Министерство образования и науки РФ
Новосибирский государственный университет
Механико-математический факультет
Кафедра алгебры и математической логики

П. Е. Алаев, Л. Л. Максимова

МАТЕМАТИЧЕСКАЯ ЛОГИКА

ЧАСТЬ I

Учебное пособие, определения и формулировки (15.06.14)

Новосибирск
2014

ОГЛАВЛЕНИЕ

РАЗДЕЛ I. ОПРЕДЕЛЕНИЯ И ФОРМУЛИРОВКИ

1. ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

1.1. Слова и операции над ними

Алфавитом называется произвольное множество символов. *Слово* в алфавите A — произвольная конечная последовательность $\Phi = a_1 a_2 \dots a_n$ символов из A. *Длина слова* $|\Phi|$ — количество символов в нём, т. е. число n. *Подслово* слова Φ — любая его часть, состоящая из идущих подряд символов, т. е. слово вида $a_t a_{t+1} \dots a_s$. *Начало* слова — это подслово вида $a_1 \dots a_s$, а *конец* слова — подслово вида $a_t \dots a_n$. *Пустое слово* — слово длины 0, вообще не содержащее символов.

Замечание. На языке теории множеств слово в алфавите A может быть определено как функция $f : \{1, 2, \dots, n\} \to A$.

Вхождением подслова в данное слово называется само подслово вместе с указанием того места, в котором оно расположено в слове (например, вместе с номером символа, с которого оно начинается). Пример: $\Psi = \mathrm{mat}$ является словом в алфавите $\{\mathrm{a}, \mathrm{m}, \mathrm{t}\}$, является подсловом слова $\Phi = \mathrm{mathematics}$, и при этом существует два вхождения слова Ψ в слово Φ.

Замена некоторого вхождения подслова Ψ в слово Φ на слово Ψ' производится так: пусть Φ_1 — та часть слова Φ, которая расположена перед вхождением Ψ, а Φ_2 — та часть, которая расположена после него; в этом случае $\Phi = \Phi_1 \Psi \Phi_2$. Тогда результатом замены является слово $\Phi_1 \Psi' \Phi_2$.

Кроме того, используется и операция *подстановки* слова Ψ вместо всех вхождений некоторого символа a в слово Φ. В этом случае все вхождения a одновременно заменяются на слово Ψ.

1.2. Формулы исчисления высказываний (ИВ)

Алфавит исчисления высказываний состоит из трёх частей:

1) *пропозициональные переменные*: они, как правило, будут обозначаться буквами $P, P_0, P_1, \dots, Q, Q_0, Q_1, \dots, R, R_0, R_1, \dots$

2) логические связки: *конъюнкция* $\&$
дизъюнкция $\vee$
импликация $\to$
отрицание $\neg$

3) вспомогательные символы: *левая скобка* (
правая скобка)

Формулы ИВ являются словами в этом алфавите и строятся по правилам:

1) пропозициональная переменная является формулой (такая формула называется *атомной*);

2) если Φ, Ψ — формулы, то $\neg\Phi$, $(\Phi \,\&\, \Psi)$, $(\Phi \vee \Psi)$, $(\Phi \to \Psi)$ — тоже формулы.

Для работы с формулами часто будет использоваться индукция. Пусть $\Delta(n)$ — некоторое утверждение, которое для каждого натурального числа n может быть истинным или ложным.

Принцип математической индукции. Если $\Delta(0)$ истинно и для всех n из истинности $\Delta(n)$ следует истинность $\Delta(n+1)$, то $\Delta(n)$ истинно для всех n.

Иногда бывает удобно использовать индукцию в следующей усиленной форме.

Возвратная индукция. Пусть для каждого n из того, что $\Delta(k)$ истинно при любом $k < n$, следует, что истинно $\Delta(n)$. Тогда $\Delta(n)$ истинно для всех n.

Встречаются и другие похожие формы индукции.

Лемма (о начале формулы). Если Φ, Ψ — формулы ИВ и слово Ψ является началом слова Φ, то $\Phi = \Psi$.

Предложение (о представлении формулы ИВ). Всякая неатомная формула ИВ единственным образом может быть представлена в одной из форм:

$$\neg\Phi,\ (\Phi\,\&\,\Psi),\ (\Phi \vee \Psi),\ (\Phi \to \Psi),$$

где Φ, Ψ — формулы ИВ.

До конца гл. 1 формулы ИВ будем называть просто *формулами*, а пропозициональные переменные — *переменными*. Если Φ — формула, то запись вида $\Phi = (\Phi_1 \circ \Phi_2)$, где $\circ \in \{\&, \vee, \to\}$, в дальнейшем всегда будет подразумевать, что Φ_1, Φ_2 — формулы, если не будет специально указано обратное.

Назовём *подформулой* формулы Φ её подслово, которое само является формулой. Всюду, где это будет иметь смысл, термином "подформула" будем обозначать некоторое вхождение подформулы.

Лемма. Каждое вхождение символа $\neg$ или (в формулу Φ является началом некоторой подформулы. Такая подформула единственна.

Предложение (о подформулах формулы ИВ). Для любой формулы Φ:

a) если Φ — атомная формула, то любая её подформула равна самой Φ;

b) если $\Phi = \neg\Phi_1$, то любая подформула Φ либо равна Φ, либо является подформулой Φ_1;

c) если $\Phi = (\Phi_1 \circ \Phi_2)$, где $\circ \in \{\&, \vee, \to\}$, то любая подформула Φ либо равна Φ, либо является подформулой Φ_1 или Φ_2.

1.3. Исчисление секвенций (ИС)

Алфавит ИС получается из алфавита ИВ добавлением символов $\vdash$ ("выводится") и запятой. *Секвенция* — слово одного из следующих видов:

$\Phi_1, \ldots, \Phi_n \vdash \Psi$ ("из $\Phi_1, \ldots, \Phi_n$ выводится Ψ"),

$\Phi_1, \ldots, \Phi_n \vdash$ ("набор $\Phi_1, \ldots, \Phi_n$ противоречив"),

$\vdash \Psi$ ("Ψ выводима"),

где $\Phi_1, \ldots, \Phi_n, \Psi$ — формулы, $n \geqslant 1$. При этом $\Phi_1, \ldots, \Phi_n$ называются *посылками* секвенции, а Ψ — её *заключением*.

Исчисление секвенций ИС задаётся аксиомами и правилами вывода. В приведённом ниже списке правил Φ, Ψ, Δ обозначают некоторые формулы, $\Gamma, \Gamma_1, \Gamma_2$ — конечные наборы формул (может быть, пустые).

Аксиомы ИС: все секвенции вида $\Phi \vdash \Phi$

Правила вывода ИС:

$$\frac{\Gamma \vdash \Phi;\quad \Gamma \vdash \Psi}{\Gamma \vdash (\Phi \,\&\, \Psi)}\ \text{(введение \&)},$$

$$\frac{\Gamma \vdash (\Phi \,\&\, \Psi)}{\Gamma \vdash \Phi}\ \text{(удаление \&)},\qquad \frac{\Gamma \vdash (\Phi \,\&\, \Psi)}{\Gamma \vdash \Psi}\ \text{(удаление \&)},$$

$$\frac{\Gamma \vdash \Phi}{\Gamma \vdash (\Phi \vee \Psi)}\ \text{(введение $\vee$)},\qquad \frac{\Gamma \vdash \Psi}{\Gamma \vdash (\Phi \vee \Psi)}\ \text{(введение $\vee$)},$$

$$\frac{\Gamma \vdash (\Phi \vee \Psi);\quad \Gamma, \Phi \vdash \Delta;\quad \Gamma, \Psi \vdash \Delta}{\Gamma \vdash \Delta}\ \text{(удаление $\vee$)},$$

$$\frac{\Gamma, \Phi \vdash \Psi}{\Gamma \vdash (\Phi \to \Psi)}\ \text{(введение $\to$)},\qquad \frac{\Gamma \vdash \Phi;\quad \Gamma \vdash (\Phi \to \Psi)}{\Gamma \vdash \Psi}\ \text{(удаление $\to$)},$$

$$\frac{\Gamma, \Phi \vdash}{\Gamma \vdash \neg\Phi}\ \text{(введение $\neg$)},\qquad \frac{\Gamma \vdash}{\Gamma \vdash \Phi}\ \text{(добавление заключения)},$$

$$\frac{\Gamma, \neg\Phi \vdash}{\Gamma \vdash \Phi}\ \text{(удаление $\neg$)},\qquad \frac{\Gamma \vdash \Phi;\quad \Gamma \vdash \neg\Phi}{\Gamma \vdash}\ \text{(сведение к противоречию)},$$

$$\frac{\Gamma_1, \Phi, \Psi, \Gamma_2 \vdash \Delta}{\Gamma_1, \Psi, \Phi, \Gamma_2 \vdash \Delta}\ \text{(перестановка)},\qquad \frac{\Gamma \vdash \Phi}{\Gamma, \Psi \vdash \Phi}\ \text{(добавление посылки)}.$$

Определим теперь понятие *дерева вывода секвенции* в ИС:

1) аксиома является деревом вывода этой аксиомы;

2) если $\dfrac{S_1; \ldots; S_k}{S}$ — правило вывода ИС, $\mathcal{D}_1, \ldots, \mathcal{D}_k$ — деревья выводов секвенций $S_1, \ldots, S_k$, соответственно, то $\dfrac{\mathcal{D}_1; \ldots; \mathcal{D}_k}{S}$ — дерево вывода секвенции S.

Секвенция S *доказуема* в ИС, если существует дерево вывода этой секвенции.

Пример. Секвенции $\Phi \vdash \neg\neg\Phi$ и $\neg\neg\Phi \vdash \Phi$ доказуемы в ИС.

1.4. Семантика исчисления высказываний

Логические связки можно рассматривать как операции на логических величинах **и** (“истина”) и **л** (“ложь”), которые определяются так:

P	Q	$(P \,\&\, Q)$	$(P \vee Q)$	$(P \to Q)$
и	**и**	**и**	**и**	**и**
и	**л**	**л**	**и**	**л**
л	**и**	**л**	**и**	**и**
л	**л**	**л**	**л**	**и**

P	$\neg P$
и	**л**
л	**и**

Пусть M — некоторое множество пропозициональных переменных. Назовём *означиванием пропозициональных переменных* из M соответствие γ, которое каждой переменной P из M сопоставляет значение $\gamma(P)$ из множества $\{\mathbf{и}, \mathbf{л}\}$.

Если Φ — формула и γ — означивание, при котором каждая переменная из Φ получает некоторое значение, то *значение формулы* Φ при означивании γ, $\Phi[\gamma]$ может быть определено индукцией по длине формулы:

1) если Φ — переменная P, то $\Phi[\gamma] = \gamma(P)$;

2) если $\Phi = (\Phi_1 \circ \Phi_2)$, где $\circ \in \{\&, \vee, \to\}$, то $\Phi[\gamma] = \Phi_1[\gamma] \circ \Phi_2[\gamma]$ (см. таблицу выше);

3) если $\Phi = \neg\Phi_1$, то $\Phi[\gamma] = \neg\Phi_1[\gamma]$.

Замечание. Значение формулы Φ при означивании γ зависит от значений только тех переменных, которые входят в Φ.

Ясно, что, если не все переменные формулы Φ получают значения при означивании γ, говорить о $\Phi[\gamma]$, вообще говоря, бессмысленно. Договоримся, что всякий раз, когда речь идёт о значении формулы при означивании γ, неявно подразумевается условие, что все её переменные обязательно получают какие-то значения.

Формула называется *тождественно истинной* (*тождественно ложной*), если она принимает значение **и** (**л**) при любом означивании переменных.

Пусть фиксировано некоторое означивание. Секвенция вида $\Phi_1, \ldots, \Phi_n \vdash \Psi$ *истинна* при этом означивании, если Ψ истинна или хотя бы одна из Φ_i ложна. Секвенция вида $\Phi_1, \ldots, \Phi_n \vdash$ *истинна*, если хотя бы одна из Φ_i ложна. Секвенция $\vdash \Psi$ *истинна*, если формула Ψ истинна.

Секвенция называется *тождественно истинной*, если она истинна при любом означивании переменных.

Теорема (о корректности ИС). Любая доказуемая в ИС секвенция тождественно истинна.

1.5. Допустимые правила вывода

Правило $\dfrac{S_1; \ldots; S_k}{S}$ называется *допустимым* в ИС, если из доказуемости секвенций $S_1, \ldots, S_k$ следует доказуемость S.

