А. Н. Колмогоров, А. Г. Драгалин

ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ

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

ИЗДАТЕЛЬСТВО
МОСКОВСКОГО УНИВЕРСИТЕТА
1982

УДК 517.1

Колмогоров А. Н., Драгалин А. Г. Введение в математическую логику. — М.: Изд-во Моск. ун-та, 1982. — 120 с.

Учебное пособие предназначено для начинающих математиков, которые желают ознакомиться со строением математического языка и математических теорий. Наряду с начальными понятиями теории множеств излагаются основы логики высказываний и логики предикатов. Изложение не предполагает специальных знаний и рассчитано на студентов младших курсов.

Библиогр. 9 назв. Ил. 2

Рецензенты:

кафедра высшей математики № 2
Ленинградского политехнического института;
чл.-кор. АН СССР В. Я. КОЗЛОВ

Андрей Николаевич Колмогоров, Альберт Григорьевич Драгалин

ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ

Заведующий редакцией С. И. Зеленский. Редактор А. А. Локшин. Мл. редактор О. М. Денисова. Художественный редактор Л. В. Мухина. Технический редактор К. С. Чистякова. Корректоры Л. А. Айдарбекова, Т. С. Милякова.

Тематический план 1982 г. № 114
ИБ № 1223

Сдано в набор 28.07.82. Подписано к печати 09.11.82. Формат 60×90¹/₁₆. Бумага тип. № 3. Гарнитура литературная. Высокая печать. Усл. печ. л. 7,50. Уч.-изд. л. 6,88. Зак. 478. Тираж 29 500 экз. Цена 25 коп. Изд. № 2540.
Ордена «Знак Почета» издательство Московского университета. 103009, Москва, ул. Герцена, 5/7. Типография ордена «Знак Почета» изд-ва МГУ. Москва, Ленинские горы

К $\frac{17020200000-175}{077(02)-82}$ 114-82

ОГЛАВЛЕНИЕ

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 предполагается изложить начала теории множеств и теории алгорифмов, теорему Геделя о полноте исчисления предикатов, обсудить программу 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 $\triangle$ в тексте отмечает начало доказательства, а знак $\square$ — 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, принятой к печати издательством Московского университета, предполагается большее внимание уделить фундаментальным результатам математической логики. Мы вновь вернемся к рассмотрению понятия множества, но уже на базе формальной аксиоматической теории Цермело — Френкеля. Таким образом, мы надеемся дать неспециалисту представление о классических результатах математической логики и подготовить будущего специалиста к изучению более подробных руководств.

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 на 1910—1913 гг.

В двадцатых годах нашего 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 девятнадцатого 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 откры-

тие в начале нашего 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 Геделя, полученная в тридцатых годах нашего 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 Геделя 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 алгоритма, 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

$$1,\ 2,\ 2/3,\ 4/2,\ e \text{ (как обозначение числа } e),\ 5-3,\ \lim_{x\to 0}\frac{e^x-1}{x}.$$

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 превра-

щается 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

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

подставляя же обозначения отрицательных чисел — ложные:

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

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).

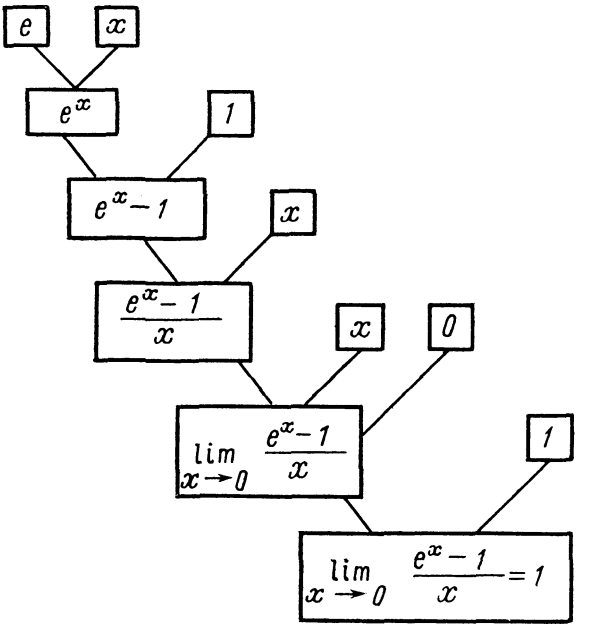


Рис. 1

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

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

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 выглядит 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, ε, δ 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:

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

§ 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*

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

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:

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

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 $S \subseteq P$».

$$\varnothing \text{ — } \textit{пустое множество},$$
$$\bigwedge^{x} \neg (x \in \varnothing).$$

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

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

Это так называемый *модус силлогизма bArbArA*.

