении. С этой целью в определении равномерной непрерывности следует поставить отрицание перед вторым членом конъюнкции, а затем, применяя законы де Моргана и отрицание импликации, пронести отрицание внутрь. В результате получим:

$$(f\colon [0, 1] \to \boldsymbol{R}) \wedge (\exists \varepsilon > 0)(\forall \delta > 0)(\exists \alpha \in [0, 1])$$
$$(\exists \beta \in [0, 1])(|\alpha - \beta| < \delta \wedge |f`\alpha - f`\beta| \geqslant \varepsilon).$$

3. У читателя должно возникнуть правильное впечатление, что практически любое математическое утверждение может быть записано формулой ZF^+, а имя любого математического объекта исследования может быть записано в виде терма этого языка.

Приведем еще один пример. *Топологическим пространством* называется, как известно, непустое множество X, на котором определено семейство S его подмножеств, называемых открытыми множествами, причем:

1) $\varnothing$ и X суть открытые множества;
2) пересечение любых двух открытых множеств вновь открыто;
3) объединение любого семейства открытых множеств открыто.

На нашем языке «быть топологическим пространством» может быть записано формулой:

$$\mathrm{Top}(x) \leftrightharpoons \exists X\, S(x = \langle X, S\rangle \wedge X \neq \varnothing \wedge S \subseteq P(X) \wedge \varnothing \in S \wedge X \in S \wedge$$
$$\wedge (\forall yz \in S)(y \cap z \in S) \wedge (\forall u \subseteq S)(\cup u \in S)).$$

4. Язык ZF^+, как мы уже отмечали, не является языком первого порядка ввиду особой структуры своих термов. Рассмотрим *язык первого порядка* ZF. Этот язык содержит один сорт переменных $x, y, z, \ldots$ для множеств и единственный атомарный предикат $\in$. Язык ZF не содержит ни констант, ни функциональных символов.

ZF составляет часть языка ZF^+. Тем не менее, как мы увидим, всякая формула ZF^+ эквивалентна некоторой формуле ZF. В этом смысле термы не являются необходимой принадлежностью языка теории множеств и введены нами лишь для удобства записи математических утверждений. В математической логике чаще употребляется именно язык ZF. А именно, для всякой формулы φ языка ZF^+ мы определим формулу φ^0 языка ZF с теми же параметрами такую, что $\varphi \equiv \varphi^0$. Что касается термов языка ZF^+, то для всякой формулы ZF^+ вида $y = t$, где t — терм и y — переменная, не входящая свободно в t, мы определим ZF-формулу $(y = t)^*$ так, что $.(y = t) \equiv (y = t)^*$. Формулы φ^0 и $(y = t)^*$ определяются одновременной индукцией по определению формул и термов п. 1 § 2:

1) $(y = x)^* \leftrightharpoons (y = x)$;
2) $(t \in r)^0 \leftrightharpoons \exists y_1 y_2((y_1 = t^* \wedge (y_2 = r)^* \wedge (y_1 \in y_2))$;
3) $(\varphi \wedge \psi)^0 \leftrightharpoons \varphi^0 \wedge \psi^0$;
   $(\varphi \vee \psi)^0 \leftrightharpoons \varphi^0 \vee \psi^0$;
   $(\varphi \supset \psi)^0 \leftrightharpoons \varphi^0 \supset \psi^0$;
   $(\neg\varphi)^0 \leftrightharpoons \neg\varphi^0$;
4) $(\forall x\varphi)^0 \leftrightharpoons \forall x\varphi^0$;
   $(\exists x\varphi)^0 \leftrightharpoons \exists x\varphi^0$;
5) $(y = \varnothing)^* \leftrightharpoons \forall x(x \notin y)$;
   $\mathrm{Prog}^0(x) \leftrightharpoons \exists u(\forall v(v \notin u) \wedge u \in x) \wedge$
   $\wedge(\forall u \in x)(\exists v \in x)\,\forall z(z \in v \equiv (z \in u \vee z = u))$;
   $(y = \omega)^* \leftrightharpoons \mathrm{Prog}^0(y) \wedge \forall x(\mathrm{Prog}^0(x) \supset y \subseteq x)$;
6) $(y = \{t, r\})^* \leftrightharpoons \exists y_1 y_2((y_1 = t)^* \wedge (y_2 = r)^* \wedge \forall z(z \in y \equiv (z = y_1 \vee z = y_2)))$;
7) $(y = Pt)^* \leftrightharpoons \exists y_1((y_1 = t)^* \wedge \forall z(z \in y \equiv z \subseteq y_1))$;
   $(y = \cup t)^* \leftrightharpoons \exists y_1((y_1 = t)^* \wedge \forall z(z \in y \equiv (\exists v \in y_1)(z \in v)))$;
8) $(y = \{x \in t \mid \varphi(x)\})^* \leftrightharpoons \exists y_1((y_1 = t)^* \wedge \forall z(z \in y \equiv (z \in y_1 \wedge \varphi^0(z))))$;
9) $(y = \{v \mid u \in t,\ (u \mapsto v),\ \varphi(u, v)\})^* \leftrightharpoons \exists y_1((y_1 = t)^* \wedge$
   $\forall v(v \in y \equiv (\exists u \in y_1)(\varphi^0(u, v) \wedge \forall w(\varphi^0(u, w) \supset u = w))))$.

Используя эту длинную индуктивную процедуру, можно по всякой ZF^+ формуле φ получить эквивалентную ZF-формулу φ^0. Доказательство эквивалентности проводится непосредственно индукцией и мы не будем на нем останавливаться.

§ 5. О континуум-гипотезе и аксиоме выбора

1. Два множества назовем *равномощными*, если существует биекция, отображающая одно множество на другое:

$$x \simeq y \leftrightharpoons \exists f((1-1)(f) \wedge \mathrm{dom}(f) = x \wedge \mathrm{rng}(f) = y).$$

Множество называется *конечным*, если оно равномощно некоторому натуральному числу (напомним, что в теории множеств каждое натуральное число отождествляется с множеством всех чисел, ему предшествующих):

$$\mathrm{Fin}(x) \leftrightharpoons (\exists n \in \omega)(x \simeq n).$$

Множество называется *счетным*, если оно равномощно множеству всех натуральных чисел:

$$\mathrm{Count}(x) \leftrightharpoons x \simeq \omega.$$

2. Теорема (Кантор).

$$.\neg(x \simeq Px).$$

▷ Предположим противное, и пусть $x \simeq Px$. Тогда существует биекция f, $\mathrm{dom}\, f = x$, $\mathrm{rng} f = Px$. Рассмотрим множество v,

$$v = \{z \in x \mid z \notin f'z\}.$$

Очевидно, $v \subseteq x$, т. е. $v \in Px$. Кроме того, по определению

$$(\forall z \in x)(z \in v \equiv z \notin (f'z)).$$

Так как f — биекция, то существует $z_0 \in x$ такое, что $f'z_0 = v$.

Подставляя в вышеописанную эквивалентность вместо z конкретное z_0 и замечая, что $f'z_0 \notin v$, получим

$$z_0 \in v \equiv z_0 \notin v,$$

что невозможно по законам логики.

Обратите внимание на аналогию между этим рассуждением и рассуждением в парадоксе Рассела. ◁

Следствие. *Множество всех подмножеств натуральных чисел несчетно*:

$$.\neg\mathrm{Count}(P\omega).$$

3. Знаменитую континуум-гипотезу Кантора можно сформулировать следующим образом: всякое семейство подмножеств натурального ряда либо конечно, либо счетно, либо равномощно множеству всех подмножеств натурального ряда. Точная формулировка:

$$(\forall y \subseteq P\omega)(\mathrm{Fin}(y) \vee \mathrm{Count}(y) \vee y \simeq P\omega).$$

Суть этого утверждения состоит в том, что не существует бесконечных множеств, имеющих мощность, строго промежуточную между мощностями множеств ω и $P\omega$.

Как показали Гёдель и Коэн, континуум-гипотеза не зависит от остальных аксиом ZF, т. е. средствами логики ее нельзя ни доказать, ни опровергнуть с помощью остальных аксиом, даже привлекая аксиому выбора.

4. *Аксиома выбора* утверждает, что для всякого семейства множеств x существует функция f такая, что если $z \in x$ и $z \notin \varnothing$, то f выдает элемент z в качестве значения на z. Функцию f можно назвать выбирающей функцией, она «выбирает» по элементу $(f'z) \in z$ из каждого множества z, $z \in x$, $z \notin \varnothing$.

Точная формулировка аксиомы выбора такова:

$$\forall x\, \exists f(\mathrm{Fnc}(f) \wedge \mathrm{dom}(f) = x \wedge (\forall z \in x)(z \notin \varnothing \supset (f'z) \in z)).$$

Истинно ли это утверждение?

Особенность этого утверждения такова, что функция f никак не определяется по множеству x — утверждается лишь ее существование. Теоремы, полученные с использованием аксиомы выбора, часто имеют ту же особенность: доказывается существование множеств, обладающих теми или иными свойствами, и в то же время не указывается никакого индивидуального примера такого множества, никакого способа его

определения. Типичный пример — доказательство существования неизмеримых множеств. На этом основании многие математики подвергли критике неограниченное использование аксиомы выбора.

Тем не менее в практических математических рассуждениях аксиома выбора довольно широко используется. Как показали Гёдель и Коэн, аксиома выбора также не зависит от аксиом ZF.

В следующем параграфе мы еще уточним общую постановку задачи о независимости утверждений от теории.

5. Мы говорим, что множество x имеет мощность меньшую или равную мощности множества y, если x можно взаимооднозначно отобразить на подмножество y. Точнее:

$$x \widetilde{\subset} y \leftrightharpoons \exists f((1-1)(f) \wedge \mathrm{dom}(f) = x \wedge \mathrm{rng}(f) \subseteq y).$$

Теорема (Кантор—Шрёдер—Бернштейн). *Если* $x \widetilde{\subset} y$ *и* $y \widetilde{\subset} x$, *то* $x \simeq y$.

▷ Достаточно показать, что если $a_1 \subseteq b \subseteq a$ и $a_1 \simeq a$, то $b \simeq a$. Пусть $(1-1)(f)$, $\mathrm{dom}(f) = a$, $\mathrm{rng}(f) = a_1$. Положим

$$a_0 = a, \quad a_1 = f``a_0, \quad a_2 = f``a_1, \quad \ldots,$$
$$b_0 = b, \quad b_1 = f``b_0, \quad b_2 = f``b_1, \quad \ldots.$$

Определим $g(x) = f(x)$, если $x \in a_n \setminus b_n$ для некоторого n. В противном случае $g(x) = x$. Тогда $(1-1)(g)$, $\mathrm{dom}(g) = a$, $\mathrm{rng}(g) = b$. ◁

Упражнение. Докажите:

$$.x \widetilde{\subset} y \wedge y \widetilde{\subset} z \supset x \widetilde{\subset} z.$$

6. Замечание. В практической математике помимо множеств употребляют иногда еще и *классы*.

Рассмотрим произвольную формулу $\varphi(x)$ языка ZF^+, в которой выделена переменная x. Удобно бывает считать, что такая формула всегда определяет некоторый объект исследования $\{x \mid \varphi(x)\}$. Этот объект называется классом всех множеств x, удовлетворяющих условию $\varphi(x)$.

Для некоторых формул $\varphi(x)$ специального вида класс $\{x \mid \varphi(x)\}$ оказывается множеством, в общем же случае понятие класса оказывается шире, чем понятие множества. Так, $\{x \mid x \notin x\}$ есть класс, не являющийся множеством, *собственный класс*. Интуитивно говоря, собственные классы — это «очень большие» совокупности неопределенной мощности. Элементы класса всегда суть множества (а не собственные классы). По аналогии с множествами над классами также могут быть определены некоторые теоретико-множественные операции. Например, если даны классы

$$X = \{x \mid \varphi(x)\}, \quad Y = \{y \mid \psi(y)\},$$

то можно определить класс

$$X \cup Y = \{x \mid \varphi(x) \vee \psi(x)\}.$$

Можно образовать класс V всех множеств, это будет собственный класс, не множество, *универсум* теории множеств.

Семейство множеств образует столь мощную структуру, что в практической математике нет реальной необходимости использовать собственные классы. Упоминания о классах обычно можно избежать, рассматривая вместо классов условия, их определяющие. Тем не менее исследуются языки и теории, содержащие классы, такова, например, известная теория Гёделя—Бернайса—Неймана.

§ 6. Аксиоматическая теория множеств Цермело—Френкеля

1. В § 1 мы ввели логико-математический язык наивной теории множеств и начали систематически развивать теорию множеств в виде серии утверждений в этом языке. Доказательства утверждений при этом являлись содержательными, «наивными». Мы исходили из представления о некоей структуре $\mathcal{M}$, объекты которой называются множествами. В этой структуре выполняются простые и естественные законы, относящиеся к множествам. Утверждения мы доказывали, так сказать, путем непосредственного изучения этой воображаемой структуры, а точнее, условий-аксиом, на нее налагаемых. Такой подход совершенно естествен для математика-неспециалиста по математической логике.

Однако более внимательный анализ показал, что предложенные аксиомы ведут к противоречиям-парадоксам. Пришлось признать, что структуры, удовлетворяющей предложенным законам наивной теории множеств, по-видимому, не существует. Выход из положения мы нашли в том, чтобы рассмотреть более ограничительную структуру $\mathcal{M}_0$, удовлетворяющую уже некоторым более стеснительным и гораздо менее естественным условиям, выражаемым в некотором более сложном языке ZF^+. Доказательства утверждений при этом оставались по-прежнему наивными.

Возникает вопрос, в какой мере законно рассмотрение структуры $\mathcal{M}_0$, не придут ли наши рассуждения вновь к парадоксам, не придется ли признать, что и структуры $\mathcal{M}_0$ не существует? А если даже рассмотрение $\mathcal{M}_0$ законно, то верна ли в $\mathcal{M}_0$, например, аксиома выбора? В современной теоретико-множественной математике накоплено большое количество проблем, которые упорно не поддаются решению обычными теоретико-множественными средствами, т. е. их не удается ни доказать, ни опровергнуть. Происходит ли это просто в силу трудности проблемы и недостаточности приложенных усилий, или же рассматриваемую проблему принципиально нельзя ни доказать, ни опровергнуть?

Решение такого рода проблем упирается в трудность изучения *семантики* рассматриваемых теорий, т. е. в трудность изучения способа понимания формул теории. Семантика богатых математических теорий, таких, как математический анализ, теория множеств и др., по необходимости является недостаточно ясной, носит отчасти философский характер. Вместо описания конкретной модели теории в таких случаях часто приходится ограничиваться лишь формулировкой *аксиом — семантических соглашений*, которым должна удовлетворять наша теория. Для изучения богатых математических теорий со сложной семантикой

с успехом может быть применен *метод формализации Гильберта*. Метод состоит в том, что на основании семантических соглашений содержательной теории $\mathscr{T}$ строится формальная аксиоматическая теория T. При этом мы стремимся, чтобы аксиомы и правила вывода T были согласованы с семантическими требованиями $\mathscr{T}$. Тогда формулы, выводимые по формальным правилам теории T, оказываются содержательно истинными с точки зрения теории $\mathscr{T}$ и отражают, таким образом, по крайней мере некоторый фрагмент содержательной теории $\mathscr{T}$. Желательно при этом, конечно, чтобы этот фрагмент был достаточно обширным и охватывал все интересующие нас черты теории $\mathscr{T}$. Формальную теорию T можно затем подвергнуть точному математическому исследованию и таким образом судить о семантике исходной неформальной теории.

Ключевым обстоятельством является здесь то, что для понимания отношения формальной выводимости $T \vdash A$ *нет необходимости* вникать в, может быть, очень сложную семантику теории $\mathscr{T}$: для установления $T \vdash A$ достаточно построить некоторое дерево вывода, т. е. описать простой синтаксический объект, составленный из строчек символов, расположенных по строго определенным правилам. Отношение $T \vdash A$ можно описать, как правило, уже в весьма элементарной теории, например в *формальной арифметике* Ar, теории, имеющей дело лишь с натуральными числами.

Формализация теорий позволяет уточнить наши семантические проблемы в виде некоторых уже синтаксических утверждений о формальных теориях.

Теория T в языке Ω называется *непротиворечивой*, если не существует предложения (т. е. формулы без параметров в языке Ω) такого, что $T \vdash A$ и $T \vdash \neg A$.

Упражнение. Покажите, что теория T непротиворечива тогда и только тогда, когда существует формула языка Ω, не выводимая в T.

Теория T называется *полной*, если для всякого предложения A в языке Ω имеем $T \vdash A$ или $T \vdash \neg A$.

Будем говорить, что предложение A *совместно с теорией* T, если из непротиворечивости теории T следует и непротиворечивость теории $T + A$, полученной добавлением к теории T формулы A в качестве новой нелогической аксиомы.

Упражнение. Докажите, что A совместно с T тогда и только тогда, когда из непротиворечивости теории T следует, что неверно $T \vdash \neg A$.

Предложение называется *независимыми от теории* T, если оба предложения A и $\neg A$ совместны с T.

Упражнение. Докажите, что предложение A независимо от теории T тогда и только тогда, когда из непротиворечивости теории T следует, что в T не выводимо ни предложение A, ни предложение $\neg A$.

2. Сформулируем теперь формальную аксиоматическую теорию Цермело—Френкеля. Это теория в языке первого порядка ZF, т. е. в языке без сложных термов. Саму аксиоматическую теорию мы также будем обозначать через ZF.

Опишем нелогические аксиомы ZF. Они формулируются параллельно семантическим соглашениям § 2, п. 2. Если в формулировке аксиомы ниже присутствуют параметры, то, как обычно, следует считать, что аксиомой является замыкание формулы кванторами общности по всем параметрам. Нелогическая аксиома теории есть всегда предложение, замкнутая формула этой теории.

1) Аксиома объемности (экстенсиональности):

$$x = y \wedge x \in z \supset y \in z.$$

2) Аксиома пустого множества:

$$\exists u \forall z (z \notin u).$$

3) Аксиома пары:

$$\exists u \forall z (z \in u \equiv (z = x \vee z = y)).$$

4) Аксиома суммы:

$$\exists u \forall z (z \in u \equiv (\exists v \in x)(z \in v)).$$

5) Аксиома множества подмножеств (аксиома степени):

$$\exists u \forall z (z \in u \equiv (z \subseteq x)).$$

6) Аксиома бесконечности:

$$\exists u (\forall z (\forall x (x \notin z) \supset z \in u) \wedge (\forall z \in u) \\ (\forall v (\forall x (x \in v \equiv (x \in z \vee x = z)) \supset v \in u))).$$

7) Аксиома выделения:

$$\exists u \forall z (z \in u \equiv (z \in x \wedge \varphi(z))),$$

здесь $\varphi(z)$ — произвольная формула языка ZF, не содержащая свободно переменной u.

8) Аксиома подстановки (аксиома замены):

$$\exists u \forall z (z \in u \equiv (\exists x \in v)(\varphi(x, z) \wedge \forall w (\varphi(x, w) \supset z = w))),$$

здесь формула $\varphi(x, z)$ не содержит свободно переменных u и v.

9) Аксиома фундирования (аксиома регулярности):

$$\exists z (z \in x) \supset (\exists z \in x) \neg \exists u (u \in z \wedge u \in x).$$

Формулировка теории ZF закончена.

Аксиомы 2)–8) выражают существование тех множеств, которые непосредственно изображаются термами языка ZF^+. Более точно, аксиома 6) говорит, что существует некоторое прогрессивное множество. Существование ω может быть уже затем доказано с помощью аксиомы выделения.

Нелогические аксиомы ZF выбраны таким образом, чтобы в полученной теории можно было вывести все формулы, содержательную истинность которых мы установили в предыдущих параграфах. Точнее, выводить следует, конечно, не сами формулы ZF^+, а их переводы

в язык ZF согласно § 4, п. 4: если в предыдущих параграфах для некоторой формулы φ языка ZF^+ мы утверждали $.\varphi$, то теперь мы можем установить $\mathrm{ZF} \vdash \varphi^0$. Проведение всех таких выводов является длинным, но вполне тривиальным упражнением в применении правил техники естественного вывода исчисления предикатов. Мы не будем на этом останавливаться, но надеемся, что читатель приобрел самостоятельно некоторый опыт в формальных выводах.

Аксиома фундирования утверждает, что в некотором смысле все множества построены исходя из пустого множества. Она не используется при выводе математических утверждений, не использовали ее и мы, но она упрощает строение универсума множеств и обычно включается в состав нелогических аксиом ZF.

Следствием аксиомы фундирования является отсутствие «самопринадлежащих» множеств, а именно

не существует множеств таких, что

$$x \in x, \quad x \in y \wedge y \in x, \quad x \in y \wedge y \in z \wedge z \in x.$$

▷ Допустим, например, что существуют множества x и y такие, что $x \in y$ и $y \in x$. Рассмотрим множество $Q = \{x, y\}$. Q не пусто и в то же время не существует элемента Q, не пересекающегося с Q, что противоречит аксиоме фундирования. ◁

Подобным образом можно установить с помощью аксиомы фундирования, что не существует последовательности множеств, «убывающих по принадлежности», т. е. функции f, $\operatorname{dom} f = \omega$, такой, что $f(n+1) \in f(n)$ для всякого $n \in \omega$.

Следствием аксиомы фундирования является также следующий принцип *индукции по принадлежности*:

$$\forall x((\forall y \in x)\varphi(y) \supset \varphi(x)) \supset \forall x \varphi(x).$$

▷ Напомним коротко доказательство этой схемы. Допустим

$$\forall x((\forall y \in x)\varphi(y) \supset \varphi(x))$$

и предположим противное, т. е. что для некоторого x $\neg\varphi(x)$. Рассмотрим функцию f, $\operatorname{dom} f = \omega$, такую, что $f(0) = \{x\}$ и $f(n+1) = \cup f(n)$. Пусть $z = \bigcup_{n \in \omega} f(n)$.

Если $u \in z$, то $u \in f(n)$ для некоторого n, и тогда $u \subseteq f(n+1)$ и, значит, $u \subseteq z$. Таким образом, $(\forall u \in z)(u \subseteq z)$ (это свойство называется *транзитивностью* множества z). Кроме того, очевидно, $x \in z$, так как $x \in f(0)$. Пусть $z' = \{u \in z \mid \neg\varphi(u)\}$. Множество z' не пусто, так как $x \in z'$. По аксиоме фундирования существует $x' \in z'$ такое, что $x' \cap z' = \varnothing$. Если $y \in x'$, то $y \notin z'$, т. е. по определению z' имеем $y \notin z \vee \varphi(y)$. Но первый член этой дизъюнкции не имеет места, так как $y \in x' \wedge x' \in z$, а множество z транзитивно. Таким образом, $\varphi(y)$. Мы установили $(\forall y \in x')\varphi(y)$. По допущению отсюда $\varphi(x')$. Но, с другой стороны, $x' \in z'$, что влечет $\neg\varphi(x')$, и мы приходим к противоречию. ◁

Часто к теории ZF добавляют еще и аксиому выбора. Точнее, если через AC обозначить точную формулировку аксиомы выбора, приведен-

ную в § 5, п. 4, то к ZF в качестве новой нелогической аксиомы следует присоединить формулу AC^0. Полученную теорию обозначают через ZFC.

3. Теория ZFC исключительно богата по своим выразительным возможностям. Практически любая доказанная математическая теорема может быть записана на языке ZF и выведена в теории ZFC. В то же время известные выводы парадоксов теории множеств не проходят в ZFC.

В естественном смысле теория ZF содержит все формальные аксиоматические теории, рассмотренные нами в [1]. Уточним этот факт, например, по отношению к *формальной арифметике* Ar. Напомним, что язык Ar содержит один сорт переменных для натуральных чисел, константу 0, функциональные символы $x+y$, $x\cdot y$, Sx для соответствующих арифметических операций. В качестве атомарных формул используется лишь равенство термов $t = r$.

Изобразим теперь элементы языка Ar в языке ZF^+, а затем с помощью стандартного перевода перейдем в язык ZF. Константу 0 языка Ar можно изобразить в виде замкнутого терма $\varnothing$ языка ZF^+. Переменные для натуральных чисел языка Ar изображаются в виде переменных, подчиненных условию $x \in \omega$. Функциональные символы языка Ar также выражаются соответствующими термами ZF^+, например, терму Sx языка Ar соответствует терм $x \cup \{x\}$ языка ZF^+.

Таким образом, всякой замкнутой формуле A языка Ar соответствует некоторая замкнутая формула A' языка ZF^+, полученная путем замены элементов языка Ar на соответствующие элементы теоретико-множественного языка. Наконец, полученную формулу A' можно перевести в язык ZF с помощью перевода, указанного в § 4, п. 4. Далее, нетрудно проверить, что *если* A *— замкнутая формула* Ar *и* $\mathrm{Ar} \vdash A$, *то* $\mathrm{ZF} \vdash A'^0$. Это доказывается с помощью громоздкой, но вполне тривиальной индукции по построению выводов в теории Ar.

Полученный перевод и является естественной *интерпретацией* теории Ar в теории ZF. Это уточнение интуитивно ясной идеи, что теория множеств содержит арифметику. Подобным образом можно построить в теории ZF интерпретации и других рассматривавшихся нами в [1] теорий. Теория ZF содержит в этом смысле все остальные изученные нами теории. Заметим, что понятие интерпретации является чисто синтаксическим: описывается формальное преобразование формул одного языка в формулы другого и доказывается, что это преобразование сохраняет выводимость. Нет никакой надобности вникать в семантику формул языка Ar или языка ZF.

Это дает возможность чисто синтаксически доказывать результаты об *относительной непротиворечивости* теорий. Так, если непротиворечива теория ZF, то непротиворечива и теория Ar. В самом деле, если Ar противоречива, то найдется предложение A такое, что $\mathrm{Ar} \vdash A \wedge \neg A$. Но тогда $\mathrm{ZF} \vdash A'^0 \wedge \neg A'^0$, так что и теория ZF также оказывается противоречивой. Подобным образом из непротиворечивости ZF следует непротиворечивость и других рассматривавшихся нами теорий. С точки

зрения оснований математики важно, что такое сведение по непротиворечивости остальных теорий к ZF происходит без обращения к семантике теорий и само может быть формулировано в очень скромной теории, например, в Ar.

4. Теперь мы можем дать уточненную формулировку независимости аксиомы выбора и континуум-гипотезы от теории множеств.

Теорема. *Аксиома выбора* (*т. е. формула* AC^0) *не зависит от теории* ZF.

Теорема. *Континуум-гипотеза не зависит от теории* ZFC.

Эти замечательные результаты были получены К. Гёделем и П. Коэном. А именно в 1939 году Гёдель показал совместимость аксиомы выбора и континуум-гипотезы с теорией ZF, построив замечательную интерпретацию ZFC с континуум-гипотезой в теории ZF, а в 1963 году Коэн показал совместимость отрицания аксиомы выбора с ZF и совместимость отрицания континуум-гипотезы с ZFC, также указав некоторые конкретные интерпретации. В настоящее время установлена независимость от ZF и от ZFC многих интересных теоретико-множественных утверждений. Доказательства этих результатов можно найти в книгах [5, 12, 13].

Обсудим в связи с вышеупомянутыми теоремами еще раз «наивный» вопрос, можно ли, например, считать континуум-гипотезу H истинным утверждением и в каком, собственно, смысле? Из вышеупомянутых результатов следует, что *если теория* ZF *непротиворечива*, то в ZFC нельзя вывести ни формулу H, ни формулу $\neg H$. Так как теория ZFC содержит все традиционно употребляемые средства доказательства математических утверждений, то отсюда следует, что H нельзя ни доказать, ни опровергнуть *традиционными математическими средствами*. Набор ZFC традиционных математических средств доказательства оказывается существенно неполным.

Можно ли предложить более мощные теории, в рамках которых вопрос относительно H решался бы уже определенным образом? Ответ тривиален. Конечно, можно. Из вышеуказанных результатов следует, что если ZF непротиворечива, то непротиворечива и теория $\mathrm{ZFC} + H$, полученная путем добавления к ZFC утверждения H в качестве новой нелогической аксиомы. Непротиворечива также и теория $\mathrm{ZFC} + \neg H$. Проблема состоит, таким образом, в том, какую из этих двух теорий предпочесть и на каких основаниях. В настоящее время не видно достаточных оснований для выбора одной из этих теорий в качестве «действительно правильной», и практические математики стараются в своих рассуждениях не использовать ни H, ни $\neg H$. Впрочем, некоторые авторитеты, например П. Коэн [12, гл. IV, § 13], считают, что более естественно рассматривать континуум-гипотезу как ложное утверждение.