Дерево вывода с допустимыми правилами определяется точно так же, как обычное дерево вывода в ИС, с дополнительным условием, что вместе с исходными правилами ИС могут использовать и любые допустимые.

Предложение (о выводе с допустимыми правилами). Если у секвенции есть дерево вывода с допустимыми правилами, то она доказуема в ИС.

Предложение (о допустимых в ИС правилах). Следующие правила допустимы в ИС:

$\dfrac{\Gamma \vdash \Phi;\ \ \Gamma, \Phi \vdash \Psi}{\Gamma \vdash \Psi}$ (сечение), $\qquad$ $\dfrac{\Gamma, \Phi \vdash \Delta;\ \ \Gamma, \Psi \vdash \Delta}{\Gamma, (\Phi \vee \Psi) \vdash \Delta}$ (разбор случаев),

$\dfrac{\Gamma \vdash (\Phi \to \Psi)}{\Gamma, \Phi \vdash \Psi}$ (удаление $\to$), $\qquad$ $\dfrac{\Gamma, \Phi, \Psi \vdash \Delta}{\Gamma, (\Phi \,\&\, \Psi) \vdash \Delta}$ (соединение посылок),

$\dfrac{\Gamma, (\Phi \,\&\, \Psi) \vdash \Delta}{\Gamma, \Phi, \Psi \vdash \Delta}$ (разделение посылок), $\qquad$ $\dfrac{\Gamma, \neg\Phi \vdash \neg\Psi}{\Gamma, \Psi \vdash \Phi}$

$\dfrac{\Gamma, \Phi \vdash \Psi}{\Gamma, \neg\Psi \vdash \neg\Phi}$ (контрапозиция), $\qquad$ $\dfrac{\Gamma, \Phi \vdash \neg\Psi}{\Gamma, \Psi \vdash \neg\Phi}$ $\qquad$ $\dfrac{\Gamma, \neg\Phi \vdash \Psi}{\Gamma, \neg\Psi \vdash \Phi}$

$\dfrac{\Phi_1, \ldots, \Phi_n \vdash \Psi}{\Delta_1, \ldots, \Delta_m \vdash \Psi}$ и $\dfrac{\Phi_1, \ldots, \Phi_n \vdash}{\Delta_1, \ldots, \Delta_m \vdash}$ (структурные), где $\{\Phi_1, \ldots, \Phi_n\} \subseteq \{\Delta_1, \ldots, \Delta_m\}$.

Пример. Доказуема секвенция $\vdash \Phi \vee \neg\Phi$.

1.6. Теорема о замене

Формулы Φ и Ψ *синтаксически эквивалентны* ($\Phi \equiv \Psi$), если доказуемы секвенции $\Phi \vdash \Psi$ и $\Psi \vdash \Phi$.

Лемма. Отношение $\equiv$ обладает следующими свойствами:

a) $\Phi \equiv \Phi$;

b) $\Phi \equiv \Psi \Rightarrow \Psi \equiv \Phi$;

c) $\Phi \equiv \Psi$, $\Psi \equiv \Delta \Rightarrow \Phi \equiv \Delta$;

d) $\Phi \equiv \Phi' \Rightarrow \neg\Phi \equiv \neg\Phi'$;

e) $\Phi \equiv \Phi'$, $\Psi \equiv \Psi' \Rightarrow (\Phi \circ \Psi) \equiv (\Phi' \circ \Psi')$, где $\circ \in \{\&, \vee, \rightarrow\}$.

Теорема (о замене для ИВ). Если в формуле Φ некоторую подформулу заменить на синтаксически эквивалентную ей формулу, то результат будет синтаксически эквивалентен Φ.

1.7. Нормальные формы

Докажем теперь, что любая формула ИВ может быть приведена через цепочку эквивалентностей к некоторому достаточно простому виду. Договоримся, что при записи формул две внешние скобки (в начале и конце формулы) могут быть опущены.

Лемма 1 (об основных эквивалентностях ИВ). Для любых формул Φ, Ψ, Δ:

a) $\Phi \,\&\, \Psi \equiv \Psi \,\&\, \Phi$ и $\Phi \vee \Psi \equiv \Psi \vee \Phi$ (коммутативность);

b) $\Phi \,\&\, (\Psi \,\&\, \Delta) \equiv (\Phi \,\&\, \Psi) \,\&\, \Delta$ и $\Phi \vee (\Psi \vee \Delta) \equiv (\Phi \vee \Psi) \vee \Delta$ (ассоциативность);

c) $\Phi \,\&\, (\Psi \vee \Delta) \equiv (\Phi \,\&\, \Psi) \vee (\Phi \,\&\, \Delta)$ и

d) $\Phi \vee (\Psi \,\&\, \Delta) \equiv (\Phi \vee \Psi) \,\&\, (\Phi \vee \Delta)$ (дистрибутивность).

Лемма 2 (об основных эквивалентностях ИВ). Для любых формул Φ, Ψ:

a) $\Phi \rightarrow \Psi \equiv \neg\Phi \vee \Psi$;

b) $\neg\neg\Phi \equiv \Phi$;

c) $\neg(\Phi \,\&\, \Psi) \equiv \neg\Phi \vee \neg\Psi$;

d) $\neg(\Phi \vee \Psi) \equiv \neg\Phi \,\&\, \neg\Psi$;

e) $\Phi \equiv \Phi \vee \Phi$ и $\Phi \equiv \Phi \,\&\, \Phi$.

Обозначим через $(\Phi_1 \vee \Phi_2 \vee \ldots \vee \Phi_n)$ формулу

$$(\ldots((\Phi_1 \vee \Phi_2) \vee \Phi_3) \ldots \vee \Phi_n),$$

а через $(\Phi_1 \,\&\, \Phi_2 \,\&\, \ldots \,\&\, \Phi_n)$ — формулу

$$(\ldots((\Phi_1 \,\&\, \Phi_2) \,\&\, \Phi_3) \ldots \,\&\, \Phi_n).$$

Иногда будем кратко обозначать их как $\bigvee\limits_{i=1}^{n} \Phi_i$ и $\bigwedge\limits_{i=1}^{n} \Phi_i$.

Лемма. Для любых формул Φ_i, Ψ_j, Δ:

a) $(\Phi_1 \vee \ldots \vee \Phi_n) \vee (\Psi_1 \vee \ldots \vee \Psi_k) \equiv (\Phi_1 \vee \ldots \vee \Phi_n \vee \Psi_1 \vee \ldots \vee \Psi_k)$;

b) $\Delta \,\&\, (\Phi_1 \vee \ldots \vee \Phi_n) \equiv ((\Delta \,\&\, \Phi_1) \vee \ldots \vee (\Delta \,\&\, \Phi_n))$;

c) пункты a) и b) останутся верными при замене $\&$ на $\vee$, а $\vee$ на $\&$.

Элементарная конъюнкция — формула вида $(\Phi_1 \,\&\, \ldots \,\&\, \Phi_n)$, $n \geqslant 1$, где каждая Φ_i — переменная или отрицание переменной.

Дизъюнктивная нормальная форма (д.н.ф.) — формула вида $(\Psi_1 \vee \ldots \vee \Psi_k)$, $k \geqslant 1$, где каждая Ψ_i — элементарная конъюнкция.

Элементарная дизъюнкция — формула вида $(\Phi_1 \vee \ldots \vee \Phi_n)$, $n \geqslant 1$, где каждая Φ_i — переменная или отрицание переменной.

Конъюнктивная нормальная форма (к.н.ф.) — формула вида $(\Psi_1 \,\&\, \ldots \,\&\, \Psi_k)$, $k \geqslant 1$, где каждая Ψ_i — элементарная дизъюнкция.

Теорема (о приведении к д.н.ф. и к.н.ф.). Любая формула синтаксически эквивалентна некоторой к.н.ф. и некоторой д.н.ф., содержащим тот же набор переменных, что и она сама.

1.8. Теорема о полноте ИС

Предложение (о тождественно истинных к.н.ф.). К.н.ф. Φ тождественно истинна тогда и только тогда, когда каждая её элементарная дизъюнкция содержит P и $\neg P$ для некоторой переменной P.

Одна из основных теорем гл. 1, теорема о полноте ИС, говорит, что переход из теоремы о корректности верен и в обратную сторону.

Теорема (о полноте ИС). Секвенция доказуема в ИС тогда и только тогда, когда она тождественно истинна.

Напомним, что запись $\Phi \equiv \Psi$ обозначает синтаксическую эквивалентность. Говорим, что Φ и Ψ *семантически эквивалентны* ($\Phi \sim \Psi$), если при любом означивании переменных значения Φ и Ψ совпадают.

Следствие. $\Phi \equiv \Psi$ тогда и только тогда, когда $\Phi \sim \Psi$.

В силу этого далее будем говорить просто про *эквивалентные* формулы.

1.9. Совершенные нормальные формы

Совершенная д.н.ф. (с.д.н.ф.) — это такая д.н.ф., что:

1) любая входящая в неё переменная входит в каждую элементарную конъюнкцию ровно один раз, с отрицанием или без;

2) любые две её элементарные конъюнкции *существенно различаются*, т. е. одна из них содержит P, а другая $\neg P$ для некоторой переменной P.

Совершенная к.н.ф. (с.к.н.ф.) определяется аналогично, с заменой $\vee$ на $\&$ и наоборот — это такая к.н.ф., что:

1) любая входящая в неё переменная входит в каждую элементарную дизъюнкцию ровно один раз, с отрицанием или без;

2) любые две элементарные дизъюнкции существенно различаются.

Теорема (о совершенных нормальных формах).

a) Любая не тождественно ложная формула эквивалентна некоторой с.д.н.ф., содержащей тот же набор переменных, что и она сама.

b) Любая не тождественно истинная формула эквивалентна некоторой с.к.н.ф., содержащей тот же набор переменных, что и она сама.

c) Нормальная форма в a) и b) единственна с точностью до перестановки элементарных конъюнкций (дизъюнкций) и их компонент.

Замечание. Тождественно ложная формула не имеет эквивалентной ей с.д.н.ф., а тождественно истинная — с.к.н.ф.

2. ТЕОРИЯ МНОЖЕСТВ

2.1. Общие свойства множеств и операции над ними

Изложение математической теории множеств было бы естественно начать с определения множества. К сожалению, попытки дать строгое и исчерпывающее определение этого понятия связаны с трудностями, о которых будет сказано позже. С интуитивной точки зрения, общее представление о множествах является очень широким обобщением тех конкретных множеств, которые встречаются в математике: множества натуральных чисел $\mathbb{N}$, его подмножеств, множества вещественных чисел $\mathbb{R}$, множества $P(\mathbb{N})$ всех подмножеств $\mathbb{N}$, множества функций из $\mathbb{N}$ в $\mathbb{R}$ и т. д.

Любое множество является некоторой совокупностью математических объектов, которые называются его *элементами*. Запись $x \in A$ означает, что x принадлежит множеству A, т. е. является его элементом. Для множеств выполняется

Аксиома экстенсиональности. Пусть A, B — множества. Тогда $A = B \Leftrightarrow$ для любого x $[x \in A \Leftrightarrow x \in B]$.

Эта аксиома говорит, что множество однозначно определяется своими элементами: если у двух множеств набор элементов один и тот же, то эти множества равны.

Введём ряд стандартных обозначений. Пусть A и B — некоторые множества:
$A \subseteq B$, если для всех x $[x \in A \Rightarrow x \in B]$ (A — *подмножество* B);
$A \subset B$, если $A \subseteq B$ и $A \neq B$ (A — *собственное подмножество* B);
$A \cup B$ — *объединение* множеств A и B:

$$x \in A \cup B \Leftrightarrow x \in A \text{ или } x \in B;$$

$A \cap B$ — *пересечение* множеств A и B:

$$x \in A \cap B \Leftrightarrow x \in A \text{ и } x \in B;$$

$A \setminus B = A - B$ — *разность* множеств A и B:

$$x \in A \setminus B \Leftrightarrow x \in A \text{ и } x \notin B;$$

$\emptyset$ — множество, не содержащее элементов (*пустое множество*);
$\{a_1, \ldots, a_k\}$ — множество, элементами которого являются $a_1, \ldots, a_k$, и только они.

Если $\Phi(x)$ — некоторое условие, которое в зависимости от x может быть истинным или ложным, то запись $\{x \mid \Phi(x)\}$ обозначает множество всех математических объектов x, для которых $\Phi(x)$ истинно (если такое множество существует). Через $P(A)$ обозначим множество всех подмножеств A, т. е. $\{B \mid B \subseteq A\}$.