*3. Какие еще существуют аналогичные правила вывода? Имеются в виду 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 вто-

рое — понятие S с тем же третьим понятием M. Возможны четыре схемы такого рода правил (в традиционной терминологии — четыре *фигуры силлогизма*):

I	II	III	IV
· (M, P) · (S, M)	· (P, M) · (S, M)	· (M, P) · (M, S)	· (P, M) · (M, S)
· (S, P)	· (S, P)	· (S, P)	· (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	cAlEmEs
cElArEnt	cAmEstrEs	fErIs*O*	frEsIs*On*
dArII	fEstIn*O*	dIsAmIs	dImAtIs
fErI*O*	bArOc*O*	b*O*cAd*O*	*bAmAlIp
		*dArAptI	*fEsAp*O*
		*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 остаются 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 $\{x|F(x)\}$ 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:

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

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 $f : M_1 \to M_2$.

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, сле-

дует 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

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

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 $a \| b$, $a \perp b$, $x < y$, $x \leqslant y$).

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:

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

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

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 им связанных.

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,

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

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 $\langle x_1, ..., x_m\rangle$, называют функцией m переменных и вместо $f(\langle x_1, ..., x_m\rangle)$, пишут $f(x_1, ..., x_m)$.

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 $\frac{1}{0}=15$ ложно (так как число 15 не равно символу «бессмысленно»), а формула $\neg\left(\frac{1}{0}=15\right)$ уже истинна.

§ 5. МАТЕМАТИЧЕСКИЕ СТРУКТУРЫ

1. С конца 19-го — начала 20-го 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):

$R1$. $a+b=b+a$.
$R2$. $a+b(b+c)=(a+b)+c$.
$R3$. $\forall a\forall b\exists!\, c(a+c=b)$.
$R4$. $a(bc)=(ab)c$.
$R5$. $a(b+c)=ab+ac$.
$R6$. $(a+b)c=ac+bc$.

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:

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

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

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

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

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

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, $1+i$ 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

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

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

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

т. е. члены пары $\langle a, b\rangle$ рассматриваются как элементы кольца $\mathbf{D}$. 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 из

1) 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

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

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 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 $BR8$.

Упражнения. 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 $\langle 1, 1, ..., 1 \rangle$, а нуль $\langle 0, 0, ..., 0 \rangle$.

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

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

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

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

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

$$e_1, e_2, ..., e_m.$$

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

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

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

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

Очевидно,

$$\bar{\bar{A}}=A,\ A\cdot\bar{A}=\varnothing.$$

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.

Л е м м а. *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) $a\bar{a}=o$.

$\triangle a=(\bar{\bar{a}}+e)+e=a+(e+e)=a$.
$a+\bar{a}=a+(a+e)=(a+a)+e=e$.
$a\bar{a}=a(a+e)=a+a=o$. □

Введем отношение $\leqslant$, положив

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

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

$$ac=(ab)c=a(bc)=ab=a.\ \square$$

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) $a<c\wedge b\leqslant c\Rightarrow a+b\leqslant c$,
(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, 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 только 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 булевому 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 $b' = \sum_{a_i < b} a_i$. 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

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

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

$$\left(\frac{1}{3}, \frac{2}{3}\right), \left(\frac{1}{9}, \frac{2}{9}\right), \left(\frac{7}{9}, \frac{8}{9}\right), \left(\frac{1}{27}, \frac{2}{27}\right),$$
$$\left(\frac{7}{27}, \frac{8}{28}\right), \ldots$$

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:

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

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

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

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

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

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 общó, 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:

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

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) $a \cap a = a$.