Можно подойти к проблеме и с иной точки зрения. В § 2–5 мы рассматривали некую воображаемую структуру $\mathcal{M}_0$ объектов, удовлетво-

ряющих аксиомам ZF. Так вот, истинно утверждение H в $\mathcal{M}_0$ или нет? Заметим, что все, что нам требовалось от $\mathcal{M}_0$ — это чтобы в ней выполнялись аксиомы ZF. Ниоткуда не следует, что все такие структуры изоморфны, вполне возможно, что в одной модели ZFC будет истинно H, а в другой — будет истинно утверждение $\neg H$. Именно так дело и обстоит. Если ZF непротиворечива, то непротиворечива и каждая из теорий ZFC+H и ZFC+$\neg H$. По известной теореме Гёделя о полноте каждая из этих теорий имеет модель и любую из этих двух моделей можно взять в качестве структуры $\mathcal{M}_0$. С точки зрения оснований математики полезно отметить, что само доказательство теоремы Гёделя о полноте в рассматриваемом случае не требует мощных теоретико-множественных идей, заложенных в аксиомах ZF, оно может быть естественно формализовано, например, в рамках арифметики второго порядка Ar2 (см. [3]).

5. Обсудим еще один вопрос, связанный с теорией ZF и часто вызывающий недоразумения. Из теоремы Гёделя о полноте следует, в частности, что если теория ZF непротиворечива, то она допускает счетную модель M. Как согласовать это обстоятельство с тем очевидным фактом, что в ZF выводимо существование несчетных множеств (например, таковым является множество $P\omega$)?

Модель M теории ZF имеет вид $\langle X, \varepsilon\rangle$, где X — непустое множество объектов модели и ε — отношение, $\varepsilon \subseteq X \times X$, которое интерпретирует принадлежность $\in$ на множестве X. При этом все аксиомы ZF истинны в этой интерпретации.

Формула $\exists x(x = P\omega)$ истинна в M, и поэтому найдется объект $a \in X$ такой, что $M \models (a = P\omega)$. (Здесь и ниже мы пишем для краткости формулы ZF^+, а не ZF. Имеется в виду, конечно, что их следует перевести в язык ZF с помощью стандартного перевода § 4, п. 4.)

Формула, утверждающая, что x счетно, имеет вид

$$\mathrm{Count}(x) \leftrightharpoons \exists f((1-1)(f) \wedge \mathrm{dom}\, f = x \wedge \mathrm{rng}\, f = \omega).$$

В ZF выводимо, что $P\omega$ — несчетное множество, и, значит, этот факт истинен в M, т. е.

$$M \models \neg\mathrm{Count}(a).$$

По определению истинности в структуре последнее означает, что не существует объекта $b \in X$ такого, что

$$M \models (1-1)(b) \wedge \mathrm{dom}\, b = a \wedge \mathrm{rng}\, b = \omega,$$

т. е. **среди элементов** X не существует объекта b такого, что в M **было бы истинно**, что b есть взаимно однозначная функция с областью определения a и областью значений ω. Какой природы само a, при этом совсем не важно, например, a может быть с внешней точки зрения счетным множеством, так что существует биекция a на ω. Просто среди элементов X необходимой биекции с точки зрения модели M не существует. Истинность утверждений зависит от того, в какой модели эти утверждения рассматриваются. Один и тот же объект, будучи элементом различных моделей, в этих моделях может обладать различными свойствами.

Указанное явление обычно называется *парадоксом Скулема*. Следует иметь в виду, конечно, что никакого парадокса в собственном смысле этого слова здесь нет. Имеется, может быть, лишь некоторая путаница понятий, сбивающая неспециалиста.

Подобное недоразумение часто связано и с категоричностью некоторых структур, например, натурального ряда.

В ZF можно доказать с помощью хорошо известных из теории чисел рассуждений, что все *структуры Пеано*, т. е. структуры вида $\langle \omega^*, 0^*, S^* \rangle$, где ω^* — множество, $0^* \in \omega^*$ и S^* — операция S^*: $\omega^* \to \omega^*$, удовлетворяющие *аксиомам Пеано* (см. § 4, п. 1), изоморфны, т. е. структуры Пеано изображают один единственный натуральный ряд с точностью до изоморфизма. В этом и состоит свойство категоричности натурального ряда.

Тем не менее, в **различных моделях** могут быть и неизоморфные натуральные ряды! Рассмотрим две модели теории ZF: $M_1 = \langle X_1, \varepsilon_1 \rangle$ и $M_2 = \langle X_2, \varepsilon_2 \rangle$. Имеем $\mathrm{ZF} \vdash \exists x (x = \omega)$, так что существуют объекты $\omega_1 \in X_1$ и $\omega_2 \in X_2$ такие, что $M_1 \models \omega_1 = \omega$ и $M_2 \models \omega_2 = \omega$. Можно рассмотреть и «множество натуральных чисел» в каждой из моделей:

$$N_1 = \{a \in X_1 \mid M_1 \models a \varepsilon_1 \omega_1\}; \quad N_2 = \{a \in X_2 \mid M_2 \models a \varepsilon_2 \omega_2\}.$$

В каждой из моделей M_i имеется свой объект O_i и своя операция S_i прибавления единицы. Но структура $\langle N_i, O_i, S_i \rangle$ совсем не обязана удовлетворять аксиомам Пеано с внешней точки зрения. Необходимо только, чтобы в **модели** M_i были истинны соответствующие формулы. Структуры $\langle N_i, O_i, S_i \rangle$ могут быть вовсе не изоморфны содержательно понимаемому натуральному ряду и не изоморфны между собой. Структура, относительно которой в модели истинно, что она есть структура Пеано, может и не быть структурой Пеано с внешней точки зрения. Мы увидим далее, что если теория ZF непротиворечива, то она действительно имеет модели с неизоморфными натуральными рядами.

6. В § 2–4 мы рассматривали принципы ZF как содержательно истинные, имеющие место в некоторой структуре $\mathcal{M}_0$, и пытались показать, что основные математические понятия можно выразить в языке ZF, а многие математические утверждения имеют место в $\mathcal{M}_0$. Средства доказательства при этом никак не уточнялись.

Затем мы определили формальную аксиоматическую теорию ZF, в которой имеется возможность получить наши предыдущие результаты в форме точных выводов. Для построения выводов в теории ZF нет необходимости вникать в семантику языка ZF, но для изучения *самой* теории ZF, например, для получения результатов о независимости, также нужна, конечно, некоторая математика. Эта математика вновь будет использоваться содержательным, неформализованным образом. По отношению к изучаемой теории ее называют *метаматематикой*. В принципе исследователь может заинтересоваться и метаматематикой теории и также попытаться ее формализовать.

Какова же должна быть метаматематика теории? С точки зрения оснований математики есть стремление сделать метаматематику как можно более бедной, с тем чтобы рассуждения в ней были максимально простыми и убедительными. В такой ситуации можно сказать, что результаты, относящиеся к очень сложной теории, получены с помощью очень убедительных приемов доказательства. Так, результаты, касающиеся независимости аксиомы выбора и континуум-гипотезы, могут быть естественно формализованы в рамках арифметики Ar так, что в этих доказательствах вовсе не будет фигурировать понятие множества. Многие другие результаты математической логики могут быть получены при ограниченном использовании теории множеств, например, в рамках арифметики второго порядка.

С другой стороны, за пределами оснований математики математическую логику можно развивать как обычную математическую дисциплину, подобную топологии или теории функций. В такой ситуации нет оснований как-то специально ограничивать метаматематику. Можно, например, в качестве метаматематики взять *саму теорию* ZF. Так и поступают во многих исследованиях по теории моделей, нестандартному анализу и т. п. В этом смысле теория ZF выступает в роли «всеобщего мира множеств» для всех математиков.

Следует подчеркнуть, что теория ZF отнюдь не является единственно возможной подходящей базой для развития математики на точной основе. Ее широкое использование объясняется значительными формальными удобствами, а также отчасти исторической традицией. В настоящее время в логике разработаны очень интересные и многообещающие подходы к развитию математических теорий, не опирающиеся на понятие множества. Одним из них является *конструктивное направление в математике*, широко разрабатываемое в нашей стране. Кроме того, имеются и другие теоретико-множественные системы, могущие с успехом конкурировать с теорией ZF. Среди них прежде всего можно назвать теорию типов Рассела и Уайтхеда, а также *теорию множеств Куайна*.

Согласно известной теореме Гёделя, непротиворечивость ZF не может быть установлена средствами ZF, т. е. практически не может быть установлена традиционными математическими средствами. Поэтому, если мы желаем исследовать непротиворечивость таких мощных теорий, приходится находить математические средства, с одной стороны, достаточно убедительные в том или ином отношении, а с другой стороны, выходящие за пределы традиционной математической практики.

Подробное обсуждение многих из затронутых здесь вопросов читатель может найти в книге [11].

7. Сделаем еще несколько замечаний относительно аксиоматического метода в математической логике. Термин «аксиоматический метод» используется в различных смыслах, что иногда ведет к недоразумениям.

Прежде всего это *содержательно аксиоматический метод*. Он употребляется, когда изучается род структур, удовлетворяющих одному и тому же

списку свойств. Например, один род структур составляют группы, другой род структур — кольца, третий род структур — структуры Пеано и т. п. Под *аксиомами* при этом понимаются просто конкретные условия, которым должна удовлетворять любая из структур изучаемого рода. Эти условия понимаются содержательно и записываются на рабочем математическом языке, например, на русском или английском. Впрочем, часто аксиомы какого-либо рода структур записывают и на точном логико-математическом языке, но понимают содержательно как утверждения о структурах; для одних структур эти аксиомы могут быть истинны, а для других — ложны.

Как понимать эти аксиомы, зависит от принятой метаматематики. Особенно это существенно в тех случаях, когда в формулировках аксиом, кроме объектов структуры, фигурируют и другие объекты, например, множества. Это так называемые *неэлементарные аксиомы*.

Так, среди аксиом для структуры Пеано $\langle \omega, O, S\rangle$ имеется и такая: для всякого подмножества $x \subseteq \omega$ выполняется принцип полной математической индукции $O \in x \wedge (\forall y \in x)(Sy \in x) \supset (\forall y \in \omega)(y \in x)$. Чтобы понимать это утверждение, следует понимать, что такое подмножество данного множества и по каким правилам следует с этими подмножествами обращаться. Если мы в качестве метаматематики принимаем содержательно понимаемые принципы ZF (так это и делается в практической математике), то понимание этой аксиомы в достаточной степени проясняется, можно получать содержательные следствия из нее, например, доказать, что все структуры Пеано изоморфны. Можно представлять себе ситуацию и так, что мы фиксировали некоторую воображаемую структуру $\mathcal{M}_0$, согласованную с принципами ZF. Только из $\mathcal{M}_0$ мы и черпаем все объекты математического исследования. После этого можно доказать, что все структуры Пеано в $\mathcal{M}_0$ изоморфны между собой.

Несколько иной подход возникает при изучении теорий *формально аксиоматическим методом*. Основные факты об изучаемых структурах мы оформляем в виде формальной аксиоматической теории T. Новые факты о теории T извлекаются (по крайней мере, в принципе) с помощью аппарата формальной выводимости. Для их получения первоначальная семантика T не имеет никакого значения, и нет необходимости привлекать модели теории T. Более того, среди моделей формальной аксиоматической теории T могут оказаться и такие, которые мы не включали в число подразумеваемых моделей. Так, если теория ZF непротиворечива, то среди ее моделей имеется и счетная модель.

Под *аксиомами* теории T теперь понимаются просто ее нелогические аксиомы, т. е. формулы специального вида, смысл этих аксиом в принципе не важен при формулировке самой теории T. Но, конечно, если мы стремимся выводить в T нетривиальные факты, следует снабдить T достаточно богатым списком аксиом. Так, если мы изучаем структуры Пеано, записывая принцип индукции на языке ZF, следует добавить в теорию и аксиомы, описывающие свойства множеств.

Глава II

Элементы теории алгорифмов

§ 1. Машины Тьюринга

1. Известно, какое большое значение в математике имеют алгорифмы. Коротко говоря, *алгорифм* есть точное предписание, в соответствии с которым по любому входному объекту из данного класса входных объектов можно эффективно получать выходные объекты. Например, алгорифм умножения десятичных рациональных чисел «столбиком» позволяет по двум десятичным записям получить некоторую третью согласно хорошо известному предписанию. Алгорифмами являются схема Горнера для вычисления значений многочлена, алгорифм Евклида для отыскания наибольшей общей меры двух отрезков, алгорифм перемножения двух квадратных матриц и многие другие.

Чтобы подвергнуть понятие алгорифма точному анализу следует несколько сузить тот класс алгорифмов, которые мы намерены рассматривать. Прежде всего мы предполагаем, что наши алгорифмы представляют собой *дискретные* предписания, подобные программам для вычислительных машин, а не подобные аналоговым или графическим вычислительным устройствам. Предписание должно содержать указания к выполнению конечного числа элементарных, четко различимых шагов. Поэтому и входные данные изучаемых алгорифмов должны представлять собой дискретные, *конструктивные объекты*, такие как натуральные числа, рациональные числа, целочисленные матрицы и т. п. Входными данными не могут быть, например, произвольные отрезки прямой или произвольные действительные числа, так как их, в общем случае, нельзя задавать конечным образом.

Заметим, что в математике заметную роль играют и точные предписания, перерабатывающие неконструктивные объекты. Такого рода алгорифмы также изучаются в математической логике, но для первоначального изучения мы ограничимся самым важным классом чисто дискретных устройств. Таким образом, алгорифм умножения десятичных рациональных чисел, схема Горнера для многочленов с рациональными коэффициентами, алгорифм перемножения квадратных матриц с натуральными элементами суть алгорифмы нашего класса, а алгорифм отыскания наибольшей общей меры двух произвольных отрезков остается пока вне нашего рассмотрения.

Понятие конструктивного объекта все еще очень расплывчато, но разумно предположить, что интересующие нас конструктивные объекты можно эффективно кодировать в виде слов в некотором алфавите. Таким образом, можно считать, что с каждым алгорифмом A связан некоторой алфавит Σ — *внешний алфавит* A, и наш алгорифм получает на вход слова в алфавите Σ и вырабатывает в качестве результатов также слова в алфавите Σ. Мы будем изучать только такие *словарные* алгорифмы.

Алгорифм является единой инструкцией, на вход которой можно подавать любое из, вообще говоря, бесконечного списка входных слов. В этом состоит свойство *массовости* алгорифма. Удобно считать, что на вход алгорифму A можно подать *любое* слово во внешнем алфавите Σ. Получив входное слово, следует применять к нему предписание алгорифма A шаг за шагом. При этом шаги предписания могут обрываться и мы получим выходное слово как результат работы алгорифма, а может случиться, что предписание ведет к бесконечной последовательности элементарных действий, и тогда алгорифм A не определен на данном входном слове.

Далее, мы считаем, что изучаемые алгорифмы обладают свойством *детерминированности*: каждый элементарный шаг однозначно определяется предыдущей ситуацией. В наш алгорифм не встроены случайные или вероятностные механизмы. В частности, если дважды проделать вычисления алгорифма над одним и тем же входом, то результаты также будут одинаковы.

Наконец, наши алгорифмы должны обладать свойством *замкнутости*, т. е. выполнение вычислений определяется только предписанием, и для вычисления не требуется привлекать, кроме входного слова, какие-либо процессы или вычисляющие устройства извне.

Можно предположить, что все действия, которые может производить любой алгорифм указанного типа, можно разложить на некоторые канонические элементарные шаги. Такой анализ привел Тьюринга (в 1936 году) к понятию вычислительных машин, названных впоследствии его именем.

2. Перейдем к точным определениям. Напомним, что *алфавит* есть по определению непустое конечное множество символов, элементы алфавита называются его *буквами*. *Слово* в алфавите Σ есть конечная последовательность (может быть и пустая) его букв. Слово в алфавите Σ имеет, следовательно, вид $a_0a_1 \ldots a_n$, где $a_i \in \Sigma$. Множество всех слов в алфавите Σ обозначим через Σ^*.

Основная операция на словах — операция приписывания слова к слову: если дано слово A, имеющее вид $a_0a_1 \ldots a_n$, и слово B вида $b_0b_1 \ldots b_m$, то можно образовать новое слово AB вида $a_0a_1 \ldots a_nb_0 \ldots b_m$, полученное *приписыванием* (в другой терминологии — *соединением*, *конкатенацией*) слов A и B.

Пустое слово обозначается через Λ. Конечно, $A\Lambda = \Lambda A = A$.

Фиксируем два алфавита Σ и S. Σ назовем *внешним алфавитом*, а S — назовем *внутренним алфавитом*, или *алфавитом состояний*. Предположим, что символы $\to$, R, L не входят ни в Σ, ни в S.

Командой назовем слово одного из следующих трех видов:

$$qa \to rb,$$
$$qa \to rbR,$$
$$qa \to rbL$$

(где $q, r \in S$; $a, b \in \Sigma$). Команды, подобно формулам языка, можно читать по-русски. Команда первого вида читается так: «находясь в состоянии q и наблюдая букву a, следует перейти в состояние r и напечатать букву b». Команда второго вида: «находясь в состоянии q и наблюдая букву a, следует перейти в состояние r, напечатать букву b и затем передвинуться вправо». Команда третьего вида читается так же, как и команда второго вида, но следует только в конце читать «...и затем передвинуться влево».

Список команд или *программа* (в алфавитах Σ, S) есть по определению конечная последовательность команд.

Пусть теперь фиксированы алфавиты Σ, S, а также две буквы q_0, $q_1 \in S$ и одна буква $a_0 \in \Sigma$. Мы называем q_0 — *начальным состоянием*, q_1 — *финальным* или *заключительным* состоянием, а букву a_0 мы назовем *бланком* (*пустой клеткой*).

Алфавит $S \times \Sigma$ мы назовем алфавитом *наблюдаемых букв*: про букву $\langle q, a\rangle \in S \times \Sigma$ мы говорим, что a *наблюдается* в состоянии q.

Конфигурацией на ленте (или *машинным словом*) называется слово в алфавите $\Sigma \cup (S \times \Sigma)$, содержащее в точности одно вхождение наблюдаемой буквы. Таким образом, конфигурация всегда имеет вид $A\langle q, a\rangle B$, где A, $B \in \Sigma^*$ и буква a наблюдается в состоянии q.

Конфигурация называется *начальной*, если она имеет вид $\langle q_0, a\rangle B$. Здесь q_0 — начальное состояние, а слово A в данном случае пусто. Конфигурация называется *финальной* (или *заключительной*), если она имеет вид $A\langle q_1, a\rangle B$, т. е. наблюдаемая буква наблюдается в заключительном состоянии.

Пусть теперь K_1 и K_2 — конфигурации и k — команда. Определим, что значит, что команда k *переводит* конфигурацию K_1 в K_2; символически мы записываем это отношение как

$$k\colon K_1 \triangleright K_2.$$

А именно, пусть K_1 имеет вид $A\langle q, a\rangle B$. Если левая часть команды k не имеет вида qa, то $k\colon K_1 \triangleright K_2$ автоматически считается ложным (команда k *неприменима* к конфигурации K_1). Пусть левая часть команды k имеет вид qa. Далее разберем три случая в зависимости от строения команды k.

1) k есть $qa \to rb$. В этом случае $k\colon K_1 \triangleright K_2 \Leftrightarrow K_2$ имеет вид $A\langle r, b\rangle B$.
2) k есть $qa \to rbR$. Здесь рассмотрим два случая:

a) слово B не пусто, $B = cB'$, тогда k: $K_1 \triangleright K_2 \Leftrightarrow K_2$ есть $Ab\langle r, c\rangle B'$;

b) слово B пусто, тогда
k: $K_1 \triangleright K_2 \Leftrightarrow K_2$ есть $Ab\langle r, a_0\rangle$.

3) k есть $qa \to rbL$. Здесь также рассмотрим два подслучая:

a) слово A не пусто, $A = A'c$, тогда
k: $K_1 \triangleright K_2 \Leftrightarrow K_2$ есть $A'\langle r, c\rangle bB$;

b) слово A пусто, тогда
k: $K_1 \triangleright K_2 \Leftrightarrow K_2$ есть $\langle r, a_0\rangle bB$.

Легко видеть, что если k: $K_1 \triangleright K_2$, то конфигурация K_2 определяется однозначно по команде k и конфигурации K_1.

Можно представлять себе, что конфигурация есть слово, записанное на некоторой ленте, разделенной на клеточки, в каждой клеточке записано по букве алфавита Σ. Над одной из букв написано еще состояние, эта буква наблюдается машиной.

Перевести K_1 в K_2 командой k — это значит «выполнить» команду k, проделать то, что «она требует». После выполнения команды наблюдаемой может стать уже иная буква левее или правее исходной. При этом, если приходится выходить за пределы ленты влево и вправо, то выполнение команды автоматически предусматривает добавление новой клеточки, на которой считается напечатанной буква a_0 — «пустая клеточка», «бланк».

Машина Тьюринга есть по определению набор

$$M = \langle \Sigma, S, \Pi, q_0, q_1, a_0\rangle,$$

Σ — внешний алфавит, q_0 — начальное состояние,

S — внутренний алфавит, q_1 — заключительное состояние,

Π — программа машины, a_0 — бланк.

Команды программы Π машины M обычно записывают вертикально, нумеруя

$$\begin{matrix} k_1 \\ k_2 \\ \vdots \\ k_m \end{matrix}$$

сверху вниз.

Мы говорим, что машина M *переводит* конфигурацию K_1 в K_2, и пишем M: $K_1 \triangleright K_2$, если

1) существует команда k_i программы машины M такая, что k_i: $K_1 \triangleright K_2$ и
2) для всех $j < i$ не существует конфигурации K_3 такой, что k_i: $K_1 \triangleright K_3$.

Таким образом, если M: $K_1 \triangleright K_2$, то конфигурация K_2 определяется однозначно по M и K_1. Конечно, вполне может оказаться, что некоторая конфигурация K_1 не переводится машиной M ни в какую конфигурацию K_2.

Протокол вычислений машины Тьюринга M есть (конечная или бесконечная) последовательность конфигураций

$$K_0, K_1, \ldots, K_n, \ldots$$

такая, что

1) K_0 — начальная конфигурация;
2) M: $K_i \triangleright K_{i+1}$;
3) если конфигурация K_i входит в протокол M: $K_i \triangleright K_{i+1}$, причем K_i не заключительная конфигурация, то K_{i+1} также входит в протокол вычислений (т. е. протокол не оканчивается конфигурацией K_i, если вычисления можно продолжить дальше);
4) протокол вычислений может содержать не более одной заключительной конфигурации, и если протокол действительно содержит заключительную конфигурацию, то этот протокол конечен и заключительная конфигурация есть последний его член.

Мы пишем $M\lfloor K_0 \rfloor = K_n$, если K_0 — начальная конфигурация, K_n — заключительная конфигурация и существует протокол вычислений машины M, начинающийся с K_0 и оканчивающийся K_n. Для данных M и K_0 протокол вычислений, если он существует, может быть только один, так что результат вычислений K_n, если он существует, определен однозначно. Мы говорим, что M *определена* на K_0, если соответствующая заключительная конфигурация K_n существует.

Машина может быть не определена на начальной конфигурации K_0 по двум причинам: либо потому, что в процессе построения протокола вычислений мы придем к конфигурации, к которой не применима ни одна команда машины, либо потому, что протокол вычислений бесконечен и не приводит к заключительной конфигурации. Разумеется, по данной машине M и конфигурации K_0 отнюдь не видно сразу, будет ли M определена на K_0, и если нет, то какой из вышеупомянутых случаев будет иметь место.

Если дано слово $A \in \Sigma^*$, то по нему можно стандартным образом изготовить некоторую начальную конфигурацию A^0 для машины M, как говорят, *подать слово A на вход* машины M. А именно если A не пусто, $A = aA'$, то следует взять $A^0 = \langle q_0, a\rangle A'$. Если же A пусто, то $A^0 = \langle q_0, a_0\rangle$. Коротко говоря, следует «заставить» машину наблюдать первую букву A в начальном состоянии. Если же в A вовсе нет букв, то, конечно, ее следует заставить наблюдать пустую клеточку машины.

С другой стороны, по любой конфигурации K машины мы можем изготовить некоторое слово $K^1 \in \Sigma^*$. Мы говорим, что слово K^1 *записано на ленте* в конфигурации K. А именно надлежит поступить следующим образом:

1) следует, во-первых, убрать состояние из наблюдаемой буквы, т. е. заменить наблюдаемую букву $\langle q, a\rangle$ в конфигурации K на обычную букву a, так что получится некоторое слово A в алфавите Σ;
2) затем следует в слове A стереть все пустые клетки, идущие, подряд, слева и справа, т. е. если $A = BCD$, где B и D составлены только из буквы a_0, а слово C не начинается и не кончается буквой a_0, то следует оставить в качестве K^1 слово C.

Может оказаться, что K^1 есть пустое слово (если в K фигурировала лишь буква a_0 из Σ).

3. Таким образом, машина Тьюринга M с внешним алфавитом Σ порождает функцию, перерабатывающую некоторые слова в алфавите Σ в слова же в алфавите Σ. А именно для $A, B \in \Sigma^*$, $M(A) = B \Leftrightarrow$ — существуют конфигурации K_0 и K_n такие, что $M\lfloor K_0\rfloor = K_n$ и $(K_0)^0 = A$, $(K_n)^1 = B$. Коротко говоря, если на вход подать слово A, то соответствующий протокол вычислений заканчивается и на ленте оказывается записанным слово B.

Заметим, что функция M может быть определена отнюдь не на всех словах в алфавите Σ. Мы говорим, что машина M *определена* на слове A, и пишем $!M(A)$, если M определена на начальной конфигурации A^0.

Машины Тьюринга можно представлять себе как определенный тип вычислительных машин, обрабатывающих слова в алфавитах и имитирующих действие реальных вычислительных машин или действия человека-вычислителя. Машина работает на ленте, разделенной на клеточки—ячейки. В каждый момент времени рассматривается лишь конечный кусок этой ленты, но по мере надобности лента продолжается неограниченно в обе стороны.

Машина может печатать на ленте некоторые буквы алфавита и обозревать в каждый момент только одну клеточку ленты. Ее действия происходят шагами, однозначным образом определяемыми ее состоянием в данный момент, содержимым обозреваемой ячейки и программой машины. Машина останавливается, когда приходит в заключительное состояние. Может оказаться, что она, стартуя с некоторого слова, никогда не остановится.

4. Определим теперь, что значит, что функция вычислима с помощью машины Тьюринга.

Напомним некоторые обозначения. Если $X_1, \ldots, X_k$ суть множества, то через $X_1 \times \ldots \times X_k$ мы обозначаем их декартово произведение, т. е. множество всех упорядоченных наборов $\langle x_1, \ldots, x_k,\rangle$, где $x_1 \in X_1, \ldots, x_k \in X_k$. Если X и Y — множества, то через $X \to Y$ мы обозначим множество всех функций с областью определения X, принимающих значения в множестве Y. Вместо $f \in (X \to Y)$ традиционно пишем $f\colon X \to Y$. Функция от k аргументов есть функция вида $f\colon X_1 \times \ldots \times X_k \to Y$, так что $f(\langle x_1, \ldots, x_k\rangle) \in Y$. Обозначение $f(\langle x_1, \ldots, x_k\rangle)$, по традиции, сокращаем до $f(x_1, \ldots, x_k)$.

Через $X \ddot{\to} Y$ обозначим теперь множество всех *частичных* функций *из* X в Y, т.е. $f\colon X \ddot{\to} Y \Leftrightarrow$ область определения f включена в X (и не обязательно совпадает со всем множеством X) и значения f принимаются из множества Y. В частности, функция $f\colon X_1 \times \ldots \times X_k \ddot{\to} Y$ от k аргументов может быть и не определена для некоторых наборов $\langle x_1, \ldots, x_k\rangle$. Множеству $X_1 \times \ldots \times X_k \ddot{\to} Y$ принадлежит, в частности, и нигде не определенная функция.