Использование теории множеств в качестве основания математики опирается на идею о том, что любой математический объект можно представить в виде множества. Тем самым понятия “множество” и “математический объект” являются синонимами. Натуральные числа традиционно представляются в виде множеств так:

$0 = \emptyset$
$1 = \{0\} = \{\emptyset\}$
$2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$
$3 = \{0, 1, 2\}$
$\vdots$
$n + 1 = n \cup \{n\}$
$\vdots$

Множество всех натуральных чисел $\{0, 1, 2, \ldots\}$ будем обозначать $\mathbb{N}$ или ω. Иногда вместо термина "множество" будем употреблять его синоним "семейство".

Если S — непустое множество, то

$$\bigcap S = \{x \mid x \in A \text{ для всех } A \in S\},$$
$$\bigcup S = \{x \mid \text{существует } A \in S \text{ такое, что } x \in A\}.$$

Иногда эти операции обозначаются как $\bigcap_{A \in S} A$ и $\bigcup_{A \in S} A$.

2.2. Упорядоченные пары и n-ки

Упорядоченный набор (*кортеж*) длины n (n-*ка*) определяется индукцией по n:
$\langle\rangle = \emptyset$
$\langle a \rangle = a$
$\langle a, b \rangle = \{\{a\}, \{a, b\}\}$
$\langle a_1, \ldots, a_n, a_{n+1} \rangle = \langle \langle a_1, \ldots, a_n \rangle, a_{n+1} \rangle$.

Набор $\langle a, b \rangle$ длины 2 часто называют *парой*.

Предложение (о равенстве n-ок). Если $\langle a_1, \ldots, a_n \rangle = \langle b_1, \ldots, b_n \rangle$, то $a_1 = b_1, \ldots, a_n = b_n$.

Пусть $A_1, \ldots, A_n$ — множества. Их *декартово произведение* — это множество:

$$A_1 \times \ldots \times A_n = \{\langle a_1, \ldots, a_n \rangle \mid a_1 \in A_1, \ldots, a_n \in A_n\}.$$

Если $A_1 = \ldots = A_n = A$, то это декартово произведение называется *декартовой степенью* множества A и обозначается A^n.

2.3. Бинарные отношения и функции

Бинарным отношением называется любое множество R, состоящее из пар. Если при этом $R \subseteq A \times B$, то R называют *бинарным отношением между A и B*, а если $R \subseteq A^2$, то R — *бинарное отношение* на множестве A.

Если R — бинарное отношение, то *обратное отношение* R^{-1} — это множество $\{\langle y, x \rangle \mid \langle x, y \rangle \in R\}$. Если R_1, R_2 — два бинарных отношения, то их *произведение* $R_1 \cdot R_2$ определяется как множество

$$\{\langle x, z \rangle \mid \text{существует } y \text{ т. ч. } \langle x, y \rangle \in R_1 \text{ и } \langle y, z \rangle \in R_2\}.$$

Лемма (о бинарных отношениях). Для любых бинарных отношений R_1, R_2, R_3:
a) $R_1 \cdot (R_2 \cdot R_3) = (R_1 \cdot R_2) \cdot R_3$;
b) $(R_1 \cdot R_2)^{-1} = R_2^{-1} \cdot R_1^{-1}$.

Функция — это бинарное отношение f, для которого выполняется условие:

$$\langle x, y_1 \rangle, \langle x, y_2 \rangle \in f \Rightarrow y_1 = y_2;$$

$\mathrm{dom}(f) = \{x \mid$ существует y т. ч. $\langle x, y\rangle \in f\}$ — *область определения* функции f;
$\mathrm{ran}(f) = \{y \mid$ существует x т. ч. $\langle x, y\rangle \in f\}$ — *множество значений* функции f;
f — *функция из A в B*, если

$$f \text{ — функция, } \mathrm{dom}(f) = A \text{ и } \mathrm{ran}(f) \subseteq B.$$

В этом случае используется обозначение $f : A \to B$.

Замечание. Если $f : A \to B$ и $x \in A$, то существует единственный y такой, что $\langle x, y\rangle \in f$. Этот y лежит в B, называется *значением* функции f в точке x и обозначается $f(x)$.

Замечание (о равенстве функций). Если f, g — функции, то $f = g$ тогда и только тогда, когда

$$\mathrm{dom}(f) = \mathrm{dom}(g) \text{ и } f(x) = g(x) \text{ при любом } x \in \mathrm{dom}(f).$$

Для любого множества A существует *тождественная функция* id_A, равная $\{\langle x, x\rangle \mid x \in A\}$. Ясно, что $\mathrm{id}_A : A \to A$ и $\mathrm{id}_A(x) = x$ при $x \in A$.

Если f и g — функции, то их *композиция* $g \circ f$ определяется как произведение бинарных отношений $f \cdot g$ (в обратном порядке).

Лемма (о композиции функций). Если $f : A \to B$, $g : B \to C$, то их композиция $g \circ f : A \to C$ и $[g \circ f](x) = g(f(x))$ при $x \in A$.

Пусть $f : A \to B$. Говорим, что:

f — функция из A *на* B (*сюръективная функция, сюръекция*), если для любого $y \in B$ найдётся $x \in A$ такой, что $f(x) = y$; обозначим это как $f : A \xrightarrow{\text{на}} B$;

f — *инъективная функция* (1–1 *функция*, *инъекция*), если для любых $x_1, x_2 \in A$ из $f(x_1) = f(x_2)$ следует $x_1 = x_2$; обозначим это как $f : A \xrightarrow{1-1} B$;

f — *биекция* из A на B, если f одновременно инъекция и функция из A на B.

Замечание. Если $f : A \to B$, то $\mathrm{ran}(f) = \{f(x) \mid x \in A\}$; f функция из A на B тогда и только тогда, когда $\mathrm{ran}(f) = B$.

Запись f^{-1} означает обратное бинарное отношение к f. Если f^{-1} при этом является функцией, то она называется *обратной функцией* к f.

Лемма (о свойствах биекций).

a) Если $f : A \xrightarrow[\text{на}]{1-1} B$, то $f^{-1} : B \xrightarrow[\text{на}]{1-1} A$, $f^{-1}(f(x)) = x$ при любом $x \in A$ и $f(f^{-1}(y)) = y$ при любом $y \in B$;

b) Если $f : A \xrightarrow[\text{на}]{1-1} B$, $g : B \xrightarrow[\text{на}]{1-1} C$, то $g \circ f : A \xrightarrow[\text{на}]{1-1} C$.

2.4. Отношения эквивалентности

Пусть R — бинарное отношение на множестве A, т. е. $R \subseteq A^2$. Говорим, что:
R *симметрично*, если $\langle a, b\rangle \in R \Rightarrow \langle b, a\rangle \in R$,
R *антисимметрично*, если $\langle a, b\rangle, \langle b, a\rangle \in R \Rightarrow a = b$,
R *транзитивно*, если $\langle a, b\rangle, \langle b, c\rangle \in R \Rightarrow \langle a, c\rangle \in R$,
R *иррефлексивно*, если $\langle a, a\rangle \notin R$ для любого a,
R *рефлексивно на* A, если $\langle a, a\rangle \in R$ для любого $a \in A$.

Отношение эквивалентности на множестве A — бинарное отношение $R \subseteq A^2$, которое симметрично, транзитивно и рефлексивно на A.

Вместо записи $\langle x, y\rangle \in R$ часто будем использовать краткое обозначение xRy и говорить, что x и y *эквивалентны* относительно R. Если $x \in A$, то множество $x/R = \{y \in A \mid xRy\}$ называется *классом эквивалентности* элемента x. Множество всех классов эквивалентности $A/R = \{x/R \mid x \in A\}$ называется *фактор-множеством* A по R.

Семейство $D \subseteq P(A)$ назовём *разбиением множества* A, если верно:

1) любое множество $B \in D$ непусто;

2) если $B_1, B_2 \in D$ и $B_1 \neq B_2$, то $B_1 \cap B_2 = \emptyset$;

3) для любого $x \in A$ существует $B \in D$ такое, что $x \in B$.

Лемма (о классах эквивалентности). Если R — отношение эквивалентности на A, то A/R — разбиение множества A.

Теорема (об отношениях эквивалентности). Переход от R к A/R задаёт биекцию между множеством всех отношений эквивалентности на A и множеством всех разбиений A.

2.5. Частично упорядоченные множества

Частичный порядок на множестве A — это бинарное отношение $R \subseteq A^2$, которое антисимметрично, транзитивно и рефлексивно на A. *Частично упорядоченное множество* (ч.у.м.) — это пара (A, R), где R — частичный порядок на A.

В дальнейшем, как правило, для частичных порядков будет использоваться символ $\leqslant$ и его модификации. Как и раньше, вместо записи $\langle x, y\rangle \in \leqslant$ используем сокращение $x \leqslant y$ и говорим, что x *меньше или равен* y относительно порядка $\leqslant$.

Пусть $\leqslant$ — частичный порядок на A, $x \in A$. Говорим, что:
x — *наибольший* элемент в A, если $y \leqslant x$ для всех $y \in A$;
x — *наименьший* элемент, если $x \leqslant y$ для всех $y \in A$;
x — *максимальный* элемент, если для любого $y \in A$ из $x \leqslant y$ следует, что $x = y$;
x — *минимальный* элемент, если для любого $y \in A$ из $y \leqslant x$ следует, что $x = y$;

Замечание. Наибольший элемент (если он существует) единственен и является максимальным, а наименьший (если существует) единственен и является минимальным.

Обозначим через $x < y$ то, что $x \leqslant y$ и $x \neq y$.

Замечание (о строгом порядке). Если $\leqslant$ — частичный порядок на A, то $<$ — иррефлексивное и транзитивное отношение на A.

Пусть $(A, \leqslant_A)$ — ч.у.м. и $B \subseteq A$. Тогда мы можем сузить порядок $\leqslant_A$ на B, определяя порядок $\leqslant_B$ как $\leqslant_A \cap B^2$. Это означает, что $x \leqslant_B y \Leftrightarrow x \leqslant_A y$ при $x, y \in B$. Отношение $\leqslant_B$ называется *индуцированным порядком* на B; легко проверить, что это действительно частичный порядок на B. Иногда мы будем говорить о множестве B как о ч.у.м., подразумевая под этим ч.у.м. $(B, \leqslant_A \cap B^2)$.

Частичный порядок $\leqslant$ на A называется *фундированным*, если любое непустое $B \subseteq A$ содержит минимальный (в B) элемент.

Предложение (критерий фундированности порядка). Частичный порядок $\leqslant$ на A является фундированным $\Leftrightarrow$ в A нет бесконечно убывающей последовательности $a_0 > a_1 > a_2 > \ldots$

Предложение (о индукции в фундированном ч.у.м.). Пусть A — ч.у.м. с фундированным порядком $\leqslant$, B — некоторое подмножество A. Допустим, что для любого $x \in A$ из того, что $y \in B$ для всех $y < x$, следует, что $x \in B$. Тогда $B = A$.

Пусть даны два ч.у.м. $(A, \leqslant_A)$ и $(B, \leqslant_B)$. Функция $f : A \to B$ называется *монотонной*, если

$$x \leqslant_A y \Rightarrow f(x) \leqslant_B f(y);$$

f — *изоморфизм между* $(A, \leqslant_A)$ и $(B, \leqslant_B)$, если f — биекция из A на B и $x \leqslant_A y \Leftrightarrow f(x) \leqslant_B f(y)$ при любых $x, y \in A$.
Ч.у.м. называются *изоморфными*, если между ними существует изоморфизм. Обозначим это как $(A, \leqslant_A) \cong (B, \leqslant_B)$.

Замечание. Изоморфность обладает свойствами отношения эквивалентности:
a) $(A, \leqslant_A) \cong (A, \leqslant_A)$;
b) если $(A, \leqslant_A) \cong (B, \leqslant_B)$, то $(B, \leqslant_B) \cong (A, \leqslant_A)$;
c) если $(A, \leqslant_A) \cong (B, \leqslant_B)$ и $(B, \leqslant_B) \cong (C, \leqslant_C)$, то $(A, \leqslant_A) \cong (C, \leqslant_C)$.

2.6. Линейно упорядоченные множества

Пусть $\leqslant$ — частичный порядок на A, $x, y \in A$. Говорим, что x, y *сравнимы* относительно $\leqslant$, если $x \leqslant y$ или $y \leqslant x$. Частичный порядок $\leqslant$ называется *линейным*, если $x \leqslant y$ или $y \leqslant x$ для любых $x, y \in A$, т. е. если любые два элемента в A сравнимы. В этом случае пара $(A, \leqslant)$ называется *линейно упорядоченным множеством* (л.у.м.).

