Введение в математическую логику и теорию алгоритмов

мех-мат МГУ, 2 курс, осень 2019 г.

Часть 1. Теория множеств

Л.Д. Беклемишев

1 Аксиомы теории множеств

Основными неопределяемыми понятиями теории множеств являются понятие *множества* и понятие *быть элементом* множества. Неформально, множество понимается как некоторая (конечная или бесконечная) совокупность объектов, рассматриваемая как единое целое, отдельный объект. Объекты, входящие в совокупность, называются *элементами* данного множества. Запись $x \in A$ означает, что x есть элемент множества A, или x *принадлежит* A. Два множества считаются равными, то есть совпадают, если у них одни и те же элементы:

$$x = y \stackrel{\text{def}}{\iff} \forall z\, (z \in x \leftrightarrow z \in y).$$

Множества сами могут быть элементами других множеств. Более того, в стандартной теории множеств Цермело–Френкеля *любые* рассматриваемые объекты являются множествами. По этой причине элементами любого множества могут быть *только* множества.[1] Такие объекты, как натуральные числа, точки прямой и т.д., в теории множеств рассматриваются как множества специального вида.

Утверждение о том, что два множества равны в том и только том случае, когда они имеют одни и те же элементы, принятое нами в качестве определения, часто называется *аксиомой объемности*. Следствием этой аксиомы является тот факт, что всякий элемент может входить в данное множество не более одного раза, например $\{1, 1, 2\} = \{1, 2\}$.

[1] Существуют теории множеств, в которых также допускаются *праэлементы*, то есть объекты, не являющиеся множествами.

Если $x = y$, то x и y являются элементами одних и тех же множеств, то есть

$$x = y \to \forall z\, (x \in z \leftrightarrow y \in z).$$

Это утверждение интуитивно очевидно, если понимать равенство как буквальное совпадение двух объектов. Его иногда называют *аксиомой равенства*.

Пустое множество $\varnothing$ определяется как множество, не содержащее ни одного элемента. Аксиома объёмности гарантирует, что любые два пустых множества равны. Существование пустого множества вытекает из существования *некоторого* множества S по аксиоме выделения (см. ниже), утверждающей, что совокупность элементов $x \in S$ таких, что $x \neq x$, является множеством: $\varnothing = \{x \in S : x \neq x\}$. Тот факт, что существует хотя бы одно множество, вытекает из чисто логических аксиом, касающихся логических связок и кванторов, о которых мы будем говорить во второй части курса.

Помимо аксиомы равенства и логических аксиом, аксиомы теории множеств выражают некоторые допустимые способы построения новых множеств из уже имеющихся. Приведём полный список этих аксиом, пояснения и комментарии следуют ниже.

Список аксиом теории множеств Цермело–Френкеля:

1. (Аксиома равенства) *Равные множества x и y являются элементами одних и тех же множеств.*

2. (Аксиома пары) *Для любых x и y найдется множество $z = \{x, y\}$, элементами которого являются в точности x и y.*

3. (Схема аксиом выделения) *Для любого свойства $\varphi(x)$ и множества X найдется множество $Y = \{x \in X : \varphi(x)\}$, содержащее те и только те элементы $x \in X$, которые удовлетворяют свойству φ.*

4. (Аксиома объединения) *Для любого множества X существует множество $Y = \bigcup X$, содержащее в точности те элементы, которые принадлежат хотя бы одному из элементов множества X.*

5. (Аксиома степени) *Для любого X существует множество $Y = \mathcal{P}(X)$ всех подмножеств X.*

6. (Аксиома бесконечности) *Существует бесконечное множество.* Существует S такое, что $\varnothing \in S$ и для любого $x \in S$ множество $x \cup \{x\} \in S$.

7. (Аксиома регулярности) *Всякое непустое множество X имеет элемент $a \in X$ такой, что $\forall x \in X\ x \notin a$.*

8. (Схема аксиом подстановки) *Пусть $\varphi(x, y)$ — такое свойство, что для любого x найдётся не более одного y, удовлетворяющего $\varphi(x, y)$. Тогда для любого X найдется множество $Y = \{y : \exists x \in X \varphi(x, y)\}$.*

9. (Аксиома выбора) *Для любого семейства непустых множеств S существует функция выбора на S, то есть такая функция f, что $f(x) \in x$ для всех $x \in S$.*

1.1 Способы задания множеств.