Нас специально интересуют функции, перерабатывающие слова. Если Δ — алфавит, то через Δ^* мы обозначаем множество всех слов в алфавите Δ. Пусть $\Delta_1, \ldots, \Delta_k$, Δ суть алфавиты. Машины Тьюринга можно приспособить для вычисления функций вида $\Delta_1^* \times \ldots \times \Delta_k^* \ddot{\to} \Delta^*$. С этой целью фиксируем некоторую новую букву q, не входящую в рассматриваемые алфавиты, и будем изображать наборы слов из $\Delta_1^* \times \ldots \times \Delta_k^*$ в виде слов в алфавите $\Delta_1 \cup \ldots \cup \Delta_k \cup \{q\}$. Например, упорядоченную тройку $\langle x_1, x_2, x_3\rangle$, где $x_i \in \Delta_i^*$, изобразим в виде одного слова $x_1 q x_2 q x_3$.

Пусть $f\colon \Delta_1^* \times \ldots \times \Delta_k^* \ddot{\to} \Delta^*$ есть (вообще говоря, частичная) функция от k аргументов. Будем говорить, что машина Тьюринга

$$M = \langle \Sigma, S, \Pi, q_0, q_1, a_0\rangle$$

вычисляет f, если

1) $\Delta \cup \Delta_1 \cup \ldots \cup \Delta_k \cup \{q\} \subseteq \Sigma$;
2) для всяких $x_1, \ldots, x_k$, $x_i \in \Delta_i^*$, набор $\langle x_1, \ldots, x_k\rangle$ принадлежит области определения функции
$$f \Leftrightarrow !M(x_1 q \ldots q x_k) \quad \text{и} \quad M(x_1 q \ldots q x_k) \in \Delta^*;$$
3) для всяких $x_1, \ldots, x_k$, $x_i \in \Delta_i^*$, если
$$!M(x_1 q \ldots q x_k) \quad \text{и} \quad M(x_1 q \ldots q x_k) \in \Delta^*,$$
то $f(x_1, \ldots, x_k) = M(x_1 q \ldots q x_k)$;
4) для удобства потребуем еще, чтобы бланк a_0 машины M был отличен от всех букв алфавита $\Delta_1 \cup \ldots \cup \Delta_k \cup \Delta \cup \{q\}$.

Подчеркнем, что внешний алфавит машины M, вычисляющей функцию f, может быть существенно шире алфавита $\Delta \cup \Delta_1 \cup \ldots \cup \Delta_k \cup \{q\}$. Как говорят, машина M — *над алфавитом* $\Delta \cup \Delta_1 \cup \ldots \cup \Delta_k \cup \{q\}$. Мы требуем, чтобы M вела себя «как функция f» лишь на входах $x_1 q \ldots q x_k$. Буквы внешнего алфавита Σ, не входящие в $\Delta \cup \ldots \cup \Delta_k \cup \{q\}$, могут использоваться при обработке слов вида $x_1 q \ldots q x_k$, но только в промежуточных конфигурациях протокола вычислений. Функция $f\colon \Delta_1^* \times \ldots \times \Delta_k^* \ddot{\to} \Delta^*$ называется *вычислимой* (*по Тьюрингу*), если существует машина Тьюринга, вычисляющая f.

5. Рассмотрим теперь функции от натуральных чисел $f\colon \omega \times \ldots \times \omega \ddot{\to} \omega$. Для таких функций также естественно вводится понятие вычислимости. Будем изображать натуральные числа в виде слов в алфавите $\{|\}$:

0	1	2	3	4	5	...
⊘	|	||	|||	||||	|||||	...

Иногда, чтобы отличать так изображаемые натуральные числа от «обычных» теоретико-множественно понимаемых натуральных чисел (например, по фон Нейману), слова из палочек называются *нумералами* соответствующих натуральных чисел. Нумерал числа n обозначают через $\overline{n}$, например $\overline{3} = |||$.

Тогда каждая функция на натуральных числах, скажем, $f\colon \omega \times \omega \dashrightarrow \omega$, естественно изображается некоторой функцией $\overline{f}\colon \{|\}^* \times \{|\}^* \dashrightarrow \{|\}^*$ на словах из палочек

$$f(m_1, m_2) = m_3 \Leftrightarrow \overline{f}(\overline{m}_1, \overline{m}_2) = \overline{m}_3.$$

Числовая функция называется вычислимой по Тьюрингу, если вычислима по Тьюрингу соответствующая функция на словах из палочек.

Функции $f\colon \omega \times \ldots \times \omega \dashrightarrow \omega$, вычислимые по Тьюрингу, называются еще *частично-рекурсивными функциями* (термин «частично» напоминает о том, что f не обязательно определена на всем множестве $\omega \times \ldots \times \omega$). Если же частично-рекурсивная функция f от k аргументов определена на всех наборах натуральных чисел $\langle n_1, \ldots, n_k \rangle$, т. е. $f\colon \omega \times \ldots \times \omega \to \omega$, то она называется общерекурсивной или даже просто *рекурсивной функцией*.

Коротко говоря, частично-рекурсивная функция — это функция, для которой существует вычисляющий ее алгорифм, заданный в виде машины Тьюринга. Для общерекурсивной функции этот алгорифм для любых входных натуральных чисел обязательно заканчивает свою работу и выдает значение функции.

Можно показать, что все обычные функции теории чисел типа $x + y$, xy, x^y, $[\sqrt{x}]$ и т. п. являются рекурсивными, не всюду определенные функции, например x/y, $x - y[\lg(x - y)]$ являются частично-рекурсивными. Следующая машина M вычисляет функцию $f(m, n) = m + 2n$. Внешний алфавит M есть $\{|, q, a_0\}$, где a_0 — бланк. Внутренний алфавит $\{q_0, q_1, q_2, q_3, q_4, q_5\}$, где q_0 — начальное, а q_1 — финальное состояние. Программа машины имеет вид:

1. $q_0| \to q_2|$
2. $q_0 q \to q_2 q$
3. $q_2| \to q_2|R$
4. $q_2 q \to q_2 q R$
5. $q_2 a_0 \to q_3 a_0 L$
6. $q_3 | \to q_4 a_0 L$
7. $q_4| \to q_4|L$
8. $q_4 q \to q_4 q L$
9. $q_4 a_0 \to q_5 \mid L$
10. $q_5 a_0 \to q_2 \mid$
11. $q_3 q \to a_0 q_1$

Протокол вычислений можно кратко описать следующим образом. Пусть начальная конфигурация имеет вид $\langle q_0 | \rangle \; ||| \; q \; ||$. Под действием команд 1, 2 машина переходит в состояние q_2: $\langle q_2 | \rangle \; ||| \; q \; ||$ и затем под действием 3 и 4 движется вправо до появления пустой клеточки справа $|||| \; q \; || \; \langle q_2, a_0 \rangle$. После этого машина двигается влево и переходит в состояние q_3: $|||| \; q \langle q_3, | \rangle$ (команда 5). Затем машина стирает обозреваемую палочку, переходит в состояние q_4 и в этом состоянии движется влево до появления пустой клеточки слева (команды 6,7,8): $\langle q_4, a_0 \rangle \; |||| \; q \; |$.

Под действием команд 9 и 10 машина печатает слева две палочки и переходит вновь в состояние q_2: $\langle q_2 \mid\rangle$ $\mid\mid\mid\mid\mid$ q $\mid$. Далее вновь начинают работать команды 3 и 4 и цикл повторяется, машина идет в конец слова, стирает после q одну палочку, идет влево и печатает слева две палочки и т. д., пока правее вовсе не останется палочек. Тогда возникнет конфигурация $\mid\mid\mid\mid\mid\mid\mid\mid$ $\langle q_3, q\rangle$. Команда 11 сотрет q, и машина остановится в заключительной конфигурации $\mid\mid\mid\mid\mid\mid\mid\mid$ $\langle q_1, a_0\rangle$.

Упражнение. Постройте машину Тьюринга, вычисляющую функцию

$$f(m, n) = m \cdot n.$$

§ 2. Тезис Чёрча

1. Кажется очевидным, что всякая функция на словах $f\colon \Sigma^* \dashrightarrow \Sigma^*$, вычислимая по Тьюрингу, эффективно вычислима. В самом деле, алгорифм для вычисления такой функции и задается собственно машиной Тьюринга, о которой идет речь в определении вычислимости.

В 1936 году Чёрч выдвинул тезис о том, что *всякая эффективно вычислимая функция является вычислимой по Тьюрингу*. Точнее говоря, Чёрч использовал не понятие вычислимости по Тьюрингу, а некоторое иное точное понятие вычислимости (понятие лямбда-определимости), математически эквивалентное нашему определению вычислимости. В свете анализа, проведенного в начале предыдущего параграфа, тезис Чёрча можно сформулировать и так: всякий словарный, дискретный, массовый, детерминированный, замкнутый алгорифм может быть задан в виде машины Тьюринга.

Коротко говоря, машины Тьюринга могут имитировать любой алгорифм указанного типа.

Сразу отметим, что тезис Чёрча не является математическим утверждением, так как в его формулировку входит понятие алгорифма в интуитивном смысле этого слова. Тезис Чёрча нельзя поэтому доказать или опровергнуть в рамках традиционной математической практики. Это не математический результат, а скорее естественно-научное наблюдение. В пользу тезиса Чёрча можно привести, однако, сильные доводы естественно-научного характера.

Во-первых, за многие столетия развития в математике накопилось огромное количество алгорифмов. Все они оказались вычислимыми по Тьюрингу. Этот экспериментальный материал должен убедить нас в справедливости тезиса Чёрча не меньше, чем, например, соответствующие эксперименты убеждают физиков в законе сохранения энергии.

Во-вторых, почти одновременно с понятием вычислимости по Тьюрингу были предложены и другие подходы к понятию вычислимости, внешне сильно отличающиеся друг от друга. Все они оказались эквивалентными. Упомянем важнейшие из этих подходов:

- исчисление равенств Эрбрана и Гёделя,
- частично-рекурсивные функции по Клини,

- лямбда-определимость Чёрча,
- канонические системы Поста,
- нормальные алгорифмы Маркова,
- алгорифмы Колмогорова—Успенского.

В-третьих, эффективно вычислимые функции с интуитивной точки зрения должны быть замкнуты относительно некоторых важных операций: композиции, разветвления, итерации и т. д. Оказывается, что семейство по Тьюрингу функций, как и ожидается, замкнуто относительно этих операций.

Наконец, отметим, что тезис Чёрча *не нужен* с чисто математической точки зрения и, собственно, в математических утверждениях никогда не применяется. Там, где нужна вычислимость в математическом рассуждении, мы всегда можем использовать вычислимость по Тьюрингу.

Тезис Чёрча важен для приложений математики в естествознании. Он объясняет ту большую роль, которую играет понятие алгорифма в точной форме (т. е., например, в форме вычислимости по Тьюрингу) в современной математике.

Например, иногда удается точно доказать, что некоторая конкретная функция f: $\Sigma^* \to \Sigma^*$ не вычислима по Тьюрингу. Тезис Чёрча указывает, что бесполезно было бы фактически искать алгорифм (в интуитивном смысле этого слова), вычисляющий f.

Функция f и интуитивно будет невычислимой.

Таким образом, открывается ценная возможность точными математическими средствами обнаружить невычислимость некоторых функций.

§ 3. Рекурсивные и рекурсивно-перечислимые множества и предикаты

1. В предыдущем параграфе мы дали определение вычислимой функции. Теперь попытаемся определить, что понимать под вычислимым предикатом. При этом следует рассматривать, конечно, *словарные* предикаты $P(x_1, \ldots, x_k)$, где x_i суть слова в некотором алфавите, например, x_1 пробегает слова в алфавите Δ_1, x_2 — слова в алфавите Δ_2, и т. д. Про такой предикат P мы говорим, что он типа $\Delta_1^* \times \ldots \times \Delta_k^*$, указывая область пробегания каждого аргументного места.

Словарному предикату P можно сопоставить некоторую функцию χ_P: $\Delta_1^* \times \ldots \times \Delta_k^* \to \{0, 1\}$, так называемую *характеристическую функцию* предиката, такую, что для всех наборов $\langle x_1, \ldots, x_k \rangle$, где $x_i \in \Delta_i^*$:

$$P(x_1, \ldots, x_k) \text{ истинно } \Leftrightarrow \chi_P(x_1, \ldots, x_k) = 1.$$

С другой стороны, словарному предикату можно сопоставить *множество-отношение* данного предиката, а именно множество $X_P \subseteq \Delta_1^* \times \ldots \times \Delta_k^*$ такое, что

$$P(x_1, \ldots, x_k) \text{ истинно } \Leftrightarrow \langle x_1, \ldots, x_k \rangle \in X_P.$$

Напротив, если задано множество слов $X \subseteq \Sigma^*$, то можно рассмотреть предикат принадлежности этого множества: для всякого слова $x \in \Sigma^*$

$$P(x) \text{ истинно } \Leftrightarrow x \text{ принадлежит } X.$$

Чаще всего рассматривают словарные предикаты, для которых алфавиты $\Delta_1, \ldots, \Delta_k$ совпадают. Например, предикаты, определенные на натуральных числах (*арифметические предикаты*), можно трактовать как словарные предикаты, определенные на нумералах, т. е. словах в алфавите $\{|\}$.

2. Наше первое определение вычислимости таково: предикат P типа $\Delta_1^* \times \ldots \times \Delta_k^*$ *рекурсивен* (или *разрешим*), если вычислима по Тьюрингу соответствующая характеристическая функция χ_P.

Интуитивно предикат P рекурсивен, если существует алгорифм, выясняющий для каждого набора $\langle x_1, \ldots, x_k \rangle$ слов, истинно $P(x_1, \ldots, x_k)$ или нет.

Повторим еще раз определение рекурсивного предиката непосредственно в терминах машин Тьюринга. Предикат P типа $\Delta_1^* \times \ldots \times \Delta_k^*$ называется рекурсивным (или разрешимым), если существует машина Тьюринга $M = \langle \Sigma, S, \Pi, q_0, q_1, a_0 \rangle$ такая, что

1) $\Delta_1 \cup \ldots \cup \Delta_k \cup \{0, 1\} \cup \{q\} \subseteq \Sigma$
(здесь, как и раньше, q — новая буква, которая служит для записи наборов слов);
2) для всяких $x_1, \ldots, x_k$ $(x_i \in \Delta_i^*)$ определено значение $M(x_1 q \ldots q x_k)$, и это значение равно 0 или 1;
3) $P(x_1, \ldots, x_k)$ истинно тогда и только тогда, когда $M(x_1 q \ldots q x_k) = 1$.

Множество $X \subseteq \Sigma^*$ назовем *рекурсивным*, если рекурсивен соответствующий предикат принадлежности $x \in X$, где x пробегает множество Σ^*.

Обычные арифметические предикаты $x \leqslant y$, $x + y = z$, «x — простое число», «x делит y» являются рекурсивными. Аккуратное доказательство этого факта состоит в непосредственном построении соответствующих разрешающих машин Тьюринга. Но и без такого построения разрешимость этих предикатов должна быть очевидной читателю. В самом деле, очевидно, что существует эффективный метод проверки, верно или нет, например, что x делит y для натуральных x и y. В дальнейшем изложении мы будем обычно опускать конкретное построение необходимых машин Тьюринга в случаях, когда ясно, что нужный алгорифм существует. Методы построения машин Тьюринга рассматриваются на семинарских занятиях, о них можно прочесть и в более подробных учебниках математической логики (см. список литературы).

Аналогично, рекурсивными являются многие обычные множества натуральных чисел: множество четных чисел, множество простых чисел, множество чисел, делящихся на 7. Число называется совершенным, если оно равно сумме своих делителей (отличных от него самого). Множе-

ство всех нечетных совершенных чисел рекурсивно, так как есть простой способ выяснять по данному числу, является ли оно нечетным и совершенным. Тем не менее неизвестно, пусто это множество или нет, так как до сих пор неизвестно, существуют ли указанные числа.

3. Второе определение вычислимости — *рекурсивная перечислимость* предиката накладывает меньшие требования на соответствующий алгорифм.

Интуитивно, предикат P рекурсивно перечислим, если существует процедура, позволяющая устанавливать истинность $P(x_1, \ldots, x_k)$ в случае, когда $P(x_1, \ldots, x_k)$ истинно. Если же $P(x_1, \ldots, x_k)$ ложно, то наша процедура иногда будет это устанавливать, а иногда процесс будет продолжаться неограниченно. Таким образом, проверяя данный набор $x_1, \ldots, x_k$ на истинность, мы не полностью уверены, что получим ответ.

Точное определение таково: предикат P типа $\Delta_1^* \times \ldots \times \Delta_k^*$ называется *рекурсивно-перечислимым*, если существует машина Тьюринга $M = \langle \Sigma, S, \Pi, q_0, q_1, a_0 \rangle$ такая, что

1) $\Delta_1 \cup \ldots \cup \Delta_k \cup \{0, 1\} \cup \{q\} \subseteq \Sigma$;
2) для всяких $x_1, \ldots, x_k$ $(x_i \in \Delta_i^*)$, *если определено значение* $M(x_1 q \ldots q x_k)$, то это значение равно 0 или 1;
3) $P(x_i, \ldots, x_k)$ истинно тогда и только тогда, когда $M(x_1 q \ldots q x_k) = 1$.

Множество $X \subseteq \Sigma^*$ назовем *рекурсивно-перечислимым*, если рекурсивно-перечислим соответствующий предикат принадлежности.

4. Непосредственно из определений видно, что *всякий рекурсивный предикат (множество) является и рекурсивно-перечислимым.*

Лемма. *Если предикат* $P(x_1, \ldots, x_k, y)$ *рекурсивно-перечислим, то рекурсивно-перечислим и предикат* $\exists y P(x_1, \ldots, x_k, y)$.

▷ Пусть y пробегает множество Δ^* и пусть M — машина, фигурирующая в определении рекурсивной перечислимости предиката $P(x_1, \ldots, x_k, y)$. Убедимся, что существует соответствующая машина M' для предиката $\exists y P(x_1, \ldots, x_k, y)$. Мы не будем выписывать программу M', а лишь опишем в содержательных терминах, как M' работает. Мы надеемся, что после этих пояснений построение M' не составит принципиальных затруднений (хотя останется довольно громоздким делом). Пересчитаем все слова в алфавите Δ в виде определенной эффективно заданной последовательности

$$Y_1, Y_2, Y_3, \ldots .$$

Рассмотрим набор $x_1, \ldots, x_k$ и опишем процесс получения значения $M'(x_1 q \ldots q x_k)$.

Вычисление происходит этапами. На первом этапе машина M' образует набор $x_1 q \ldots q x_k Y_1$ и делает один шаг в вычислении значения $M(x_1 q \ldots q x_k q Y_1)$. Если за один шаг обнаружилось $M(x_1 q \ldots q x_k q Y_1) = 1$, то работа M' заканчивается, и полагаем $M'(x_1 q \ldots q x_k) = 1$.

На втором этапе (если на первом этапе работа не закончилась) машина M' производит уже два шага в вычислении двух значений:

$$M(x_1q\ldots qx_kqY_1)$$

и

$$M(x_1q\ldots qx_kqY_2).$$

Если за два шага вычислений M обнаружится, что хоть одно из значений равно единице, то работу M' заканчиваем и полагаем $M'(x_1q\ldots qx_k)=1$.

На третьем этапе (если на предыдущих этапах работа не закончилась) машина M' производит уже три шага в вычислении трех значений:

$$M(x_1q\ldots qx_kqY_1),$$
$$M(x_1q\ldots qx_kqY_2),$$
$$M(x_1q\ldots qx_kqY_3).$$

Если за три шага вычислений M обнаружится, что хоть одно из этих значений равно единице, то работу M' заканчиваем и полагаем $M'(x_1q\ldots qx_k)=1$. И так далее, выполняем этап за этапом.

Если на некотором этапе вычислится значение $M(x_1q\ldots qx_kqY_i)=0$, то мы вычеркиваем набор $x_1q\ldots qx_kqY_i$ из списка подвергаемых испытанию, но из-за этого набора работу не заканчиваем, а переходим к следующему этапу в поисках набора, для которого $M(x_1q\ldots qx_kqY_i)=1$. Машина M' и будет подтверждать рекурсивную перечислимость $\exists\, yP(x_1,\ldots,x_k,y)$.

Заметим, что M' принимает лишь значение 1 или не определена. Поэтому даже если $P(x_1,\ldots,x_k,y)$ — рекурсив ный предикат, машина M' подтверждает лишь рекурсивную перечислимость $\exists\, yP(x_1,\ldots,x_k,y)$. И действительно, как мы увидим ниже, может быть построен рекурсивный предикат P такой, что предикат $\exists\, yP$ уже только рекурсивно-перечислим, но не рекурсивен. ◁

Лемма. *Для всякого рекурсивно-перечислимого предиката $Q(x_1,\ldots,x_k)$ существует рекурсивный предикат $P(x_1,\ldots,x_k,y)$ такой, что*

$$Q(x_1,\ldots,x_k)\Leftrightarrow\exists\, yP(x_1,\ldots,x_k,y).$$

▷ Пусть M — машина, фигурирующая в определении рекурсивной перечислимости Q. Рассмотрим следующий предикат: $P(x_1,\ldots,x_k,y)$ истинно $\Leftrightarrow$ y есть конечный протокол вычислений машины M такой, что в начальной конфигурации y на ленте записан набор $x_1q\ldots qx_k$, а в конечной конфигурации y на ленте записана единица. Конечные протоколы M мы рассматриваем как слова в подходящем алфавите Δ так, что $y\in\Delta^*$.

Можно убедиться, что предикат P разрешим. Интуитивно очевидно, что по данному слову y можно эффективно выяснить, действительно ли y является протоколом вычислений машины M и что записано на ленте в различных конфигурациях протокола y. Аккуратное доказательство, которое мы опустим, состоит в громоздком построении соответствующей распознающей машины.

Теперь по свойству машины M имеем

$$Q(x_1, \ldots, x_k) \Leftrightarrow \exists y P(x_1, \ldots, x_k, y). \quad \triangleleft$$

Последняя лемма оправдывает термин «перечислимый» в отношении рекурсивно-перечислимого предиката Q. Чтобы убедиться в истинности $Q(x_1, \ldots, x_k)$, следует последовательно перечислять все слова $Y_1, Y_2, \ldots$ в некотором алфавите Δ и последовательно проверять на истинность рекурсивный предикат P:

$$P(x_1, \ldots, x_k, Y_1), \quad P(x_1, \ldots, x_k, Y_2), \quad \ldots.$$

Если Q истинен, то этот процесс закончится и мы найдем соответствующее Y_i. Если же Q ложно, то процесс будет продолжаться неограниченно и мы можем так и не узнать, что Q ложно.

5. Отметим еще, что применение логических связок $\wedge$, $\vee$, $\supset$, $\neg$ к рекурсивным предикатам дает рекурсивные же предикаты.

Доказательство состоит в непосредственном построении распознающих машин для сложных предикатов по данным машинам составляющих предикатов. С интуитивной точки зрения метод распознавания истинности, например предиката $P(x_1, \ldots, x_k) \vee Q(x_1, \ldots, x_k)$ очевиден, если известен метод распознавания истинности для P и Q.

Что касается рекурсивно-перечислимых предикатов, то применение связок $\wedge$, $\vee$ к ним ведет вновь к рекурсивно-перечислимым предикатам. Однако в общем случае это уже неверно для связок $\supset$ и $\neg$. Позже мы обсудим пример рекурсивно-перечислимого предиката, отрицание которого не рекурсивно перечислимо.

Если рассмотреть отношения, соответствующие предикатам, то из предыдущих замечаний следует, что объединение и пересечение любых двух рекурсивных (рекурсивно-перечислимых) множеств вновь рекурсивно (рекурсивно-перечислимо). Дополнение рекурсивного множества слов в некотором алфавите (до множества всех слов в этом алфавите) вновь рекурсивно. Но дополнение рекурсивно-перечислимого множества может быть и не рекурсивно-перечислимо.

В языке арифметики Ar естественно определить

$$x \leqslant y \leftrightharpoons \exists z(x + z = y),$$
$$x < y \leftrightharpoons x \leqslant y \wedge \neg(x = y).$$

Если дан арифметический предикат $P(x, y_1, \ldots, y_n)$, то можно определить новые предикаты, полученные путем применения *ограниченных кванторов*:

$$(\forall x \leqslant z)P(x, y_1, \ldots, y_n) \leftrightharpoons \forall x(x \leqslant z \supset P(x, y_1, \ldots, y_n));$$
$$(\exists x \leqslant z)P(x, y_1, \ldots, y_n) \leftrightharpoons \exists x(x \leqslant z \wedge P(x, y_1, \ldots, y_n));$$
$$(\forall x < z)P(x, y_1, \ldots, y_n) \leftrightharpoons \forall x(x < z \supset P(x, y_1, \ldots, y_n));$$
$$(\exists x < z)P(x, y_1, \ldots, y_n) \leftrightharpoons \exists x(x < z \wedge P(x, y_1, \ldots, y_n)).$$

Результирующие предикаты уже от аргументов $z, y_1, \ldots, y_n$. Заметим

$$\neg(\forall\, x \leqslant z)P(x, y_1, \ldots, y_n) \Leftrightarrow (\exists\, x \leqslant z)\neg P(x, y_1, \ldots, y_n).$$

Упражнение. Укажите аналогичные законы для преобразования отрицаний остальных ограниченных кванторов.

Применение ограниченного квантора к рекурсивному (рекурсивно-перечислимому) предикату приводит к рекурсивному же (рекурсивно-перечислимому) предикату. Доказательство состоит в непосредственном построении соответствующих машин Тьюринга для результирующих предикатов по данным машинам Тьюринга.

6. Теорема Поста. *Если предикаты P и $\neg P$ одновременно рекурсивно-перечислимы, то они необходимо оба и рекурсивны.*

▷ Пусть P и $\neg P$ — предикаты типа $\Delta_1^* \times \ldots \times \Delta_k^*$ и пусть M_1 и M_2 — машины Тьюринга, фигурирующие в определении рекурсивной перечислимости для P и $\neg P$ соответственно. Определим машину M', распознающую истинность, например, предиката P. Как и раньше, мы не будем выписывать программу M', а лишь опишем, как M' работает. Рассмотрим набор $\langle x_1, \ldots, x_k\rangle$ и опишем процесс получения значения $M'(x_1 q \ldots q x_k)$. Вычисление происходит этапами. На первом этапе машина M' производит один шаг в вычислении значений $M_1(x_1 q \ldots q x_k)$ и $M_2(x_1 q \ldots q x_k)$. На втором этапе производятся два шага вычисления $M_1(x_1 q \ldots q x_k)$ и $M_2(x_1 q \ldots q x_k)$. На третьем этапе — три шага вычисления этих двух значений и так далее. Вычисление заканчивается, как только вычислится одно из значений $M_1(x_1 q \ldots q x_k)$ или $M_2(x_1 q \ldots q x_k)$. Если обнаружится, что $M_1 = 1$ или $M_2 = 0$, то положим $M' = 1$. Если же окажется, что $M_1 = 0$ или $M_2 = 1$, то $M' = 0$.

Из определения машин M_1 и M_2 следует, что не может быть одновременно $M_1 = 1$ и $M_2 = 1$ (это означало бы, что для набора $\langle x_1, \ldots, x_k\rangle$ истинны одновременно P и $\neg P$). Также не может быть одновременно $M_1 = 0$ и $M_2 = 0$ (что означало бы, что набор $\langle x_1, \ldots, x_k\rangle$ не удовлетворяется ни P, ни $\neg P$). В то же время необходимо $M_1(x_1 q \ldots q x_k) = 1$ или $M_2(x_1 q \ldots q x_k) = 1$, так как $P(x_1, \ldots, x_k)$ или $\neg P(x_1, \ldots, x_k)$. Отсюда следует, что алгорифм M' действительно распознает истинность предиката P. ◁

7. Упомянем теперь предварительно о некоторых результатах теории алгорифмов, относящихся собственно к логике.

Ясно, что формулы и термы такого логико-математического языка, как ZF^+, можно трактовать как слова в подходящем алфавите Σ. В самом деле, как видно из определения гл. I, § 2, п. 1, выражения ZF^+ строятся с помощью символов: , (формальная запятая), (,), $\in$, $\wedge$, $\vee$, $\supset$, $\neg$, $\forall$, $\exists$, {, }, |, $\varnothing$, ω, P, $\cup$, $\mapsto$ и бесконечного набора переменных. Но переменные в свою очередь, можно рассматривать как слова, составленные из двух символов v и | и скобок, если положить $x \leftrightharpoons (v\,|)$, $y \leftrightharpoons (v\,||)$, $z \leftrightharpoons (v\,|||)$ и т. д.

