

МГТУ ФН-12 МГТУ ФН-12 МГТУ ФН-12

Московский государственный технический университет  
имени Н.Э. Баумана

---

Факультет «Фундаментальные науки»  
Кафедра «Математическое моделирование»

**А.Н. Канатников**

# **МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ**

**Конспект лекций**

Для студентов кафедры ИУ9

Москва  
2009

МГТУ ФН-12 МГТУ ФН-12 МГТУ ФН-12

## 6. ПРИМЕРЫ ФОРМАЛЬНЫХ ТЕОРИЙ

Рассмотрим построение формальных теорий, описывающих некоторые конкретные математические дисциплины.

### 6.1. Теория групп

Подбор составляющих любой формальной теории — творческий процесс, не дающий однозначного результата. В основе, конечно, лежат содержательные аксиомы соответствующей дисциплины. В теории групп встречаются объекты одного типа. Значит, можно использовать один сорт переменных. Для обозначения операции группы нужен один функциональный символ арности 2. Но есть еще две вторичные операции, точнее очевидная константа и унарная операция вычисления обратного элемента. Для записей условий нужен хотя бы один предикатный символ и наиболее уместным является символ равенства. Это бинарный символ, но чтобы бинарный предикатный символ мог расцениваться именно как знак равенства, нужны некоторые требования (аксиомы).

Учитывая вышесказанное опишем формальную теорию групп  $G$ . Рассмотрим односортный логико-математический язык с одной константой, которую мы обозначим через  $e$ , двумя функциональными символами  $m(x, y)$  и  $i(x)$  и одним бинарным предикатным символом  $p(x, y)$ . Правила вывода — стандартные для исчисления предикатов. Запишем нелогические аксиомы:

- 1)  $p(x, y) \rightarrow (p(x, z) \rightarrow p(y, z));$
- 2)  $p(x, y) \rightarrow p(m(x, z), m(y, z));$
- 3)  $p(x, y) \rightarrow p(m(z, x), m(z, y));$
- 4)  $p(m(m(x, y), z), m(x, m(y, z)));$
- 5)  $p(m(x, e), x);$
- 6)  $p(m(x, i(x)), e).$

Напомним, что нелогические аксиомы любой формальной теории должны быть замкнутыми формулами. Поэтому здесь неявно предполагается, что аксиомы теории групп замкнуты кванторами всеобщности по всем свободным переменным.

Запись нелогических аксиом прямо следует описанию логико-математического языка, но неудобна для восприятия человеком. Введем альтернативные обозначения  $x * y$  вместо  $m(x, y)$ ,  $x^{-1}$  вместо  $i(x)$ ,  $1$  вместо  $e$  и  $x = y$  вместо  $p(x, y)$ . Тогда перечисленные аксиомы будут выглядеть следующим образом:

- 1°  $(x = y) \rightarrow ((x = z) \rightarrow (y = z));$
- 2°  $(x = y) \rightarrow (x * z = y * z);$
- 3°  $(x = y) \rightarrow (z * x = z * y);$
- 4°  $(x * y) * z = x * (y * z);$
- 5°  $x * 1 = x;$
- 6°  $x * x^{-1} = 1.$

Из рассмотренных аксиом (в любой записи) первая характеризует предикат, вторая и третья связывают предикат с основной операцией, а последние три фиксируют свойства операций группы. Вообще говоря, бинарный предикат определяет на носителе интерпретации отношение, и если мы хотим рассматривать предикат как равенство, указанное отношение должно быть отношением эквивалентности, т.е. должны быть истинными утверждения о рефлексивности, симметричности и транзитивности. В аксиоме 1 можно усмотреть рефлексивность, но не хватает двух других свойств.

Не следует ожидать, что выбором некоторых формул в качестве аксиом можно гарантировать, что рассматриваемый предикат будет именно равенством, т.е. истинным при совпадении объектов, обозначаемых двумя термами. Для теории групп такие попытки даже вредны. Дело в том, что термин „равны“ следует понимать как „неразличимы“, т.е. это могут быть разные, вообще говоря, объекты, но подпадающие под одно понятие. В математике формирование понятий связано с отношением эквивалентности. Так и здесь: отношение  $x = y$  на самом деле — это отношение эквивалентности.