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

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

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

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

$\triangleright$ 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. $\square$

Положим по определению

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

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

$\triangleright$ (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 $A3$. $\square$

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

$\triangleright$ (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 $a \cup b \leqslant c$. $\square$

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

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

$\triangleright$ (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 $a \cap \bar{a} = b \cap \bar{b}$. $\square$

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) $a \cup o = a$, $a \cap o = o$;

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

Важная характеристика дополнения определяется следующим свойством:

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

$$\triangleright\ c = \underset{(19)}{o} \cup c \underset{(15)}{=} (a \cap \bar{a}) \cup c \underset{A4}{=} (a \cup c) \cap (\bar{a} \cup c) =$$

$$= e \cap (\bar{a} \cup c) \underset{(20)}{=} \bar{a} \cup c, \text{ т. е. } \bar{a} \leqslant c.$$

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

$$= o \cup (\bar{a} \cap c) \underset{(19)}{=} \bar{a} \cap c, \text{ т. е. } c \leqslant \bar{a}. \ \square$$

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

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

Следующие два равенства называются *законами де Моргана:*

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

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

$\triangleright$ (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, $(a \cup b) \cup c = (a \cup b) \cup (\bar{a} \cap \bar{b}) = (a \cup b \cup \bar{a}) \cap (a \cup b \cup \bar{b}) = e \cap e = e$. $\square$

Следующая эквивалентность называется *законом контрапозиции:*

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

$\triangleright$ 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 $\overline{\bar{a} \cap \bar{b}} = \bar{\bar{b}}$ и ввиду (24) и (22) $a \cup b = b$, т. е. $a \leqslant b$. $\square$

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

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

Определим *разность* двух элементов

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

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

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

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

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

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

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

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 $\bigcup$. 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 $f(a_1, ..., a_n)$, отображающих $\mathbf{D}^n$ в $\mathbf{D}$.

Имеется четыре попарно не равносильных операции над одним высказыванием:

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

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

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

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:

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

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

$$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B) \Leftrightarrow F_{13}(A, B).$$

В этом базисе конъюнкция и дизъюнкция выражаются так:

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

2. Будем считать буквы P, Q, R, ... 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_{13}, «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

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

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 $F(P_1, ..., P_n)$ от пропозициональных переменных $P_1, ..., P_n$ соответствует булева функция $f(x_1, ..., x_n)$ кольца $\mathbf{F}_n$.

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

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

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

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

Примеры тавтологий:

$$A \vee \neg A \text{ (закон исключенного третьего)},$$

$$\neg\neg A \equiv A \text{ (закон двойного отрицания)},$$

$$\neg(A \wedge \neg A) \text{ (закон противоречия)},$$

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

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

Чтобы убедиться, что формула $F(P_1, ..., P_n)$ является тавтологией, достаточно проделать довольно громоздкую, но всегда выполнимую процедуру вычисления соответствующей функции $f(x_1, ..., x_n)$ 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 $P_1, ..., P_n$ будем называть *совершенным конъюнктивным членом* конъюнкцию $A_1 \wedge ... \wedge A_n$, 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, ... Даль-

нейшие 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

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

Здесь A, B_1, ..., B_m суть формулы, Q_1, ..., Q_m — попарно различные пропозициональные буквы. Через $A(Q_1,\ \ldots,\ Q_m\|$

$B_1, ..., B_m$) мы обозначим результат одновременного замещения всех вхождений букв Q_1, ..., Q_m в A на формулы B_1, ..., 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

$$A_1, A_2, ..., A_n,$$

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, ..., 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:

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

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

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

Получим

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

Из аксиомы 1) подстановкой $(P_1, P_2 \| A, (A \supset A))$ 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 $(P_1, P_2 \| A, A)$ 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), 2) ... 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, ..., которые мы обозначаем через x, y, z, ..., и, кроме того, *предикатные буквы* вида P^i_j, где i, $j=0$, 1, 2, ... Буква P^i_j называется i-местной (i-арной) предикатной буквой. Нульместные предикатные буквы назовем *пропозициональными*. Предикатные буквы обозначаем через P, Q, R, ...