Аналогично выражения языков Ar, Ar2, ZF также можно трактовать как слова в некоторых алфавитах. Это происходит потому, что выражения рассматриваемых языков строятся из конечного числа явно указанных символов по строго фиксированным правилам. Такие языки назовем *явно заданными*. Мы не будем давать точного математического определения явно заданного языка. Читатель, если угодно, под явно заданным языком может понимать просто один из конкретных логико-математических языков, описанных в книге [1] или в этой книге, хотя изложенные общие результаты верны и по отношению ко многим другим языкам. Следует иметь в виду, однако, что в принципе рассматриваются и логико-математические языки, выражения которых заданы некоторым косвенным теоретико-множественным способом. Для них представление выражений в виде слов некоторого алфавита, может быть и невозможным. Таковы, например, языки, содержащие несчетное множество констант. Однако языки, используемые для построения формальных аксиоматических теорий, обычно оказываются явно заданными.

Таким образом, явно заданный язык Ω определяет алфавит Σ_Ω такой, что выражения Ω суть специальные слова в этом алфавите. Мы считаем, что множество Fm_Ω всех формул языка Ω и множество Tm_Ω всех термов языка Ω суть рекурсивные подмножества множества Σ_Ω^* всех слов алфавита Σ_Ω. По отношению к конкретному языку, например ZF^+, это может быть строго доказано путем построения соответствующей распознающей машины Тьюринга. Впрочем, интуитивно соответствующая распознающая процедура должна быть ясной и без этого громоздкого построения: по каждому слову в алфавите языка всегда можно судить, является ли это слово формулой ZF^+ или не является.

Далее, множество A_{X_Ω} всех аксиом исчисления предикатов явно заданного языка Ω также является рекурсивным подмножеством Σ_Ω^*, так как по формуле всегда можно судить, имеет ли она вид аксиомы исчисления предикатов или нет (например, имеет ли рассматриваемая формула вид $A \supset (B \supset A)$).

Дерево формул в языке Ω мы определяли (см. введение) как некоторую двумерную фигуру, но должно быть ясно, что дерево формул явно заданного языка можно трактовать и как слово в некотором алфавите. Так, вместо $\dfrac{D_1, D_2}{A}$ можно писать $(D_1, D_2/A)$ и т. п. Существенно при этом, что множество всех деревьев выводов является рекурсивным подмножеством множества всех слов этого алфавита, так как по слову можно эффективно выяснить, является ли оно деревом формул и выполняется ли в этом дереве необходимое структурное требование.

Заметим теперь, что множество нелогических аксиом в рассмотренных нами формальных аксиоматических теориях, таких, как Ar, Ar2, ZF, также является рекурсивным множеством, и это теории в явно заданных языках. Мы назовем такие аксиоматические теории *явно заданными*. Опять-таки не будем давать строгого математического определения яв-

но заданной аксиоматической теории, читатель может считать, что это просто одна из рассмотренных нами теорий.

Фиксируем некоторый обширный алфавит Σ_0 такой, что выводы во всех явно заданных (интересующих нас) формальных аксиоматических теориях записываются в виде слов в алфавите Σ_0.

Для явно заданной формальной аксиоматической теории T рассмотрим предикат $\mathrm{Prf}_T(y, x)$, где x, y суть слова в алфавите Σ_0. А именно $\mathrm{Prf}_T(y, x)$ истинно тогда и только тогда, когда y есть дерево вывода теории T с нижней формулой x. Важный факт состоит в том, что это рекурсивный предикат. Для конкретной теории, например для ZF, это может быть аккуратно проверено, путем построения соответствующей машины Тьюринга, но процедура распознавания истинности этого предиката должна быть и без того ясной: по данному слову y следует сначала выяснить, является ли это слово выводом теории T, и затем нужно определить, верно ли, что нижней формулой этого вывода является формула x.

Для явно заданной теории T рассмотрим предикат $\mathrm{Pr}_T(x)$, где x — слово в алфавите Σ_0. А именно $\mathrm{Pr}_T(x)$ истинно тогда и только тогда, когда x есть формула, выводимая в теории T. Очевидно,

$$\mathrm{Pr}_T(x) \Leftrightarrow \exists\, y \mathrm{Prf}_T(y, x).$$

Отсюда следует

Теорема. *Множество формул, выводимых в явно заданной формальной аксиоматической теории T, рекурсивно-перечислимо. В частности, рекурсивно-перечислимо множество формул, выводимых в исчислении предикатов явно заданного языка.*

▷ См. § 3, п. 4. ◁

Множество всех предложений, выводимых в теории T, обозначим через $[T]$. Для явно заданных теорий это — рекурсивно-перечислимое множество. Теория называется *разрешимой*, если это множество оказывается рекурсивным. Известно, что теории Ar, Ar2, ZF неразрешимы. Замечательно, что некоторые важные формальные аксиоматические теории разрешимы. Такова, например, элементарная теория действительных чисел (см. [5]).

Обозначим через $\mathrm{Th}_{\mathrm{Ar}}(\omega)$ множество всех предложений языка Ar, истинных в стандартной модели ω. Известно, что это множество не является даже рекурсивно-перечислимым.

В силу известной теоремы Гёделя о полноте множество всех логических законов языка Ω совпадает с множеством формул, выводимых в исчислении предикатов этого языка. Таким образом, для явно заданного языка множество всех его логических законов оказывается рекурсивно-перечислимым. Для рассмотренных нами до сих пор языков множество логических законов не является рекурсивным. Но можно указать простые языки, для которых это множество рекурсивно. Таким, например, будет язык с одним сортом переменных, без констант и функциональных символов и с конечным набором *одноместных* предикатов (так называемая теория *одноместных предикатов*).

§ 4. Примитивно-рекурсивные функции, гёделева нумерация, арифметика с примитивно-рекурсивными термами

1. Определим теперь важный класс общерекурсивных арифметических функций. Функции этого класса называются *примитивно-рекурсивными*.

С этой целью введем индуктивно понятие *примитивно-рекурсивного (п. р.) описания*. Каждое п. р. описание представляет собой слово вида $(k, l, \ldots)$, где k, l — натуральные числа. Число l называется количеством аргументов описания, $l > 0$. Каждому п. р. описанию одновременно сопоставляется арифметическая функция — примитивно-рекурсивная функция, *имеющая данное описание*. Определение содержит семь пунктов, первые три пункта составляют базис индукции, а последние представляют собой индуктивный шаг, показывая, как можно строить новые п. р. описания из уже имеющихся.

1) $(1, 1), F(x) = x + 1$.
2) $(2, 1), F(x) = x$.
3) $(3, 1, m), F(x) = m$ для произвольного натурального числа m.
4) Пусть $l > 0$, $1 \leqslant i_1, \ldots, i_s \leqslant l$ и g — п. р. описание с s аргументами, причем g сопоставлена функция G. Тогда можно определить новое п. р. описание $(4, l, g, i_1, \ldots, i_s)$, которому сопоставляется функция

$$F(x_1, \ldots, x_l) = G(x_{i_1}, \ldots, x_{i_s}).$$

Мы говорим, что F получена из G путем перестановки, отождествления и введения фиктивных аргументов.

5) Пусть g — п. р. описание с l аргументами, которому сопоставлена функция G, и h — п. р. описание с p аргументами, которому сопоставлена функция H. Тогда можно определить новое п. р. описание $(5, l + p - 1, g, h)$, которому сопоставляется функция

$$F(y_1, \ldots, y_p, x_2, \ldots, x_l) = G(H(y_1, \ldots, y_p), x_2, \ldots, x_l).$$

Мы говорим, что F получена из G и H подстановкой.

6) Пусть g — п. р. описание с двумя аргументами, которому сопоставлена функция G, и m — произвольное натуральное число. Тогда можно образовать новое п. р. описание $(6, 1, g, m)$, которому сопоставляется функция F, удовлетворяющая следующим тождествам:

$$\begin{cases} F(0) = m, \\ F(x + 1) = G(x, F(x)). \end{cases}$$

Мы говорим, что F получается из G и m с помощью примитивной рекурсии.

7) Пусть h — п. р. описание с m аргументами и g — п. р. описание с $m+2$ аргументами. Тогда можно определить новое п. р. описание $(7, m+1, g, h)$, которому сопоставляется функция F такая, что

$$\begin{cases} F(0, x_1, \ldots, x_m) = H(x_1, \ldots, x_m), \\ F(x+1, x_1, \ldots, x_m) = G(x, F(x, x_1, \ldots, x_m), x_1, \ldots, x_m). \end{cases}$$

В этой ситуации мы также говорим, что F получена из функций G и H примитивной рекурсией.

Арифметическая функция называется примитивно-рекурсивной, если она сопоставлена по указанным выше правилам какому-либо п. р. описанию.

Упражнение. Обозначим через $+$ примитивно-рекурсивную функцию от двух аргументов, имеющую следующее п. р. описание:

$$(7, 2(4, 3(1, 1), 2), (2, 1)).$$

Убедитесь, что выполняются следующие тождества:

$$y + 0 = y;$$
$$y + (x+1) = (y+1) + 1.$$

Постройте естественное п. р. описание для функции умножения двух натуральных чисел.

Совершенно ясно, что всякая п. р. функция является вычислимой, так как процесс определения такой функции с помощью примитивно-рекурсивного описания дает одновременно и способ вычисления значений функции для любых числовых значений ее аргументов. Точный математический факт состоит в том, что *всякая примитивно-рекурсивная функция — общерекурсивна*. Доказательство состоит в том, чтобы указать соответствующую машину Тьюринга для каждого примитивно-рекурсивного описания. Это построение осуществляется индукцией по длине рассматриваемого п. р. описания.

Обратное, как мы увидим дальше, неверно: существуют общерекурсивные функции, не являющиеся примитивно-рекурсивными. Тем не менее п. р. функции образуют весьма обширный класс вычислимых функций, замкнутый относительно многих естественных операций: все практически определяемые общерекурсивные функции, как правило, оказываются примитивно-рекурсивными.

Арифметический предикат $P(x_1, \ldots, x_n)$ назовем *примитивно-рекурсивным*, если существует примитивно-рекурсивная функция $f(x_1, \ldots, x_n)$, принимающая в качестве значений лишь 0 и 1, и такая, что

$$P(x_1, \ldots, x_n) \Leftrightarrow f(x_1, \ldots, x_n) = 1.$$

Мы часто будем опускать громоздкую проверку того, что те или иные конкретные функции или предикаты являются примитивно-рекурсивными. Подробные методы для такой проверки развиваются, например, в книгах [3, 4, 18].

2. С помощью примитивно-рекурсивных функций можно определить взаимно однозначное соответствие между парами натуральных чисел и натуральными числами.

Точнее, можно определить три п. р. функции $j(x, y)$, $j_1(z)$, $j_2(z)$ такие, что выполняются следующие тождества:

$$j_1(j(x, y)) = x,$$
$$j_2(j(x, y)) = y,$$
$$j(j_1(z), j_2(z)) = z.$$

Например, можно определить

$$j(x, y) = (\max{}^2\{x, y\} + y) + (\max\{x, y\} - x).$$

Тогда дополнительно выполняются соотношения:

$$j(0, 0) = 0, \quad x \leqslant j(x, y), \quad y \leqslant j(x, y).$$

Далее, нумерация n-ок натуральных чисел при каждом n может быть введена, например, с помощью следующих примитивно-рекурсивных функций:

$$\nu_1(x) = x,$$
$$\nu_2(x_1, x_2) = j(x_1, x_2),$$
$$\nu_{n+1}(x_1, x_2, \ldots, x_{n+1}) = j(x_i, \nu_n(x_2, \ldots, x_n)),$$

для которых имеются соответствующие обратные п. р. функции

$$\delta_i^n(\nu_n(x_1, \ldots, x_n)) = x_i,$$

где $n \geqslant 1$, $1 \leqslant i \leqslant n$.

Наконец, можно ввести единое примитивно-рекурсивное взаимно однозначное соответствие между n-ками натуральных чисел при всех n и натуральными числами. А именно для каждого натурального $n \geqslant 1$ определим

$$c(x_0, \ldots, x_{n-1}) = j(n - 1, \nu_n(x_0, \ldots, x_{n-1})) + 1,$$

а пустому набору натуральных чисел, при $n = 0$, сопоставим число 0.

Таким образом, натуральные числа в зависимости от способа кодирования можно отождествлять с парами, тройками и произвольными кортежами натуральных чисел.

Упомянем еще несколько примитивно-рекурсивных функций в связи с нашей нумерацией. Двуместная п. р. функция $x*y$ соединения кортежей такова, что

$$c(x_0, \ldots, x_{m-1}) * c(y_0, \ldots, y_{n-1}) = c(x_0, \ldots, x_{m-1}, y_0, \ldots, y_{n-1}),$$
$$x * 0 = 0 * x = x.$$

Двуместная п. р. функция $[x]_z$ «высекает» элемент кортежа x: $[0]_z = 0$, $[c(x_0, x_1, \ldots, x_{n-1}]_z = x_z$ при $z < n$ и $[c(x_0, x_1, \ldots, x_{n-1})]_z = 0$ при $z \geqslant n$. Примитивно-рекурсивная функция $\mathrm{lh}\,(x)$ определяет длину кортежа:

$$\mathrm{lh}\,(0) = 0, \quad \mathrm{lh}\,(c(x_0, x_1, \ldots, x_{n-1})) = n.$$

3. Мы намерены систематическим образом нумеровать натуральными числами слова в различных алфавитах, и прежде всего нас интересуют слова в алфавите Σ_0 (см. § 3, п. 7), который мы назовем *основным алфавитом*. Будем считать, что основной алфавит содержит буквы q и $|$, так что в нем можно естественно записывать наборы натуральных чисел, если отождествлять натуральные числа со словами в алфавите $|$.

Фиксируем бесконечную последовательность различных символов-букв: $a_0, a_1, a_2, \ldots$, которую назовем *основной последовательностью букв*. Алфавит назовем *простым*, если он состоит из конечного числа букв основной последовательности. Простой алфавит назовем *приведенным*, если он содержит буквы основной последовательности лишь с нечетными номерами. Будем считать, что алфавит Σ_0 содержит ровно k букв и эти буквы встречаются в основной последовательности в качестве первых k букв с нечетными номерами, т. е. алфавит Σ_0 состоит в точности из букв $a_1, a_3, \ldots, a_{2k+1}$. Таким образом, основной алфавит является приведенным.

Пусть A — слово в простом алфавите, имеющее вид $a_{i_1}a_{i_2}\ldots a_{i_m}$. Сопоставим этому слову натуральное число $\gamma A = c(i_1, \ldots, i_m)$. Для пустого слова положим $\gamma\Lambda = 0$. Натуральное число γA назовем *гёделевым номером* слова A. Отображение γ устанавливает взаимно однозначное соответствие между всеми словами в простых алфавитах и натуральными числами.

Далее мы желали бы нумеровать натуральными числами машины Тьюринга. Нас интересуют главным образом машины, обрабатывающие слова в основном алфавите, т. е. вычисляющие функции типа $\Sigma_0^*\ddot{\to}\Sigma_0^*$, но некоторая сложность возникает из-за того, что такие машины могут содержать и другие буквы, используемые, например, в промежуточных вычислениях. Машину Тьюринга назовем *приведенной*, если ее внешний алфавит и алфавит ее внутренних состояний суть приведенные алфавиты.

Лемма. *Для каждой машины Тьюринга M, вычисляющей функцию f: $\Sigma_0^*\ddot{\to}\Sigma_0^*$, может быть построена приведенная машина Тьюринга M', вычисляющая ту же самую функцию.*

▷ Достаточно взаимно однозначным образом заменить все буквы внутреннего и внешнего алфавитов машины M, отличные от букв основного алфавита, на некоторые буквы из основной последовательности с нечетными номерами. ◁

В частности, если $\Delta_1, \Delta_2, \ldots, \Delta_k, \Delta$ суть алфавиты, включенные в основной алфавит Σ_0 и не содержащие буквы q, а машина M вычисляет функцию f: $\Delta_1^* \times \ldots \times \Delta_k^*\ddot{\to}\Delta^*$, то может быть построена приведенная машина M', вычисляющая ту же функцию.

Пусть теперь M — приведенная машина Тьюринга,

$$M = \langle \Sigma, S, \Pi, q_0, q_1, a_0 \rangle.$$

Можно трактовать тогда M как слово в *простом* алфавите. А именно будем считать, что буквы $\to, R, L$ участвующие в написании команд машины, входят в основную последовательность в качестве букв с *четными*

номерами. Например, это есть соответственно буквы a_0, a_2, a_4. Машина M как слово в простом алфавите получится, если написать подряд друг за другом следующие слова:

1) последовательность букв Σ (для определенности можно считать, что буквы записываются в порядке возрастания номеров в основной последовательности);
2) разделительная буква с четным номером (например, это может быть a_6);
3) последовательность букв S;
4) разделительная буква a_6;
5) последовательность команд Π, $k_1 k_2 \ldots k_m$;
6) разделительная буква a_6;
7) слово $q_0 q_1 a_0$.

Таким образом, каждую приведенную машину Тьюринга можно рассматривать как слово в простом алфавите, и, следовательно, каждая такая машина имеет определенный гёделев номер.

Далее, конечные протоколы работы приведенных машин Тьюринга также очевидным образом можно трактовать как слова в простом алфавите и, следовательно, приписать таким протоколам гёделевы номера.

4. Пусть $\Delta_1, \ldots, \Delta_k, \Delta$ — алфавиты, включенные в основной алфавит и не содержащие разделительной буквы q. Пусть f — функция типа $\Delta_1^* \times \ldots \times \Delta_k^* \ddot{\to} \Delta^*$. Определим тогда функцию f^γ: $\omega \times \ldots \times \omega \ddot{\to} \omega$, «моделирующую» работу функции на гёделевых номерах. А именно:

1) если набор $m_1, \ldots, m_k$ натуральных чисел таков, что хоть одно из m_i не является гёделевым номером слова алфавита Δ_i, то $f(m_1, \ldots, m_k) = 0$;
2) для всякого набора слов $A_1, \ldots, A_k, A$, где $A_i \in \Delta_i^*$, $A \in \Delta$, имеем $f(A_1, \ldots, A_k) = A \Leftrightarrow f^\gamma(\gamma A_1, \ldots, \gamma A_k) = \gamma A$.

Аналогично для всякого словарного предиката P типа $\Delta_1^* \times \ldots \times \Delta_k^*$ можно ввести моделирующий арифметический предикат P^γ такой, что

1) если набор $m_1, \ldots, m_k$ таков, что хоть одно из натуральных чисел m_i не является гёделевым номером слова алфавита Δ_i, то $P(m_1, \ldots, m_k)$ ложно;
2) для всякого набора слов $A_1, \ldots, A_k, A_i \in \Delta_i^*$: $P(A_1, \ldots, A_k) \Leftrightarrow P^\gamma(\gamma A_1, \ldots, \gamma A_k)$.

Лемма. *Функция f вычислима тогда и только тогда, когда вычислима функция f^γ.*
Предикат P рекурсивен (рекурсивно-перечислим) тогда и только тогда, когда рекурсивен (рекурсивно-перечислим) предикат P^γ.

Громоздкое доказательство, состоящее в построении необходимых машин по исходным машинам, мы опускаем.

5. Отождествим натуральные числа со словами в алфавите |. Тогда гёделев номер натурального числа как слова отнюдь не совпадает с самим этим натуральным числом (за исключением нуля). Но соответствие между натуральным числом и его гёделевым номером является примитивно-рекурсивным. Точнее, могут быть построены две одноместные примитивно-рекурсивные функции Gd и Gd^{-1} такие, что для всякого натурального числа m:

$$\mathrm{Gd}(m) = \gamma m, \quad \mathrm{Gd}^{-1}(\gamma m) = m.$$

6. Гёделева нумерация открывает возможность говорить о сложных конструктивных объектах на языке арифметики. Мы хотели бы записывать различные свойства этих объектов на языке Ar, а затем доказывать их в формальной аксиоматической теории Ar. Основная трудность при осуществлении этой программы состоит в том, что в теории Ar мало функций — лишь сложение и умножение. Поэтому мы сформулируем более выразительную аксиоматическую теорию Ar^+, в которой, грубо говоря, имеется функциональный символ для каждой примитивно-рекурсивной функции.

Язык Ar^+ содержит один сорт переменных $x, y, z, \ldots$, константу 0 и для каждого примитивно-рекурсивного описания p от l аргументов — функциональный символ от l аргументов. Для конкретности можно считать, что само п. р. описание p, как слово в алфавите (,), ,, |, и является функциональным символом Ar^+. В частности, в Ar^+ имеются и все функциональные символы Ar (см. введение). Например, S имеет п. р. описание (1, 1), + имеет п. р. описание (7, 2, (4, 3, (1, 1), 2), (2, 1)).

Термы языка Ar^+ строятся последовательно из переменных и константы 0 с помощью функциональных символов. Точнее, индуктивное определение терма языка Ar^+ состоит из следующих трех пунктов:

1) всякая переменная есть терм;
2) константа 0 есть терм;
3) если f — функциональный символ от l аргументов и уже построены некоторые термы $t_1, \ldots, t_l$, то можно построить новый терм $f(t_1, \ldots, t_l)$.

Атомарные формулы Ar^+ имеют вид $(t = r)$, где t, r — произвольные термы языка Ar^+.

Таким образом, язык Ar естественно рассматривать как часть языка Ar^+: всякое выражение Ar является в то же время и выражением языка Ar^+.

Нелогические аксиомы Ar^+, так же как и нелогические аксиомы Ar, делятся на три группы: аксиомы равенства, аксиомы Пеано и определяющие аксиомы для п. р. описаний. Аксиомы равенства и аксиомы Пеано имеют тот же вид, что и в Ar, с той лишь разницей, что в схеме аксиом индукции теперь допускается произвольная формула языка Ar^+. Определяющие же аксиомы для п. р. описаний просто копируют те тожде-

ства, которым должны по определению удовлетворять те п. р. функции, которые имеют эти описания.

Если m — натуральное число, то через $\widetilde{m}$ или через $m\tilde{}$ обозначим терм Ar вида $SS\ldots S0$, где функциональный символ S берется m раз. Это естественное изображение числа m в языке Ar. Примерами аксиом теории Ar^+ являются следующие формальные равенства:

$$(2, 1)(x) = x;$$
$$(3, 1, m)(x) = \widetilde{m};$$
$$(6, 1, g, m)(0) = \widetilde{m};$$
$$(6, 1, g, m)(Sx) = g(x, (6, 1, g, m)(x)),$$

где g — произвольное п. р. описание с двумя аргументами.

Таким образом, теория Ar составляет часть теории Ar^+: все, что выводится в Ar, выводится и в Ar^+.

Ar^+ является уже весьма выразительной теорией и позволяет записать и доказать практически все обычные факты, относящиеся к теории чисел. В частности, при наличии некоторого навыка в построении формальных выводов несложно установить выводимость в Ar^+ всех необходимых нам свойств гёделевых номеров слов в простых алфавитах.

7. Замечательно, что, как обнаружил Гёдель, теории Ar и Ar^+ оказываются по существу эквивалентными. Это объясняется тем, что, используя некоторые теоретико-числовые соображения, удается равенства сложных термов языка Ar^+ изобразить формулами теории Ar, т. е. формулами, содержащими лишь сложение и умножение.

Точнее, для всякой формулы A языка Ar^+ определяется ее перевод-формула A^0 языка Ar, содержащая те же параметры, что и формула A. Далее, для каждого терма t языка Ar^+ и переменной y определяется формула $(y = t)^*$ языка Ar с теми же параметрами, что и формула $y = t$. Этот перевод обладает многими свойствами, которые и следует от него ожидать. Мы перечислим их в следующих шести леммах.

Лемма 1. *Если A — формула* Ar, *t — терм* Ar, *то в* Ar *выводимы эквивалентности*:

$$A^0 \equiv A,$$
$$(y = t)^* \equiv (y = t).$$

Лемма 2. *Если A — формула* Ar^+ *и t — терм* Ar^+, *то в* Ar^+ *выводимы эквивалентности*:

$$(y = t)^* \equiv (y = t).$$

Лемма 3. *Если A — формула* Ar^+, *t — терм* Ar^+, *то имеют место следующие эквивалентности*:

$$\mathrm{Ar}^+ \vdash A \Leftrightarrow \mathrm{Ar} \vdash A^0,$$
$$\mathrm{Ar}^+ \vdash (y = t) \Leftrightarrow \mathrm{Ar} \vdash (y = t)^*.$$

Лемма 4. *Если A — формула* Ar, *то*

$$\mathrm{Ar}^+ \vdash A \Leftrightarrow \mathrm{Ar} \vdash A.$$

Последняя лемма показывает, что относительно узкого языка Ar обе теории эквивалентны. Дополнительно можно отметить, что указанный перевод сохраняет логическую структуру формул. Это обстоятельство проявляется в том, что имеют место следующие две леммы.

Лемма 5. *В теории* Ar *выводимы эквивалентности*

$$(A \wedge B)^0 \equiv A^0 \wedge B^0,$$
$$(A \vee B)^0 \equiv A^0 \vee B^0,$$
$$(A \supset B)^0 \equiv A^0 \supset B^0,$$
$$(\neg A)^0 \equiv \neg A^0,$$
$$(\forall x A)^0 \equiv \forall x A^0,$$
$$(\exists x A)^0 \equiv \exists x A^0.$$

Здесь A, B — произвольные формулы языка Ar^+.

Лемма 6. *В теории* Ar *выводимы следующие эквивалентности*

$$(t = r)^0 \equiv \exists y((y = t)^* \wedge (y = r)^*),$$
$$(A(x \parallel t))^0 \equiv \exists y((A(x \parallel y))^0 \wedge (y = t)^*),$$
$$(z = r(x \parallel t))^* \equiv \exists y((z = r(x \parallel y))^* \wedge (y = t)^*).$$

Здесь A — формула Ar^+, t, r — *термы* Ar^+ *и переменная y не входит свободно в A, r, t.*

Мы не будем заниматься точной формулировкой перевода и доказательством лемм 1–6. Необходимую технику для этого заинтересованный читатель может найти в руководствах [3, 4].

Заметим в заключение, что теория Ar^+, так же как и теория Ar, является явно заданной. Формулы, термы, выводы теории Ar^+ естественно трактуются как слова в основном алфавите и, следовательно, имеют гёделевы номера.

§ 5. Некоторые теоремы общей теории алгорифмов

1. Универсальная функция. Для каждого $n \geqslant 1$ рассмотрим $(n+2)$-местный *предикат Клини*, определенный на натуральных числах:

$$T_n(e, x_1, \ldots, x_n, z).$$

А именно, $T_n(e, x_1, \ldots, x_n, z)$ истинно тогда и только тогда, когда e есть гёделев номер некоторой (приведенной) машины Тьюринга M,

а z есть гёделев номер конечного протокола вычислений Z для машины M, на вход которой подан набор чисел $x_1, \ldots, x_n$ (т. е. подано слово $x_1 q \ldots q x_n$, где натуральные числа рассматриваются как слова в алфавите $|$), причем Z содержит заключительную конфигурацию.

Довольно очевидно, что T_n — разрешимый предикат, так как по данным $e, x_1, \ldots, x_n, z$ можно судить, верно T_n или нет. Важный факт (который мы оставим без проверки, детали читатель может найти, например, в [2]) состоит в том, что этот предикат *примитивно-рекурсивен*, т. е. существует примитивно-рекурсивная функция $t_n(e, x_1, \ldots, x_n, z)$, принимающая в качестве значений лишь 0 и 1, и такая, что

$$T_n(e, x_1, \ldots, x_n, z) \Leftrightarrow t_n(e, x_1, \ldots, x_n, z) = 1.$$

Может быть построена также одноместная примитивно-рекурсивная функция $U(z)$ такая, что если z — гёделев номер конечного протокола вычислений Z некоторой (приведенной) машины Тьюринга M и Z содержит заключительную конфигурацию K такую, что на ленте K записано натуральное число k, то $U(z) = k$. Если же z не имеет указанного вида, то $U(z) = 0$.

Если $P(y, x_1, \ldots, x_s)$ — общерекурсивный (в частности, примитивно-рекурсивный) предикат, то можно определить частично-рекурсивную функцию $f(x_1, \ldots, x_s)$ следующей инструкцией: для данного набора $x_1, \ldots, x_s$ выясняем последовательно, истинно ли $P(0, x_1, \ldots, x_s)$, $P(1, x_1, \ldots, x_s)$, $P(2, x_1, \ldots, x_s)$, ... Как только дойдем до наименьшего m такого, что $P(m, x_1, \ldots, x_s)$ истинно, положим $f(x_1, \ldots, x_s) = m$. Если же такого m не существует, то функция $f(x_1, \ldots, x_s)$ по определению на наборе $x_1, \ldots, x_s$ считается неопределенной. Приведенную инструкцию можно оформить в виде программы некоторой машины Тьюринга и, таким образом, доказать частичную рекурсивность f.