Наиболее распространённые способы определения множеств следующие:

1) Конечные множества задаются перечислением элементов в фигурных скобках, например $\{a, b, c\}$. Существование соответствующих множеств следует из аксиомы пары, в частности для любого a существует множество $\{a\}$, единственным элементом которого является a. (Не надо путать одноэлементное множество $\{a\}$ и само множество a, которое может иметь любое число элементов.) В силу аксиомы пары $\{a\}$ можно определить как $\{a, a\}$. Тогда для любых множеств x, a

$$x \in \{a\} \iff x = a.$$

Упражнение 1.1 Проверьте, что для любых множеств x, y

$$x = y \iff \{x\} = \{y\}. \tag{1}$$

Заметим, что $\{\{a, b\}, c\} \neq \{a, b, c\}$ (почему?). Множество $\{a, b, c\}$ можно формально определить с помощью аксиомы пары, применяемой три раза, и аксиомы объединения:

$$\{a, b, c\} = \bigcup \{\{a, b\}, \{c\}\}.$$

Аналогично определяются четверки и т.д.

2) Говорят, что x есть *подмножество* множества y, если всякий элемент x принадлежит y:

$$x \subset y \overset{\text{def}}{\iff} \forall z\, (z \in x \to z \in y).$$

Очевидно, $x = y$ если и только если $x \subset y$ и $y \subset x$.

Нельзя путать $\subset$ и $\in$: пустое множество есть подмножество любого множества, но отнюдь не всегда является элементом данного множества, например $\varnothing \subset \varnothing$, но $\varnothing \notin \varnothing$. Другой пример: отрезок $[0, 1]$ является подмножеством действительной прямой $\mathbb{R}$, но не является элементом $\mathbb{R}$, то есть действительным числом.

Собственным подмножеством данного множества y называется его подмножество, отличное от самого y:

$$x \subsetneqq y \overset{\text{def}}{\iff} (x \subset y \wedge y \neq x).$$

3) В силу аксиомы степени, совокупность всех подмножеств данного множества x есть множество (обозначаемое $\mathcal{P}(x)$). По определению

$$y \in \mathcal{P}(x) \overset{\text{def}}{\iff} y \subset x.$$

Упражнение: перечислите элементы множеств $\mathcal{P}(\varnothing)$, $\mathcal{P}(\mathcal{P}(\varnothing))$, $\mathcal{P}(\{0, 1, 2\})$.

4) Наиболее распространённым и интуитивным, и в то же время проблематичным, способом определения множеств является использование схемы аксиом выделения. Для множества $Y = \{x \in X : \varphi(x)\}$ мы по определению имеем

$$y \in Y \overset{\text{def}}{\iff} (y \in X \wedge \varphi(y)).$$

Примеры:

$\{n \in \mathbb{N} : \exists m \in \mathbb{N}\, 2m = n\}$ задаёт множество чётных натуральных чисел.

$\{z \in \mathbb{C} : |z| \leq 1\}$ задаёт единичный круг на комплексной плоскости.

$\{f \in \mathbb{Z}[X] : f(0) = 0\}$ задаёт множество многочленов с целыми коэффициентами, имеющих корень в нуле.

Свойства $\varphi(x)$, о которых идёт речь в аксиоме выделения, относятся к используемому нами языку. Интуитивно говоря, $\varphi(x)$ есть некоторое точное описание того признака множеств x, по которому мы собираем элементы воедино в новое множество. В качестве таковых нам годятся любые описания, использующие лишь логический аппарат — логические связки и кванторы — и понятие принадлежности. (Пользуясь точной логической терминологией, φ выражается формулой языка логики предикатов первого порядка в сигнатуре с бинарным предикатом $\in$.)