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, ..., x_n — индивидные переменные, то $P(x_1, ..., x_n)$ есть формула.

2) Если A и B — формулы, то формулами являются и следующие комбинации символов:

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

3) Если A — формула и x — индивидная переменная, то $\forall xA$ и $\exists xA$ суть формулы.

Все формулы строятся из формул вида 1) с помощью последовательного применения правил 2) и 3). Например, формулой является выражение

$$(\exists u_1 P^2_1(u_1, u_2)\supset P^1_1(u_2)),$$

которое, используя метаобозначения, будем записывать (опуская также внешние скобки) как

$$\exists xP(x, y)\supset Q(y).$$

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

1) В формулу $P(x_1, ..., x_n)$ переменные x_1, ..., x_n входят свободным образом.

2) Свободное вхождение переменной x в формулы A и B остается свободным и в формулах $(A\wedge B)$, $(A\vee B)$, $(A\supset B)$, $\neg A$, $\forall yA$, $\exists yA$, если переменная y отлична от x.

3) Свободное вхождение переменной x в формулу A делается связанным в формулах $\forall xA$, $\exists xA$.

4) Связанные вхождения в A и B остаются связанными в формулах

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

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:

$$|P(y_1, ..., y_n)| = f(y_1, ..., y_n),$$

где $f: M^n \to \mathbf{D}$.

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:

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

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

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

(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 $\pi \in \text{Srt}$ 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 $c \in \text{Cnst}$ языка приписан определенный сорт $\pi \in \text{Srt}$. 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, ... 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 — суть 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, и $f(t_1, \ldots, t_m)$ — 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 ес-

ли 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 $\tilde{l}$ на множестве всех термов языка Ω рекурсией:

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

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

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

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

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

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

Таким образом, можно было бы дать и не индуктивное, *явное* определение функции $\tilde{l}$. 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 $\mathrm{Tm}^{\pi}_{\Omega}$ 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 $\mathrm{At\,Fm}_{\Omega}$.

4. *Формулы* языка Ω определяются индуктивно с помощью следующих ниже семи пунктов. Первый пункт представляет собой базис индукции, а остальные шесть пунк-

тов 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) $\dfrac{A, x}{\forall xA}$, т. е. если уже построена формула A и x — произвольная переменная языка Ω, то разрешается построить новую формулу $\forall xA$; подобным образом следует трактовать и следующий пункт:

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

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 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 формула 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 обладают и формулы $\forall xA$, $\exists xA$.

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 $P(t_1, \ldots, t_m)$ 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 $\forall xA$, $\exists xA$.

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 A формулой языка Ω мы связали некоторый объект $F(A)$;

Б. пусть задано правило, в соответствии с которым, ес-

ли 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 $F(\forall xA)$ и $F(\exists xA)$.

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

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

Упражнение. Проверьте, что $l(\forall x\exists z((P(f(x, y))\wedge \exists xQ(x, z))\supset \exists yQ(x, y)))=6$.

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»:

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

Таким образом, дизъюнкция и конъюнкция связывают сильнее, чем импликации, 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

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

сокращенно запишем в виде

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

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 $\forall xA$, $\exists xA$ 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 кван-

торную 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):

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

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

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

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 $QyA \Leftrightarrow$ $\Leftrightarrow x$ 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. $\mathrm{Fv}(QxA) = \mathrm{Fv}(A) \setminus \{x\}$.

Здесь $\cup$ обозначает объединение множеств, $\setminus$ 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, ... 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:

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

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

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

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

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» Σ, а переменная j остается свободной — параметром суммы. Вместо j мож-

но 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 $B^x_z \approx C^y_z$.