Отметим, что в  $\mathbf{G}$  сохраняются все правила естественного вывода, а доказательство теорем представляет собой частный вывод, в котором роль гипотез играют нелогические аксиомы. Для сокращения вывода сами нелогические аксиомы удобно заменить некоторыми правилами вывода, нелогическими правилами естественного вывода. Так, аксиомам 2 и 3 соответствуют правила

$$\frac{\Gamma \vdash X = Y}{\Gamma \vdash X * Z = Y * Z}, \quad \frac{\Gamma \vdash X = Y}{\Gamma \vdash Z * X = Z * Y}, \quad (6.1)$$

а аксиомы 4–6 трансформируются в схемы выводимых формул:

$$\vdash (X * Y) * Z = X * (Y * Z), \quad \vdash X * 1 = X, \quad \vdash X * X^{-1} = 1. \quad (6.2)$$

Например, первое из правил (6.1) устанавливается следующим образом:

$$\begin{array}{c} \Gamma \vdash X * Z = Y * Z \\ \swarrow \quad \searrow \\ \Gamma \vdash X = Y \quad \Gamma \vdash X = Y \rightarrow X * Z = Y * Z \\ \quad \quad \quad \vdash X = Y \rightarrow X * Z = Y * Z \\ \quad \quad \quad \vdash \forall z (X = Y \rightarrow X * z = Y * z) \\ \quad \quad \quad \vdash \forall y \forall z (X = y \rightarrow X * z = y * z) \\ \quad \quad \quad \vdash \forall x \forall y \forall z (x = y \rightarrow x * z = y * z) \end{array}$$

Обращаем внимание на переход от переменной (например  $x$ ) к произвольной формуле (в данном случае  $X$ ) через снятие квантора с подстановкой. Аналогично устанавливаются секвенции (6.2). Приведем вывод второй из них:

$$\vdash X * 1 = X \Leftarrow \forall x (x * 1 = x).$$

Аксиома 1 позволяет установить правила

$$\vdash X = X, \quad \frac{\Gamma \vdash X = Y}{\Gamma \vdash Y = X}, \quad \frac{\Gamma \vdash X = Y; \Gamma \vdash Y = Z}{\Gamma \vdash X = Z},$$

выражающие свойства, характеризующие отношение эквивалентности (рефлексивность, симметричность, транзитивность).

В принципе формулу  $X = X$  (точнее  $\forall x (x = x)$ ) следовало бы ввести как аксиому поддержки формального равенства. Однако в данном случае эта формула оказывается выводимой в теории  $\mathbf{G}$ . Действительно,

$$\begin{array}{c} \vdash X = X \\ \swarrow \quad \searrow \\ \vdash X * 1 = X \rightarrow X = X \quad \vdash X * 1 = X \\ \swarrow \quad \searrow \\ \vdash X * 1 = X \rightarrow (X * 1 = X \rightarrow X = X) \quad \vdash X * 1 = X \\ \quad \quad \quad \vdash \forall z (X * 1 = X \rightarrow (X * 1 = z \rightarrow X = z)) \\ \quad \quad \quad \vdash \forall y \forall z (X * 1 = y \rightarrow (X * 1 = z \rightarrow y = z)) \\ \quad \quad \quad \vdash \forall x \forall y \forall z (x = y \rightarrow (x = z \rightarrow y = z)) \end{array}$$

Используя доказанную рефлексивность, можно доказать и симметричность:

$$\begin{array}{c}
 \Gamma \vdash Y = X \\
 \swarrow \quad \searrow \\
 \Gamma \vdash X = Y \quad X = Y \vdash Y = X \\
 \swarrow \quad \searrow \\
 X = Y, X = X \vdash Y = X \quad \vdash X = X \\
 \downarrow \\
 X = Y \vdash X = X \rightarrow Y = X \\
 \downarrow \\
 \vdash X = Y \rightarrow (X = X \rightarrow Y = X) \\
 \downarrow \\
 \vdash \forall x \forall y \forall z (x = y \rightarrow (x = z \rightarrow y = z))
 \end{array}$$