Отсюда видно, что аккуратную формулировку аксиом теории множеств Цермело–Френкеля нельзя дать, не вводя *формального языка* теории множеств, с которым мы познакомимся лишь позже. Тем не менее, на практике ситуация не столь сложна. Язык теории множеств является универсальным в том смысле, что на нём можно выразить любое стандартное математическое понятие. Поэтому при применении схемы аксиом выделения мы можем использовать в качестве φ любое строгое математическое описание свойства φ, не задумываясь о переводе этого описания на формальный язык. Это позволяет пользоваться аксиомой выделения, оставаясь на неформальном уровне (как и поступают большинство математиков). Примеры смотри выше.

Описаний может быть много, поэтому аксиома выделения называется *схемой аксиом* — для каждого свойства φ получается своя аксиома.

Свойства φ, о которых идет речь в аксиоме выделения, могут зависеть от параметров. Например, эта аксиома для каждого числа $a \in \mathbb{R}$ позволяет сформировать множество $\{x \in \mathbb{R} : x > a\}$, задаваемое свойством $x > a$ множеств x, зависящим от параметра a. С точки зрения формального языка параметры представляют собой свободные переменные формулы, задающей свойство множеств x.

Парадокс Рассела и «множество» всех множеств. Классы. При корректном использовании схемы аксиом выделения всегда предполагается заданным исходное множество X тех объектов, из которых происходит выделение новых объектов, удовлетворяющих свойству φ. Таким образом, аксиома выделения позволяет формировать подмножества *уже заданного* множества по какому-либо признаку. Запись $\{x : \varphi(x)\}$, где $\varphi(x)$ — некоторое свойство, допустима. Однако, она должна сопровождаться обоснованием того, почему данная совокупность является множеством (существует).

Стандартный пример некорректного использования этого обозначения известен как *парадокс Рассела*. Рассмотрим «множество» всех таких множеств, которые не являются элементами себя самих:

$$R = \{x : x \notin x\}.$$

Тогда если $R \in R$, то (по определению R) должно быть $R \notin R$. Если же $R \notin R$, то $R \in R$. Противоречие.

Стандартное объяснение данного парадокса состоит в том, что совокупность R не является множеством. В некотором смысле оно слишком велико, чтобы быть множеством. Аксиома выделения не позволяет сформировать множество R, не имея объемлющего его множества.

Совокупности множеств, определяемые некоторым свойством φ, но не обязательно являющиеся множествами, называются *классами*. По-существу, говорить о классе или о свойстве, определяющем данный класс, одно и то же. Например, совокупность V всех вообще множеств является классом, но не множеством. В противном случае множество R можно было бы получить с помощью аксиомы выделения: $R = \{x \in V : x \notin x\}$. (Из аксиомы регулярности, кстати, следует, что $R = V$, но для нас это не столь важно.)

Можно говорить о множествах как элементах некоторого класса (так же как можно говорить о множествах, обладающих некоторым свойством), но не имеет смысла говорить о классах как элементах других классов (общие «совокупности свойств» не рассматриваются как множества или классы).

1.2 Функции и отношения.

Интуитивно, функцией из множества A в множество B мы называем правило, которое сопоставляет каждому элементу A некоторый элемент B. На практике конкретные правила могут быть определены самыми разными способами: формулами, словесными описаниями, программами, и т.д. В теории множеств функция $f : A \to B$ отождествляется с её графиком, то есть с множеством упорядоченных пар $\{\langle x, y\rangle : f(x) = y\}$. Таким образом, для того, чтобы определить общее понятие функции, нам необходимо сначала ввести упорядоченные пары.

Пары и декартовы произведения. Определить упорядоченные пары значит сопоставить каждой паре множеств x, y некоторое множество z, обозначаемое $\langle x, y\rangle$, таким образом, чтобы для всех x_1, x_2, y_1, y_2

$$\langle x_1, y_1\rangle = \langle x_2, y_2\rangle \iff (x_1 = x_2 \text{ и } y_1 = y_2). \tag{2}$$

Это можно сделать разными способами. Один из наиболее простых и элегантных способов (по Куратовскому) состоит в следующем:

$$\langle x, y\rangle := \{\{x, y\}, \{x\}\}.$$

Чтобы проверить основное свойство (2) заметим, что

$$\{x\} = \bigcap\langle x, y\rangle \tag{3}$$
$$\{x, y\} = \bigcup\langle x, y\rangle. \tag{4}$$