Замечание. Если $(A, \leqslant)$ — л.у.м. и элемент $x \in A$, то:

a) x является минимальным тогда и только тогда, когда является наименьшим;

b) x является максимальным тогда и только тогда, когда является наибольшим.

Пусть $(A, \leqslant)$ — л.у.м. Подмножество $S \subseteq A$ называется *начальным сегментом* A, если для любых $x, y \in A$ из $x \in S$ и $y \leqslant x$ следует, что $y \in S$.

Лемма (о свойствах начальных сегментов). Пусть дано л.у.м. $(A, \leqslant)$. Тогда:

a) если S_1, S_2 — начальные сегменты, то $S_1 \subseteq S_2$ или $S_2 \subseteq S_1$;

b) если S — начальный сегмент, а x — минимальный элемент в $A \setminus S$, то $S \cup \{x\}$ — тоже начальный сегмент;

c) объединение любого семейства начальных сегментов — снова начальный сегмент.

Начальным отрезком A, отсекаемым элементом $x \in A$, называется множество $A_x = \{y \in A \mid y < x\}$.

Замечание. Начальный отрезок всегда является начальным сегментом.

Лемма (признак изоморфизма л.у.м.). Если $(A, \leqslant)$, $(B, \leqslant)$ — л.у.м. и $f : A \to B$ — монотонная биекция, то f — изоморфизм.

2.7. Вполне упорядоченные множества

Вполне упорядоченное множество (в.у.м.) — это пара $(A, \leqslant)$, где $\leqslant$ — линейный фундированный порядок на A. Иногда такой порядок называют *полным*.

Лемма (о начальных сегментах в.у.м.). Любой начальный сегмент в.у.м. $(A, \leqslant)$ либо равен A, либо является начальным отрезком.

Замечание. Если $(A, \leqslant)$ — в.у.м. и $B \subseteq A$, то B с порядком, индуцированным из A, тоже является в.у.м.

Лемма. Если $(A, \leqslant)$ — в.у.м. и $f : A \xrightarrow{1-1} A$ — монотонная функция, то $f(x) \geqslant x$ при всех $x \in A$.

Предложение (об изоморфизме начальных сегментов). Различные начальные сегменты в.у.м. не могут быть изоморфны друг другу.

Предложение (об изоморфизмах в.у.м.). Если два в.у.м. изоморфны, то изоморфизм между ними единственен.

Предположим, что $f : A \to C$ и $B \subseteq A$. Определим *сужение* функции f на B, $f|_B$, как $\{\langle x, y\rangle \in f \mid x \in B\}$.

Замечание. $f|_B$ — функция, $\mathrm{dom}(f|_B) = B$ и $f|_B(x) = f(x)$ при $x \in B$.

Теорема (о сравнимости в.у.м.). Если даны два в.у.м., то одно из них изоморфно начальному сегменту другого.

2.8. Аксиома выбора, лемма Цорна, теорема Цермело

Ещё одна важная аксиома теории множеств —

Аксиома выбора. Для любого множества A существует функция $f : P(A)\setminus\{\emptyset\} \to A$ т. ч. $f(X) \in X$ для всех $X \in P(A) \setminus \{\emptyset\}$.

Мы уже использовали её выше в некоторых доказательствах. Она играет ключевую роль и в доказательстве леммы Цорна.

Пусть $(A, \leqslant)$ — ч.у.м. Подмножество $B \subseteq A$ называется *цепью*, если любые два элемента из B сравнимы, т. е. $x \leqslant y$ или $y \leqslant x$ для любых $x, y \in B$.

Элемент $x \in A$ называется *верхней гранью* подмножества $B \subseteq A$, если $y \leqslant x$ для всех $y \in B$, и *нижней гранью*, если $x \leqslant y$ для всех $y \in B$. Если в множестве всех верхних граней B есть наименьший элемент, то он называется *супремумом* B и обозначается $\sup(B)$. Наибольший элемент множества всех нижних граней называется *инфимумом* B и обозначается $\inf(B)$.

Лемма Цорна (принцип максимума). Если в ч.у.м. у каждой цепи есть верхняя грань, то в этом ч.у.м. есть максимальный элемент.

Говорим, что множество можно *вполне упорядочить*, если на нём существует линейный фундированный порядок, т. е. порядок, при котором оно станет вполне упорядоченным.

Теорема Цермело. Любое множество можно вполне упорядочить.

Ниже будет показано, что аксиома выбора, лемма Цорна и теорема Цермело в некотором смысле равносильны.

2.9. Парадокс Рассела

Рассмотрим совокупность

$$M_R = \{A \mid A \text{ — множество и } A \notin A\}.$$

Предположим, что само M_R является множеством. Возможны два варианта:

1) $M_R \notin M_R$. Тогда $A = M_R$ подходит под определение и $M_R \in M_R$. Противоречие.

2) $M_R \in M_R$. Вновь полагая $A = M_R$, получаем, что по определению $M_R \notin M_R$. Противоречие.

Это рассуждение называется парадоксом Рассела. Оно показывает, что совокупность M_R нельзя считать множеством. Подход, который первоначально использовался в работах основателя теории множеств Георга Кантора и предполагал, что множеством можно считать любую совокупность математических объектов, иногда называют наивной теорией множеств. Парадокс Рассела показывает, что наивная теория множеств нуждается в корректировке. Открытие парадоксов наивной теории множеств привело к появлению аксиоматических теорий множеств.

Заметим, что к подобному противоречию приводит и существование множества всех множеств. Если совокупность $M = \{A \mid A \text{ — множество}\}$ является множеством, то стандартные правила работы с множествами говорят, что $M_R = \{A \in M \mid A \notin A\}$ тоже является множеством.

2.10. Аксиоматическая теория множеств ZFC

Аксиомы теории множеств Цермело – Френкеля (ZF) могут быть заданы следующим образом.

1. Аксиома экстенсиональности. Множества a и b равны тогда и только тогда, когда для любого x $[x \in a \Leftrightarrow x \in b]$.

2. Аксиома пары. Для любых множеств a, b существует множество $\{a, b\}$.

3. Аксиома объединения. Для любого множества a существует множество $\bigcup a = \{y \mid \text{существует } x \in a \text{ такой, что } y \in x\}$.

4. Аксиома множества подмножеств. Для любого множества a существует множество $P(a) = \{b \mid b \subseteq a\}$.

5. Аксиома подстановки. Пусть a — множество, а $\Phi(x, y)$ — условие, обладающее свойством: для каждого $x \in a$ существует не более одного y такого, что $\Phi(x, y)$. Тогда существует множество $a' = \{y \mid \text{существует } x \in a \text{ такой, что } \Phi(x, y)\}$.

6. Аксиома бесконечности. Существует множество, которое содержит $\emptyset$ и вместе с каждым x содержит и $x \cup \{x\}$.

7. Аксиома регулярности. Для любого непустого множества a существует элемент $x \in a$ такой, что $x \cap a = \emptyset$.

Точная формализация понятия "условие $\Phi(x, y)$" из аксиомы 5 может быть дана с помощью формул исчисления предикатов (ИП), которые появятся в нашем курсе позже. Тем самым список аксиом является пока не совсем формальным. Теория множеств Цермело – Френкеля с аксиомой выбора (ZFC) получается из ZF добавлением аксиомы выбора.

8. Аксиома выбора. Для любого множества a существует функция $f : P(a) \setminus \{\emptyset\} \to a$ т. ч. $f(x) \in x$ для всех $x \in P(a) \setminus \{\emptyset\}$.

ZFC является наиболее известной и широко распространённой теорией множеств. В нашем курсе мы пользуемся её аксиомами, считая, что они выполняются для множеств. При этом мы не ставим перед собой задачу строго вывести все результаты курса из её аксиом. Если мы работаем в рамках ZFC и хотим рассматривать некоторую совокупность как множество, то сначала нужно доказать, используя аксиомы ZFC, что такое множество существует. Приведём три примера таких доказательств.

Пример 1. Если A — множество и $\Psi(x)$ — некоторое условие, то существует множество $B = \{x \in A \mid \Psi(x)\}$.

Пример 2. Существует пустое множество $\emptyset$.

Пример 3. Для любых множеств A и B существуют множества $A \cup B$, $A \cap B$ и $A \times B$.

Аксиомы 1 и 7 просто фиксируют некоторые важные свойства множеств, аксиомы 2 – 5 задают некоторые конструкции, которые позволяют строить новые, однозначно заданные множества из уже имеющихся, а аксиома 6 гарантирует, что существует по крайней мере одно бесконечное множество. Аксиома выбора является в этом смысле особой — она утверждает существование некоторого объекта, но не указывает, как его можно построить или задать в явном виде. Из-за этого доказательства, использующие только ZF без аксиомы выбора, иногда рассматриваются как более конструктивные.

Предложение. В теории множеств ZF аксиома выбора следует из теоремы Цермело. Тем самым аксиома выбора, теорема Цермело и лемма Цорна равносильны в ZF.

Смысл аксиомы регулярности можно пояснить с помощью следующей леммы.

Лемма. В рамках ZFC без аксиомы регулярности эта аксиома равносильна

утверждению: не существует последовательности множеств $x_0, x_1, x_2, \ldots$
т. ч. $x_0 \ni x_1 \ni x_2 \ni \ldots$

Если некоторая совокупность множеств сама, возможно, не является множеством, но может быть задана как совокупность всех множеств, обладающих некоторым фиксированным свойством, то её часто называют *классом*. Например, мы можем говорить о классе всех множеств, всех бинарных отношений или всех функций.

2.11. Мощности

Немного позже мы дадим точное определение *мощности множества* A, которая обозначается $|A|$. Базисным понятием для теории мощностей является, однако, не само понятие мощности, а понятие равномощности множеств. Говорим, что множества A и B *равномощны*, если существует биекция $f : A \xrightarrow[\text{на}]{1-1} B$. Обозначим это символической записью $|A| = |B|$. Приведённое определение — точная формализация того, что в A и B содержится одинаковое количество элементов.

Замечание (о равномощности). Равномощность обладает свойствами отношения эквивалентности — для любых множеств A, B, C верно:

a) $|A| = |A|$;

b) $|A| = |B| \Rightarrow |B| = |A|$;

c) $|A| = |B|$ и $|B| = |C| \Rightarrow |A| = |C|$.

Запись $|A| \leqslant |B|$ говорит, что существует инъекция $f : A \xrightarrow{1-1} B$. Это определение формализует то, что количество элементов в A меньше или равно количеству элементов в B. Запись $|A| < |B|$ означает, что $|A| \leqslant |B|$ и $|A| \neq |B|$.

Замечание. Из $|A| \leqslant |B|$ и $|B| \leqslant |C|$ следует, что $|A| \leqslant |C|$.

Лемма (о порядке на мощностях). Если A и B — непустые множества, то равносильно:

a) $|A| \leqslant |B|$;

b) существует функция $g : B \xrightarrow{\text{на}} A$;

c) A равномощно некоторому подмножеству B.

Если $f : A \to B$ и $A_1 \subseteq A$, то через $f[A_1]$ обозначим $\{f(x) \mid x \in A_1\}$. Это множество называют *образом* A_1 относительно f и иногда обозначают как $f(A_1)$. Напомним, что $f[A] = \mathrm{ran}(f)$.

Теорема Кантора – Бернштейна. Если $|A| \leqslant |B|$ и $|B| \leqslant |A|$, то $|A| = |B|$.

Теорема (о сравнимости мощностей). Мощности любых двух множеств сравнимы, т. е. $|A| \leqslant |B|$ или $|B| \leqslant |A|$ для любых множеств A, B.

Теорема Кантора. $|A| < |P(A)|$ для любого множества A.

Заметим, что теорема Кантора тоже показывает, что множества всех множеств не существует: если M — множество всех множеств, то $P(M) \subseteq M$, и тем самым $|P(M)| \leqslant |M|$. Это рассуждение называется *парадоксом Кантора*.

Множество A называется *конечным множеством мощности* k, если $|A| = |\mathbb{N}_k|$, где $k \in \mathbb{N}$, а $\mathbb{N}_k = \{x \in \mathbb{N} \mid x < k\}$. Множество *бесконечно*, если оно не является конечным. Множество A *счётно*, если $|A| = |\mathbb{N}|$, и *континуально*, если $|A| = |\mathbb{R}|$, где $\mathbb{R}$ — множество вещественных чисел.