Транзитивность можно получить из аксиомы 1 с доказанным свойством симметричности:

$$\begin{array}{c}
 \Gamma \vdash X = Z \\
 \swarrow \quad \searrow \\
 \Gamma \vdash X = Y \wedge Y = Z \quad X = Y \wedge Y = Z \vdash X = Z \\
 \swarrow \quad \searrow \quad \downarrow \\
 \Gamma \vdash X = Y \quad \Gamma \vdash Y = Z \quad X = Y, Y = Z \vdash X = Z \\
 \swarrow \quad \searrow \\
 Y = X, Y = Z \vdash X = Z \quad X = Y \vdash Y = X \\
 \downarrow \quad \downarrow \\
 Y = X \vdash Y = Z \rightarrow X = Z \quad X = Y \vdash X = Y \\
 \downarrow \\
 \vdash Y = X \rightarrow (Y = Z \rightarrow X = Z) \\
 \downarrow \\
 \vdash \forall x \forall y \forall z (x = y \rightarrow (x = z \rightarrow y = z))
 \end{array}$$

Действие симметричности, рефлексивности и транзитивности можно записывать как цепочку равенств:  $X = Y = Z = \dots$

Отметим, что существование левой единицы и левого обратного в аксиомах не оговорено. Однако это можно получить из существования правой единицы и правого обратного для каждого элемента. Действительно, докажем, что правый обратный является левым:

$$\begin{aligned}
 x^{-1} * x &= (x^{-1} * x) * 1 = (x^{-1} * x) * (x^{-1} * (x^{-1})^{-1}) = x^{-1} * (x * (x^{-1} * (x^{-1})^{-1})) = \\
 &= x^{-1} * ((x * x^{-1}) * (x^{-1})^{-1}) = x^{-1} * (1 * (x^{-1})^{-1}) = (x^{-1} * 1) * (x^{-1})^{-1} = x^{-1} * (x^{-1})^{-1} = 1.
 \end{aligned}$$

Теперь докажем, что правая единица является левой:

$$1 * x = (x * x^{-1}) * x = x * (x^{-1} * x) = x * 1 = x.$$

Остальные свойства могут быть получены использованием цепи равенств. Докажем формулу  $(A * X = A) \rightarrow (X = 1)$ , означающую, что правая единица единственная. Содержательное рассуждение таково. Если  $A * X = A$ , то  $A^{-1} * (A * X) = A^{-1} * A = 1$ . Но  $A^{-1} * (A * X) = (A^{-1} * A) * X = 1 * X = X$ . Поэтому  $X = 1$ .

Соответствующий вывод формулы  $(A * X = A) \rightarrow (X = 1)$  может быть таким (для сокращения знак умножения опущен):

$$\begin{array}{c}
 \vdash AX = A \rightarrow X = 1 \\
 \downarrow \\
 AX = A \vdash X = 1 \\
 \swarrow \quad \searrow \\
 AX = A \vdash X = A^{-1}A \quad AX = A \vdash A^{-1}A = 1 \\
 \swarrow \quad \searrow \quad \downarrow \\
 AX = A \vdash X = A^{-1}AX \quad AX = A \vdash A^{-1}AX = A^{-1}A \quad \vdash A^{-1}A = 1 \\
 \downarrow \quad \downarrow \\
 AX = A \vdash A^{-1}AX = X \quad AX = A \vdash AX = A \\
 \swarrow \quad \searrow \\
 \vdash A^{-1}AX = 1 * X \quad \vdash 1 * X = X \\
 \downarrow \\
 \vdash A^{-1}A = 1
 \end{array}$$

## 6.2. Формальная арифметика

Рассмотрим формальную теорию  $AP$ , описывающую элементарную теорию чисел (арифметику), т.е. теорию натуральных чисел с арифметическими операциями. Отметим, что при построении формальных систем всегда руководствуются некоторой реальной математической дисциплиной, которая в таком случае обеспечивает *естественную интерпретацию* строящейся теории. Построенная теория может иметь множество интерпретаций (как теория  $G$ ). Но может быть (а в некоторых случаях должно быть) так, что все интерпретации являются изоморфными, т.е. между этими интерпретациями есть взаимно однозначное соответствие, сохраняющее все свойства этих интерпретаций.

Так должно быть в случае формальной арифметики, поскольку наличие нескольких моделей натуральных чисел, ясно различающихся по своим свойствам, вряд ли можно считать приемлемым. Подчеркнем, что под натуральным мы будем понимать целое неотрицательное число (т.е. включая нуль).