Здесь через B^x_z обозначен результат замещения всех свободных вхождений переменной x в B на переменную z. Аналогично понимается C^y_z. 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:

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

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:

$$T\theta,$$

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

$$T^{\,x_1, \ldots, x_k}_{\,t_1, \ldots, t_k}.$$

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 $\operatorname{dom}\theta' = \operatorname{dom}\theta \setminus \{z\}$ 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) $\left(\exists y P(x, y, z)\right)_{f(x, z)}^{x}$;

4) $\left(\exists z \forall y P(x, y) \supset Q(x)\right)_{f(x, z)}^{x}$;

5) $\left(\forall y P(x, y) \supset Q(x)\right)_{f(x, z)}^{x}$;

6) $\left(P(x, y) \supset \forall y Q(y)\right)_{f(x, y), z}^{x, y}$;

7) $\left(\forall y P(y, z) \vee \exists y R(x, y)\right)_{f(x, y), z}^{x, y}$;

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, ... 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, она зависит 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 произвести 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 $x \in \operatorname{dom}\theta$ 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 $x \in \operatorname{dom}\theta \cap \cap \operatorname{Fv}(QzB)$ терм $\theta(x)$ не содержит свободно переменной z.

6. Если для всех $x \in \operatorname{dom}\theta$ 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 $x \in \operatorname{dom}(\theta)$ 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

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

т. е. из $\operatorname{Fv}(T)$ 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 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 QxB. Тогда рассмотрим два случая.

1) «Простой случай». Какую переменную $y \in \mathrm{dom}\,\theta \cap \mathrm{Fv}(A)$ ни взять, все параметры соответствующего терма $\theta(y)$ отличны от x. Тогда определим

$$[A\theta] \rightleftharpoons Qx[B(\theta - \{x\})].$$

2) «Сложный случай». Найдется переменная $y \in \mathrm{dom}\,\theta \cap \mathrm{Fv}(A)$, 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

$$[A\theta] \rightleftharpoons Qu[(B^x_u)(\theta - \{x\})].$$

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 $(A(x_1, \ldots, x_k \| t_1, \ldots, t_k))$. Если не возникает разночтений, эту запись сокращаем до $A(x_1, \ldots, x_k \| t_1, \ldots, t_k)$ 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 $A(x, y \| t, r)$.

Упражнение. Произведите правильную подстановку:

1) $(\exists y P(z, y, x))(x, y, z \| z, z, y))$;

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

§ 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. п. 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 $\mathrm{Cnst}\subseteq \subseteq \mathrm{Cnst}(D)$. 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 $\{\underline{a}\,|\,a\in D_\pi\}$. 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 $\bar{a}$. 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:

$$D : \pi \mapsto D_\pi \qquad (\pi \in \mathrm{Srt}).$$

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 $\tilde{c} \in D_\pi$, т. е. следует задать функцию

$$\widehat{\mathrm{Cnst}} : c \mapsto \tilde{c}.$$

3) Каждому функциональному символу $f \in \mathrm{Fn}$ вида $(\pi_1 \ldots \pi_k \to \pi)$ следует сопоставить функцию $\tilde{f}$ 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

$$\widehat{\mathrm{Fn}} : f \mapsto \tilde{f}.$$

4) Каждому предикатному символу $P \in \mathrm{Pr}$ вида $(\pi_1, \ldots, \pi_k)$ следует сопоставить предикат $\tilde{P}$ 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 $\tilde{P}$ (т. е. $\tilde{P}$ есть 0 или 1).

Это соответствие задается функцией

$$\widehat{\mathrm{Pr}} : P \mapsto \tilde{P}.$$

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 $|c|_M = \tilde{c}$;

2) если t имеет вид a для $a \in D_\pi$, то $|t|_M = a$;

3) $|f(t_1, \ldots, t_k)|_M = \tilde{f}(|t_1|_M, \ldots, |t_k|_M)$.

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 $t \in \mathrm{Tm}^\pi_\Omega$ 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) $M \models P(t_1, \ldots, t_k) \leftrightarrows \tilde{P}(|t_1|_M, \ldots, |t_k|_M) = 1$;

2) $M \models A \wedge B \leftrightarrows M \models A$ и $M \models B$;

3) $M \models A \vee B \leftrightarrows M \models A$ или $M \models B$;

4) $M \models A \supset B \leftrightarrows$ если $M \models A$, то $M \models B$;

5) $M \models \neg A \leftrightarrows$ неверно, что $M \models A$;

6) $M \models \forall x A \leftrightarrows$ для всякого $a \in D_\pi$, $M \models A^x_{\underline{a}}$;

7) $M \models \exists x A \leftrightarrows$ 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 $M = A^x_a$ *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 $M \models A^x_a$. 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 — *эквивалентность* — с помощью знакомого нам сокращения:

$$A \equiv B \rightleftharpoons (A \supset B) \wedge (B \supset A).$$

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 импликации 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, ..., 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, ..., A_k.