Будем говорить, что функция f получена из предиката P *операцией минимизации*, а значение $f(x_1, \ldots, x_s)$ обозначим через $\mu y P(y, x_1, \ldots, x_s)$ (читается: «наименьшее y такое, что $P(y, x_1, \ldots, x_s)$»).

Уточним еще понятие подстановки для частично определенных функций. Пусть, например, g — одноместная, а f — s-местная частичные функции. Рассмотрим функцию h, определяемую следующим образом: $h(x_1, \ldots, x_s)$ определено тогда и только тогда, когда: 1) определено $f(x_1, \ldots, x_s)$ и 2) определено значение $g(f(x_1, \ldots, x_s))$, и в этом случае

$$h(x_1, \ldots, x_s) = g(f(x_1, \ldots, x_s)).$$

В такой ситуации мы говорим, что функция h *получена подстановкой* функции f в функцию g. Такое определение подстановки для частичных функций обеспечивает, что функция h оказывается частично-рекурсивной, коль скоро таковы функции f и g.

Кратко определение h можно записать в виде

$$h(x_1, \ldots, x_s) \simeq g(f(x_1, \ldots, x_s)).$$

Знак $\simeq$ (условное равенство) здесь и далее означает, что выражение слева определено тогда и только тогда, когда определено выражение справа, и в случае определенности эти выражения совпадают.

Определим теперь для каждого $n \geqslant 1$ $(n+1)$-местную частично-рекурсивную функцию $\mathscr{U}_n$ таким образом, что

$$\mathscr{U}_n(e, x_1, \ldots, x_n) \simeq U(\mu z T_n(e, x_1, \ldots, x_n, z)).$$

Основное свойство $\mathscr{U}_n$ выражается следующей классической *теоремой Клини о нормальной форме.*

Теорема. *Для всякой частично-рекурсивной функции f найдется натуральное m такое, что для всех $x_1, \ldots, x_n$:*

$$f(x_1, \ldots, x_n) \simeq \mathscr{U}_n(m, x_1, \ldots, x_n).$$

▷ В качестве такого m можно взять гёделев номер машины Тьюринга, вычисляющей функцию f. Требуемое утверждение вытекает из определения предиката T_n и функции f. ◁

Пусть K — произвольный класс n-местных (вообще говоря, частичных) функций. Функция $g(x, x_1, \ldots, x_n)$ называется *универсальной для класса K*, если:

1) для всякого натурального m соответствующая n-местная функция $g(m, x_1, \ldots, x_n)$ принадлежит K;
2) для всякой функции $f(x_1, \ldots, x_n)$ из K найдется натуральное m такое, что n-местная функция $g(m, x_1, \ldots, x_n)$ совпадает с f.

Непосредственным следствием предыдущей теоремы является следующая

Теорема об универсальной функции. *Частично-рекурсивная функция $\mathscr{U}_n$ является универсальной для класса всех n-местных частично-рекурсивных функций.*

Укажем сразу же и некоторый отрицательный результат.

Теорема. *Не существует $(n+1)$-местной частично-рекурсивной функции, универсальной для класса всех n-местных общерекурсивных функций.*

▷ Ограничимся случаем $n = 1$. Допустим, что такая функция $G(x, x_1)$ существует. Так как при каждом m функция $G(m, x_1)$ общерекурсивна, то функция $G(x, x_1)$ определена при всех x, x_1 и, таким образом, также является общерекурсивной. Но тогда общерекурсивна и функция $g(x) = G(x, x) + 1$. Рассмотрим m такое, что $g(x) = G(m, x)$. Имеем

$$G(m, x) = g(x) = G(x, x) + 1.$$

Подставляя сюда вместо x число m, получим противоречие. ◁

Идею этого доказательства можно использовать для построения общерекурсивной функции, не являющейся примитивно-рекурсивной.

Определим функцию $g(y, x)$ следующей инструкцией: если y не есть гёделев номер п. р. описания, то $g(y, x) = 0$; если же y есть гёделев номер п. р. описания функции F, то $g(y, x) = F(x)$.

Указанную инструкцию можно преобразовать в машину Тьюринга и, таким образом, доказать, что g — общерекурсивная функция. Рассмотрим теперь общерекурсивную функцию F такую, что $F(x) = g(x, x) + 1$.

Лемма. *Общерекурсивная функция F не является примитивно-рекурсивной.*

▷ Предположим противное, и пусть m — гёделев номер п. р. описания функции F. Тогда

$$g(m, x) = F(x) = g(x, x) + 1.$$

Подставляя вместо x натуральное m, получим противоречие. ◁

Для каждого натурального m соответствующую n-местную частично-рекурсивную функцию $U(\mu z T_n(m, x_1, \ldots, x_n, z))$ мы обозначим через $\{m\}^n$. Число m назовем *гёделевым номером частично-рекурсивной функции* $\{m\}^n$. Таким образом, всякая частично-рекурсивная функция имеет некоторый гёделев номер. Индекс n в обозначении $\{m\}^n$ будем иногда опускать (и очень надеемся, что читатель не спутает это традиционное обозначение частично-рекурсивной функции с обозначением одноэлементного множества в теории множеств).

Из определения предиката T_n очевидно, что

$$!\{m\}^n(x_1, \ldots, x_n) \Leftrightarrow \exists z T_n(m, x_1, \ldots, x_n, z).$$

Напомним, что выражение слева означает, что функция $\{m\}^n$ определена на наборе $x_1, \ldots, x_n$.

Лемма. *Для всякого рекурсивно-перечислимого множества A натуральных чисел существует частично-рекурсивная функция g такая, что g принимает лишь одно значение* 1, *и для всякого x*

$$!g(x) \Leftrightarrow x \in A.$$

▷ Если A рекурсивно-перечислимо, то существует машина Тьюринга M, вычисляющая предикат $x \in A$ согласно определению § 3, п. 3. Определим теперь функцию g инструкцией: $g(x) = 1$ тогда и только тогда, когда $M(x) = 1$; во всех остальных случаях g не определена. Эту инструкцию можно оформить в виде некоторой машины Тьюринга, вычисляющей g. ◁

Если m — гёделев номер функции g, о которой идет речь в лемме, то, очевидно,

$$x \in A \Leftrightarrow \exists z T_1(m, x, z).$$

Натуральное m, для которого выполняется эта эквивалентность, мы назовем *гёделевым номером рекурсивно-перечислимого множества A*. Рекурсивно-перечислимое множество с гёделевым номером m обозначим через $\mathscr{W}_m$. Таким образом, по определению

$$x \in \mathscr{W}_m \Leftrightarrow \exists z T_1(m, x, z).$$

2. Невычислимые множества и функции.

Теорема. *Множество натуральных чисел* $\{x \mid \exists z T_1(x, x, z)\}$ *рекурсивно-перечислимо, но не рекурсивно.*

▷ Рекурсивная перечислимость рассматриваемого множества следует из леммы в § 3, п. 4 и рекурсивности предиката T_1. Если бы наше множество было рекурсивным, то рекурсивно было бы и его дополнение $A = \{x \mid \neg\exists z T_1(x, x, z)\}$, а следовательно, A было бы и рекурсивно-перечислимым. Покажем, однако, что множество A отлично от всякого рекурсивно-перечислимого множества. В самом деле, рассмотрим произвольное рекурсивно-перечислимое множество $\mathscr{W}_m$ и предположим, что $A = \mathscr{W}_m$. Тогда для всякого x

$$\exists z T_1(m, x, z) \Leftrightarrow x \in \mathscr{W}_m \Leftrightarrow x \in A \Leftrightarrow \neg\exists z T_1(x, x, z).$$

Подставляя в эту цепочку эквивалентностей вместо x число m, приходим к противоречию. ◁

Следствие. *Множество натуральных чисел* $\{x \mid \neg\exists z T_1(x, x, z)\}$ *не является рекурсивно-перечислимым.*

▷ Фактически это уже доказано нами выше, но следует также и непосредственно из формулировки предыдущей теоремы и теоремы Поста § 3, п. 6. ◁

Следствие. *Существует всюду определенная невычислимая функция.*

▷ Определим функцию g следующим образом: для каждого натурального x положим $g(x) = 1$, если $\exists z T_1(x, x, z)$, и $g(x) = 0$, если $\neg\exists z T_1(x, x, z)$. g — всюду определена и если бы была вычислимой, то оказалась бы общерекурсивной функцией. Но $g(x) = 1 \Leftrightarrow \exists z T_1(x, x, z)$ и предикат справа оказался бы рекурсивным. ◁

3. Проблема остановки. Мы говорим, что *проблема остановки* для машины Тьюринга M *разрешима*, если существует общерекурсивная функция h, принимающая лишь два значения 0 или 1, и такая, что $h(x) = 1$ тогда и только тогда, когда машина M, работая на входе x, дает конечный протокол вычислений.

Неформально говоря, проблема остановки разрешима, если существует «распознаватель остановки» h, узнающий по x, остановится машина M на x или нет.

Теорема. *Существует машина Тьюринга M с неразрешимой проблемой остановки.*

▷ Пусть $a(x)$ — общерекурсивная функция, тождественно равная нулю. Рассмотрим частично-рекурсивную функцию $g(x)$, равную $a(\mu z T_1(x, x, z))$. Тогда $!g(x) \Leftrightarrow \exists z T_1(x, x, z)$ и $!g(x) \Rightarrow g(x) = 0$. Пусть M' — приведенная машина Тьюринга, вычисляющая g. «Подправим» программу машины M' и получим машину M такую, что

1) M также вычисляет g,
2) если машина M' на входе x дает конечный протокол вычислений без заключительной конфигурации или конечный протокол, в заключительной конфигурации которого на ленте записано непустое слово, то машина M на входе x не остановится, т. е. порождает бесконечный протокол вычислений.

Такую модификацию машины M' всегда можно произвести, дописав несколько команд снизу в программе M', изменив ее заключительное состояние и расширив алфавит.

Тогда $\exists z T_1(x, x, z) \Leftrightarrow M$ остановится на x. Теперь невозможность соответствующей функции h для M следует из теоремы п. 2. ◁

Подчеркнем, что для M неразрешима именно *массовая проблема* остановки: не существует *единого* алгорифма h, который бы узнавал, остановится ли M на x *для всякого* натурального числа x. Если же исследователю предложить конкретное натуральное число m и спросить, верно ли, что M остановится на входе m, то нет оснований полагать, что наш исследователь не справится с этим вопросом по некотором размышлении. Невозможен лишь единый механический способ решения этого вопроса для всех m сразу.

4. Рекурсивно-неотделимые множества. Напомним, что через ω мы обозначаем множество всех натуральных чисел. Два множества A_0, $A_1 \subseteq \omega$ назовем *рекурсивно-отделимыми*, если существуют два рекурсивно-перечислимых множества B_0, B_1 такие, что

$$A_0 \subseteq B_0, \quad A_1 \subseteq B_1, \quad B_0 \cap B_1 = \varnothing, \quad B_0 \cup B_1 = \omega.$$

Про множества B_0 и B_1 мы будем говорить, что они *рекурсивно отделяют* множества A_0 и A_1. По теореме Поста (§ 3, п. 6) множества B_0 и B_1 в этом случае необходимо являются и рекурсивными.

Упражнение. Если множества A_0, A_1 рекурсивно-неотделимы и не пересекаются (т. е. $A_0 \cap A_1 = \varnothing$), то оба они не рекурсивны. Более того, всякое множество C такое, что $A \subseteq C$, $C \cap B = \varnothing$ так же не рекурсивно.

Определим два предиката:

$$W_0(x, y) \rightleftharpoons T_1(j_2 x, x, y) \wedge (\forall z \leqslant y)\neg T_1(j_1 x, x, z);$$
$$W_1(x, y) \rightleftharpoons T_1(j_1 x, x, y) \wedge (\forall z \leqslant y)\neg T_1(j_2 x, x, z).$$

Можно проверить, что оба предиката примитивно-рекурсивны.

Определим теперь два рекурсивно-перечислимых множества:

$$V_0 \rightleftharpoons \{x \mid \exists y W_0(x, y)\};$$
$$V_1 \rightleftharpoons \{x \mid \exists y W_1(x, y)\}.$$

Теорема. *Рекурсивно-перечислимые множества V_0, V_1 не пересекаются и являются рекурсивно-неотделимыми.*

▷ Допустим, что $x \in V_0$ и $x \in V_1$. Тогда найдутся y_0 и y_1 такие, что $W_0(x, y_0)$ и $W_1(x, y_1)$, т. е.

1) $T_1(j_2x, x, y_0)$;
2) $(\forall z \leqslant y_0)\neg T_1(j_1x, x, z)$;
3) $T_1(j_1x, x, y_1)$;
4) $(\forall z \leqslant y_1)\neg T_1(j_2x, x, z)$.

Из 1) и 4) следует, что $y_1 < y_0$, в то время как из 2) и 3) следует $y_0 < y_1$, и мы приходим к противоречию.

Итак, множества V_0 и V_1 не пересекаются.

Рассмотрим теперь произвольные перечислимые множества B_0B_1 такие, что $V_0 \subseteq B_0$, $V_1 \subseteq B_1$, $B_0 \cap B_1 = \varnothing$, и покажем, что в этом случае необходимо $B_0 \cup B_1 \neq \omega$.

Пусть B_0 имеет гёделев номер m_0 и B_1 — номер m_1. Положим $m = j(m_0, m_1)$. Мы утверждаем, что $m \notin B_0$ и $m \notin B_1$. Докажем, например, $m \notin B_0$ ($m \notin B_1$ доказывается аналогично).

С этой целью предположим противное и пусть $m \in B_0$. Тогда $m \in \mathscr{W}_{m_0}$, т. е. $\exists y T_1(m_0, m, y)$, и ввиду $m_0 = j_1m$

$$\exists y T_1(j_1m, m, y). \tag{1}$$

Далее, ввиду $m \in B_0$ и $B_0 \cap B_1 = \varnothing$ имеем

$$m \notin B_1, \tag{2}$$

т. е. $m \notin \mathscr{W}_{m_1}$, что означает $\neg\exists y T_1(m_1, m, y)$, что, в свою очередь, ввиду $m_1 = j_2m$ означает

$$\forall y \neg T(j_2m, m, y). \tag{3}$$

Из (1) и (3) следует

$$\exists y(T_1(j_1m, m, y) \wedge (\forall z \leqslant y)\neg T_1(j_2m, m, z)),$$

т. е. $\exists y W_1(m, y)$ и, следовательно, $m \in B_1$. Однако это противоречит утверждению (2). ◁

Теорема о непополнимой функции. *Существует частично-рекурсивная функция f, принимающая в качестве значений лишь 0 и 1, и такая, что не существует общерекурсивной функции h, пополняющей f, т. е. такой функции h, что для всякого x, для которого определено $f(x)$, имеет место $f(x) = h(x)$.*

▷ Согласно лемме § 5 п. 1 найдутся частично-рекурсивные функции g_0 и g_1 такие, что $x \in V_i \Leftrightarrow !g_i(x)$. Определим теперь частично-рекурсивную функцию f следующей инструкцией: для данного x вычисляем одновременно $g_0(x)$ и $g_1(x)$. Если определено $g_0(x)$, то положим $f(x) = 0$, если же определено $g_1(x)$, то положим $f(x) = 1$. Если же не определены обе функции, то считается неопределенной и $f(x)$. Заметим, что не могут быть одновременно определены оба значения $g_0(x)$ и $g_1(x)$, так как $V_0 \cap V_1 = \varnothing$.

Мы утверждаем, что функция f — искомая.

Предположим, что существует общерекурсивное пополнение функции f. Пусть это будет общерекурсивная функция h. Пусть a —

примитивно-рекурсивная функция такая, что $a(0) = 0$, $a(x+1) = 1$. Определим $h'(x) = a(h(x))$. Тогда h' является общерекурсивной функцией, принимающей лишь значения 0 и 1 и также пополняющей f. Определим, далее, рекурсивные множества:

$$B_0 = \{x \mid h'(x) = 0\}, \quad B_1 = \{x \mid h'(x) = 1\}.$$

Из определений легко видеть, что B_0, B_1 рекурсивно отделяют множества V_0, V_1, что невозможно по предыдущей теореме. ◁

5. Теорема о рекурсии. Фиксируем набор натуральных чисел

$$a = \langle e, k_1, \ldots, k_m \rangle$$

и определим для этого набора натуральное число t_a следующим образом. Построим приведенную машину M_a. А именно для всякого набора $y_1, \ldots, y_n$ натуральных чисел значение $M_a(y_1 q \ldots y_n q)$ определено тогда и только тогда, когда определена универсальная функция

$$\mathscr{U}_{m+n}(e, k_1, \ldots, k_m, y_1, \ldots, y_n),$$

и тогда

$$M_a(y_1 q \ldots q y_n) = \mathscr{U}_{m+n}(e, k_1, \ldots, k_m, y_1, \ldots, y_n).$$

Теперь в качестве t_a возьмем гёделев номер машины M_a.

Заметим теперь, что наша инструкция дает способ вычисления по набору a соответствующего t_a. Эту инструкцию можно оформить в виде машины Тьюринга. Таким образом, функция

$$S_n^m(e, x_1, \ldots, x_m) = t_{\langle e, x_1, \ldots, x_m \rangle}$$

является общерекурсивной. Более тщательный анализ показывает, что S_n^m является даже примитивно-рекурсивной функцией. Таким образом, имеет место

Лемма. *Может быть построена примитивно-рекурсивная функция S_n^m от $(m+1)$ аргументов такая, что для всякого набора натуральных чисел $e, x_1, \ldots, x_m, y_1, \ldots, y_n$ имеем*

$$\{e\}(x_1, \ldots, x_m, y_1, \ldots, y_n) \simeq \{S_n^m(e, x_1, \ldots, x_m)\}(y_1, \ldots, y_n).$$

Теорема Клини о рекурсии. *Для всякой частично-рекурсивной функции $\psi(z, x_1, \ldots, x_n)$ можно построить натуральное число e такое, что*

$$\{e\}(x_1, \ldots, x_n) \simeq \psi(e, x_1, \ldots, x_n).$$

▷ Рассмотрим частично-рекурсивную функцию

$$\varphi(y, x_1, \ldots, x_n) \simeq \psi(S_n^1(y, y), x_1, \ldots, x_n).$$

Пусть f — ее гёделев номер и $e = S_n^1(f, f)$. Мы утверждаем, что это e — искомое. В самом деле,

$$\{e\}(x_1, \ldots, x_n) \simeq \{S_n^1(f, f)\}(x_1, \ldots, x_n) \simeq \{f\}(f, x_1, \ldots, x_n) \simeq$$
$$\simeq \varphi(f, x_1, \ldots, x_n) \simeq \psi(S_n^1(f, f), x_1, \ldots, x_n) \simeq \psi(e, x_1, \ldots, x_n). \quad ◁$$

Элементы теории доказательств

§ 1. Неполнота и неразрешимость аксиоматических теорий

Мы установим неполноту и неразрешимость некоторых аксиоматических теорий. Большую часть доказательств мы проводим для конкретной аксиоматической теории Ar^+, но развитые методы, как мы увидим, будут применимы и ко многим другим теориям.

1. Теорема о неподвижной точке. Напомним, что если A — слово в простом алфавите, то через γA мы обозначаем его гёделев номер (гл. II, § 4, п. 3). Далее, если m — натуральное число, то через $\widetilde{m}$ или через $\widetilde{m}$ мы обозначим терм языка Ar^+, естественно изображающий натуральное число в языке Ar^+, т. е. терм вида $SS\ldots S0$, где функциональный символ S берется m раз (гл. II, § 4, п. 6). Таким образом, для каждого слова в простом алфавите можно определить терм — естественное изображение этого слова в Ar^+:

$$[A] \leftrightharpoons (\gamma A)\widetilde{\ }.$$

Пусть $t(x_1, \ldots, x_n)$, $r(x_1, \ldots, x_n)$ — термы Ar^+, где $x_1, \ldots, x_n$ — список различных переменных, среди которых содержатся все параметры термов t и r. Функциональные символы t и r задают примитивно-рекурсивные описания некоторых примитивно-рекурсивных функций и, таким образом, сами термы естественно определяют некоторые примитивно-рекурсивные функции $F(x_1, \ldots, x_n)$ и $G(x_1, \ldots, x_n)$ соответственно.

Лемма. *Для всяких натуральных* $k_1, \ldots, k_n$

1) *если* $F(k_1, \ldots, k_n) = G(k_1, \ldots, k_n)$, *то*

$$\mathrm{Ar}^+ \vdash t(\widetilde{k}_1, \ldots, \widetilde{k}_n) = r(\widetilde{k}_1, \ldots, \widetilde{k}_n);$$

2) *если* $F(k_1, \ldots, k_n) \neq G(k_1, \ldots, k_n)$, *то*

$$\mathrm{Ar}^+ \vdash \neg t(\widetilde{k}_1, \ldots, \widetilde{k}_n) = r(\widetilde{k}_1, \ldots, \widetilde{k}_n).$$

Мы не будем доказывать эту техническую лемму (см., например, [3, 4]). Суть ее состоит в том, что система Ar^+ обладает достаточными выразительными возможностями: произвольное примитивно-рекурсивное вычисление с конкретными натуральными числами выразимо в Ar^+.

Заметим, что мы отнюдь не утверждаем, например, что если $F(k_1, \ldots, k_n) = G(k_1, \ldots, k_n)$ для всех натуральных чиселz $k_1, \ldots, k_n$, то $\mathrm{Ar}^+ \vdash t(x_1, \ldots, x_n) = r(x_1, \ldots, x_n)$ со *свободными переменными* $x_1, \ldots, x_n$. Как мы увидим позже, это неверно и в общем случае. Речь идет лишь о выводимости формальных равенств с *конкретными натуральными числами* $k_1, \ldots, k_n$.

Вышеприведенную лемму называют леммой о нумерической выразимости примитивно-рекурсивных функций в Ar^+. Слово «нумерической» как раз подчеркивает, что речь идет о выводимости конкретных числовых равенств. Если t, r —замкнутые термы, то в стандартной модели ω они имеют определенное числовое значение. Из предыдущей леммы следует, что:

$$\text{если} \quad \omega \models t = r, \quad \text{то} \quad \mathrm{Ar}^+ \vdash t = r;$$
$$\text{если} \quad \omega \models \neg t = r, \quad \text{то} \quad \mathrm{Ar}^+ \vdash \neg t = r.$$

Теорема о неподвижной точке. *Пусть A — формула Ar^+ и x — переменная. Тогда может быть построена формула B такая, что*

$$\mathrm{Ar}^+ \vdash B \equiv A([B]).$$

Здесь $A([B]) \leftrightharpoons A(x \parallel [B])$.

▷ Фиксируем переменную x. Рассмотрим примитивно-рекурсивную функцию $\mathrm{SUB}(y, z)$ такую, что если y есть гёделев номер некоторой формулы C, то $\mathrm{SUB}(y, z)$ есть гёделев номер формулы $C(x \parallel z)$. Функция SUB имеет определенное примитивно-рекурсивное описание, и, следовательно, можно определить соответствующий ей терм $\mathrm{Sub}(y, z)$ теории Ar^+.

Теперь по данной формуле A построим формулу

$$A' \leftrightharpoons A(\mathrm{Sub}(x, x)). \tag{1}$$

и определим

$$B \leftrightharpoons A'([A']). \tag{2}$$

Отсюда следует, что

$$\gamma B = \mathrm{SUB}(\gamma A', \gamma A'),$$

и по предыдущей лемме тогда

$$\mathrm{Ar}^+ \vdash [B] = \mathrm{Sub}([A'], [A']). \tag{3}$$

Далее, мы видим, что в Ar^+ выводима следующая цепочка эквивалентностей:

$$B \equiv A'([A']) \equiv A'(\mathrm{Sub}([A'], [A'])) \equiv A([B]).$$

Здесь первая эквивалентность вытекает из определения (2) формулы B. Вторая эквивалентность имеет место ввиду определения (1) формулы A'. Третья эквивалентность следует из выводимости (3). ◁

2. Теорема Гёделя о неполноте. С помощью гёделевой нумерации выводимость в теории Ar^+ может изучаться в рамках самой формальной теории Ar^+ (см. по этому поводу гл. II, § 3, п. 7 и § 4, п. 6). В частности, может быть построен примитивно-рекурсивный предикат $\mathrm{PRF}(y, x)$, истинный тогда и только тогда, когда y есть гёделев номер вывода Ar^+ для формулы с гёделевым номером x. Как всякий примитивно-рекурсивный предикат, он может быть выражен в форме $F(y, x) = 1$ для некоторой примитивно-рекурсивной функции F, принимающей лишь значения 0 и 1. Если f — п. р. описание функции F, то предикату PRF в Ar^+ естественно соответствует формула $f(y, x) = S0$, которую мы обозначим через $\mathrm{Prf}(y, x)$.

Рассмотрим теперь формулу

$$\mathrm{Pr}(x) \leftrightharpoons \exists y\, \mathrm{Prf}(y, x),$$

которая утверждает, что x есть гёделев номер формулы Ar^+, выводимой в Ar^+.

Пусть A_0 — конкретная формула, отрицание которой выводимо в Ar^+. Например, можно взять в качестве A_0 формулу $0 = S0$. Рассмотрим замкнутую формулу

$$\mathrm{Con} \leftrightharpoons \forall y \neg \mathrm{Prf}(y, [0 = S0]).$$

Эта формула утверждает, что теория Ar^+ непротиворечива.

С помощью теоремы о неподвижной точке определим теперь замкнутую *формулу Гёделя* ν таким образом, что

$$\mathrm{Ar}^+ \vdash \nu \equiv \neg \mathrm{Pr}([\nu]). \tag{1}$$

Исходя из этой эквивалентности, можно сказать, что формула ν «утверждает, что она сама не выводима».

Лемма 1. *Если теория* Ar^+ *непротиворечива, то формула* ν *не выводима в* Ar^+.

▷ Предположим противное, и пусть p — гёделев номер вывода формулы в теории Ar^+. Тогда имеет место $\mathrm{PRF}(p, \gamma\nu)$, и по лемме п. 1 отсюда $\mathrm{Ar}^+ \vdash \mathrm{Prf}(\widetilde{p}, [\nu])$ и, далее, $\mathrm{Ar}^+ \vdash \mathrm{Pr}([\nu])$, что ввиду (1) влечет $\mathrm{Ar}^+ \vdash \neg\nu$. С другой стороны, по допущению $\mathrm{Ar}^+ \vdash \nu$, и мы заключаем, что теория Ar^+ противоречива вопреки предположению. ◁

Замечание. Напомним, что теория T называется непротиворечивой, если не существует формулы A теории T такой, что одновременно $T \vdash A$ и $T \vdash \neg A$. Теория T непротиворечива тогда и только тогда, когда существует формула, не выводимая в T. Читателю может показаться, что допущение о непротиворечивости излишне в формулировке предыдущей леммы. Кажется очевидным, что это допущение и так имеет место. Теория Ar^+, конечно, непротиворечива. В самом деле, все выводимые в Ar^+ формулы истинны в стандартной модели ω в то время, как, например, формула $0 = S0$ ложна в стандартной модели и, следовательно, не выводима в Ar^+.

Дело в том, что мы хотели бы, чтобы и формулировка, и доказательство леммы 1 естественно формализовались в теории Ar^+, а, как мы увидим ниже, формула Con как раз не выводима в Ar^+. Только что намеченное нами доказательство непротиворечивости Ar^+ использует некоторые теоретико-множественные соображения из теории моделей и не может быть непосредственно переведено в язык Ar^+.

Пусть T — теория в языке Ar^+. Будем говорить, что теория T *ω-непротиворечива*, если не существует формулы $A(y)$ с одной свободной переменной такой, что

1) $T \vdash \exists\, y A(y)$,
2) для всякого натурального m имеет место $T \vdash \neg A(\widetilde{m})$.

Упражнение. Докажите, что если T *ω-непротиворечива*, то теория T и просто непротиворечива.

Лемма 2. *Если* Ar^+ *ω-непротиворечива, то в* Ar^+ *не выводима формула* $\neg\nu$.