Логико-математический язык должен быть односортным. Есть одна константа, которую мы обозначим через 0, две основные арифметические операции сложение и умножение реализуем двумя бинарными функциональными символами, которые будем обозначать в инфиксной форме знаками  $+$  и  $\cdot$  (этот знак по традиции опускается между двумя переменными). Описание двух операций кольца недостаточно. Характерным свойством натуральных чисел является переход к следующему натуральному числу, вытекающий из процесса пересчета предметов. Это отразим унарным функциональным символом, который будем обозначать в виде  $x^+$ . Наконец, нужен предикатный символ, в качестве которого выбираем формальное равенство.

В основе нашей формальной теории лежит аксиоматика натуральных чисел Пеано, включающая пять аксиом:

P1. 0 — натуральное число.

P2. Если  $n$  — натуральное число, то  $n^+$  — натуральное число.

P3. Если  $m, n$  — натуральные числа и  $m^+ = n^+$ , то  $m = n$ .

P4. Если  $n$  — натуральное число, то  $n^+ \neq 0$ .

P5. Пусть  $A$  — некоторое свойство, которым могут обладать натуральные числа. Предположим, что: а) 0 обладает свойством  $A$ ; б) из того, что  $n$  обладает свойством  $A$ , вытекает, что и  $n^+$  обладает свойством  $A$ . Тогда любое натуральное число обладает свойством  $A$ .

Нетрудно убедиться в том, что все эти аксиомы необходимы. Первые две дают, по существу, индуктивное определение натуральных чисел. Отсутствие аксиомы P3 приводит к существованию древовидной модели, в которой некоторые ветви начинаются не с нуля. Аксиома P4 препятствует появлению циклической модели (например, комплексных корней  $n$ -й степени из 1). Наконец, аксиома P5 обеспечивает связность натурального ряда, т.е. свойство, что любое натуральное число получается с помощью аксиом P1 и P2. Она же лежит в основе принципа математической индукции. С помощью этой аксиомы вводятся основные арифметические операции — сложение и умножение:

P6.  $m + 0 = m$ ;

P7.  $m + n^+ = (m + n)^+$ ;

P8.  $m \cdot 0 = 0$ ;

P9.  $m \cdot n^+ = m \cdot n + m$ .

При построении формальной теории первые две аксиомы Пеано не нужны, поскольку реализуются на уровне логико-математического языка. Например, первая аксиома фактически утверждает, что в языке арифметики есть константа. В то же время в состав аксиом необходимо включить аксиомы поддержки формального равенства. Кроме того, в состав аксиом мы включаем формулы определения арифметических операций. Все аксиомы, кроме аксиомы индукции, должны быть замкнутыми формулами (хотя для краткости мы кванторы опустим,

неявно полагая, что формулы замкнуты кванторами всеобщности по всем свободным переменным). Исключение составляет аксиома индукции. Эта аксиома связана с произвольным свойством, которое характеризуется некоторым предикатом  $A$ , и задается некоторой схемой.

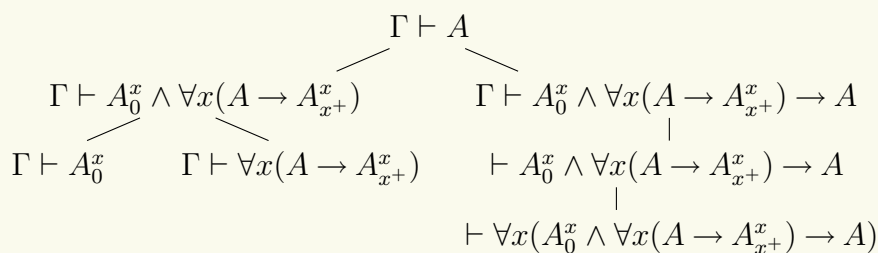
В результате мы получаем одну схему аксиом и восемь аксиом:

- A1.  $(A_0^x \wedge \forall x(A \rightarrow A_{x^+}^x)) \rightarrow A.$
- A2.  $(x^+ = y^+) \rightarrow (x = y).$
- A3.  $\neg(x^+ = 0).$
- A4.  $(x = y) \rightarrow ((x = z) \rightarrow (y = z)).$
- A5.  $(x = y) \rightarrow (x^+ = y^+).$
- A6.  $x + 0 = x.$
- A7.  $x + y^+ = (x + y)^+.$
- A8.  $x \cdot 0 = 0.$
- A9.  $xy^+ = xy + x.$