Мы хотели бы полностью проанализировать, как зависит истинность формулы A от истинности формул A_1, ..., A_k. Такой анализ дает построение *таблицы Куайна* для формулы A.

Построение таблицы начинается с того, что под каждой из формул $A_1, ..., A_k$ мы выписываем всевозможные комбинации нулей и единиц. Возникает k столбцов из нулей и единиц, каждый столбец длиной 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, ..., A_k рассматри-

ваемая 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:

$$(t + r) \leftrightharpoons g(t, r),$$

$$(t \cdot r) \leftrightharpoons h(t, r),$$

$$St \leftrightharpoons f(t).$$

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

$$\neg x+y=y+x,$$
$$\neg x=0\supset\exists z(Sz=x),$$
$$Sx=Sy\supset x=y.$$

Можно ввести сокращенные обозначения для формул Ar, естественные с точки зрения интерпретации ω:

$$x\leqslant y\leftrightharpoons\exists z(x+z=y),$$
$$x<y\leftrightharpoons x\leqslant y\wedge\neg x=y,$$
$$(x\text{ — четно})\leftrightharpoons\exists y(x=y+y),$$
$$(x\mid y)\leftrightharpoons\neg x=0\wedge\exists z(x\cdot z=y),$$
$$(x\text{ — простое})\leftrightharpoons\neg x=0\wedge\neg x=S0\wedge$$
$$\forall z((z\mid x)\supset z=S0\vee z=x).$$

Можно выразить некоторые высказывания в языке

1) $\forall x((x\text{ — простое})\supset\exists y((x<y)\wedge(y\text{ — простое})))$ «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

$$A^x{}_0 \wedge \forall x(A \supset A^x{}_{Sx}) \supset \forall x A.$$

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

$$x+y=y+x,$$
$$Sx=Sy \supset x=y,$$
$$\forall x \exists z(x+z=0),$$
$$\neg x=0 \subset \exists y(x \cdot y=S0).$$

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 простроена 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, ... (сорт 0) и переменные для векторов a, b, c, ... (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:

f — одноместный вида $(0 \to 0)$,

g, h — двуместные вида $(0, 0 \to 0)$,

p — двуместный вида $(1, 1 \to 1)$,

q — двуместный вида $(0, 1 \to 1)$.

Обозначим

$$Sx \leftrightharpoons f(x),$$

$$(x + y) \leftrightharpoons g(x, y),$$

$$(x \cdot y) \leftrightharpoons h(x, y),$$

$$(a + b) \leftrightharpoons p(a, b),$$

$$(x \cdot a) \leftrightharpoons q(x, a).$$

Наконец, наш язык содержит два двуместных предикатных символа: P вида $(0, 0)$ и Q вида $(1, 1)$. Введем обозначение:

$$(x = y) \leftrightharpoons P(x, y),$$
$$(a = b) \leftrightharpoons Q(a, b).$$

Вот несколько формул языка Vect:

$$x \cdot (a + b) = x \cdot a + x \cdot b,$$
$$x \cdot (y \cdot a) = (x \cdot y) \cdot a,$$
$$\forall a \exists b\, (a + b = 0_1),$$
$$0_0 \cdot a = 0_1,$$
$$\exists a \exists b \forall x \forall y\, (x \cdot a + y \cdot b = 0_1 \supset x = 0_0 \wedge y = 0_0).$$

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

$$t \in X \rightleftharpoons Q(t, X).$$

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:

$X \subseteq Y \rightleftharpoons \forall x (x \in X \supset x \in Y)$,

$X = Y \rightleftharpoons (X \subseteq Y) \wedge (Y \subseteq X)$,

$X \subset Y \rightleftharpoons (X \subseteq Y) \wedge \neg (X = Y)$,

(X — бесконечно) $\rightleftharpoons$

$$\forall x \exists y (x \leqslant y \wedge y \in X).$$

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 $\mathrm{dom}\,\theta = \mathrm{Fv}(A) \setminus \{x\}$.