В силу (1) имеем $x_1 = x_2$, если и только если $\{x_1\} = \{x_2\}$, поэтому по паре $\langle x, y\rangle$ её первый элемент однозначно восстанавливается. Второй элемент также однозначно восстанавливается, поскольку множество $z := \bigcup\langle x, y\rangle \setminus \bigcap\langle x, y\rangle$ непусто, если и только если $x \neq y$. Отсюда, $\{y\} = z$, если z непусто, иначе $\{y\} = \{x\}$.

Множество всех упорядоченных пар элементов множеств A и B называется *декартовым произведением* A и B:

$$A \times B = \{\langle x, y\rangle : x \in A \text{ и } y \in B\}.$$

Заметим, что если $x \in A$ и $y \in B$, то $\langle x, y\rangle \in \mathcal{P}(\mathcal{P}(A \cup B))$, поэтому $A \times B$ существует в силу аксиомы выделения (множество $\mathcal{P}(\mathcal{P}(A \cup B))$ существует по аксиомам объединения и степени).

Бинарные отношения, отношения эквивалентности. *Бинарным отношением между множествами A и B* называется любое подмножество $R \subset A \times B$. Если $A = B$, то говорят о *бинарном отношении на множестве A*. Вместо $\langle x, y\rangle \in R$ часто пишут xRy.

Примерами отношений являются:

1. отношение равенства $\{\langle x, x\rangle : x \in A\}$;
2. отношение неравенства $\{\langle x, y\rangle : x \neq y,\ x, y \in A\}$;
3. отношение порядка на $\mathbb{R}$: $\{\langle x, y\rangle : x \leq y,\ x, y \in \mathbb{R}\}$;
4. отношение параллельности на множестве всех прямых на плоскости;
5. отношение инцидентности между множеством всех точек и множеством всех прямых на плоскости;
6. отношение делимости на множестве всех натуральных чисел.

Определение 1.2 Бинарное отношение R на множестве A называется

- *рефлексивным*, если $\forall x \in A\ xRx$;
- *симметричным*, если $\forall x, y \in A\ (xRy \to yRx)$;
- *транзитивным*, если $\forall x, y, z \in A\ (xRy \wedge yRz \to xRz)$.

Отношение, обладающее всеми тремя этими свойствами называется *отношением эквивалентности.*

Упражнение 1.3 *Определите, какие из приведённых выше примеров являются отношениями эквивалентности.*

Пусть R — отношение эквивалентности на множестве A и $a \in A$. *Классом эквивалентности* элемента a называется подмножество $a_R := \{x \in A : aRx\}$ множества A. Имеют место следующие простые свойства:

- $a \in a_R$.
- Если aRb, то $a_R = b_R$. (В самом деле, если bRx, то aRx по транзитивности. Если aRx, то bRa по симметричности, откуда bRx по транзитивности.)
- Если неверно, что aRb, то $a_R \cap b_R = \varnothing$. (В противном случае, если $x \in a_R \cap b_R$, то aRx и bRx. Отсюда xRb по симметричности и aRb по транзитивности.)

Определение 1.4 *Разбиением* множества A называется такое семейство S непустых подмножеств A, что

- множества из S попарно не пересекаются;
- $\forall x \in A\, \exists B \in S\, x \in B$.

Таким образом, мы доказали следующую теорему.

Теорема 1.5 *Каждое отношение эквивалентности R на непустом множестве A определяет разбиение A на классы эквивалентности.*

Верно и обратное утверждение: с каждым разбиением множества A можно связать (единственное) отношение эквивалентности, для которого множества данного разбиения являются классами эквивалентности.

В самом деле, если S — данное разбиение, то для любых $x, y \in A$ достаточно положить

$$xRy \overset{\text{def}}{\iff} \exists B \in S\, (x \in B \wedge y \in B).$$

Нетрудно проверить, что такое R в самом деле является отношением эквивалентности на A.