Как и в случае теории  $\mathbf{G}$ , эти аксиомы удобно преобразовать в правила вывода:

- $$\begin{array}{l}
\text{C1. } \frac{\Gamma \vdash A_0^x; \Gamma \vdash \forall x(A \rightarrow A_{x^+}^x)}{\Gamma \vdash A}; \\
\text{C2. } \frac{\Gamma \vdash X^+ = Y^+}{\Gamma \vdash X = Y}; \\
\text{C3. } \vdash \neg(X^+ = 0); \\
\text{C4. } \vdash X = X; \\
\text{C5. } \frac{\Gamma \vdash X = Y}{\Gamma \vdash Y = X}; \\
\text{C6. } \frac{\Gamma \vdash X = Y; \Gamma \vdash Y = Z}{\Gamma \vdash X = Z}; \\
\text{C7. } \frac{\Gamma \vdash X = Y}{\Gamma \vdash X^+ = Y^+}; \\
\text{C8. } \vdash X + 0 = X; \\
\text{C9. } \vdash X + Y^+ = (X + Y)^+; \\
\text{C10. } \vdash X \cdot 0 = 0; \\
\text{C11. } \vdash X \cdot Y^+ = X \cdot Y + X.
\end{array}$$

Все эти правила устанавливаются так же как и в теории групп. Например правило C1:



Отметим, что в этом правиле выбор переменной  $x$  не является существенным: последний шаг может идти с переименованием. На практике в качестве переменной  $x$  следует выбирать любую, не входящую свободно в формулы списка  $\Gamma$ .

Правила С4–С6 отражают характерные черты формального равенства как предиката для отношения эквивалентности, они полностью определяются аксиомами А4 и А6. Вывод этих правил повторяет вывод соответствующих правил формальной теории групп.

Многие ключевые факты арифметики (например, коммутативность сложения) вытекают из сформулированных аксиом. В их доказательстве особую роль играет схема аксиом, отражающая принцип математической индукции. Рассмотрим некоторые формулы.

1.  $(X = Y) \rightarrow (X + Z = Y + Z).$

◀ На содержательном уровне рассуждение таково. При  $z = 0$  равенство  $X + z = Y + z$  сводится к очевидному равенству  $X + 0 = Y + 0$ , вытекающему из цепочки  $X + 0 = X = Y = Y + 0$ . Если верно равенство  $X + z = Y + z$ , то  $X + z^+ = (X + z)^+ = (Y + z)^+ = Y + z^+$ . На основании метода математической индукции делаем вывод, что равенство  $X + z = Y + z$  верно для любого  $z$ . Формальный вывод рассматриваемой формулы строится на сведении к правилу C1 и может выглядеть так:

$$\begin{array}{c}
 \vdash X = Y \rightarrow X + Z = Y + Z \\
 \quad \quad \quad \downarrow \\
 X = Y \vdash X + Z = Y + Z \\
 \quad \quad \quad \downarrow \\
 X = Y \vdash \forall z (X + z = Y + z) \\
 \quad \quad \quad \downarrow \\
 X = Y \vdash X + z = Y + z \\
 \swarrow \quad \quad \searrow \\
 X = Y \vdash X + 0 = Y + 0 \quad X = Y \vdash \forall z (X + z = Y + z \rightarrow X + z^+ = Y + z^+) \\
 \quad \quad \quad \downarrow \quad \quad \quad \downarrow \\
 \boxed{1} \quad \quad \quad X = Y \vdash X + z = Y + z \rightarrow X + z^+ = Y + z^+ \\
 \quad \quad \quad \downarrow \\
 X = Y, X + z = Y + z \vdash X + z^+ = Y + z^+ \\
 \quad \quad \quad \downarrow \\
 X + z = Y + z \vdash X + z^+ = Y + z^+ \\
 \quad \quad \quad \downarrow \\
 \boxed{2}
 \end{array}$$

Обе ветки заканчиваются секвенциями, которые можно обосновать цепочкой равенств. Ветка  $\boxed{1}$  подробно раскрывается так:

$$\begin{array}{c}
 X = Y \vdash X + 0 = Y + 0 \\
 \swarrow \quad \quad \searrow \\
 X = Y \vdash X + 0 = X \quad X = Y \vdash X = Y + 0 \\
 \quad \quad \quad \downarrow \quad \quad \quad \downarrow \quad \quad \quad \downarrow \\
 \vdash X + 0 = X \quad X = Y \vdash X = Y \quad X = Y \vdash Y = Y + 0 \\
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \downarrow \\
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \vdash Y = Y + 0 \\
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \downarrow \\
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \vdash Y + 0 = Y
 \end{array}$$