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

$$(A\theta)^{x}_{\underline{a}} = A(\theta(\overset{x}{\underline{a}})) \quad .)$$

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:

$\neg$	A	$\vee$	B	$\supset$	$\neg$	(A	$\wedge$	$\neg$	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:

$\neg$	$\exists x \neg$A	$\supset$	$\forall x$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

$$\mathrm{dom}\,\theta = \mathrm{Fv}(A) \setminus \{x\}.$$

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, $M \models \exists x \neg (A\theta)$, 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. $\forall x A \sim \forall y (A(x \| y))$,

20. $\exists x A \sim \exists y (A(x \| y))$.

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 $A(x_1, \ldots, x_k \| t_1, \ldots, t_k) \sim B(x_1, \ldots, x_k \| t_1, \ldots, t_k)$.

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 $B(P\|U)$ — результат *правильной подстановки (замены)* P в формуле B на формальный предикат U.

А. Пусть B есть атомарная формула $Q(r_1, \ldots, r_m)$. Если Q отлична от P, то $B(P\|U)=B$. Если же Q есть P, то $B(P\|U)=A(x_1, \ldots, x_k\|r_1, \ldots, r_m)$.

В этом случае, конечно, $k=m$.

Б. B есть $(C\Delta D)$, тогда

$$B(P\|U)=C(P\|U)\Delta D(P\|U).$$

B есть $\neg C$, тогда $B(P\|U)=\neg(C(P\|U))$.

В. B имеет вид QzC. Здесь следует рассмотреть два случая.

1) U не содержит свободно z, или P не входит фактически в C. Напомним, что все вхождения $x_1, \ldots, x_k$ в U считаются связанными. В рассматриваемом случае

$$B(P\|U)=Qz(C(P\|U)).$$

2) U содержит свободно z, и P входит фактически в C. Выберем тогда новую переменную u и положим

$$B(P\|U)=Qu((C_u^z)(P\|U)).$$

В соответствии с этим определением нетрудно увидеть, что формула $R(x)\vee\forall z\neg\forall xQ(x, z)$ представима как результат правильной подстановки

$$(R(x)\vee\forall zP(z))(P\|z\ \neg\forall xQ(x, z)).$$

Теперь мы можем продолжить описание логических законов

23. $\models\forall x_1 \ldots x_k(A\equiv B)\supset .\ C(P\|x_1 \ldots x_kA)\equiv C(P\|x_1 \ldots x_kB)$.

24. Если $A\sim B$, то

$$C(P\|x_1 \ldots x_kA)\sim C(P\|x_1 \ldots x_kB).$$

Именно это правило и решает задачу, поставленную в начале п. 5. Логические законы можно использовать, заменяя эквивалентные подформулы внутри формулы.

Формулу вида $C(P\|x_1 \ldots x_kA)$ 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 призводить 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

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

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

$$Q \wedge \neg\, Q. \square$$

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, ..., образовывать формулы с помощью только логических связок, без кванторов. Такие формулы называются *пропозициональными.*

Делая подстановочные примеры, можно из логических законов пропозиционального 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, § 2, 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 $\forall xA$ и для всякого объекта a имеем $M \models (A_a^x)\theta$, то $M \models (\forall xA)\theta$.

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 $\forall xA$ этого дерева *получена* из A по правилу обобщения; нижней формулой этого дерева является, конечно, формула $\forall xA$.

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 $\forall xC$ и получена в выводе из формулы C по правилу обобщения. Таким образом C выведена с помощью вывода меньшей высоты, чем вывод $\forall xC$, поэтому к выводу C можно применить индуктивное предположение. По структурному требованию x не есть параметр гипотез вывода формулы C. Чтобы показать $M \models (\forall xC)\theta$, 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 $\vdash \forall x A \supset \supset \forall y (A(x \| y))$. 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 п. 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 Γ_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

$$\Gamma \vdash A \supset \forall x C. \quad \square$$

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 $\Gamma, \Delta \vdash B$. □

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 $\dfrac{\Gamma,\ A \vdash B;\ \Gamma,\ B \vdash A}{\Gamma \vdash A \equiv B}$; удаление $\dfrac{\Gamma \vdash A;\ \Gamma \vdash A \equiv B}{\Gamma \vdash B}$; $\dfrac{\Gamma \vdash B;\ \Gamma \vdash A \equiv B}{\Gamma \vdash A}$.