▷ Предположим противное, и пусть $\mathrm{Ar}^+ \vdash \neg\nu$. Согласно (1) тогда $\mathrm{Ar}^+ \vdash \mathrm{Pr}([\nu])$, т. е. $\mathrm{Ar}^+ \vdash \exists\, y \mathrm{Prf}(y, [\nu])$. С другой стороны, возьмем произвольное натуральное m. Имеем $\neg\mathrm{PRF}(m, \gamma\nu)$, так как по лемме 1 формула ν не выводима. По лемме в п. 1 отсюда $\mathrm{Ar}^+ \vdash \neg\mathrm{Prf}(\widetilde{m}, [\nu])$, и мы получаем ω-противоречие в Ar^+. ◁

Теорема Гёделя о неполноте. *Если теория* Ar^+ *ω-непротиворечива, то формула ν и формула $\neg\nu$ не выводимы в этой теории.*

▷ Это следствие лемм 1 и 2. ◁

Замечание. Напомним, что теория называется полной, если для всякой замкнутой формулы A имеем $T \vdash A$ или $T \vdash \neg A$. Теория Ar^+ оказывается, таким образом, неполной.

Формула ν истинна в стандартной модели ω, так как в силу леммы 1 не существует вывода ν в Ar^+ и, следовательно, истинна формула $\neg\mathrm{Pr}([\nu])$. Таким образом, ν — пример истинного предложения, не выводимого в Ar^+.

Далее, неверно, что $\mathrm{Ar}^+ \vdash \neg\mathrm{Prf}(y, [\nu])$ со свободной переменной y, так как иначе было бы нетрудно получить $\mathrm{Ar}^+ \vdash \nu$. В то же время для всякого конкретного натурального числа m имеем $\mathrm{Ar}^+ \vdash \neg\mathrm{Prf}(\widetilde{m}, [\nu])$. Теории Ar^+ как бы не хватает «обобщающей абстракции», в силу чего и возникает ее неполнота.

Рассмотрим теорию $T = \mathrm{Ar}^+ + \neg\nu$, получаемую добавлением к Ar^+ в качестве новой нелогической аксиомы (ложного!) предложения $\neg\nu$. Теория T непротиворечива, так как если бы в T выводилось противоречие, то по законам логики $\mathrm{Ar}^+ \vdash \nu$. Тем не менее теория T ω-противоречива. Действительно, $\neg\nu$ эквивалентно $\exists\, y \mathrm{Prf}(y, [\nu])$, так что $T \vdash \exists\, y \mathrm{Prf}(y, [\nu])$. В то же время, для всякого натурального m по лемме 1 $\neg\mathrm{PRF}(m, \gamma\nu)$, и, значит, в Ar^+ и тем более в T выводимо $\neg\mathrm{Prf}(\widetilde{m}, [\nu])$.

3. Вторая теорема Гёделя. Как формулировка, так и доказательство леммы 1 предыдущего пункта касаются лишь конструктивных объектов и после перехода к гёделевым номерам допускают естественную формализацию в рамках теории Ar^+. Проводя такую формализацию, мы получим, что имеет место утверждение

$$\mathrm{Ar}^+ \vdash \mathrm{Con} \supset \neg\mathrm{Pr}([\nu]).$$

Далее, имеет место следующее утверждение:
$\neg\exists\, y\mathrm{PRF}(y, \gamma\nu) \Rightarrow (\mathrm{Ar}^+$ *непротиворечива*$)$.

▷ В самом деле, пусть Ar^+ противоречива. Тогда в Ar^+ выводима всякая формула и, в частности, ν. Если D — вывод ν в Ar^+, то имеет место $\mathrm{PRF}(\gamma D, \gamma\nu)$ и, следовательно, $\exists\, y\mathrm{PRF}(y, \gamma\nu)$ вопреки предположению. ◁

Только что приведенное доказательство допускает несложную формализацию внутри теории Ar^+, в результате чего получаем утверждение

$$\mathrm{Ar}^+ \vdash \neg\exists\, y\mathrm{Prf}(y, [\nu]) \supset \mathrm{Con},$$

т. е.

$$\mathrm{Ar}^+ \vdash \neg\mathrm{Pr}([\nu]) \supset \mathrm{Con}.$$

Сопоставляя две полученные выводимости, заключаем

$$\mathrm{Ar}^+ \vdash \neg\mathrm{Pr}([\nu]) \equiv \mathrm{Con}.$$

С другой стороны, по построению ν имеем

$$\mathrm{Ar}^+ \vdash \nu \equiv \neg\mathrm{Pr}([\nu]).$$

Таким образом, окончательно

$$\mathrm{Ar}^+ \vdash \mathrm{Con} \equiv \nu.$$

Теорема (вторая теорема Гёделя). *Если теория* Ar^+ *непротиворечива, то формула* Con *не выводима в* Ar^+.

▷ Это следствие предыдущей выводимости и леммы 1 предыдущего пункта. ◁

Вторая теорема Гёделя утверждает факт принципиальной важности: непротиворечивость рассматриваемой теории не может быть доказана средствами самой теории. Для доказательства непротиворечивости теории необходимо привлекать понятия, выходящие за ее рамки. Так выше нам удалось установить непротиворечивость теории Ar^+, привлекая теоретико-модельные соображения. Подобным образом можно показать, что непротиворечивость ZF не может быть установлена в рамках самой теории ZF. Очень интересной задачей является отыскание достаточно убедительных средств, выходящих за пределы ZF.

4. Теорема о неполноте в форме Россера. Как показал Россер, с помощью подходящего подбора формулы в теореме о неполноте можно заменить требование ω-непротиворечивости на более слабое требование простой непротиворечивости.

Рассмотрим примитивно-рекурсивную функцию $\mathrm{NEG}(x)$ такую, что если x — гёделев номер формулы A, то $\mathrm{NEG}(x)$ есть гёделев номер формулы $\neg A$. По примитивно-рекурсивному описанию этой функции можно построить соответствующий терм $\mathrm{Neg}(x)$ теории Ar^+.

С помощью теоремы о неподвижной точке построим формулу ρ так, что

$$\mathrm{Ar}^+ \vdash \rho \equiv \forall y(\mathrm{Prf}(y, [\rho]) \supset (\exists z \leqslant y)\mathrm{Prf}(z, \mathrm{Neg}([\rho]))).$$

Теорема Россера о неполноте. *Если теория* Ar^+ *непротиворечива, то в ней не выводимы ни формула* ρ*, ни формула* $\neg\rho$.

▷ Предположим, что $\mathrm{Ar}^+ \vdash \rho$. Тогда найдется m такое, что $\mathrm{PRF}(m, \gamma\rho)$. Если бы для некоторого i было бы $\mathrm{PRF}(i, \gamma(\neg\rho))$, то теория Ar^+ оказалась бы противоречивой вопреки предположению.

Таким образом, имеем

$$\mathrm{PRF}(m, \gamma\rho) \wedge (\forall z \leqslant m)\neg\mathrm{PRF}(z, \mathrm{NEG}(\gamma\rho)).$$

Это примитивно-рекурсивное соотношение может быть выведено в Ar^+, и мы получаем

$$\mathrm{Ar}^+ \vdash \mathrm{Prf}(\widetilde{m}, [\rho]) \wedge (\forall z \leqslant \widetilde{m})\neg\mathrm{Prf}(z, \mathrm{Neg}([\rho])).$$

Отсюда

$$\mathrm{Ar}^+ \vdash \exists y(\mathrm{Prf}(y, [\rho]) \wedge (\forall z \leqslant y)\neg\mathrm{Prf}(z, \mathrm{Neg}([\rho]))).$$

Но эта последняя формула логически эквивалентна $\neg\rho$. Таким образом, $\mathrm{Ar}^+ \vdash \rho$, что противоречит допущению $\mathrm{Ar}^+ \vdash \rho$.

Допустим теперь, что $\mathrm{Ar}^+ \vdash \neg\rho$. Тогда найдется натуральное m такое, что $\mathrm{PRF}(m, \mathrm{NEG}(\gamma\rho))$, и по лемме п. 1 тогда $\mathrm{Ar}^+ \vdash \mathrm{Prf}(\widetilde{m}, \mathrm{Neg}([\rho]))$.

Отсюда по законам формальной арифметики получим

$$\mathrm{Ar}^+ \vdash (\forall y \geqslant \widetilde{m})(\exists z \leqslant y)\mathrm{Prf}(z, \mathrm{Neg}([\rho])),$$

и, далее, ослабляя это утверждение,

$$\mathrm{Ar}^+ \vdash (\forall y \geqslant \widetilde{m})(\mathrm{Prf}(y, [\rho]) \supset (\exists z \leqslant y)\mathrm{Prf}(z, \mathrm{Neg}([\rho]))). \qquad (1)$$

Кроме того, имеет место содержательное утверждение

$$(\forall y \leqslant m)(\mathrm{PRF}(y, \gamma[\rho]) \Rightarrow (\exists z \leqslant y)\mathrm{PRF}(z, \mathrm{NEG}(\gamma\rho))), \qquad (2)$$

просто в силу того, что для всякого y предикат $\mathrm{PRF}(y, \gamma\rho)$ ложен (иначе было бы $\mathrm{Ar}^+ \vdash \rho$ и Ar^+ оказалась бы противоречивой).

Примитивно-рекурсивное соотношение (2) может быть выделено в Ar^+, и таким образом:

$$\mathrm{Ar}^+ \vdash (\forall y \leqslant \widetilde{m})(\mathrm{Prf}(y, [\rho]) \supset (\exists z \leqslant y)\mathrm{Prf}(z, \mathrm{Neg}([\rho]))). \qquad (3)$$

Сопоставляя (1) и (3), по законам формальной арифметики получим

$$\mathrm{Ar}^+ \vdash \forall y(\mathrm{Prf}(y, [\rho]) \supset (\exists z \leqslant y)\mathrm{Prf}(z, \mathrm{Neg}([\rho]))),$$

что есть не что иное, как $\mathrm{Ar}^+ \vdash \rho$. Таким образом, $\mathrm{Ar}^+ \vdash \rho$ и $\mathrm{Ar}^+ \vdash \neg\rho$, и мы опять приходим к противоречию. ◁

5. Теорема Лёба. Так называется следующая

Теорема. *Если* $\mathrm{Ar}^+ \vdash \mathrm{Pr}([A]) \supset A$, *то* $\mathrm{Ar}^+ \vdash A$.

▷ По теореме о неподвижной точке найдем формулу ψ такую, что

$$\mathrm{Ar}^+ \vdash \psi \equiv (\mathrm{Pr}([\psi]) \supset A). \tag{1}$$

Лемма. $\mathrm{Ar}^+ \vdash \psi \Rightarrow \mathrm{Ar}^+ \vdash A$.

▷ Пусть $\mathrm{Ar}^+ \vdash \psi$ и m — соответствующий вывод. Тогда $\mathrm{PRF}(\overline{m}, \gamma\psi)$ и, значит, $\mathrm{Ar}^+ \vdash \mathrm{Prf}(\overline{m}, [\psi])$, отсюда $\mathrm{Ar}^+ \vdash \mathrm{Pr}([\psi])$. Ввиду (1) тогда $\mathrm{Ar}^+ \vdash \psi \equiv A$. По допущению отсюда $\mathrm{Ar}^+ \vdash A$. ◁

Формализуя доказательство этой леммы, получим

$$\mathrm{Ar}^+ \vdash \mathrm{Pr}([\psi]) \supset \mathrm{Pr}([A]). \tag{2}$$

Далее, по допущению теоремы имеем

$$\mathrm{Ar}^+ \vdash \mathrm{Pr}([A]) \supset A. \tag{3}$$

Из (2) и (3)

$$\mathrm{Ar}^+ \vdash \mathrm{Pr}([\psi]) \supset A,$$

что ввиду (1) дает $\mathrm{Ar}^+ \vdash \psi$. Но тогда по лемме имеем $\mathrm{Ar}^+ \vdash A$. ◁

6. Неразрешимость. Обозначим через $[\mathrm{Ar}^+]^0$ множество всех гёделевых номеров предложений, выводимых в Ar^+ и через $[\mathrm{Ar}^+]^1$ — множество всех гёделевых номеров предложений, опровержимых в Ar^+, т. е.

$$[\mathrm{Ar}^+]^1 \rightleftharpoons \{\gamma B \mid \mathrm{Ar}^+ \vdash \neg B, B \text{ — предложение }\}.$$

Теорема. *Множества* $[\mathrm{Ar}^+]^0$ *и* $[\mathrm{Ar}^+]^1$ *всех номеров выводимых и соответственно опровержимых предложений* Ar^+ *рекурсивно-неотделимы.*

▷ Рассмотрим примитивно-рекурсивные предикаты $W_0(x, y)$ и $W_1(x, y)$ (гл. II, § 5, п. 4). Они задаются арифметическими формулами, которые мы также будем обозначать через W_0 и W_1. Как было показано во второй главе, множества $V_0 = \{x \mid \exists y W_0(x, y)\}$ и $V_1 = \{x \mid \exists y W_1(x, y)\}$ не пересекаются, т. е.

$$\exists y W_1(x, y) \Rightarrow \neg\exists y W_0(x, y).$$

Доказательство этого утверждения можно формализовать в Ar^+ и получить

$$\mathrm{Ar}^+ \vdash \exists y W_1(x, y) \supset \neg\exists y W_0(x, y). \tag{1}$$

Определим теперь формулу $B(x) \leftrightharpoons \exists y W_0(x, y)$.

Если $m \in V_0$, то существует k такое, что $W_0(m, k)$, значит, $\mathrm{Ar}^+ \vdash W_0(\widetilde{m}, \widetilde{k})$, следовательно, $\mathrm{Ar}^+ \vdash \exists y W_0(\widetilde{m}, y)$, т. е. $\mathrm{Ar}^+ \vdash B(\widetilde{m})$ и, значит, $\gamma B(\widetilde{m}) \in [\mathrm{Ar}^+]^0$. Итак,

$$m \in V_0 \Rightarrow \gamma B(\widetilde{m}) \in [\mathrm{Ar}^+]^0. \tag{2}$$

Пусть теперь $m \in V_1$, тогда существует k такое, что $W_1(m, k)$. Отсюда $\mathrm{Ar}^+ \vdash W_1(\widetilde{m}, \widetilde{k})$ и, далее, $\mathrm{Ar}^+ \vdash \exists y W_1(\widetilde{m}, y)$. Ввиду (1) тогда $\mathrm{Ar}^+ \vdash \neg\exists y W_0(\widetilde{m}, y)$, т. е. $\mathrm{Ar}^+ \vdash \neg B(\widetilde{m})$, и, таким образом, $B(\widetilde{m}) \in [\mathrm{Ar}^+]^1$. Итак,

$$m \in V_1 \Rightarrow \gamma B(\widetilde{m}) \in [\mathrm{Ar}^+]^1. \tag{3}$$

Предположим противное, и пусть B_0, B_1 рекурсивно отделяют множества $[\mathrm{Ar}^+]^0$, $[\mathrm{Ar}^+]^1$, т. е. B_0, B_1 — рекурсивно-перечислимы,

$$[\mathrm{Ar}^+]^0 \subseteq B_0, [\mathrm{Ar}^+]^1 \subseteq B_1, \tag{4}$$

$$B_0 \cap B_1 = \varnothing, B_0 \cup B_1 = \omega. \tag{5}$$

Определим тогда рекурсивно-перечислимые множества $B_i' = \{m \mid \gamma B(\widetilde{m}) \in B_i\}$. Ввиду (2)–(4) имеем $V_i \subseteq B_i'$, а в силу (5) $B_0' \cap B_1' = \varnothing$, $B_0' \cup B_1' = \omega$. Таким образом, оказывается, что множества V_0, V_1 также рекурсивно-отделимы, что невозможно. ◁

Теорема о неразрешимости. *Пусть T — непротиворечивая теория в языке Ar^+, в которой выводятся все нелогические аксиомы Ar^+. Тогда T неразрешима.*

▷ Все, что выводится в Ar^+, выводится и в T, так что $[T]^0 \subseteq [\mathrm{Ar}^+]^0$. Ввиду непротиворечивости T очевидно $[T]^0 \cap [\mathrm{Ar}^+]^1 = \varnothing$. Если T была бы разрешимой, то множество $[T]^0$ было бы рекурсивным. Тогда рекурсивным оказалось бы и дополнение $\omega \setminus [T]^0$ этого множества. Но тогда множества $[T]^0$ и $\omega \setminus [T]^0$ рекурсивно отделяют множества $[\mathrm{Ar}^+]^0$ и $[\mathrm{Ar}^+]^1$. ◁

Следствие. *Если Ar^+ непротиворечива, то Ar^+ — неразрешимая теория.*

▷ Достаточно в теореме взять Ar^+ в качестве T. ◁

7. Распространение результатов на другие теории.

Мы подробно исследовали теорию Ar^+, но все теоремы настоящего параграфа имеют место и по отношению ко многим другим теориям. Достаточно, чтобы рассматриваемая теория T обладала следующими двумя свойствами:

1) она должна быть явно заданной. Это нужно для того, чтобы на языке арифметики можно было бы говорить о выводимости в теории, например, чтобы был общерекурсивен предикат $\mathrm{PRF}_T(y, x)$ и можно было построить соответствующую арифметическую формулу $\mathrm{Prf}_T(y, x)$, утверждающую, что y есть гёделев номер вывода в теории T формулы с гёделевым номером x;

2) теория T должна содержать арифметику Ar^+. Это нужно для того, чтобы в рамках теории T можно было бы вывести необходимые свойства арифметических предикатов и, значит, доказать внутри T необходимые свойства предиката выводимости самой теории T. Понятие «содержать арифметику» при этом может трактоваться очень широко. Достаточно, чтобы теория Ar^+ в том или ином смысле интерпретировалась бы в теории T, например, достаточно, чтобы существовал некоторый перевод A^0 формул языка Ar^+ в формулы теории T, перевод, обладающий свойствами, аналогичными указанным в гл. II, § 4, п. 7.

Теории Ar, Ar^+, Ar2, ZF удовлетворяют этим требованиям. Следовательно, все эти теории, в случае их непротиворечивости, неполны, неразрешимы и множества их выводимых и опровержимых предложений рекурсивно-неотделимы. Для каждой из указанных теорий T можно рассмотреть арифметическую формулу $\mathrm{Con}T$, утверждающую, что теория T непротиворечива:

$$\mathrm{Con}T \leftrightharpoons \neg\exists\, y \mathrm{Prf}_T(y, [A_0]),$$

где A_0 — фиксированное предложение T, отрицание которого выводимо в T.

Если теория T непротиворечива, то формула $\mathrm{Con}T$ (точнее, ее перевод в теорию T) не выводится в T. В этом и состоит вторая теорема Гёделя, сформулированная применительно к теории T.

Мы не будем заниматься далее уточнением класса теорий, для которых имеют место наши теоремы, а упомянем еще об одном классическом результате.

Внимательный анализ показывает, что результат о неразрешимости Ar^+ в п. 6 получается, если вместо всей теории Ar^+ взять лишь фрагмент Ar^- теории Ar, содержащий лишь конечное число нелогических аксиом из Ar. Обозначим конъюнкцию всех аксиом Ar^- через A. Это — предложение языка Ar. Из определения выводимости следует, что

$$\mathrm{Ar}^- \vdash B \Leftrightarrow \vdash A \supset B,$$

где справа стоит выводимость в логике предикатов.

Теорема о неразрешимости исчисления предикатов. *Множество формул, выводимых в исчислении предикатов (в языке* Ar*), не рекурсивно.*

▷ Предположим, что это множество рекурсивно. Тогда существует общерекурсивная функция f такая, что $f(\gamma B) = 1 \Leftrightarrow \vdash B$ для всякой формулы B. Определим тогда общерекурсивную функцию h следующей инструкцией: $h(x)$ равно 0 или 1 и $h(x) = 1 \Leftrightarrow x$ есть гёделев номер некоторой формулы B языка Ar и $f(\gamma(A \supset B)) = 1$. Тогда $h(\gamma B) = 1 \Leftrightarrow \mathrm{Ar}^- \vdash B$, и теория Ar^- оказывается разрешимой. ◁

§ 2. Теорема Гёделя о полноте исчисления предикатов

1. Нетрудно проверить, что всякая формула, выводимая в исчислении предикатов, является общезначимой, т. е. логическим законом. Теорема Гёделя о полноте утверждает, что верно и обратное, т. е. всякий логический закон необходимо выводится в исчислении предикатов. Таким образом, исчисление предикатов является адекватным инструментом для получения логических законов.

Напомним, что теория T в языке Ω называется *непротиворечивой*, если не существует формулы C языка Ω такой, что одновременно $T \vdash C$, $T \vdash \neg C$.

Основным результатом этого параграфа является следующая ниже фундаментальная теорема о существовании модели, также, по существу, доказанная Гёделем.

Теорема. *Всякая непротиворечивая теория T в языке Ω первого порядка имеет модель.*

▷ Пусть Ω — язык первого порядка и T — непротиворечивая формальная аксиоматическая теория в языке Ω. Мы опишем некоторую модель M для теории T.

Ограничимся случаем, когда язык Ω содержит лишь счетное или конечное множество символов. Теорема верна и для произвольных языков первого порядка, причем и метод доказательства в основном остается тем же, но возникает необходимость в использовании некоторых специфически теоретико-множественных средств, например в так называемой трансфинитной индукции.

Пусть X — множество всех нелогических аксиом теории T.

Фиксируем счетное множество V констант, не входящих в язык Ω, и рассмотрим язык Ψ, получающийся из Ω добавлением множества V в качестве множества новых констант. Через St_Ψ обозначим множество всех предложений в языке Ψ. Фиксируем некоторое предложение C языка Ω и определим $\top \leftrightharpoons C \vee \neg C$ и $\bot \leftrightharpoons C \wedge \neg C$. Пусть Γ и Δ — конечные множества формул языка Ψ, $\Gamma = \{A_1, \ldots, A_m\}$, $\Delta = \{B_1, \ldots, B_k\}$. Через $\Gamma \to \Delta$ обозначим формулу

$$\top \wedge A_1 \wedge \ldots \wedge A_m \supset B_1 \vee \ldots \vee B_k \vee \bot.$$

Если $k > 0$, $m > 0$, то эта формула эквивалентна $A_1 \wedge \ldots \wedge A_m \supset B_1 \vee \ldots \vee B_k$. Если $m > 0$, $k = 0$, то $\Gamma \to \Delta$ эквивалентна $\neg(A_1 \wedge \ldots \wedge A_m)$. Если $m = 0$, $k > 0$, то эта формула эквивалентна $B_1 \vee \ldots \vee B_k$. Наконец, при $m = 0$, $k = 0$ эта формула эквивалентна $\bot$.

Пару множеств $Y, Z \subseteq \mathrm{St}_\Psi$ назовем *совместной*, если для всяких конечных $\Gamma \subseteq Y$, $\Delta \subseteq Z$ формула $\Gamma \to \Delta$ не выводима в исчислении предикатов.

Пару множеств $Y, Z \subseteq \mathrm{St}_\Psi$ назовем *полной*, если

1) $(A \wedge B) \in Y \Rightarrow A \in Y$ и $B \in Y$;
2) $(A \wedge B) \in Z \Rightarrow A \in Z$ или $B \in Z$;
3) $(A \vee B) \in Y \Rightarrow A \in Y$ или $B \in Y$;
4) $(A \vee B) \in Z \Rightarrow A \in Z$ и $B \in Z$;
5) $(A \supset B) \in Y \Rightarrow A \in Z$ или $B \in Y$;
6) $(A \supset B) \in Z \Rightarrow A \in Y$ и $B \in Z$;
7) $\neg A \in Y \Rightarrow A \in Z$;
8) $\neg A \in Z \Rightarrow A \in Y$;
9) $\forall x A(x) \in Y \Rightarrow$ для всякого замкнутого терма t языка Ψ $A(t) \in Y$;
10) $\exists x A(x) \in Z \Rightarrow$ существует константа $c \in V$, $A(c) \in Z$;
11) $\exists x A(x) \in Y \Rightarrow$ существует константа $c \in V$, $A(c) \in Y$;
12) $\exists x A(x) \in Z \Rightarrow$ для всякого замкнутого терма T языка Ψ $A(t) \in Z$.

Лемма. *Существует полная и совместная пара множеств Y, Z такая, что $X \subseteq Y$.*

▷ Множества Y, Z будем строить постепенно. На каждом этапе будут возникать множества Y_n, Z_n и мы определим $Y = \bigcup_{n\in\omega} Y_n$, $Z = \bigcup_{n\in\omega} Z_n$. При переходе к следующему этапу мы увеличиваем запас формул, так что $Y_n \subseteq Y_{n+1}$, $Z_n \subseteq Z_{n+1}$. Добавление формул производится таким образом, чтобы обеспечить условия полноты 1)–12) в окончательных множествах Y, Z. Чтобы систематически обрабатывать все формулы, входящие в Y_n, Z_n, удобно занумеровать формулы натуральными числами и рассматривать их в порядке номеров.

Перейдем теперь к точным определениям. *Нумерованным множеством формул* назовем всякое множество F пар вида $\langle n, A\rangle$, где n — натуральное число и A — предложение языка Ψ. При этом выполняются условия:

a) $\langle n, A\rangle \in F$, $\langle n, B\rangle \in F \Rightarrow A = B$;
b) существует лишь конечное число нечетных n таких, что $\langle n, A\rangle \in F$.

Если $\langle n, A\rangle \in F$, то число n назовем *очередью* формулы A в множестве F. По условию, очередь полностью определяет формулу A в F. Кроме того, лишь конечное число формул имеет нечетную очередь.

По нумерованному множеству F можно образовать множество формул

$$F' = \{A \in \mathrm{St}_\Psi \mid (\exists n \in \omega)(\langle n, A\rangle) \in F)\}.$$

Нумерованная пара множеств есть по определению пара нумерованных множеств F, G такая, что из $\langle n, A\rangle \in F$, $\langle m, B\rangle \in G$ следует $n \neq m$. В этом случае $F \cup G$ есть нумерованное множество. Элемент $\langle n, A\rangle \in F \cup G$ с наименьшей очередностью назовем *очередным* в F, G. *Вес* пары F, G есть натуральное число h, определяемое следующим образом. Если $F \cup G$ не содержит элементов с нечетной очередностью, то $h = 0$. Если же $2k - 1$ есть наибольшая нечетная очередь в $F \cup G$, то определим $h = k$. Таким образом, если h — вес F, G, то $F \cup G$ заведомо не содержит элементов с очередями $2h+1$, $2h+3$ и т.д.

Занумеруем все замкнутые термы языка Ψ в единую последовательность:

$$t_1, t_2, \ldots, t_n \ldots,$$

а также все константы из V — в последовательность

$$c_1, c_2, \ldots, c_n \ldots.$$

Приступим к доказательству леммы. Построим нумерованную пару F_1, G_1 такую, что $F_1' = X, G_1' = \{C \wedge \neg C\}$, перенумеровав все формулы из F_1', G_1' *четными* числами. Вес h_1 этой пары равен нулю. Кроме того, каждая из формул $F_1' \cup G_1'$ не содержит констант из V, так как принадлежит языку Ω. Пара множества F_1', G_1' совместна, так как множество X непротиворечиво.

Далее, индуктивно определим последовательность нумерованных пар F_1, G_1; F_2, G_2; ...; F_n, G_n; ... таким образом, что каждое множество формул $F_n' \cup G_n'$ содержит лишь конечное множество констант из V и пара F_n', G_n' совместна. Вес пары F_n, G_n обозначим через h_n.

Итак, пусть уже построена пара F_n, G_n, покажем, как следует определить F_{n+1}, G_{n+1}. Пусть $\langle m, A\rangle$ есть очередной элемент пары F_n, G_n. Выбросим элемент $\langle m, A\rangle$ из того множества F_n или G_n, куда $\langle m, A\rangle$ входит, и добавим в это же множество новый элемент $\langle 2h_n + 1, A\rangle$. Положенную пару обозначим через P_n, Q_n. Очевидно,

$$P_n' = F_n', \quad Q_n' = G_n'.$$

Далее, разберем случаи в зависимости от вида элемента $\langle m, A\rangle$.

1) $\langle m, A\rangle \in F_n$, $A = A_1 \wedge A_2$. Тогда $F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_1\rangle, \langle 2h_n + 5, A_2\rangle\}$, $G_{n+1} = Q_n$.

Заметим, что пара F_{n+1}', G_{n+1}' совместна, так как в противном случае нашлись бы конечные множества $\Gamma \subseteq F_n'$, $\Delta \subseteq G_n'$ такие, что $\vdash \{A_1, A_2\} \cup \Gamma \to \Delta$. Тогда по правилам исчисления предикатов $\vdash \{A_1 \wedge A_2\} \cup \Gamma \to \Delta$ и, так как $A_1 \wedge A_2 \in F_n'$, пара F_n', G_n' оказалась бы несовместной.