Мы не будем доказывать некоторые свойства конечных множеств, считая их почти очевидными: например то, что подмножество конечного множества является конечным. Они могут быть доказаны через свойства натуральных чисел.

Предложение. Любое бесконечное множество содержит счётное подмножество.

Множество A *не более чем счётно*, если $|A| \leqslant |\mathbb{N}|$.

Следствие (описание не более чем счётных множеств). Множество не более чем счётно тогда и только тогда, когда оно конечно или счётно.

2.12. Мощности объединения и произведения множеств

Лемма (о сохранении мощностей).
a) Если $|A| = |A_1|$ и $|B| = |B_1|$, то $|A \times B| = |A_1 \times B_1|$.
b) Если при этом $A \cap B = A_1 \cap B_1 = \emptyset$, то $|A \cup B| = |A_1 \cup B_1|$.

Лемма. $|\mathbb{N}^2| = |\mathbb{N}|$.

Лемма. Если A — бесконечное множество, а B — конечное, то $|A \cup B| = |A|$.

Если A, B — два множества, то они сравнимы по мощности: $|A| \leqslant |B|$ или $|B| \leqslant |A|$. Обозначим через $\max\{|A|, |B|\}$ бóльшую из этих мощностей, т. е. $|B|$ в первом случае и $|A|$ во втором.

Теорема (о мощности объединения). Если одно из множеств A, B бесконечно, то $|A \cup B| = \max\{|A|, |B|\}$.

Теорема. Если A — бесконечное множество, то $|A^2| = |A|$.

Теорема (о мощности произведения). Если A, B — непустые множества и одно из них бесконечно, то

$$|A \times B| = \max\{|A|, |B|\}.$$

Индексированное семейство $\{A_i\}_{i \in I}$ — это функция f такая, что $\mathrm{dom}(f) = I$ и $f(i) = A_i$ при $i \in I$.

Теорема (об объединении семейства). Пусть A — бесконечное множество. Если $\{A_i\}_{i \in I}$ — семейство множеств, $|I| \leqslant |A|$ и $|A_i| \leqslant |A|$ при всех $i \in I$, то $|\bigcup\limits_{i \in I} A_i| \leqslant |A|$.

Предложение (о мощности множества слов). Если A — непустой алфавит, то мощность множества слов в этом алфавите равна $\max\{|A|, |\mathbb{N}|\}$.

2.13. Континуум-гипотеза

По теореме Кантора $|\mathbb{N}| < |P(\mathbb{N})|$, и известно, что $|P(\mathbb{N})| = |\mathbb{R}|$. Тем самым континуальная мощность строго больше счётной. Возникает естественный вопрос, существуют ли между ними промежуточные мощности. Этот вопрос интересовал ещё Г. Кантора и был сформулирован Д. Гильбертом в его знаменитом списке из 23 нерешённых проблем в 1900 г.

Континуум-гипотеза (CH): не существует множества A т. ч. $|\mathbb{N}| < |A| < |\mathbb{R}|$.

В отличие от многих других математических проблем, её решение оказалось довольно неожиданным.

Теорема Гёделя – Коэна. Если теория множеств ZFC непротиворечива, то континуум-гипотезу нельзя ни доказать, ни опровергнуть в рамках ZFC.

Такие утверждения называются *неразрешимыми в* ZFC. Поскольку почти любое математическое доказательство может быть переписано как доказательство в рамках ZFC, эта теорема является веским аргументом в пользу того, что континуум-гипотеза вообще не может быть ни доказана, ни опровергнута методами современной математики. У неё есть естественное обобщение.

Обобщённая континуум-гипотеза (GCH): если множество B бесконечно, то не существует множества A т. ч. $|B| < |A| < |P(B)|$.

Про неё тоже известно, что она неразрешима в ZFC. Если она верна, то начальная цепочка бесконечных мощностей выглядит так: $|\mathbb{N}| < |P(\mathbb{N})| < |P(P(\mathbb{N}))| < \ldots$ Чтобы заменить последнее многоточие на что-то более строгое, необходимо понятие ординала.

2.14. Ординалы

Отношение изоморфизма разбивает класс всех в.у.м. на подклассы: каждый подкласс состоит из всех в.у.м., которые изоморфны некоторому фиксированному в.у.м. В каждом таком подклассе можно естественным образом выбрать одно фиксированное в.у.м., которое можно считать его каноническим представителем. Оно является множеством специального вида, которое называется ординалом. Ординалы иногда называют также *трансфинитными числами*.

Замечание. Если $n \geqslant 1$, то не существует таких множеств $x_1, \ldots, x_n$, что $x_1 \in x_2 \in \ldots \in x_n \in x_1$. В частности, не существует x такого, что $x \in x$.

Множество α называется *транзитивным*, если из $x \in \alpha$ и $y \in x$ следует, что $y \in \alpha$. Множество α — *ординал*, если оно транзитивно и любые различные элементы в нём сравнимы относительно $\in$. Последнее означает, что один из случаев $x \in y$, $x = y$, $y \in x$ выполняется для любых $x, y \in \alpha$. В дальнейшем ординалы часто будут обозначаться греческими буквами $\alpha, \beta, \ldots$

Лемма (об элементах ординала). Если α — ординал и $\beta \in \alpha$, то β — ординал.

Определим на классе ординалов порядок $\leqslant$ так: $\alpha \leqslant \beta$, если $\alpha \in \beta$ или $\alpha = \beta$. Запись $\alpha < \beta$, как обычно, обозначает $\alpha \leqslant \beta$ и $\alpha \neq \beta$. Ясно, что $\alpha < \beta$ равносильно $\alpha \in \beta$.

Лемма. Любой ординал α с порядком $\leqslant$ на его элементах является в.у.м.

Далее, говоря об ординале как о в.у.м., мы будем подразумевать, что на его элементах задан этот порядок $\leqslant$ (*естественный порядок* на ординале).

Лемма (о порядке на ординалах). Для любых ординалов α, β равносильно:

a) $\alpha \leqslant \beta$;

b) $\alpha \subseteq \beta$.

Теорема (о свойствах ординалов). Класс ординалов с порядком $\leqslant$ обладает свойствами в.у.м. — для любых ординалов α, β, γ верно:

a) $\alpha \leqslant \alpha$;

b) $\alpha \leqslant \beta$ и $\beta \leqslant \alpha \Rightarrow \alpha = \beta$;

c) $\alpha \leqslant \beta$ и $\beta \leqslant \gamma \Rightarrow \alpha \leqslant \gamma$;

d) $\alpha \leqslant \beta$ или $\beta \leqslant \alpha$;

e) в любом непустом множестве ординалов есть минимальный элемент.

Определим $\alpha + 1$ как $\alpha \cup \{\alpha\}$.

Замечание. Если α — ординал, то $\alpha + 1$ тоже является ординалом, $\alpha < \alpha + 1$ и не существует ординала β такого, что $\alpha < \beta < \alpha + 1$.

Предложение (о супремуме множества ординалов). Объединение любого множества ординалов A вновь является ординалом, который является супремумом множества A.

Обозначим ординал из предыдущего предложения как $\sup(A)$.

Выше мы определяли натуральные числа так: $0 = \emptyset$ и $n + 1 = n \cup \{n\}$. Легко проверить, что $\emptyset$ является наименьшим ординалом. Следовательно, ординалами будут и все множества $1, 2, \ldots$ Они образуют начальный сегмент в классе всех ординалов. Их супремум равен множеству всех натуральных чисел $\omega = \{0, 1, 2, \ldots\}$. Тем самым ω — ординал, следующий за всеми натуральными числами. Далее будут идти $\omega + 1$, $(\omega + 1) + 1$ и т. д.

Теорема (о связи в.у.м. и ординалов). Для любого в.у.м. существует единственный изоморфный ему ординал.

Предложение (принцип трансфинитной индукции). Пусть $\Phi(x)$ — некоторое условие. Пусть для любого ординала α из того, что $\Phi(\beta)$ верно для всех $\beta < \alpha$, следует, что верно $\Phi(\alpha)$. Тогда $\Phi(\alpha)$ верно для всех ординалов α.

Как и в аксиоме подстановки ZFC, точное определение условия $\Phi(x)$ требует использования формул ИП. Тем самым предложение сформулировано пока не совсем формально. Приведём в ещё более неформальном виде другой полезный факт.

Предложение (принцип трансфинитной рекурсии). Пусть существует условие, которое для каждого ординала α однозначно задаёт некоторое множество f_α в предположении, что при $\beta < \alpha$ множества f_β уже определены. Тогда каждому ординалу α действительно можно сопоставить множество f_α так, чтобы указанная связь между f_α и f_β, $\beta < \alpha$, выполнялась. При этом f_α определено однозначно.

Трансфинитную рекурсию тоже часто называют индукцией, говоря о задании f_α индукцией по ординалам.

Ординал α — *предельный*, если $\alpha \neq 0$ и его нельзя представить в виде $\beta + 1$ для некоторого ординала β.

Пример. Для любых двух ординалов α, β существуют ординалы $\alpha + \beta$ и $\alpha \cdot \beta$, обладающие свойствами:

a) $\alpha + 0 = \alpha$ и $\alpha \cdot 0 = 0$;

b) $\alpha + (\beta + 1) = (\alpha + \beta) + 1$ и $\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha$;

c) $\alpha + \lambda = \sup\{\alpha + \beta \mid \beta < \lambda\}$ и $\alpha \cdot \lambda = \sup\{\alpha \cdot \beta \mid \beta < \lambda\}$, если λ — предельный ординал.

Отметим, что на языке ординалов определение натурального числа звучит так: α — *натуральное число*, если сам α и любой его элемент — непредельный ординал. Те свойства натуральных чисел, которые мы использовали выше, могут быть выведены из этого определения. В частности, принцип индукции для натуральных чисел становится следствием более общего принципа трансфинитной индукции, а

построение каких-то объектов f_n индукцией по натуральному числу n — частным случаем принципа трансфинитной рекурсии.

2.15. Кардиналы

Ординал μ называется *кардиналом*, если он неравномощен никакому строго меньшему ординалу.

Теорема (основное свойство кардиналов). Для любого множества A существует единственный кардинал μ_A такой, что $|\mu_A| = |A|$.

Предложение. Если A, B — множества, то

a) $|A| = |B| \Leftrightarrow \mu_A = \mu_B$;

b) $|A| \leqslant |B| \Leftrightarrow \mu_A \leqslant \mu_B$.

Определим теперь понятие мощности: $|A|$, *мощность* множества A — это кардинал, равномощный A, т. е. μ_A. Последнее предложение показывает, что это определение согласуется с нашей системой обозначений.

Пример. Ординал ω и все натуральные числа $n \in \omega$ являются кардиналами.

3. ЯЗЫК ИСЧИСЛЕНИЯ ПРЕДИКАТОВ И ЕГО СЕМАНТИКА

3.1. Формулы исчисления предикатов (ИП)

Чтобы определить понятие формулы ИП, нужно сначала зафиксировать некоторое множество символов, которое называется сигнатурой (или языком). Оно соответствует тому набору исходных понятий, о которых мы собираемся говорить на языке формул, и состоит из трёх частей — предикатных, функциональных и константных символов.

Определим *сигнатуру* Σ как четвёрку вида $(\mathrm{Pr}_\Sigma, \mathrm{Fn}_\Sigma, \mathrm{Cn}_\Sigma, \nu)$, где множества $\mathrm{Pr}_\Sigma, \mathrm{Fn}_\Sigma, \mathrm{Cn}_\Sigma$ попарно не пересекаются, а функция $\nu : \mathrm{Pr}_\Sigma \cup \mathrm{Fn}_\Sigma \to \mathbb{N} \setminus \{0\}$. Элементы множества Pr_Σ называются *предикатными символами*, элементы Fn_Σ — *функциональными символами*, а элементы Cn_Σ — *константными символами*, или просто *константами*. Функция ν каждому предикатному и функциональному символу сопоставляет ненулевое натуральное число, которое называется *местностью* этого символа.

Поскольку сигнатура — всего лишь набор символов, её строгое определение не очень существенно. Если, например, $\mathrm{Pr}_\Sigma = \{P_1, \ldots, P_t\}$, $\mathrm{Fn}_\Sigma = \{f_1, \ldots, f_s\}$, $\mathrm{Cn}_\Sigma = \{c_1, \ldots, c_r\}$, то сигнатуру Σ будем иногда обозначать так:

$$\Sigma = (P_1^{n_1}, \ldots, P_t^{n_t}; f_1^{m_1}, \ldots, f_s^{m_s}; c_1, \ldots, c_r),$$

где n_i — местность символа P_i, а m_j — местность f_j.