Ветка  $\boxed{2}$  раскрывается аналогично (список  $\Gamma$  содержит одну формулу  $X + z = Y + z$ ):

$$\begin{array}{c}
 \Gamma \vdash X + z^+ = Y + z^+ \\
 \swarrow \quad \quad \searrow \\
 \Gamma \vdash X + z^+ = (X + z)^+ \quad \Gamma \vdash (X + z)^+ = Y + z^+ \\
 \quad \quad \quad \downarrow \quad \quad \quad \downarrow \quad \quad \quad \downarrow \quad \quad \quad \downarrow \\
 \vdash X + z^+ = (X + z)^+ \quad \Gamma \vdash (X + z)^+ = (Y + z)^+ \quad \Gamma \vdash (Y + z)^+ = Y + z^+ \\
 \quad \quad \quad \downarrow \quad \quad \quad \downarrow \quad \quad \quad \downarrow \\
 \quad \quad \quad \Gamma \vdash X + z = Y + z \quad \vdash (Y + z)^+ = Y + z^+ \\
 \quad \quad \quad \quad \quad \quad \downarrow \\
 \quad \quad \quad \quad \quad \quad \vdash Y + z^+ = (Y + z)^+
 \end{array}$$

Как видим, формальный вывод заметно длиннее содержательного. ►

## 2. $0 + X = X$ .

◀ Содержательное доказательство основано на замене  $Z$  переменной и применении индукции по этой переменной. Имеем  $0 + 0 = 0$ . Если  $0 + x = x$ , то  $0 + x^+ = (0 + x)^+ = x^+$ . Значит,

$0 + x = x$ . Формальное доказательство следующее:

$$\begin{array}{c}
 \vdash 0 + X = X \\
 | \\
 \vdash \forall x(0 + x = x) \\
 | \\
 \vdash 0 + x = x \\
 \swarrow \quad \searrow \\
 \vdash 0 + 0 = 0 \quad \vdash \forall x(0 + x = x \rightarrow 0 + x^+ = x^+) \\
 | \\
 \vdash 0 + x = x \rightarrow 0 + x^+ = x^+ \\
 | \\
 0 + x = x \vdash 0 + x^+ = x^+ \\
 \swarrow \quad \searrow \\
 0 + x = x \vdash 0 + x^+ = (0 + x)^+ \quad 0 + x = x \vdash (0 + x)^+ = x^+ \\
 | \quad | \\
 \vdash 0 + x^+ = (0 + x)^+ \quad 0 + x = x \vdash 0 + x = x
 \end{array}$$

Отметим переход от формулы  $X$  к переменной  $x$ , совершенный в начале вывода. Это стандартная подготовка к применению индукции, состоящая в замене одной из подформул переменной, которая становится переменной индукции. ►

3.  $X^+ + Y = X + Y^+$ .

◀ Ограничимся содержательным рассуждением. Имеем  $x^+ + 0 = x^+ = (x + 0)^+ = x + 0^+$ . Пусть  $x^+ + y = x + y^+$ . Тогда  $x^+ + y^+ = (x^+ + y)^+ = (x + y^+)^+ = x + y^{++}$ . Таким образом,  $x^+ + y = x + y^+$ . ►

4.  $X = Y \rightarrow Z + X = Z + Y$ .

◀ Содержательное рассуждение можно строить на переменной  $z$ , поставленной взамен формулы  $Z$ . при  $z = 0$  имеем  $0 + X = X = Y = 0 + Y$  (использовано уже установленное свойство 2). Пусть доказано, что  $z + X = z + Y$ . Тогда, согласно свойству 3

$$z^+ + X = z + X^+ = (z + X)^+ = (z + Y)^+ = z + Y^+ = z^+ + Y.$$

В соответствии с методом математической индукции, если  $X = Y$ , то  $z + X = z + Y$ . ►

5.  $(X + Y) + Z = X + (Y + Z)$ .