2) $\langle m, A\rangle \in G_n$, $A = A_1 \wedge A_2$.

Заметим, что одна из пар

$$F_n', G_n' \cup \{A_1\}$$

или

$$F_n', G_n' \cup \{A_2\}$$

необходимо совместна. Действительно, в противном случае найдутся конечные множества $\Gamma \subseteq F_n'$ и $\Delta \subseteq G_n'$ такие, что $\vdash \Gamma \to \Delta \cup \{A_1\}$ и $\vdash \Gamma \to \Delta \cup \{A_2\}$. А тогда по правилам исчисления предикатов $\vdash \Gamma \to \Delta \cup \{A_1 \wedge A_2\}$, так как $A_1 \wedge A_2 \in G_n'$, пара F_n', G_n' оказалась бы несовместной. Пусть совместна пара $F_n', G_n' \cup \{A_i\}$. Положим $F_{n+1} = P_n$, $G_{n+1} = Q_n \cup \{\langle 2h_n + 3, A_i\rangle\}$.

3) $\langle m, A\rangle \in F_n$, $A = A_1 \vee A_2$.

Заметим, что одна из пар

$$\{A_1\} \cup F_n', G_n'$$

или

$$\{A_2\} \cup F'_n, G'_n$$

необходимо совместна! Действительно, в противном случае найдутся конечные множества Γ и Δ, $\Gamma \subseteq F'_n$, $\Delta \subseteq G'_n$, такие, что $\vdash \{A_1\} \cup \Gamma \to \Delta$ и $\vdash \{A_2\} \cup \Gamma \to \Delta$. А тогда $\vdash \{A_1 \vee A_2\} \cup \Gamma \to \Delta$, и пара F'_n, G'_n оказалась бы несовместной. Пусть совместна пара $\{A_i\} \cup F'_n, G'_n$. Определим $F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_i\rangle\}$, $G_{n+1} = Q_n$.

4) $\langle m, A\rangle \in G_n$, $A = A_1 \vee A_2$. Тогда $F_{n+1} = P_n$, $G_{n+1} = Q_n \cup \{\langle 2h_n + 3, A_1\rangle, \langle 2h_n + 5, A_2\rangle\}$.

5) $\langle m, A\rangle \in F_n$, $A = A_1 \supset A_2$.

Заметим, что одна из пар

$$\{A_2\} \cup F'_n, G'_n$$

или

$$F'_n, G'_n \cup \{A_1\}$$

необходимо совместна. В противном случае для некоторых $\Gamma \subseteq F'_n$, $\Delta \subseteq G'_n$ было бы $\vdash \{A_2\} \cup \Gamma \to \Delta$ и $\vdash \Gamma \to \Delta \cup \{A_1\}$. Но тогда $\vdash \{A_1 \supset A_2\} \cup \Gamma \to \Delta$ и пара F'_n, G'_n оказалась бы несовместной.

Если совместна пара $\{A_2\} \cup F'_n, G'_n$, то определим $F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_2\rangle\}$, $G_{n+1} = Q_n$. Если же совместна пара $F'_n, G'_n \cup \{A_1\}$, то определим $F_{n+1} = P_n$, $G_{n+1} = Q_n \cup \{\langle 2h_n + 3, A_1\rangle\}$.

6) $\langle m, A\rangle \in G_n$, $A = A_1 \supset A_2$. Тогда

$$F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_1\rangle\},$$
$$G_{n+1} = Q_n \cup \{\langle 2h_n + 5, A_2\rangle\}.$$

7) $\langle m, A\rangle \in F_n$, $A = \neg A_1$. Тогда

$$F_{n+1} = P_n, G_{n+1} = Q_n \cup \{\langle 2h_n + 3, A_1\rangle\}.$$

8) $\langle m, A\rangle \in G_n$, $A = \neg A_1$. Тогда

$$F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_1\rangle\}, \quad G_{n+1} = Q_n.$$

9) $\langle m, A\rangle \in F_n$, $A = \forall x A_1(x)$.

Пусть $t_1, \ldots, t_n$ — первые n термов в последовательности всех замкнутых термов языка Ψ. Тогда

$$F_{n+1} = P_n \cup \{\langle 2(h_n + j) + 1, A_1(t_j)\rangle \mid j = 1, \ldots, n\}, \quad G_{n+1} = Q_n.$$

10) $\langle m, A\rangle \in G_n$, $A = \forall x A_1(x)$. Выберем первую константу $a \in V$, не встречающуюся в $F'_n \cup G'_n$. Положим $F_{n+1} = P_n$, $G_{n+1} = Q_n \cup \{\langle 2h_n + 3, A_1(a)\rangle\}$. Заметим, что пара F'_{n+1}, G'_{n+1} совместна. В противном случае для некоторых $\Gamma \subseteq F'_n$, $\Delta \subseteq G'_n$ было бы $\vdash \Gamma \to \Delta \cup \{A_1(a)\}$. Так как константа a не встречается в Γ и Δ, то в выводе $\vdash \Gamma \to \Delta \cup \{A_1(a)\}$ ее можно заменить на новую переменную z, не входящую в вывод, и получить вывод $\vdash \Gamma \to \Delta \cup \{A_1(z)\}$ и затем по правилам исчисления предикатов получить $\vdash \Gamma \to \Delta \cup \{\forall x A_1(x)\}$, что влечет, ввиду $\forall x A_1(x) \in G'_n$ несовместность пары F'_n, G'_n.

11) $\langle m, A\rangle \in F_n$, $A = \exists x A_1(x)$. Выберем первую константу $a \in V$, не встречающуюся в $F'_n \cup G'_n$. Положим $F_{n+1} = P_n \cup \{\langle 2h_n + 3, A_1(a)\rangle\}$, $G_{n+1} = Q_n$. Заметим, что пара F'_{n+1}, G'_{n+1} совместна.

12) $\langle m, A\rangle \in G_n$, $A = \exists x A_1(x)$. Пусть $t_1, \ldots, t_n$ — первые n термов в последовательности всех замкнутых термов языка Ψ. Тогда $F_{n+1} = P_n$, $G_{n+1} = Q_n \cup \{\langle 2(h_n + j) + 1, A_1(t_j)\rangle \mid j = 1, \ldots, n\}$.

Наконец, если для элемента $\langle m, A\rangle$ не выполняется ни один из случаев 1)–12), то определим $F_{n+1} = P_n$, $G_{n+1} = Q_n$. Таким образом, по сравнению с F_n и G_n в этом случае происходит лишь изменение очереди у очередного элемента, в то время как $F'_{n+1} = F_n$, $G'_{n+1} = G'_n$.

Теперь остается положить

$$Y = \bigcup_{n\in\omega} F'_n, \quad Z = \bigcup_{n\in\omega} G'_n.$$

Каждая пара F'_n, G'_n была совместной, откуда и следует совместность Y, Z. Нетрудно проверить и полноту Y, Z. Проверим, например, выполнение требования 6) полноты.

Пусть $(A \supset B) \in Z$. Тогда $\langle m, A \supset B\rangle \in G_n$ для некоторых m и n. Увеличивая в случае необходимости номер n, можно добиться, чтобы элемент $\langle m, A \supset B\rangle$ был очередным в G_n. По построению тогда $A \in F'_{n+1}$, $B \in G'_{n+1}$, т. е. $A \in Y$ и $B \in Z$. Лемма доказана. ◁

Теперь мы можем описать искомую модель M. В качестве объектов модели возьмем множество всех выражений вида $[t]$, где t — произвольный замкнутый терм языка Ψ. Константе c языка Ω сопоставим объект $[c]$ модели M. Далее, m-местному функциональному символу f языка Ω сопоставим функцию $\widetilde{f}$ в модели. А именно для произвольных объектов $[t_1], \ldots, [t_m]$ модели M определим $\widetilde{f}([t_1], \ldots, [t_m]) = [f(t_1, \ldots, t_m)]$, где справа в квадратных скобках стоит замкнутый терм языка Ψ.

Наконец, m-местному предикатному символу P языка Ω сопоставим предикат $\widetilde{P}$ модели M. А именно $\widetilde{P}([t_1], \ldots, [t_m])$ истинно тогда и только тогда, когда формула $P(t_1, \ldots, t_m)$ принадлежит множеству Y, указанному в лемме.

Описание M закончено. Необходимо проверить, что предложения из множества X истинны в M. С этой целью докажем следующие два утверждения, устанавливающие связь множеств Y, Z с истинностью в модели M. Пусть

A — формула, оцененная в модели M, и

A^* — предложение языка Ψ, которое получается из A стиранием всех квадратных скобок. Тогда

a) $A^* \in Y \Rightarrow M \models A$,

b) $A^* \in Z \Rightarrow$ неверно, что $M \models A$.

Оба утверждения будем доказывать одновременно индукцией по построению формулы A.

Если A — атомарна и $A^* \in Y$, то $M \models A$ по определению истинности в M. Если $A^* \in Z$, то ввиду совместимости Y, Z имеем $A^* \notin Y$, и значит, не $M \models A$.

Пусть $A = A_1 \wedge A_2$. Если $A^* \in Y$, то ввиду полноты $A_1^*, A_2^* \in Y$. Тогда по индуктивному предположению $M \models A_1, M \models A_2$, т. е. $M \models A_1 \wedge A_2$. Если $A^* \in Z$, то опять-таки ввиду полноты, $A_1^* \in Z$ или $A_2^* \in Z$. По индуктивному предположению тогда не $M \models A_1$ или $M \models A_2$, что означает не $M \models A_1 \wedge A_2$.

Подобным образом рассматриваются и остальные случаи строения A. Рассмотрим еще, например, случай, когда $A = \exists x A_1(x)$. Если $A^* \in Y$, то ввиду полноты $A_1^*(a) \in Y$ для некоторой константы из V. По индуктивному предположению $M \models A_1([a])$, т. е. $M \models \exists x A_1(x)$. Если $A^* \in Z$, то ввиду полноты $A_1^*(t) \in Z$ для всякого замкнутого терма t языка Ψ. По индуктивному предположению не $M \models A_1([t])$ для всякого t и, следовательно, не $M \models \exists x A_1(x)$.

Теперь, так как $X \subseteq Y$, из утверждения а) следует, что $M \models A$ для всех $A \in X$ и, значит, M есть модель теории T. ◁

2. Отметим некоторые следствия основной теоремы п. 1.

Теорема Мальцева о компактности. *Пусть X — множество предложений языка Ω. Если каждое конечное подмножество множества X имеет модель, то и все множество X также имеет модель.*

▷ В самом деле, в условиях теоремы X образует непротиворечивую аксиоматическую теорию, так как если бы в X выводилось противоречие, то нашлось бы конечное множество $\Gamma \subseteq X$, $\Gamma \vdash C \wedge \neg C$, и конечное множество Γ не имело бы модели. По основной теореме X имеет модель. ◁

Теорема о полноте исчисления предикатов. *Если формула A есть логический закон, то A выводится в исчислении предикатов.*

▷ Можно считать, что A есть предложение, замыкая в случае необходимости A кванторами общности. Если A не выводится в исчислении предикатов, то теория T с единственной нелогической аксиомой $\neg A$ непротиворечива (так как из $\neg A \vdash C \wedge \neg C$ следует $\vdash A$). По основной теореме тогда $\neg A$ имеет модель M. Но тогда неверно, что $M \models A$, и, значит, A не есть логический закон. ◁

3. Добавим к языку Ar новую константу c и к теории Ar добавим бесконечную серию нелогических аксиом $0 < c$, $\widetilde{1} < c$, $\widetilde{2} < c, \ldots$. Здесь $\widetilde{n}$ есть терм вида $SS \ldots S0$, соответствующий натуральному числу n.

Каждая конечная подтеория полученной теории T имеет модель. В самом деле, если в конечную подтеорию входят лишь аксиомы, $\widetilde{n} < c$ с числами n, меньшими j, то достаточно взять стандартную модель ω и сопоставить константе c число $(j+1)$.

По теореме о компактности вся теория T имеет модель. Эта модель будет, конечно, и моделью Ar, но это будет *нестандартная модель*, неизоморфная ω. Действительно, константе c в этой модели соответ-

ствует объект, больший, чем все стандартные объекты, соответствующие обычным натуральным числам $0, 1, 2, \ldots$.

Заметим, что это имеет место, несмотря на известную теорему о категоричности натурального ряда. Мы уже обсуждали этот эффект в главе о теории множеств.

4. Если язык первого порядка Ω содержит не более чем счетное множество символов, то модель M для непротиворечивой теории T, описанная в основной теореме, оказывается счетной. Отсюда следует факт, являющийся вариантом так называемой теоремы Лёвенгейма—Скулема.

Теорема. *Пусть Ω — язык первого порядка со счетным множеством символов и T — непротиворечивая теория в языке Ω. Тогда теория T имеет модель со счетным носителем.*

В частности, если Ω — язык первого порядка со счетным множеством символов и M — произвольная модель для языка Ω, то существует и счетная модель M' такая, что

$$\mathrm{Th}_\Omega(M) = \mathrm{Th}_\Omega(M').$$

Здесь через $\mathrm{Th}_\Omega(M)$ мы обозначаем множество всех предложений языка Ω, истинных в модели M.

В общепринятой терминологии это замечание можно сформулировать следующим образом: *всякая модель в счетном языке элементарно-эквивалентна счетной модели.*

5. Из полученных результатов следует, что если теория множеств ZF непротиворечива, то она имеет счетную модель. И это несмотря на то, что в ZF можно доказать существование несчетного множества! Это и есть так называемый парадокс Скулема, который мы уже обсуждали (гл. I, § 6, п. 5). Еще раз подчеркнем, что указанное обстоятельство не является парадоксом в собственном смысле этого слова и никакого противоречия в полученном результате нет.

§ 3. Теорема об устранении сечения

1. Ключевую роль в теории доказательств играет понятие выводимости в исчислении предикатов. Поэтому важно преобразовать выводы в исчислении предикатов к виду, удобному для обнаружения выводимости. Это существенно и потому, что в настоящее время актуальна задача автоматического поиска вывода в аксиоматических теориях с привлечением вычислительных машин. Основой большинства методов поиска вывода в исчислении предикатов является знаменитая теорема Г. Генцена об устранении сечения, полученная в 1934 году, вариант которой мы изложим в этом параграфе.

Фиксируем некоторый логико-математический язык Ω.

Набором формул мы назовем конечное множество формул языка Ω, в котором допускаются повторения формул. Порядок формул в наборе Γ не имеет значения, но для каждой формулы указано, в скольких, экземплярах она присутствует в Γ. В соответствии с этим следует трактовать и операции над наборами. Например, при объединении $\Gamma \cup \Delta$ наборов количество экземпляров каждой формулы суммируется. Объединение $\Gamma \cup \Delta$ мы будем коротко записывать в виде $\Gamma\Delta$, так что $\Gamma\Delta$ и $\Delta\Gamma$ есть один и тот же набор. Набор $A\Gamma$ получается из набора Γ присоединением одного экземпляра формулы A.

Секвенцией назовем фигуру вида $\Gamma \to \Delta$, где Γ и Δ — наборы формул.

Сформулируем теперь некоторое исчисление, в котором будут выводиться секвенции. *Аксиомы* этого исчисления суть произвольные секвенции вида

$$A\Gamma \to \Delta A,$$

где A — произвольная *атомарная* формула Ω.

Правила вывода исчисления секвенций построены весьма симметрично и вводят логические связки слева и справа:

$$(\supset\to)\ \frac{B\Gamma \to \Delta;\ \Gamma \to \Delta A}{(A \supset B)\Gamma \to \Delta};\qquad (\to\supset)\ \frac{A\Gamma \to \Delta B}{\Gamma \to \Delta(A \supset B)};$$

$$(\wedge\to)\ \frac{AB\Gamma \to \Delta}{(A \wedge B)\Gamma \to \Delta};\qquad (\to\wedge)\ \frac{\Gamma \to \Delta A;\ \Gamma \to \Delta B}{\Gamma \to \Delta(A \wedge B)};$$

$$(\vee\to)\ \frac{A\Gamma \to \Delta;\ B\Gamma \to \Delta}{(A \vee B)\Gamma \to \Delta};\qquad (\to\vee)\ \frac{\Gamma \to \Delta AB}{\Gamma \to \Delta(A \vee B)};$$

$$(\neg\to)\ \frac{\Gamma \to \Delta A}{\neg A\Gamma \to \Delta};\qquad (\to\neg)\ \frac{A\Gamma \to \Delta}{\Gamma \to \Delta\neg A};$$

$$(\forall\to)\ \frac{A(x \parallel t)\,\forall x A\Gamma \to \Delta}{\forall x A\Gamma \to \Delta};\qquad (\to\forall)\ \frac{\Gamma \to \Delta(A(y \parallel x))}{\Gamma \to \Delta\forall y A};$$

$$(\exists\to)\ \frac{A(y \parallel x)\Gamma \to \Delta}{\exists y A\Gamma \to \Delta};\qquad (\to\exists)\ \frac{\Gamma \to \Delta\exists x A(A(x \parallel t)}{\Gamma \to \Delta\exists x A}.$$

Здесь в правилах $(\to\forall)$, $(\exists\to)$ переменная x не входит свободно в нижнюю секвенцию рассматриваемого правила вывода.

Выводы в исчислении секвенций мы будем записывать в виде деревьев аналогично выводам в исчислении предикатов (см. введение). Высота вывода по-прежнему есть количество секвенций в наиболее длинной ветви вывода. Кроме того, мы не будем делать различия между формулами и секвенциями, отличающимися лишь переименованием связанных переменных. Таким образом, если имеется вывод с нижней секвенцией S, то этот же вывод считается автоматически и выводом любой секвенции, полученной из S переименованием связанных переменных.

Будем писать $\vdash \Gamma \to \Delta$, если секвенция $\Gamma \to \Delta$ выводима в нашем исчислении секвенций.

Выводы в исчислении секвенций имеют замечательную особенность: секвенции, расположенные выше всякого правила вывода, состоят лишь из подформул формул в секвенции, расположенной в заключении правила вывода. Коротко говоря, при рассмотрении правил вывода «снизу вверх» формулы в секвенциях лишь дробятся, никакие посторонние формулы не появляются. В этом и состоит так называемое *свойство подформульности* исчисления секвенций. Это обстоятельство во многих случаях чрезвычайно облегчает поиск вывода данной секвенции.

Основной результат параграфа состоит в том, что описанное исчисление секвенций эквивалентно обычному исчислению предикатов, и таким образом поиск вывода в исчислении предикатов эквивалентен поиску вывода в нашем исчислении секвенций. Для доказательства основного результата нам придется подробно исследовать исчисление секвенций. Ключевым фактом здесь является теорема об *устранении правила сечения*. Так называется следующее правило вывода:

$$\frac{\Gamma \to \Delta A;\ A\Gamma \to \Delta}{\Gamma \to \Delta}.$$

Теорема утверждает, что это правило допустимо в исчислении секвенций, т. е. если в исчислении секвенций выводимы посылки $\Gamma \to \Delta A$ и $A\Gamma \to \Delta$ этого правила, то необходимо выводима и секвенция $\Gamma \to \Delta$, являющаяся заключением рассматриваемого правила. Таким образом, если в выводах использовать наряду с другими и правило сечения, то теорема утверждает, что все применения правила сечения можно затем устранить и получить вывод без сечений.

Заметим, что наша версия исчисления секвенций несколько отличается от той, которую использовал Генцен (см. [15]).

2. Лемма. *Для всякой формулы A языка Ω имеем*

$$\vdash A\Gamma \to \Delta A \ (\textit{без сечения}).$$

▷ Доказательство проведем индукцией по количеству логических символов в A. Если A — атомарная формула, то наша секвенция является просто аксиомой. Рассмотрим несколько случаев индукции, оставляя остальные случаи читателю.

Пусть $A = B \wedge C$. По индуктивному предположению $\vdash BC\Gamma \to \Delta B$ и $\vdash BC\Gamma \to \Delta C$. Тогда по правилу $(\to \wedge)$ имеем $\vdash BC\Gamma \to \Delta(B \wedge C)$ и затем по правилу $(\wedge \to)$ $\vdash (B \wedge C)\Gamma \to \Delta(B \wedge C)$.

Пусть $A = \forall x B(x)$. Пусть z — переменная, не входящая свободно в секвенцию $\forall x B(x)\Gamma \to \Delta \forall x B(x)$. По индуктивному предположению $\vdash B(z)\forall x B(x)\Gamma \to \Delta B(z)$. По правилу $(\forall \to)$ отсюда имеем $\vdash \forall x B(x)\Gamma \to \Delta B(z)$ и затем по правилу $(\to \forall)$ окончательно получаем $\vdash \forall x B(x)\Gamma \to \Delta \forall x B(x)$. ◁

Если S — секвенция, то через $S(x \parallel t)$ обозначим результат правильной подстановки терма t вместо свободных вхождений переменной x в каждую формулу, член этой секвенции.

3. Лемма. *Если* $\vdash S$, z *— переменная и* t *— терм, то* $\vdash S(z \parallel t)$, *причем вывод результирующей секвенции имеет ту же высоту и то же количество секвенций, что и данный вывод.*

▷ Доказательство проведем индукцией по построению данного вывода $\vdash S$. Если S — аксиома, то $S(z \parallel t)$ — также аксиома.

Далее следует рассмотреть все случаи, когда S получена по одному из правил вывода. Рассмотрим для примера лишь случай, когда S получена по правилу $(\to \forall)$. Тогда S имеет вид $\Gamma \to \Delta \forall y A$ и получена из секвенции вида $\Gamma \to \Delta A(y \parallel x)$, где переменная x не входит свободно в S.

Выберем переменную u, отличную от всех переменных, фигурирующих в рассматриваемых формулах и термах. По индуктивному предположению из выводимости $\Gamma \to \Delta A(y \parallel x)$ следует выводимость секвенции $\Gamma \to \Delta(A(y \parallel x)(x \parallel u))$, т. е. секвенции $\Gamma \to \Delta A(y \parallel u)$. Вновь используя индуктивное предположение, получим, что выводима секвенция $\Gamma(z \parallel t) \to \Delta(z \parallel t) A(y \parallel u)(z \parallel t)$. Применяя затем правило $(\to \forall)$, заключаем, что $\vdash \Gamma(z \parallel t) \to \Delta(z \parallel t) \forall u A(y \parallel u)(z \parallel t)$. Но с точностью до переименования связанных переменных формула $\forall u(A(y \parallel u)(z \parallel t))$ совпадает с $(\forall y A)(z \parallel t)$. Таким образом, полученный вывод доставляет и вывод секвенции

$$\Gamma(z \parallel t) \to \Delta(z \parallel t)(\forall y A)(z \parallel t). \qquad \triangleleft$$

4. Лемма. *В исчислении секвенций допустимы следующие правила добавления*:

$$\frac{\Gamma \to \Delta}{A\Gamma \to \Delta}; \qquad \frac{\Gamma \to \Delta}{\Gamma \to \Delta A}.$$

Допустимость означает, что из выводимости секвенции $\Gamma \to \Delta$ *вытекает, что и обе секвенции* $A\Gamma \to \Delta$ *и* $\Gamma \to \Delta A$ *также выводимы. Более того, можно утверждать при этом, что результирующие выводы имеют не большую высоту и не больше секвенций в своем составе, чем данный вывод.*

▷ Доказательство ведем индукцией по высоте данного вывода $\vdash \Gamma \to \Delta$. Если $\Gamma \to \Delta$ — аксиома, то аксиомами являются и обе секвенции $A\Gamma \to \Delta$, $\Gamma \to \Delta A$. Далее следует разобрать все случаи, когда $\Gamma \to \Delta$ получена по одному из правил вывода. Пусть, например, $\Gamma \to \Delta$ получена по правилу $(\exists \to)$. В этом случае $\Gamma \to \Delta$ имеет вид $\exists y B\Gamma' \to \Delta$ и получена из секвенции вида $B(y \parallel x)\Gamma' \to \Delta$. Выберем новую переменную u, не фигурирующую в рассматриваемых секвенциях. По предыдущей лемме 3 имеем $\vdash B(y \parallel x)(x \parallel u)\Gamma' \to \Delta$, т. е. $\vdash B(y \parallel u)\Gamma' \to \Delta$, причем высота и количество секвенций в полученном выводе не меняются. По индуктивному предположению далее $\vdash B(y \parallel u)A\Gamma' \to \Delta$ и $\vdash B(y \parallel u)\Gamma' \to \Delta A$. Отсюда по правилу $(\exists \to)$ выводим $\exists u(B(y \parallel u))A\Gamma' \to \Delta$, $\exists u(B(y \parallel u))\Gamma' \to \Delta A$, что с точностью

до переименования связанных переменных совпадает с искомыми секвенциями. Переименование переменной x в новую переменную u в этом рассуждении нам понадобилось, чтобы после добавления формулы A выполнялись бы ограничения на переменные в применении правила $(\exists \to)$. ◁

5. Лемма. *В исчислении секвенций обратимы все правила вывода. Это означает, что если выводимо заключение какого-либо правила вывода нашего исчисления секвенций, то выводимы и (обе) его посылки. При этом вновь можно утверждать, что результирующие выводы имеют не большую высоту и не большее количество секвенций, чем данный вывод.*

▷ Для правил $(\forall \to)$ и $(\to \exists)$ это следует непосредственно из допустимости правила добавления (п. 4). Для каждого из остальных правил вывода лемму доказываем отдельно индукцией по высоте вывода заключения.

Рассмотрим, например, правило $(\supset\to)$. Пусть дано $\vdash (A \supset B)\Gamma \to \Delta$, докажем, что $\vdash B\Gamma \to \Delta$ и $\vdash \Gamma \to \Delta A$ индукцией по высоте данного вывода. Если исходный вывод есть аксиома, то обе результирующие секвенции также являются аксиомами (здесь существенно, что формула $A \supset B$ не атомарная, в то время как формулы, фигурирующие явно в формулировке аксиом, атомарны). Далее следует рассмотреть случай, когда секвенция $(A \supset B)\Gamma \to \Delta$ получена по одному из правил вывода. Здесь существенны два подслучая: *a*) указанное правило не относится к явно выписанной формуле $A \supset B$; *b*) когда это правило относится к указанной формуле.

В случае *a*) рассуждения однотипны. Пусть, например, $(A \supset B)\Gamma \to \Delta$ получена по правилу $(\to \forall)$. Тогда эта секвенция имеет вид $(A \supset B)\Gamma \to \Delta'\forall y C$ и получена из секвенции $(A \supset B)\Gamma \to \Delta' C(y \parallel x)$. По индуктивному предположению выводимы секвенции $B\Gamma \to \Delta'(C(y \parallel x))$ и $\Gamma \to \Delta' A(C(y \parallel x))$. Применяя к ним правило $(\to \forall)$, получим искомые секвенции.

В случае *b*) утверждение тривиально. Искомые секвенции являются посылками правила вывода $(\supset\to)$ и, следовательно, выводимы. ◁

6. Лемма. *В исчислении секвенций допустимы правила сокращения*:

$$\frac{AA\Gamma \to \Delta}{A\Gamma \to \Delta}; \qquad \frac{\Gamma \to \Delta AA}{\Gamma \to \Delta A},$$

т. е. из выводимости посылок этих правил следует и выводимость их заключений, причем опять-таки высота и количество секвенций в выводах заключений не превосходят этих же показателей в выводах соответствующих посылок.

▷ Для всякого натурального n установим следующее утверждение: если дан вывод секвенции S такой, что либо слева, либо справа в S повторяется некоторая формула A (т. е. S имеет вид $AA\Gamma \to \Delta$ или $\Gamma \to \Delta AA$),

причем данный вывод имеет высоту $\leqslant n$, то выводима и секвенция S', полученная заменой двух отмеченных экземпляров формулы A одним экземпляром (т. е. S' имеет вид $A\Gamma \to \Delta$ или соответственно $\Gamma \to \Delta A$); при этом вывод S' имеет не большую высоту и не большее количество секвенций, чем данный вывод S.

Указанное утверждение докажем индукцией по n. При $n = 1$ секвенция S оказывается аксиомой. Но тогда S' также, очевидно, является аксиомой.

Далее следует разобрать все случаи, когда секвенция S получена по одному из правил вывода. Здесь существенны два подслучая:

a) правило, по которому получена S, не касается ни одного из рассматриваемых экземпляров сокращаемой формулы A;

b) правило, по которому получена S, касается одного из экземпляров сокращаемой формулы A.