Выбрав сигнатуру Σ, можно определить исчисление $\mathrm{ИП}_\Sigma$. Сначала определим термы и формулы $\mathrm{ИП}_\Sigma$. Алфавит $\mathrm{ИП}_\Sigma$ состоит из четырёх непересекающихся частей:

1) символы из Σ;

2) *предметные переменные*: $v_0, v_1, v_2, \ldots$;

3) *логические символы*: $\&, \vee, \to, \neg, \exists, \forall, =$;

4) *вспомогательные символы*: запятая и две скобки, левая и правая.

Символ $\exists$ называется *квантором существования*, а $\forall$ — *квантором всеобщности*. Символы $\&, \vee, \to$ и $\neg$ называют *связками*. Предметные переменные в гл. 3 часто будут называться просто *переменными* и обозначаться символами x, y, z и производными от них.

Терм $\mathrm{ИП}_\Sigma$ — слово в этом алфавите, которое строится по правилам:

1) любая переменная x — терм;

2) любая константа c из Σ — терм;

3) если f — функциональный символ из Σ местности m, а $t_1, \ldots, t_m$ — термы, то $f(t_1, \ldots, t_m)$ — терм.

Формула $\mathrm{ИП}_\Sigma$ — слово в этом алфавите, которое строится по правилам:

1) если P — предикатный символ из Σ местности n, а $t_1, \ldots, t_n$ — термы, то $P(t_1, \ldots, t_n)$ — формула;

2) если t_1, t_2 — термы, то $t_1 = t_2$ — формула;

3) если Φ, Ψ — формулы, то $\neg\Phi$, $(\Phi \,\&\, \Psi)$, $(\Phi \vee \Psi)$, $(\Phi \to \Psi)$ — тоже формулы;

4) если Φ — формула, x — переменная, то $\exists x\, \Phi$ и $\forall x\, \Phi$ — тоже формулы.

Формулы из пунктов 1 и 2 называются *атомными*. Две последние формулы могут читаться так: “существует x такой, что верно Φ” и “для всех x верно Φ”.

Как и для ИВ, *подформулой* формулы Φ называется её подслово, которое само является формулой. Везде, где это имеет смысл, подформулой называем некоторое вхождение подформулы. Отметим без доказательства, что для формул ИП_Σ нетрудно получить аналоги ряда утверждений, доказанных для формул ИВ в гл. 1.

Лемма. Если Φ, Ψ — формулы ИП_Σ и Ψ является началом Φ, то $\Phi = \Psi$.

Предложение (о представлении термов и формул ИП).

a) Любой терм ИП_Σ единственным образом может быть представлен в одной из форм:

$$x,\ c,\ f(t_1, \ldots, t_k),$$

где x — переменная, c — константа, f — функциональный символ, t_i — термы ИП_Σ.

b) Любая формула ИП_Σ единственным образом может быть представлена в одной из форм:

$$P(t_1, \ldots, t_k),\ t_1 = t_2,\ \neg\Phi,\ (\Phi \,\&\, \Psi),\ (\Phi \vee \Psi),\ (\Phi \to \Psi),\ \exists x\, \Phi,\ \forall x\, \Phi,$$

где P — предикатный символ, t_i — термы, Φ, Ψ — формулы ИП_Σ, x — переменная.

Как правило, в дальнейшем мы будем работать с некоторой фиксированной сигнатурой Σ. До конца гл. 3 термы и формулы ИП_Σ будем называть просто *термами* и *формулами*. Если нужно будет подчеркнуть то, что их сигнатурные символы лежат в Σ, они будут называться термами и формулами сигнатуры Σ. Если Φ — формула, то запись вида $\Phi = (\Phi_1 \circ \Phi_2)$, где $\circ \in \{\&, \vee, \to\}$, в дальнейшем всегда будет подразумевать, что Φ_1, Φ_2 — формулы, если не будет специально указано обратное. Точно так же запись $\Phi = P(t_1, \ldots, t_k)$ для формулы Φ и $t = f(t_1, \ldots, t_k)$ для терма t будет подразумевать, что t_i — термы при $i \leqslant k$.

Предложение (о подформулах формулы ИП). Для любой формулы Φ:

a) если Φ — атомная формула, то любая её подформула равна самой Φ;

b) если $\Phi = (\Phi_1 \circ \Phi_2)$, где $\circ \in \{\&, \vee, \to\}$, то любая подформула Φ либо равна Φ, либо является подформулой Φ_1 или Φ_2;

c) если $\Phi = \neg\Phi_1$, $\Phi = \exists x\, \Phi_1$ или $\Phi = \forall x\, \Phi_1$, то любая подформула Φ либо равна Φ, либо является подформулой Φ_1.

Из этих утверждений легко следует

Замечание. В любой формуле каждое вхождение квантора $\forall$ или $\exists$ является началом некоторой подформулы. Такая подформула единственна.

Эта подформула называется *областью действия* данного квантора. Квантор, за которым следует переменная x, называется *квантором по переменной* x. Вхождение переменной x в формулу называется *связанным вхождением*, если оно находится в области действия квантора по переменной x. В противном случае оно называется *свободным вхождением*.

Переменная x называется *свободной переменной* формулы Φ, если в Φ есть свободные вхождения x. Смысл этого определения состоит в том, что свободные переменные формулы Φ — те переменные, от которых зависит значение Φ. Формула, у которой нет свободных переменных, называется *предложением*. Отметим, что

понятие свободного вхождения переменной может быть задано индуктивно.

Лемма (о свободных вхождениях). Для любой формулы Φ и переменной x верно:

a) если Φ — атомная формула, то любое вхождение x в Φ является свободным;

b) если $\Phi = \neg\Phi_1$ или $\Phi = (\Phi_1 \circ \Phi_2)$, где $\circ \in \{\&, \vee, \to\}$, то свободные вхождения x в Φ — это в точности свободные вхождения x в Φ_1 и в Φ_2;

c) если $\Phi = \exists x\, \Phi_1$ или $\forall x\, \Phi_1$, то Φ не содержит свободных вхождений x;

d) если $\Phi = \exists y\, \Phi_1$ или $\forall y\, \Phi_1$, где $y \neq x$, то свободные вхождения x в Φ — в точности свободные вхождения x в Φ_1.

3.2. Алгебраические системы

Пусть A — множество, $k \geqslant 1$ — натуральное число. Любое отображение $P : A^k \to \{\mathbf{и}, \mathbf{л}\}$ называется *k-местным предикатом* на множестве A, а любая функция $f : A^k \to A$ — *k-местной функцией* на множестве A.

Пусть фиксирована сигнатура Σ. *Алгебраическая система* $\mathfrak{A}$ сигнатуры Σ — это пара вида $\mathfrak{A} = (A, \Sigma^{\mathfrak{A}})$, где A — непустое множество, а $\Sigma^{\mathfrak{A}}$ — интерпретация сигнатуры в A. *Интерпретация сигнатуры* — это соответствие, которое каждому символу из Σ сопоставляет его интерпретацию по следующим правилам:
1) если $P \in \mathrm{Pr}_\Sigma$ и $\nu(P) = k$, то его интерпретация $P^{\mathfrak{A}}$ — k-местный предикат на A;
2) если $f \in \mathrm{Fn}_\Sigma$ и $\nu(f) = k$, то его интерпретация $f^{\mathfrak{A}}$ — k-местная функция на A;
3) если $c \in \mathrm{Cn}_\Sigma$, то его интерпретация $c^{\mathfrak{A}}$ — элемент A.

Множество A называется *носителем* системы $\mathfrak{A}$. Алгебраические системы иногда называют также *моделями* или *структурами*. Для краткости часто будем называть их просто *системами*. Если сигнатура задана в виде

$$\Sigma = (P_1, \ldots, P_t; f_1, \ldots, f_s; c_1, \ldots, c_r),$$

то алгебраическая система этой сигнатуры часто будет обозначаться как

$$\mathfrak{A} = (A, P_1^{\mathfrak{A}}, \ldots, P_t^{\mathfrak{A}}, f_1^{\mathfrak{A}}, \ldots, f_s^{\mathfrak{A}}, c_1^{\mathfrak{A}}, \ldots, c_r^{\mathfrak{A}}).$$

Пусть $\mathfrak{A}, \mathfrak{B}$ — две системы сигнатуры Σ с носителями A и B соответственно. Функция $\beta : A \to B$ называется *изоморфизмом* между $\mathfrak{A}$ и $\mathfrak{B}$, если β является биекцией, *сохраняющей* интерпретацию Σ:

1) если $P \in \mathrm{Pr}_\Sigma$, то $P^{\mathfrak{A}}(a_1, \ldots, a_k) = P^{\mathfrak{B}}(\beta(a_1), \ldots, \beta(a_k))$ для любых $a_i \in A$;

2) если $f \in \mathrm{Fn}_\Sigma$, то $\beta(f^{\mathfrak{A}}(a_1, \ldots, a_k)) = f^{\mathfrak{B}}(\beta(a_1), \ldots, \beta(a_k))$ для любых $a_i \in A$;

3) если $c \in \mathrm{Cn}_\Sigma$, то $\beta(c^{\mathfrak{A}}) = c^{\mathfrak{B}}$.

Если между $\mathfrak{A}$ и $\mathfrak{B}$ существует изоморфизм, они называются *изоморфными* ($\mathfrak{A} \cong \mathfrak{B}$). Изоморфные системы являются, по сути, одной и той же системой, с точностью до замены одного носителя на другой. Свойства носителя системы часто переносят на саму систему: например, мощностью системы называют мощность её носителя, элементами системы — элементы носителя и т. д.

Замечание. Если две системы изоморфны, то их мощности равны.

Система $\mathfrak{B}$ называется *подсистемой* системы $\mathfrak{A}$, если $B \subseteq A$ и интерпретация любого символа из Σ в $\mathfrak{A}$ и $\mathfrak{B}$ совпадает на B. Последнее означает, что:

1) $P \in \mathrm{Pr}_\Sigma \Rightarrow P^{\mathfrak{A}}(b_1, \ldots, b_k) = P^{\mathfrak{B}}(b_1, \ldots, b_k)$ для любых $b_i \in B$;

2) $f \in \mathrm{Fn}_\Sigma \Rightarrow f^{\mathfrak{A}}(b_1, \ldots, b_k) = f^{\mathfrak{B}}(b_1, \ldots, b_k)$ для любых $b_i \in B$;

3) $c \in \mathrm{Cn}_\Sigma \Rightarrow c^{\mathfrak{A}} = c^{\mathfrak{B}}$.

Это определение означает, что интерпретация Σ в $\mathfrak{B}$ — просто сужение интерпретации Σ в $\mathfrak{A}$ на множество B. Поскольку подсистема однозначно определяется своим носителем, иногда подсистемой называют и само множество B.

Если $f : A^k \to A$ и $B \subseteq A$, то скажем, что B *замкнуто относительно* f, если $f(b_1, \ldots, b_k) \in B$ для любых $b_1, \ldots, b_k \in B$.

Предложение (о подсистемах). Пусть $\mathfrak{A}$ — алгебраическая система с носителем A, а $B \subseteq A$. В $\mathfrak{A}$ есть подсистема с носителем B тогда и только тогда, когда B непусто, замкнуто относительно $f^{\mathfrak{A}}$ для всех $f \in \mathrm{Fn}_\Sigma$ и содержит $c^{\mathfrak{A}}$ для всех $c \in \mathrm{Cn}_\Sigma$.

Предложение. Пусть $\mathfrak{A}$ — алгебраическая система с носителем A, а непустое $X \subseteq A$. Тогда в $\mathfrak{A}$ существует наименьшая (по включению) подсистема, содержащая X.

Подсистема с указанным свойством называется *подсистемой, порождённой множеством* X.

3.3. Истинность формул в алгебраических системах

Введём несколько обозначений, облегчающих работу с формулами и термами. Часто терм бывает удобно обозначать как $t(x_1, \ldots, x_k)$. Договоримся, что такая запись может быть использована только в том случае, когда все переменные этого терма входят в набор $x_1, \ldots, x_k$ и все переменные из этого набора различны. Аналогичная запись $\Phi(x_1, \ldots, x_k)$ может быть использована для формулы, но только в том случае, когда все её свободные переменные входят в набор $x_1, \ldots, x_k$ и все его элементы различны. При этом запись Φ может обозначать как предложение, так и произвольную формулу. Кроме того, набор $x_1, \ldots, x_k$ часто будем сокращать до $\bar{x}$.