◀ Содержательное доказательство основано на методе математической индукции по переменной  $z$ , включенной в формулу взамен  $Z$ . Согласно свойству 4 имеем:  $(X + Y) + 0 = X + Y = X + (Y + 0)$ , поскольку  $Y = Y + 0$ . Предположим  $(X + Y) + z = X + (Y + z)$ . Тогда

$$(X + Y) + z^+ = ((X + Y) + z)^+ = ((X + (Y + z)))^+ = X + (Y + z)^+ = X + (Y + z^+).$$

В соответствии с методом математической индукции заключаем, что  $(X + Y) + z = X + (Y + z)$ . ►

6.  $X + Y = Y + X$ .

◀ Заменяем формулу  $Y$  индуктивной переменной  $y$ . При  $y = 0$  имеем  $X + 0 = X = 0 + X$ . Если  $X + y = y + X$ , то  $X + y^+ = (X + y)^+ = (y + X)^+ = y + X^+ = y^+ + X$ . Значит,  $X + y = y + X$  для любого значения переменной  $y$ . ►

7.  $X + Y = 0 \rightarrow X = 0$ .

◀ Заменяем формулу  $X$  индуктивной переменной  $x$ . При  $x = 0$  имеем формулу  $0 + Y = 0 \rightarrow 0 = 0$ , которая получается из истинной формулы  $0 = 0$  присоединением посылки. Пусть формула

$x + Y = 0 \rightarrow x = 0$  истинна. Тогда

$$\begin{array}{c}
 \vdash (x^+ + Y = 0) \rightarrow (x^+ = 0) \\
 \quad \quad \quad \downarrow \\
 \quad \quad \quad x^+ + Y = 0 \vdash x^+ = 0 \\
 \quad \quad \quad \swarrow \quad \quad \searrow \\
 x^+ + Y = 0 \vdash (x + Y)^+ = 0 \quad (x + Y)^+ = 0 \vdash x^+ = 0 \\
 \swarrow \quad \quad \searrow \quad \quad \swarrow \quad \quad \searrow \\
 x^+ + Y = 0 \vdash (x + Y)^+ = x^+ + Y \quad x^+ + Y = 0 \vdash x^+ + Y = 0 \quad \Gamma \vdash (x + Y)^+ = 0 \quad \Gamma \vdash \neg((x + Y)^+ = 0) \\
 \quad \quad \quad \downarrow \quad \quad \quad \downarrow \quad \quad \quad \downarrow \\
 \vdash (x + Y)^+ = x^+ + Y \quad \quad \quad \vdash \neg((x + Y)^+ = 0)
 \end{array}$$

Следовательно, формула  $x + Y = 0 \rightarrow x = 0$  истинна при любом  $x$ . Отметим, что индуктивное предположение об истинности формулы  $x + Y = 0 \rightarrow x = 0$  фактически не нужно: общезначимость формулы  $(x^+ + y = 0) \rightarrow (x^+ = 0)$  устанавливается без использования аксиомы индукции. ►

8.  $0 \cdot X = 0$ .

◀ Заменяем формулу  $X$  индуктивной переменной  $x$ . При  $x = 0$  равенство  $0 \cdot 0 = 0$  вытекает из правила С10. Предположим  $0 \cdot x = 0$ . Тогда  $0 \cdot x^+ = 0 \cdot x + 0 = 0 + 0 = 0$ . Значит, формула  $0 \cdot x = 0$  истинна для любого значения переменной  $x$ . ►

9. Введем обозначение  $1 = 0^+$ . Тогда  $X \cdot 1 = X$  и  $1 \cdot X = X$ .

◀ Для первого равенства имеем  $x \cdot 1 = x \cdot 0^+ = x \cdot 0 + x = 0 + x = x$ . Второе равенство  $1 \cdot x$  верно при  $x = 0$  (по аксиоме). Пусть  $1 \cdot x = x$ . Тогда  $1 \cdot x^+ = 1 \cdot x + 1 = 1 \cdot x + 0^+ = x + 0^+ = (x + 0)^+ = x^+$ . Значит,  $1 \cdot x = x$ . ►

10.  $X^+ \cdot Y = X \cdot Y + Y$ .