В случае *a*) рассуждения однотипны. Пусть, например, S имеет вид $AA\Gamma \to \Delta'(C \supset D)$ и получена по правилу $(\to\supset)$ из секвенции $AAC\Gamma \to \Delta' D$. Из выводимости этой последней секвенции и индуктивного предположения следует, что выводима секвенция $AC\Gamma \to \Delta' D$. Затем, применяя правило $(\to\supset)$ к этой секвенции, получим вывод секвенции S'.

В случае *b*) существенна обратимость правил вывода. Допустим, например, что A имеет вид $(C \supset D)$ и секвенция S имеет вид $(C \supset D)(C \supset D)\Gamma \to \Delta$ и получена по правилу вывода $(\supset\to)$ из двух секвенций $D(C \supset D)\Gamma \to \Delta$ и $(C \supset D)\Gamma \to \Delta C$. Используя обратимость правила $(\supset\to)$, из выводимости последних двух секвенций заключаем, что выводимы и секвенции $DD\Gamma \to \Delta$ и $\Gamma \to \Delta CC$, причем с помощью выводов не большей сложности, чем соответствующие выводы предыдущих секвенций. По индуктивному предположению отсюда заключаем, что выводимы и секвенции $D\Gamma \to \Delta$ и $\Gamma \to \Delta C$. По правилу $(\supset\to)$ отсюда получим вывод $(C \supset D)\Gamma \to \Delta$.

Рассмотрим еще случай, когда секвенция S имеет вид $\Gamma \to \Delta \exists\, yB(y)\, \exists\, yB(y)$ и получена из секвенции $\Gamma \to \Delta B(t)\, \exists\, yB(y)\, \exists\, yB(y)$ по правилу вывода $(\to \exists)$. Тогда по индуктивному предположению $\vdash \Gamma \to \Delta B(t)\, \exists\, yB(y)$ и к этой последней секвенции достаточно применить правило $(\to \exists)$, чтобы получить вывод S'. ◁

7. Теорема Генцена. *В исчислении секвенций допустимо правило сечения*:

$$\frac{\Gamma \to \Delta A;\ A\Gamma \to \Delta}{\Gamma \to \Delta}.$$

▷ Утверждение докажем индукцией по количеству логических символов в формуле A. При фиксированной сложности A утверждение будем доказывать индукцией по сумме высот данных выводов $\Gamma \to \Delta A$ и $A\Gamma \to \Delta$.

Начало этой двойной индукции состоит в рассмотрении случая, когда A — атомарная формула и обе выводимые секвенции суть аксиомы. Мы утверждаем, что в этом случае $\Gamma \to \Delta$ также является аксиомой. В самом деле, если $A \in \Gamma$ и $A \in \Delta$, то это очевидно. Пусть, например, $A \notin \Gamma$. Тогда ввиду того что $\Gamma \to \Delta A$ является аксиомой, найдется атомарная формула B такая, что $B \in \Gamma$ и $B \in \Delta$. Но тогда $\Gamma \to \Delta$ является аксиомой.

Разберем теперь несколько случаев индукции.

Пусть A имеет вид $(C \supset D)$ и дано $\vdash \Gamma \to \Delta(C \supset D)$ и $\vdash (C \supset D)\Gamma \to \Delta$. Ввиду обратимости правил $(\to\supset)$ и $(\supset\to)$ выводимы секвенции $C\Gamma \to \Delta$, $D\Gamma \to \Delta$, $\Gamma \to \Delta C$. Применяя правило добавления к $D\Gamma \to \Delta$, получим $\vdash DC\Gamma \to \Delta$. Из $\vdash C\Gamma \to \Delta D$ и $\vdash DC\Gamma \to \Delta$ по правилу сечения (его можно применить в силу индукции по сложности формулы) получим $\vdash C\Gamma \to \Delta$. Затем применим правило сечения с секвенцией $\vdash \Gamma \to \Delta C$ и получим $\vdash \Gamma \to \Delta$.

Пусть A имеет вид $\exists\, xB(x)$ и дано $\vdash \Gamma \to \Delta \exists\, xB(x)$ и $\vdash \exists\, xB(x)\Gamma \to \Delta$. Если $\Gamma \to \Delta \exists\, xB(x)$ есть аксиома, то $\Gamma \to \Delta$ — также аксиома, и поэтому $\vdash \Gamma \to \Delta$ (мы пользуемся тем, что $\exists\, xB(x)$ — не атомарная формула). Пусть $\Gamma \to \Delta \exists\, xB(x)$ получена по некоторому правилу вывода. Здесь следует разобрать два подслучая: *a*) это правило вывода не относится к рассматриваемому вхождению $\exists\, xB(x)$ и *b*) это правило вывода есть $(\to \exists\,)$, относящееся к рассматриваемому вхождению $\exists\, xB(x)$.

В случае *a*) рассуждения однотипны для всех правил. Пусть, например, $\Gamma \to \Delta \exists\, xB(x)$ имеет вид $\Gamma \to \Delta' \neg D \exists\, xB(x)$ и получена из $D\Gamma \to \Delta' \exists\, xB(x)$ по правилу $(\to \neg)$. Из данной выводимости $\vdash \exists\, xB(x)\Gamma \to \Delta' \neg D$ ввиду обратимости правила $(\to \neg)$ заключаем $\vdash \exists\, xB(x)D\Gamma \to \Delta'$, причем высота этого последнего вывода не больше, чем высота вывода секвенции $\exists\, xB(x)\Gamma \to \Delta' \neg D$. По индуктивному предположению (индукции по сумме высот выводов) применим сечение к $D\Gamma \to \Delta' \exists\, xB(x)$ и $\exists\, xB(x)D\Gamma \to \Delta'$ и получим в результате $\vdash D\Gamma \to \Delta'$. После этого применим $(\to \neg)$ и получим $\vdash \Gamma \to \Delta$.

В случае *b*) секвенция $\Gamma \to \Delta \exists\, xB(x)$ получена по правилу $(\to \exists\,)$ из секвенции $\Gamma \to \Delta B(t) \exists\, xB(x)$. Из данного вывода $\vdash \exists\, xB(x)\Gamma \to \Delta$ по правилу добавления получим $\vdash \exists\, xB(x)\Gamma \to \Delta B(t)$, причем высота результирующего вывода не увеличивается. По индуктивному предположению (индукции по сумме высот выводов) применим сечение к

$$\Gamma \to \Delta B(t) \exists\, xB(x) \quad \text{и} \quad \exists\, xB(x)\Gamma \to \Delta B(t)$$

и получим $\vdash \Gamma \to \Delta B(t)$.

Далее, из $\vdash \exists\, xB(x)\Gamma \to \Delta$ ввиду обратимости правила $(\exists \to)$ получим $\vdash B(y)\Gamma \to \Delta$ с новой переменной y. Затем по лемме о подстановке (п. 3) отсюда получим $\vdash B(t)\Gamma \to \Delta$. По предположению индукции (индукции по сложности формулы) можно применить сечение к $\Gamma \to \Delta B(t)$ и $B(t)\Gamma \to \Delta$ и таким образом получить $\vdash \Gamma \to \Delta$. ◁

8. Теперь мы готовы установить эквивалентность исчисления предикатов и нашего исчисления секвенций. Эта эквивалентность формулируется в двух следующих леммах.

Лемма. *Если в исчислении предикатов выводится формула* A, *то в исчислении секвенций выводится секвенция* $\to A$.

▷ Доказательство проведем индукцией по построению вывода $\vdash A$ в исчислении предикатов. Сначала следует вывести в исчислении секвенций все аксиомы исчисления предикатов. Это несложное упражнение на выводимость в исчислении секвенций. Рассмотрим лишь два примера.

Установим $\vdash\to (A \supset C) \supset . (B \supset C) \supset (A \vee B \supset C)$. В самом деле, по лемме п. 2 $\vdash (A \supset C), (B \supset C) \to (A \supset C)$. Ввиду обратимости правила $(\to\supset)$ тогда

$$\vdash A \supset C, \quad B \supset C, \quad A \to C.$$

Аналогично имеем

$$\vdash A \supset C, \quad B \supset C, \quad B \to C.$$

Из этих двух секвенций по правилу $(\vee \to)$ выводим

$$\vdash A \supset C, \quad B \supset C, \quad A \vee B \to C.$$

Применяя несколько раз правило $(\to\supset)$, выведем требуемую секвенцию.

Установим $\vdash\to \forall x(C \supset A(x)) \supset . C \supset \forall x A(x)$, где C не содержит свободно x. По лемме п. 2

$$\vdash \forall x(C \supset A(x)), \quad C \supset A(x) \to C \supset A(x).$$

По правилу $(\forall \to)$ отсюда

$$\vdash \forall x(C \supset A(x)) \to C \supset A(x).$$

Ввиду обратимости правила $(\to\supset)$ имеем

$$\vdash \forall x(C \supset A(x)), \quad C \to A(x).$$

Применяя $(\to \forall)$ получим

$$\vdash \forall x(C \supset A(x)), \quad C \to \forall x A(x)$$

(заметим, что ограничения на переменные в этом правиле выполнены именно потому, что C не содержит свободно x). Применяя к последней секвенции несколько раз правило $(\to\supset)$, получим выводимость требуемой секвенции.

Далее необходимо проверить, что правила вывода исчисления предикатов сохраняют выводимость в исчислении секвенций. Пусть, например, $\vdash\to A$ и $\vdash\to (A \supset B)$. Покажем, что в этой ситуации $\vdash\to B$.

Ввиду обратимости правила $(\to\supset)$ из $\vdash\to (A \supset B)$ следует $\vdash A \to B$. Из $\vdash\to A$ по правилу добавления получим $\vdash\to B, A$. Теперь остается применить сечение к выводимым секвенциям $\to B, A$ и $A \to B$, в результате чего и получим секвенцию $\to B$. ◁

Для каждой секвенции $\Gamma \to \Delta$ определим некоторую формулу $(\Gamma \to \Delta)^0$ — перевод секвенции в формулу исчисления предикатов. А именно, перевод $A_1, \ldots, A_n \to B_1, \ldots, B_m$ есть по определению формула $A_1 \wedge \ldots \wedge A_n \supset B_1 \vee \ldots \vee B_m$. Перевод секвенции $\to B_1, \ldots, B_m$ есть формула $B_1 \vee \ldots \vee B_m$. Перевод секвенции $A_1, \ldots, A_n \to$ есть формула $\neg(A_1 \wedge \ldots \wedge A_n)$. Наконец, перевод секвенции $\to$ есть формула $A \wedge \neg A$ для некоторой фиксированной формулы A.

Лемма. *Если секвенция S выводится в исчислении секвенций, то формула S^0 выводится в исчислении предикатов.*

▷ Необходимо убедиться, что перевод всякой аксиомы исчисления секвенций выводится в исчислении предикатов и что перевод всякого правила вывода допустим в исчислении предикатов. Проверить все эти факты можно с помощью техники естественного вывода в исчислении предикатов (см. нашу книгу [1]), но можно воспользоваться и теоремой о полноте исчисления предикатов и убедиться, что если переводы посылок некоторого правила вывода исчисления секвенций являются логическими законами, то логическим законом является и заключение. ◁

§ 4. О программе Гильберта обоснования математики

1. Пример наивной теории множеств показывает, что привлекательная математическая теория может оказаться внутренне противоречивой. Причины этого можно искать в своеобразии

а) объектов исследования в математике,

б) способов рассуждения относительно этих объектов.

Объекты исследования в математике не являются, как правило, экспериментально наблюдаемыми, это мысленные объекты, возникающие как результат сложной многоступенчатой абстракции действительности. В самом деле, в каком именно смысле существуют иррациональные числа, неизмеримые множества действительных чисел, функция Дирихле, нигде не плотное совершенное множество Кантора и т. п.?

Способ рассуждения относительно таких сложных объектов также получается путем сложной экстраполяции способов рассуждения, применяемых в обыденной жизни или по крайней мере в обычном научном обиходе.

Однако так применяемые способы рассуждения по отношению к мысленным объектам могут вести к неожиданным следствиям. Например, математик склонен, по-видимому, считать, что множество точек в трехмерном координатном евклидовом пространстве $\{\langle x, y, z\rangle \mid \sqrt{x^2 + y^2 + z^2} \leqslant 1\}$ служит хорошей моделью геометрического тела — шара в трехмерном пространстве. Тем не менее в ZFC можно доказать,

что этот «шар» можно разбить на четыре подмножества, из которых с помощью движений в евклидовом пространстве можно сложить два шара, равных первоначальному!

Такого рода следствия вызывают подозрение, что ряд фактов, полученных в рамках определенной математической теории, даже непротиворечивой, просто не имеет никакого отношения к физической реальности и является результатом слишком далеко зашедшей экстраполяции! Это, в свою очередь, вызывает ряд трудных философских вопросов, касающихся ценности математического рассуждения, убедительности математического рассуждения, соответствия между установленными математическими фактами и законами окружающего нас мира.

Далее, может вызывать беспокойство принципиальная неполнота математических теорий. Как мы уже отмечали, доказано, что многие интересные теоретико-множественные утверждения (например, континуум-гипотеза) не могут быть ни выведены, ни опровергнуты в системе ZFC. При этом не видно никаких интуитивно очевидных принципов, которые следовало бы добавить к ZFC, чтобы решить вопрос об истинности таких утверждений. Напротив, эксперименты показывают, что можно предложить равно содержательные и математически интересные аксиоматики, расширяющие ZFC, в которых вопрос об истинности рассматриваемых утверждений решается по-разному. Это вновь наводит на мысль, что принципиально неверно ставить вопрос о том, истинна ли континуум-гипотеза «на самом деле». Никакого «на самом деле» нет. Континуум-гипотеза есть утверждение о мысленных объектах, и вопрос об ее истинности существенно зависит от способов рассуждения, применяемых к таким объектам.

Гёдель доказал, что всякая достаточно богатая и эффективно аксиоматизированная формальная аксиоматическая теория необходимо неполна. Таким образом, невозможно эффективно описать в виде формальной аксиоматической теории даже такую сравнительно узкую область математики, как теория натуральных чисел. Более того, при попытке такого описания найдутся суждения, независимые от построенной теории, т. е. такие, что без противоречия можно присоединить как суждение, так и его отрицание. По теореме о существовании модели (§ 4) тогда и теория с присоединенным суждением, и теория с отрицанием суждения обе имеют модели, что вновь можно рассматривать как довод в пользу отсутствия некоторой «настоящей, единственно правильной» теории.

Наконец, классический способ рассуждения часто ведет к тому, что доказывается существование объектов и в то же время не указывается никакого способа построения этих объектов, даже если речь идет об объектах простой природы, которые в принципе можно было бы эффективно задавать. Например, доказывается, что всякая непрерывная на отрезке функция достигает максимума в некоторой точке, однако предлагаемое доказательство не дает никакого способа отыскания этой точки. В пользу этой теоремы часто приводят два следующих довода: во-первых, эта теорема кажется геометрически очевидной, во-вторых, никому не удалось

пока придумать пример непрерывной функции, не имеющей на отрезке максимума, и тем самым опровергнуть теорему. На первый довод можно ответить, что он не имеет отношения к делу. Факт может быть геометрически и очевиден, но мы в этой теореме имеем дело не с интуитивной геометрией, а с некоторой точной теоретико-множественной моделью непрерывности, и вопрос состоит в том, достаточно ли соответствует эта модель интуиции. Приводимое довольно хитроумное теоретико-множественное доказательство как раз и призвано убедить нас, что модель выбрана удачно. Но мы оспариваем сейчас именно это доказательство, а не интуитивную очевидность факта. Что касается второго довода, то мы и без этой теоремы знаем, что некоторые непрерывные функции имеют максимум. Весь смысл теоремы состоит в том, что для всякой непрерывной функции найдется точка, в которой достигается максимум. Но что значит слово «найдется» в этой теореме и в чем ценность такого доказательства существования объекта, когда не дается никакого способа его построения?

2. Мы видим, что как объект исследования, так и способ рассуждения традиционной математики, и прежде всего теоретико-множественной математики, вызывают серьезную критику.

Неограниченное использование теоретико-множественных концепций ведет к парадоксам.

Неясно, в какой мере объект исследования в математике адекватно соответствует реальности.

Способ рассуждения в математике приводит к неэффективным доказательствам существования даже в случае простых объектов исследования.

Причины парадоксов можно видеть в способах образования понятий, например, в использовании неограниченной аксиомы свертывания.

Чтобы избежать парадоксов, достаточно пользоваться ограниченной теорией множеств, например в рамках системы Цермело—Френкеля. Труднее справиться с остальными возражениями. Кроме того, остается неясным, будет ли система Цермело—Френкеля непротиворечивой. Пока у нас имеется лишь прагматическое наблюдение, что известные парадоксы обычным образом не выводятся в этой системе.

Неэффективность в математике связана с тем обстоятельством, что способы рассуждения, относящиеся к конечным множествам, были экстраполированы на бесконечные совокупности. Действительно, пусть, например, $P(x)$ некоторый предикат, где переменная x рассматривается как пробегающая натуральные числа. Утверждение $\exists x P(x) \vee \neg\exists x P(x)$ рассматривается как безусловно верное (это частный случай закона исключенного третьего), но как узнать, что именно верно $\exists x P(x)$ или $\neg\exists x P(x)$? Мы можем последовательно перебирать натуральные числа $0, 1, 2, \ldots$ и убеждаться последовательно, что $\neg P(0), \neg P(1), \ldots$, но ввиду бесконечности множества натуральных чисел таким способом невозможно убедиться, что $\neg\exists x P(x)$. Надежда может состоять лишь в удачном отыскании натурального n, для которого $P(n)$.

Можно отметить также, что современные физические представления не дают оснований считать, что в природе имеются актуально существующие бесконечные множества. Математика же довольно часто оперирует с бесконечными множествами, такими, как ω, $P(\omega)$ и т. д., как с некоторыми законченными и данными объектами исследования. В этом состоит применение *абстракции актуальной бесконечности* в математике. Многие математики, начиная с Гаусса, возражали против применения этой абстракции, тем не менее актуально бесконечные множества широко и существенным образом используются в современной математике.

Более осторожным является применение в математике *абстракции потенциальной осуществимости*, когда мы признаем лишь возможность неограниченного продолжения построений, отвлекаясь от технических, временных трудностей, но не считаем, что существует множество всех результатов этого построения. Такого рода абстракции вполне достаточно, например, для построения большей части теории натуральных чисел.

3. Радикальный подход к решению обсужденных выше трудностей был предложен Гильбертом в серии работ 1926–1928 гг.

Он предложил разделить суждения классической математики на *действительные* (или *реальные*) и *идеальные*. Только действительные предложения рассматриваются как имеющие содержательный смысл. Действительные предложения должны относиться только к простым конструктивным объектам, не могут использовать актуальной бесконечности. Понимание, в каких случаях действительное предложение истинно, не должно вызывать возражений с точки зрения предыдущей критики. Идеальные же предложения могут быть сколь угодно сложными, они присоединяются к действительным только с целью систематизации теории, для облегчения выводов действительных предложений. Сами по себе идеальные предложения могут и не иметь содержательного смысла.

Рассматриваемая математическая теория позволяет выводить как идеальные, так и реальные суждения. Важно лишь, чтобы для теории выполнялся следующий *принцип корректности*: всякий раз, когда в рассматриваемой теории выводится действительное суждение, оно оказывается истинным с точки зрения содержательного смысла.

Конкретизируем эту идею следующим образом. Рассмотрим формальную аксиоматическую теорию ZF. Это очень богатая выразительными возможностями теория, имеющая дело с очень сложными объектами исследования, в том числе и с актуально бесконечными множествами.

Как нам хорошо известно, в теории ZF интерпретируется теория Ar — формальная арифметика. Фиксируем в языке Ar класс S предложений вида

$$\forall x_1 \ldots x_n A(x_1, \ldots, x_n),$$

где A — *разрешимый предикат*. Например, A может иметь вид равенства $(t = r)$ или более сложный вид, но допускающий эффективную проверку для конкретных натуральных чисел. Так, хорошо известно, что

в языке Ar можно построить формулу $A(n, x, y, z)$ с четырьмя параметрами, естественно выражающую предикат $x^{n+3} + y^{n+3} \neq z^{n+3}$. Тогда великая теорема Ферма

$$\forall xyzn(x^{n+3} + y^{n+3} \neq z^{n+3})$$

может быть элементом S.

Каждому предложению $B \in S$ соответствует формула B^* языка ZF, полученная интерпретацией B в языке ZF. Формулы вида B^* для $B \in S$ и назовем реальными предложениями ZF.

Реальным предложениям можно приписать содержательный смысл естественным образом. Если $B = \forall x_1, \ldots, x_n A(x_1, \ldots, x_n)$, то B содержательно истинно, если для всех натуральных чисел $m_1, \ldots, m_n$ результат проверки оцененной формулы $A(m_1, \ldots, m_n)$ на истинность всегда дает истину. Указанное определение содержательной истинности реальных предложений полностью формулируется в терминах натуральных чисел, не требует привлечения актуально бесконечных множеств и использует лишь абстракцию потенциальной осуществимости: требуется, чтобы для всякого осуществимого набора $m_1, \ldots, m_n$ можно было довести процесс вычисления значения $A(m_1, \ldots, m_n)$ до конца. Множество всех натуральных чисел как актуально завершенная совокупность при этом не используется. Элементарность этого определения подтверждается и тем, что оно легко формализуется в теории Ar. Таким образом, логические средства, используемые для определения содержательной истинности реальных суждений, не вызывают, по-видимому, предыдущей критики.

Отметим теперь важный факт. *Если теория* ZF *непротиворечива, то она удовлетворяет принципу корректности, т. е. всякое выводимое в* ZF *реальное предложение содержательно истинно.*

В самом деле, пусть ZF — непротиворечивая теория. Возьмем произвольный набор чисел $m_1, \ldots, m_n$ и вычислим истинностное значение $A(m_1, \ldots, m_n)$. Мы утверждаем, что это окажется истина. В самом деле, иначе разрешимый предикат $\neg A$ на наборе $m_1, \ldots, m_n$ принимает значение «истина». Путем громоздкого, но в принципе несложного рассуждения (привлекающего машину Тьюринга, участвующую в определении разрешимого предиката A) можно показать, что тогда в Ar выводится $\neg A(\widetilde{m}_1, \ldots, \widetilde{m}_n)$ и, значит, $\exists x_1, \ldots, x_n \neg A(x_1, \ldots, x_n)$ (здесь $\widetilde{m}_i$ есть $S \ldots S0$ m_i раз) и затем $\neg\forall x_1, \ldots, x_n A(x_1, \ldots, x_n)$. Используя интерпретацию в ZF, получим вывод $\neg(\forall x_1, \ldots, x_n A(x_1, \ldots, x_n))^*$. Если $(\forall x_1, \ldots, x_n A(x_1, \ldots, x_n))^*$ было бы выводимо в ZF, то ZF оказалось бы противоречивой теорией.

Подобное рассуждение применимо и ко многим другим теориям. Таким образом, особое значение приобретает непротиворечивость рассматриваемой теории.

Отметим еще, что внимательный анализ показывает, что утверждение о непротиворечивости ZF (и многих других теорий) может быть само записано как *реальное* утверждение. Поэтому, даже если мы

не в состоянии доказать непротиворечивость теории, мы можем *понимать* это утверждение в некотором содержательном смысле и, следовательно, искать содержательные основания для того, чтобы доверять ему или не доверять.

4. Каким же образом можно доказывать непротиворечивость теорий?

Классическим методом здесь является *метод интерпретаций*, с помощью которого вопрос о непротиворечивости одной теории сводится к такому же вопросу относительно другой теории. Фактически метод этот возник задолго до развития точных способов описания теорий методами математической логики. Аналитическая геометрия Декарта (1619) может рассматриваться как интерпретация геометрии средствами анализа. Кэли и Клейн (1871) предложили известную интерпретацию геометрий Лобачевского в геометрии Евклида.

С современной точки зрения метод интерпретаций состоит в построении относительной интерпретации одной формальной аксиоматической теории в другой. При этом, как мы уже отмечали, из непротиворечивости второй теории вытекает непротиворечивость первой.

Но как доказывать непротиворечивость мощных теорий, таких, как ZF и арифметика высокого порядка, для которых уже трудно найти надежную математическую теорию для их обоснования?

Гильберт предложил метод доказательства непротиворечивости, не требующий непосредственно применения интерпретаций.

Можно заметить, что хотя ZF описывает и сложную теорию, *сама формулировка* этой формальной аксиоматической теории требует очень элементарных средств. Кроме того, само понятие непротиворечивости формальной аксиоматической теории ZF очень элементарно и не требует упоминания об актуально бесконечных множествах: непротиворечивость ZF означает просто, что всякая строчка символов языка ZF не является выводом формулы вида $C \wedge \neg C$. Но если формулировка проблемы столь элементарна, то можно надеяться и доказать ее столь же элементарными средствами, не вникая в содержание теории, а изучая лишь формальную структуру выводов теории.

Суть программы Гильберта обоснования математики состоит в том, что сначала изучаемую теорию следует формализовать, а затем уже установить ее непротиворечивость логическими средствами, не вызывающими сомнений, *финитными* методами.

Например, непротиворечивость ZF можно выразить в языке Ar, и было бы заманчиво вывести это утверждение в формальной теории Ar. Тогда вопрос о непротиворечивости ZF свелся бы к вопросу о приемлемости гораздо более простой теории Ar.

К сожалению, эта программа не осуществима в полной мере. Как показал Гёдель в 1932 г., непротиворечивость всякой достаточно богатой и эффективно аксиоматизированной теории не может быть доказана средствами самой этой теории.

Отсюда следует, в частности, что непротиворечивость ZF нельзя установить даже в ZF и подавно нельзя установить в Ar (при условии, конечно, что эти теории непротиворечивы).

Для доказательства непротиворечивости теорий следует искать логические средства, достаточно убедительные, но не формализуемые в рамках исходной теории. Такие логические средства должны иметь интуитивный смысл с некоторой содержательной точки зрения. Необходимые логические средства были разработаны в рамках теории неклассических логик, и, прежде всего, *математического интуиционизма* [16]. В настоящее время непротиворечивость теорий Ar или Ar2 можно считать надежно установленной. Непротиворечивость такой теории, как ZF, гораздо более проблематична.

Независимо от проблемы установления непротиворечивости, метод формализации математических теорий, предложенный Гильбертом, является центральным методом в современной теории доказательств.

Литература

1. *Колмогоров А. Н., Драгалин А. Г.* Введение в математическую логику. М.: Издательство Московского университета, 1982. См. также наст. издание.
2. *Клини С. К.* Математическая логика. М.: Мир, 1973.
3. *Клини С. К.* Введение в метаматематику. М.: ИЛ, 1957.
4. *Мендельсон Э.* Введение в математическую логику. М.: Наука, 1976.
5. *Шенфилд Дж.* Математическая логика. М.: Наука, 1975.
6. *Гудстейн Р. Л.* Математическая логика. М.: ИЛ, 1961.
7. *Гильберт Д., Бернайс П.* Основания математики. Т. 1, 2. М.: Наука, 1979, 1982.
8. *Новиков П. С.* Элементы математической логики. М.: Физматгиз, 1959.
9. *Ершов Ю. Л., Палютин Е. А.* Математическая логика. М.: Наука, 1979.
10. *Бурбаки Н.* Теория множеств. М.: 1965.
11. *Френкель А., Бар-Хиллел И.* Основания теории множеств. М.: Мир, 1966.
12. *Коэн П. Дж.* Теория множеств и континуум-гипотеза. М.: Мир, 1969.
13. *Йех Т.* Теория множеств и метод форсинга. М.: Мир, 1973.
14. *Такеути Г.* Теория доказательств. М.: Мир, 1978.
15. Математическая теория логического вывода. Сборник переводов. М.: Наука, 1967.
16. *Драгалин А. Г.* Математический интуиционизм. Введение в теорию доказательств. М.: Наука, 1979. См. также: *Драгалин А. Г.* Конструктивная теория доказательств и нестандартный анализ. М.: УРСС, 2003. С. 27–230.
17. *Мальцев А. И.* Алгоритмы и рекурсивные функции. М.: Наука, 1965.
18. *Роджерс Х.* Теория рекурсивных функций и эффективная вычислимость. М.: Мир, 1972.
19. *Лавров И. А., Максимова Л. Л.* Задачи по теории множеств, математической логике и теории алгорифмов. М.: Наука, 1975.

Именной указатель*

---

* Именной указатель составлен *Е. Г. Драгалиной-Чёрной.*

Предметный указатель*

* Предметный указатель составлен *Е. Г. Драгалиной-Чёрной.*

Содержание