Пусть фиксирована сигнатура Σ и $\mathfrak{A}$ — система этой сигнатуры. Если дан терм $t(x_1, \ldots, x_k)$ и $a_1, \ldots, a_k \in \mathfrak{A}$, то мы можем определить его *значение* в системе $\mathfrak{A}$ при значениях переменных $x_1 = a_1, \ldots, x_k = a_k$. Обозначим это значение как $t^{\mathfrak{A}}(a_1, \ldots, a_k)$. Оно определяется индукцией по длине терма:

1) если $t(\bar{x})$ — переменная x_i, то $t^{\mathfrak{A}}(\bar{a}) = a_i$;

2) если $t(\bar{x})$ — константа c, то $t^{\mathfrak{A}}(\bar{a}) = c^{\mathfrak{A}}$;

3) если $t(\bar{x}) = f(t_1(\bar{x}), \ldots, t_n(\bar{x}))$, то $t^{\mathfrak{A}}(\bar{a}) = f^{\mathfrak{A}}(t_1^{\mathfrak{A}}(\bar{a}), \ldots, t_n^{\mathfrak{A}}(\bar{a}))$.

Тем самым значение терма — элемент $\mathfrak{A}$.

Замечание. Значение терма зависит только от системы и значений входящих в него переменных. При этом оно не зависит от интерпретации тех символов из сигнатуры, которые не входят в терм.

Пусть дана формула $\Phi(x_1, \ldots, x_k)$ и $a_1, \ldots, a_k \in \mathfrak{A}$. Дадим определение того, что эта формула *истинна* в $\mathfrak{A}$ при значениях переменных $x_1 = a_1, \ldots, x_k = a_k$. Обозначим это как

$$\mathfrak{A} \models \Phi(a_1, \ldots, a_k).$$

Если формула не является истинной, то по определению является *ложной*, и это обозначается как $\mathfrak{A} \not\models \Phi(a_1, \ldots, a_k)$. Определим истинность индукцией по длине формулы:

1) если $\Phi(\bar{x}) = P(t_1(\bar{x}), \ldots, t_n(\bar{x}))$, то
$$\mathfrak{A} \models \Phi(\bar{a}) \Leftrightarrow P^{\mathfrak{A}}(t_1^{\mathfrak{A}}(\bar{a}), \ldots, t_n^{\mathfrak{A}}(\bar{a})) = \textbf{и};$$
2) если $\Phi(\bar{x})$ — формула $t_1(\bar{x}) = t_2(\bar{x})$, то
$$\mathfrak{A} \models \Phi(\bar{a}) \Leftrightarrow t_1^{\mathfrak{A}}(\bar{a}) = t_2^{\mathfrak{A}}(\bar{a});$$
3) если $\Phi(\bar{x}) = \neg\Psi(\bar{x})$, то
$$\mathfrak{A} \models \Phi(\bar{a}) \Leftrightarrow \mathfrak{A} \not\models \Psi(\bar{a});$$
4) если $\Phi(\bar{x}) = \Phi_1(\bar{x}) \,\&\, \Phi_2(\bar{x})$, то
$$\mathfrak{A} \models \Phi(\bar{a}) \Leftrightarrow \mathfrak{A} \models \Phi_1(\bar{a}) \text{ и } \mathfrak{A} \models \Phi_2(\bar{a});$$
5) если $\Phi(\bar{x}) = \Phi_1(\bar{x}) \vee \Phi_2(\bar{x})$, то
$$\mathfrak{A} \models \Phi(\bar{a}) \Leftrightarrow \mathfrak{A} \models \Phi_1(\bar{a}) \text{ или } \mathfrak{A} \models \Phi_2(\bar{a});$$
6) если $\Phi(\bar{x}) = \Phi_1(\bar{x}) \to \Phi_2(\bar{x})$, то
$$\mathfrak{A} \models \Phi(\bar{a}) \Leftrightarrow \mathfrak{A} \not\models \Phi_1(\bar{a}) \text{ или } \mathfrak{A} \models \Phi_2(\bar{a});$$
7) если $\Phi(\bar{x}) = \exists y\ \Psi(\bar{x}, y)$, где $y \notin \{x_1, \ldots, x_k\}$, то
$$\mathfrak{A} \models \Phi(\bar{a}) \Leftrightarrow \text{существует } b \in \mathfrak{A} \text{ такой, что } \mathfrak{A} \models \Psi(\bar{a}, b);$$
8) если $\Phi(\bar{x}) = \forall y\ \Psi(\bar{x}, y)$, где $y \notin \{x_1, \ldots, x_k\}$, то
$$\mathfrak{A} \models \Phi(\bar{a}) \Leftrightarrow \text{для всех } b \in \mathfrak{A} \text{ верно, что } \mathfrak{A} \models \Psi(\bar{a}, b).$$

Можно заметить, что в этом списке отсутствуют ещё два пункта: случаи, когда $\Phi(x_1, \ldots, x_k)$ равна $\exists x_i\, \Psi$ или $\forall x_i\, \Psi$ для некоторого $i \leqslant k$. Поскольку x_i в этом случае не является свободной переменной $\Phi(\bar{x})$, значение a_i просто отбрасывается. Можно переобозначить формулу как $\Phi(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k)$ и использовать пункт 7 или 8. Приведём для ясности формальное определение:

7') если $\Phi(x_1, \ldots, x_k) = \exists x_i\ \Psi(x_1, \ldots, x_k)$, то $\mathfrak{A} \models \Phi(a_1, \ldots, a_k) \Leftrightarrow$ существует $b \in \mathfrak{A}$ такой, что $\mathfrak{A} \models \Psi(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_k)$;

8') если $\Phi(x_1, \ldots, x_k) = \forall x_i\ \Psi(x_1, \ldots, x_k)$, то $\mathfrak{A} \models \Phi(a_1, \ldots, a_k) \Leftrightarrow$ для всех $b \in \mathfrak{A}$ верно, что $\mathfrak{A} \models \Psi(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_k)$.

Тем самым значение формулы ИП — истина или ложь.

Замечание. Значение формулы зависит только от системы и значений её свободных переменных. При этом оно не зависит от интерпретации тех символов из сигнатуры, которые не входят в формулу.

Предложение (о сохранении формул при изоморфизме). Пусть $\mathfrak{A}, \mathfrak{B}$ — две системы сигнатуры Σ, $\beta : \mathfrak{A} \to \mathfrak{B}$ — изоморфизм и $\Phi(x_1, \ldots, x_k)$ — формула. Если $a_1, \ldots, a_k \in \mathfrak{A}$, то
$$\mathfrak{A} \models \Phi(a_1, \ldots, a_k) \Leftrightarrow \mathfrak{B} \models \Phi(\beta(a_1), \ldots, \beta(a_k)).$$

Если Γ — бесконечное множество формул, то множество его свободных переменных тоже может быть бесконечным. В такой ситуации удобно использовать понятие означивания. Назовём *означиванием переменных в системе* $\mathfrak{A}$ любую функцию $\gamma : V \to \mathfrak{A}$, где V — некоторое множество переменных. Как и в случае с

ИВ, договоримся, что всякий раз, когда речь идёт о значении терма или формулы в системе при данном означивании, неявно подразумевается условие, что все переменные терма и все свободные переменные формулы получают какие-то значения из системы при этом означивании. Запись $\mathfrak{A} \models \Phi[\gamma]$ говорит, что формула Φ истинна в $\mathfrak{A}$ при означивании γ. Если $\Phi = \Phi(x_1, \ldots, x_k)$, то это означает, что $\mathfrak{A} \models \Phi(\gamma(x_1), \ldots, \gamma(x_k))$.

Формула называется *тождественно истинной (ложной)*, если она истинна (ложна) в любой системе при любом означивании. Формулы Φ и Ψ *семантически эквивалентны* ($\Phi \sim \Psi$), если в любой системе при любом означивании они истинны или ложны одновременно. Множество формул Γ называется *выполнимым*, если существует система и означивание, при которых все формулы из Γ истинны.

Лемма (об отрицании перед квантором). Для любой формулы Φ верно, что $\neg\exists x\, \Phi \sim \forall x\, \neg\Phi$ и $\neg\forall x\, \Phi \sim \exists x\, \neg\Phi$.

В отличие от теоремы о замене для ИВ, в следующем предложении используется семантическая эквивалентность, и доказательство становится почти очевидным.

Предложение (о замене для ИП). Если в формуле Φ некоторую подформулу заменить на семантически эквивалентную ей формулу, то результат будет семантически эквивалентен Φ.

3.4. Прямые произведения алгебраических систем

В математике часто рассматриваются прямые произведения двух алгебраических систем. Обобщим это понятие на произвольное семейство систем.

Пусть $\{A_i\}_{i\in I}$ — индексированное семейство множеств. Его *прямое произведение* $\prod_{i\in I} A_i = \{\alpha$ — функция $\mid \mathrm{dom}(\alpha) = I$ и $\alpha(i) \in A_i$ при $i \in I\}$.

Замечание. Если $I = \{1, \ldots, n\}$, то элементы $\prod_{i\in I} A_i$ можно естественным образом отождествить с элементами множества $A_1 \times \ldots \times A_n$.

Пусть фиксирована сигнатура Σ, $\{\mathfrak{A}_i\}_{i\in I}$ — семейство систем этой сигнатуры и A_i — носитель $\mathfrak{A}_i$. *Прямое произведение* $\prod_{i\in I} \mathfrak{A}_i$ этого семейства — это система $\mathfrak{A}$ с носителем $\prod_{i\in I} A_i$, в которой интерпретация символов из Σ задаётся так:

1) если $P \in \mathrm{Pr}_\Sigma$, то

$P^{\mathfrak{A}}(\alpha_1, \ldots, \alpha_n) = \mathbf{и} \Leftrightarrow P^{\mathfrak{A}_i}(\alpha_1(i), \ldots, \alpha_n(i)) = \mathbf{и}$ для всех $i \in I$;

2) если $f \in \mathrm{Fn}_\Sigma$, то

$f^{\mathfrak{A}}(\alpha_1, \ldots, \alpha_n)(i) = f^{\mathfrak{A}_i}(\alpha_1(i), \ldots, \alpha_n(i))$ для всех $i \in I$;

3) если $c \in \mathrm{Cn}_\Sigma$, то $c^{\mathfrak{A}}(i) = c^{\mathfrak{A}_i}$ для всех $i \in I$.

Предложение (о прямом произведении). Пусть формула $\Phi(x_1, \ldots, x_k)$ построена из атомных формул с помощью $\&$, $\forall$ и $\exists$. Если $\mathfrak{A} = \prod_{i\in I} \mathfrak{A}_i$ и $\alpha_1, \ldots, \alpha_k \in \mathfrak{A}$, то

$$\mathfrak{A} \models \Phi(\alpha_1, \ldots, \alpha_k) \Leftrightarrow \forall i \in I \;\; \mathfrak{A}_i \models \Phi(\alpha_1(i), \ldots, \alpha_k(i)).$$

Если $\bar{x}$ — сокращение для набора $x_1, \ldots, x_k$, то запись $\forall\bar{x}$ — сокращение для $\forall x_1 \ldots \forall x_k$, а $\exists\bar{x}$ — для $\exists x_1 \ldots \exists x_k$.

Следствие. Пусть предложение Φ имеет вид $\forall \bar{x}\ [\Psi(\bar{x}) \to \Delta(\bar{x})]$, где формулы $\Psi(\bar{x}), \Delta(\bar{x})$ построены из атомных формул с помощью $\&, \forall$ и $\exists$. Если Φ истинно во всех системах $\mathfrak{A}_i$, $i \in I$, то истинно и в $\prod_{i\in I} \mathfrak{A}_i$.

Предложение Φ называется *тождеством*, если оно имеет вид $\forall \bar{x}\ \Delta(\bar{x})$, где $\Delta(\bar{x})$ — атомная формула, и *квазитождеством*, если имеет вид

$$\forall \bar{x}\ \big[(\Psi_1(\bar{x}) \,\&\, \ldots \,\&\, \Psi_n(\bar{x})) \to \Delta(\bar{x})\big],$$

где $n \geqslant 0$ и $\Psi_i(\bar{x}), \Delta(\bar{x})$ — атомные формулы. При $n = 0$ квазитождество превращается в тождество $\forall \bar{x}\ \Delta(\bar{x})$. Следствие, в частности, говорит, что квазитождество, истинное во всех $\mathfrak{A}_i$, $i \in I$, истинно и в их прямом произведении. Истинность тождеств сохраняется в обе стороны.