◀ Содержательное доказательство проводится индукцией по переменной  $y$ , включенной в формулу взамен подформулы  $Y$ . При  $y = 0$  имеем  $X^+ \cdot 0 = 0 = 0 + 0 = X \cdot 0 + 0$ . Пусть  $X^+ \cdot y = X \cdot y + y$ . Тогда

$$\begin{aligned}
 X^+ \cdot y^+ &= X^+ \cdot y + X^+ = (X \cdot y + y) + X^+ = X \cdot y + (y + X^+) = \\
 &+ X \cdot y + (y^+ + X) = X \cdot y + (X + y^+) = (X \cdot y + X) + y^+ = X \cdot y^+ + y^+.
 \end{aligned}$$

Поэтому формула  $X^+ \cdot y = X \cdot y + y$  верна при любом значении переменной  $y$ . ►

11. Умножение коммутативно:  $X \cdot Y = Y \cdot X$ .

◀ Содержательное доказательство проводится индукцией по переменной  $x$ , включенной в формулу взамен  $X$ . При  $x = 0$  имеем  $x \cdot Y = 0 \cdot Y = 0 = Y \cdot 0 = Y \cdot x$ , т.е. при  $x = 0$  формула верна. Пусть  $x \cdot Y = Y \cdot x$ . Тогда

$$x^+ \cdot Y = x \cdot Y + Y = Y \cdot x + Y = Y \cdot x^+.$$

Следовательно, формула  $x \cdot Y = Y \cdot x$  верна при любом значении переменной  $x$ . ►

12. Умножение дистрибутивно относительно сложения:  $(X + Y) \cdot Z = X \cdot Z + Y \cdot Z$ .

◀ Доказательство также строится на принципе математической индукции по переменной  $z$ , включенной в формулу взамен подформулы  $Z$ . При  $z = 0$  имеем

$$(X + Y) \cdot 0 = 0 = 0 + 0 = X \cdot 0 + Y \cdot 0.$$

Пусть  $(X + Y) \cdot z = X \cdot z + Y \cdot z$ . Тогда

$$(X + Y) \cdot z^+ = (X + Y) \cdot z + (X + Y) = (X \cdot z + Y \cdot z) + (X + Y) = (X \cdot z + X) + (Y \cdot z + Y) = X \cdot z^+ + Y \cdot z^+.$$



# ОГЛАВЛЕНИЕ

|                                                            |           |
|------------------------------------------------------------|-----------|
| <b>1. Алгебра высказываний</b>                             | <b>2</b>  |
| 1.1. Введение . . . . .                                    | 2         |
| 1.2. Алгебра логики . . . . .                              | 4         |
| 1.3. Тавтологии и эквивалентность формул . . . . .         | 6         |
| 1.4. Функции алгебры логики . . . . .                      | 10        |
| <b>2. Исчисление высказываний</b>                          | <b>15</b> |
| 2.1. Основные положения теории $N$ . . . . .               | 15        |
| 2.2. Правила естественного вывода . . . . .                | 17        |
| 2.3. Глобальные свойства теории $N$ . . . . .              | 22        |
| <b>3. Алгебра предикатов</b>                               | <b>27</b> |
| 3.1. Предикаты и кванторы . . . . .                        | 27        |
| 3.2. Логико-математические языки . . . . .                 | 28        |
| 3.3. Переименования и подстановки . . . . .                | 31        |
| 3.4. Семантика логико-математического языка . . . . .      | 34        |
| 3.5. Логические законы . . . . .                           | 36        |
| 3.6. Замены . . . . .                                      | 39        |
| 3.7. Упрощение формул . . . . .                            | 41        |
| <b>4. Исчисление предикатов</b>                            | <b>43</b> |
| 4.1. Построение теории $P$ . . . . .                       | 43        |
| 4.2. Правила естественного вывода . . . . .                | 44        |
| 4.3. Глобальные свойства теории $P$ . . . . .              | 46        |
| <b>5. Генценовские формальные системы</b>                  | <b>54</b> |
| 5.1. Исчисление $GV$ . . . . .                             | 54        |
| 5.2. Исчисление $GP$ . . . . .                             | 58        |
| <b>6. Примеры формальных теорий</b>                        | <b>61</b> |
| 6.1. Теория групп . . . . .                                | 61        |
| 6.2. Формальная арифметика . . . . .                       | 64        |
| <b>7. Метод резолюций</b>                                  | <b>70</b> |
| 7.1. Скулемовские функции . . . . .                        | 70        |
| 7.2. Метод резолюций для исчисления высказываний . . . . . | 72        |
| 7.3. Метод резолюций для исчисления предикатов . . . . .   | 75        |