▷ 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 $\vdash \exists\, xA(x) \supset \exists\, yA(y)$. Отсюда Γ, $\exists\, xA(x) \vdash \exists y A(y)$. Следовательно, по модус поненс Γ, $\exists x A(x) \vdash C$.

$\equiv$-введение. Из Γ, $A \vdash B$ и Γ, $B \vdash A$ 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* С). Допустим, что $\exists\, xA(x)$, 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 рассуждению *от противного, 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. исполь-

зовать $\neg$-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

$$A, \neg A \wedge \neg B \vdash A$$

и

$$A, \neg A \wedge \neg B \vdash \neg A.$$

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 $\vdash \exists\, xA(x) \supset \neg\forall x \neg\, A(x)$. С этой целью допустим $\exists x A(x)$ и выведем $\neg\forall x \neg\, A(x)$, т. е. выведем

$$\exists\, xA(x) \vdash \neg\forall x \neg\, A(x).$$

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 форму-

ле 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 Геделя 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) $f : \Sigma^* \to \{0, 1\}$, 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 $V \subseteq \Sigma^*$, $f: V \to \{0, 1\}$, 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 Геделя и Черча 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 Геделя 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 Гедель

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 Сколемом в 20-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, $x^2\rightleftharpoons x\cdot x$. Если ввести естественное сокращение: $x\leqslant y \rightleftharpoons \exists z(x+z^2=y)$, 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, $x<y\rightleftharpoons(x\leqslant y)\wedge x\neq y$. 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, ..., форму-

лам 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:

$$\neg\exists\, b(A\in b\wedge B\in b\wedge C\in b)\wedge A\notin a\vee$$
$$B\notin a\wedge C\notin a\wedge\exists D(D\in a\wedge[ADB])\supset$$
$$\exists\, E(E\in a\wedge([AEC]\vee[BEC])).$$

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.

* Приложение 1

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 и 111.

Для понимания механизма действия изложенной теории полезно выписать 16 кодовых слов длины 7.

* Приложение 2

ПРИМЕНЕНИЯ К КОНТАКТНЫМ СХЕМАМ

На рис. 2а 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. 2а пропускает ток из узла 1 в узел 2 в том и только в том случае, если сигналы x, y, z удовлетворяют условию

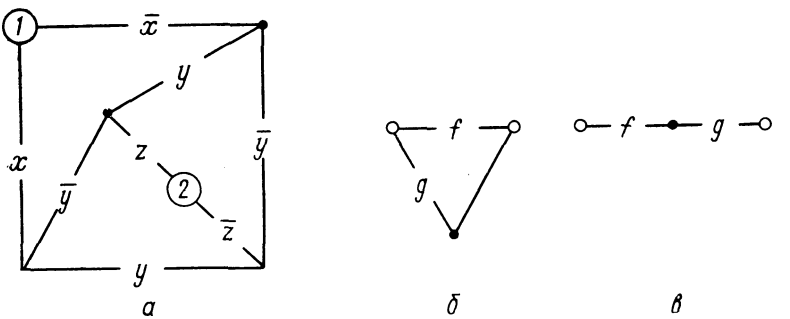
$$x\bar{y}z \cup \bar{x}yz \cup xy\bar{z} \cup \bar{x}\bar{y}\bar{z} = 1,$$

т. е.

$$x+y+z=1.$$

Схемы такого типа с двумя выделенными узлами (на рис. 2а 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. 2б) и последовательных (рис. 2в) 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.

А. Н. Колмогоров,
А. Г. Драгалин

ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ

ИЗДАТЕЛЬСТВО МОСКОВСКОГО УНИВЕРСИТЕТА