3.5. Фильтрованные произведения алгебраических систем

Пусть I — непустое множество. Семейство множеств $F \subseteq P(I)$ называется *центрированным*, если $A_1 \cap A_2 \cap \ldots \cap A_n \neq \emptyset$ для любых $A_1, \ldots, A_n \in F$, $n \geqslant 1$. Семейство F называется *фильтром на* I, если выполняются условия:

1) $\emptyset \notin F$ и $I \in F$;

2) если $A, B \in F$, то $A \cap B \in F$;

3) если $A \subseteq B \subseteq I$ и $A \in F$, то $B \in F$.

Фильтр F — *ультрафильтр*, если $A \in F$ или $I \setminus A \in F$ для любого $A \subseteq I$.

Теорема (о существовании ультрафильтров). a) Любое центрированное семейство в $P(I)$ может быть расширено до фильтра на I.

b) Любой фильтр на I может быть быть расширен до ультрафильтра на I.

Пусть фиксирована сигнатура Σ, $\{\mathfrak{A}_i\}_{i\in I}$ — семейство алгебраических систем и F — фильтр на I. Определим *фильтрованное произведение* $\prod^F_{i\in I} \mathfrak{A}_i$ семейства $\{\mathfrak{A}_i\}_{i\in I}$ по фильтру F.

Пусть A_i — носитель $\mathfrak{A}_i$ при $i \in I$. Зададим на $\prod_{i\in I} A_i$ отношение $\sim_F$ так: $\alpha \sim_F \beta \Leftrightarrow \{i \in I \mid \alpha(i) = \beta(i)\} \in F$.

Лемма. Отношение $\sim_F$ является отношением эквивалентности.

Кратко обозначим класс эквивалентности $\alpha/\!\sim_F$ как α/F.

Пусть $\mathfrak{A} = \prod_{i\in I} \mathfrak{A}_i$ — построенное выше прямое произведение семейства $\{\mathfrak{A}_i\}_{i\in I}$. Если в сигнатуре Σ нет предикатных символов, то фильтрованное произведение $\mathfrak{A}' = \prod^F_{i\in I} \mathfrak{A}_i$ задаётся просто как факторизация $\mathfrak{A}$ по $\sim_F$: носитель $\mathfrak{A}'$ равен $\{\alpha/F \mid \alpha \in \mathfrak{A}\}$,

1) если $f \in \mathrm{Fn}_\Sigma$, то $f^{\mathfrak{A}'}(\alpha_1/F, \ldots, \alpha_n/F) = f^{\mathfrak{A}}(\alpha_1, \ldots, \alpha_n)/F$;

2) если $c \in \mathrm{Cn}_\Sigma$, то $c^{\mathfrak{A}'} = c^{\mathfrak{A}}/F$.

Определение для предикатных символов выглядит сложнее:

3) если $P \in \mathrm{Pr}_\Sigma$, то

$P^{\mathfrak{A}'}(\alpha_1/F, \ldots, \alpha_n/F) = \mathbf{и} \Leftrightarrow \{i \in I \mid P^{\mathfrak{A}_i}(\alpha_1(i), \ldots, \alpha_n(i)) = \mathbf{и}\} \in F$.

Лемма. Определение $\prod^F_{i\in I} \mathfrak{A}_i$ является корректным.

Если F — ультрафильтр на I, то построенную систему называют также *ультрапроизведением* семейства $\{\mathfrak{A}_i\}_{i\in I}$ по F.

Замечание. Если фильтр $F = \{I\}$, то фильтрованное произведение $\prod^F_{i\in I} \mathfrak{A}_i$ изоморфно прямому произведению $\prod_{i\in I} \mathfrak{A}_i$.

Скажем, что формула $\Phi(x_1, \ldots, x_k)$ *фильтруется по фильтру* F, если для любого семейства систем $\{\mathfrak{A}_i\}_{i\in I}$ и любых элементов $\alpha_1/F, \ldots, \alpha_k/F \in \prod_{i\in I}^F \mathfrak{A}_i$
$\prod_{i\in I}^F \mathfrak{A}_i \models \Phi(\alpha_1/F, \ldots, \alpha_k/F) \Leftrightarrow$

$$\big\{i \in I \mid \mathfrak{A}_i \models \Phi(\alpha_1(i), \ldots, \alpha_k(i))\big\} \in F.$$

Лемма 1. Атомная формула фильтруется по любому фильтру.

Лемма 2. Любая формула Φ семантически эквивалентна формуле Φ', в которой нет $\vee$, $\to$ и $\forall$.

Теорема Лося. Любая формула фильтруется по любому ультрафильтру.

3.6. Теорема компактности Мальцева

Пусть фиксирована сигнатура Σ. Напомним, что множество формул Γ называется выполнимым, если существует система $\mathfrak{A}$ и означивание, при которых все формулы из Γ истинны. Назовём множество Γ *локально выполнимым*, если любое его конечное подмножество выполнимо. Ясно, что выполнимое множество является и локально выполнимым.

Теорема компактности Мальцева. Любое локально выполнимое множество формул является выполнимым.

Пусть Γ — множество предложений, $\mathfrak{A}$ — алгебраическая система. Будем писать, что $\mathfrak{A} \models \Gamma$, если $\mathfrak{A} \models \Phi$ для всех $\Phi \in \Gamma$. Система $\mathfrak{A}$ называется *моделью* множества Γ, если $\mathfrak{A} \models \Gamma$.

Предложение (признак существования бесконечной модели). Если для каждого натурального n у множества предложений Γ есть модель мощности больше или равной n, то у Γ есть бесконечная модель.

3.7. Формулировка аксиом ZFC на языке формул ИП

Обозначим класс всех множеств как $\mathbb{V}$. Этот класс иногда называют *универсумом* теории множеств. Заменяя запись $a \in b$ на $\in(a, b) = \mathbf{и}$, а $a \notin b$ на $\in(a, b) = \mathbf{л}$, мы можем рассматривать пару $(\mathbb{V}, \in)$ как объект, "подобный" алгебраической системе сигнатуры $\Sigma = (\in^2)$, где $\in$ — предикатный символ.

Он не является алгебраической системой, поскольку $\mathbb{V}$ не является множеством. Тем не менее, многие свойства алгебраических систем могут быть перенесены на $\mathbb{V}$. В частности, мы можем говорить об истинности формул сигнатуры Σ в $\mathbb{V}$. Значениями свободных переменных при этом являются элементы $\mathbb{V}$, т. е. произвольные множества. Истинность атомных формул, которые имеют вид $\in(x, y)$ и $x = y$, считается заданной изначально, логические связки определяются стандартно, а значение кванторов $\exists x$ и $\forall x$ понимается в том смысле, что "существует множество x такое, что..." и "для всех множеств x верно, что...".

Тогда аксиомы ZFC, о которых шла речь выше, могут быть легко переписаны в виде предложений ИП_Σ. Например, аксиома пары приобретает вид

$$\forall x \forall y \exists z \forall t \ \big(t \in z \leftrightarrow (t = x \vee t = y)\big),$$

где запись $\Phi \leftrightarrow \Psi$ является сокращением для $(\Phi \to \Psi)\,\&\,(\Psi \to \Phi)$, а $t \in z$ — для $\in(t, z)$. Говоря, что мы принимаем аксиомы ZFC, мы подразумеваем, что эти предложения истинны в $\mathbb{V}$.

Выше мы говорили, что классом множеств может быть названа совокупность всех множеств, удовлетворяющих некоторому условию. Теперь можно привести более строгую формулировку: под "условием" мы понимаем свойство, которое может быть записано в виде формулы ИП_Σ. В этой формуле можно использовать дополнительный параметр, поэтому общее определение звучит так: (определимый) *класс множеств* — это совокупность всех множеств a, для которых в $\mathbb{V}$ верно $\Psi(a, p)$, где $\Psi(x, y)$ — формула ИП_Σ, а p — некоторое фиксированное множество, которое называется *параметром*.

То же самое относится и к другим упоминаниям о неформальных "условиях" выше. Например, условие $\Phi(x, y)$ из аксиомы подстановки — это любое условие, записанное в виде формулы с параметром. Точная формулировка аксиомы подстановки звучит так: пусть $a, p \in \mathbb{V}$, $\Psi(x, y, z)$ — формула ИП_Σ и для любого $b \in a$ существует не более одного $c \in \mathbb{V}$ такого, что $\Psi(b, c, p)$. Тогда существует множество

$$a' = \{c \mid \text{существует } b \in a \text{ такой, что } \Psi(b, c, p)\}.$$

Тем самым мы получаем счётное множество предложений ИП_Σ, соответствующих аксиоме подстановки, поскольку для каждой формулы $\Psi(x, y, z)$ необходимо записать отдельное предложение.

3.8. Предварённая нормальная форма

Если Φ — формула, t — терм, а x — переменная, то запись $\Phi[x/t]$ обозначает результат подстановки терма t вместо всех свободных вхождений x в Φ. Если таких вхождений нет, то формула не меняется, т. е. $\Phi[x/t] = \Phi$. В более общем виде, запись $\Phi[x_1/t_1, \ldots, x_n/t_n]$ означает, что мы одновременно подставляем t_i вместо всех свободных вхождений x_i при $i = 1, \ldots, n$. Легко показать, что результат такой подстановки снова будет формулой.

Если формула Φ обозначена как $\Phi(x_1, \ldots, x_n, \bar{y})$, а термы $t_i = t_i(\bar{z})$, то вместо $\Phi[x_1/t_1, \ldots, x_n/t_n]$ часто используется более удобная запись $\Phi(t_1(\bar{z}), \ldots, t_n(\bar{z}), \bar{y})$.

Скажем, что терм t *свободен для* x в Φ, если никакое свободное вхождение x в Φ не находится в области действия квантора по переменной из t. Смысл этого определения состоит в том, что в этом случае подстановка $\Phi[x/t]$ корректно изменяет значение формулы. Покажем, что это понятие может быть определено индукцией по Φ.

Лемма (о свободных термах). Пусть Φ — формула, t — терм и x — переменная. Тогда

a) если Φ — атомная формула, то t свободен для x в Φ;

b) если $\Phi = \neg\Phi_1$, то t свободен для x в $\Phi \Leftrightarrow$ свободен для x в Φ_1;

c) если $\Phi = (\Phi_1 \circ \Phi_2)$, где $\circ \in \{\&, \vee, \to\}$, то t свободен для x в $\Phi \Leftrightarrow$ свободен для x в Φ_1 и Φ_2;

d) если Φ равна $\exists x\, \Phi_1$ или $\forall x\, \Phi_1$, то t свободен для x в Φ;

e) если Φ равна $\exists y\, \Phi_1$ или $\forall y\, \Phi_1$, где $y \neq x$, то t свободен для x в $\Phi \Leftrightarrow$ (t свободен для x в Φ_1 и (в t нет вхождений y или в Φ_1 нет свободных вхождений x)).

Терм t называется *константным*, если в нём нет переменных. Это означает, что он построен только из констант и функциональных символов.

Замечание. a) Переменная x всегда свободна для x в любой формуле.

b) Если t — константный терм, то t свободен для x в любой формуле.

Предложение (о подстановке значений термов). Пусть $\Phi(x_1, \ldots, x_n)$ — формула, терм $t_i(\bar{y})$ свободен для x_i в $\Phi(\bar{x})$ при $i \leqslant n$ и $\Phi'(\bar{y}) = \Phi(t_1(\bar{y}), \ldots, t_n(\bar{y}))$. Тогда в любой системе $\mathfrak{A}$ при любом наборе $\bar{a}$

$$\mathfrak{A} \models \Phi'(\bar{a}) \Leftrightarrow \mathfrak{A} \models \Phi(d_1, \ldots, d_n),$$

где $d_i = t_i^{\mathfrak{A}}(\bar{a})$ при $i \leqslant n$.

Лемма (о замене связанной переменной). Пусть y — переменная, не входящая в формулу Φ. Тогда $\exists x\, \Phi \sim \exists y\ \Phi[x/y]$, а $\forall x\, \Phi \sim \forall y\ \Phi[x/y]$.

Предварённая нормальная форма — формула вида

$$Q_1 x_1 \ldots Q_n x_n\ \Phi,$$

где $Q_i \in \{\forall, \exists\}$, а Φ — бесквантворная формула (т. е. формула без кванторов).

Теорема (о приведении к предварённой нормальной форме). Любая формула семантически эквивалентна некоторой предварённой нормальной форме.