Определение 1.6 Множество всех классов эквивалентности A по отношению R называется *фактормножеством* и обозначается A/R:

$$A/R = \{x_R : x \in A\}.$$

(Почему A/R является множеством?)

Пример 1.7 Если считать известным определение натурального ряда $\mathbb{N}$ (см. ниже), то множество целых чисел $\mathbb{Z}$ удобно рассматривать как фактормножество. Целое число можно представить разностью двух натуральных чисел $m - n$. При этом некоторые пары задают одно и то же число. Поэтому множество целых чисел $\mathbb{Z}$ определяется как

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/{=_{\mathbb{Z}}},$$

где отношение эквивалентности $=_{\mathbb{Z}}$ задаётся следующим образом:

$$\langle m_1, n_1\rangle =_{\mathbb{Z}} \langle m_2, n_2\rangle \overset{\text{def}}{\iff} m_1 + n_2 = n_1 + m_2.$$

Пример 1.8 Рациональное число $q = \frac{m}{n}$ можно рассматривать как пару $\langle m, n\rangle$, где $m \in \mathbb{Z}$ и $n \in \mathbb{N} \setminus \{0\}$. Однако некоторые пары задают одно и то же рациональное число q. Поэтому мы вводим отношение эквивалентности $=_{\mathbb{Q}}$ на $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ по правилу

$$\langle m_1, n_1\rangle =_{\mathbb{Q}} \langle m_2, n_2\rangle \overset{\text{def}}{\iff} m_1 n_2 = n_1 m_2.$$

(Проверьте, что $=_{\mathbb{Q}}$ в самом деле есть отношение эквивалентности.) Две дроби равны тогда и только тогда, когда соответствующие пары эквивалентны. Поэтому рациональные числа можно отождествить с соответствующими классами эквивалентности и официальное определение множества рациональных чисел $\mathbb{Q}$ — это

$$\mathbb{Q} := \mathbb{Z} \times (\mathbb{N} \setminus \{0\})/{=_{\mathbb{Q}}}.$$

Функции. Отношение $R \subset A \times B$ называется

- *тотальным*, если $\forall x \in A\, \exists y \in B\, xRy$;
- *сюръективным*, если $\forall y \in B\, \exists x \in A\, xRy$;
- *функциональным*, если $\forall x \in A\, \forall y_1, y_2 \in B\, (xRy_1 \wedge xRy_2 \to y_1 = y_2)$;
- *инъективным*, если $\forall y \in B\, \forall x_1, x_2 \in A\, (x_1Ry \wedge x_2Ry \to x_1 = x_2)$.

Функцией f из A в B называется тотальное и функциональное бинарное отношение между A и B (обозначение $f : A \to B$). Слово *отображение* есть синоним слова функция. Если f — функция, то мы пишем $f(x) = y$ вместо $\langle x, y\rangle \in f$.

Пример 1.9 Функция $f : \mathbb{R} \to \mathbb{R}$ определяемая как $f(x) = x^2$ отождествляется с множеством пар $\{\langle x, y\rangle \in \mathbb{R}^2 : y = x^2\}$. Это множество обычно называется *графиком* функции f.

Пример 1.10 Для любого множества A имеется *тождественная функция* $\mathrm{id}_A : A \to A$ такая, что $\mathrm{id}_A = \{\langle x, x\rangle : x \in A\}$. Другими словами, $\mathrm{id}_A(x) = x$ для всех $x \in A$.

Замечание 1.11 Данное нами выше определение функции с формальной точки зрения сводит понятие функции к понятию множества. Такое определение отчасти противоречит интуиции, поскольку мы привыкли думать о функциях *интенсионально*, то есть как о предписаниях, определяющих единственный $y \in B$ для каждого $x \in A$. Наше интуитивное представление о функциях также имеет некоторый *динамический* аспект: изменение x на y. Теоретико-множественное определение функции игнорирует все эти аспекты. Оно подчёркивает тот факт, что любое мыслимое соответствие, однозначно связывающее y с x, определяет функцию.

Множество всех функций $f : A \to B$ обозначается B^A.

Пример 1.12 $\{0,1\}^{\mathbb{N}}$ есть множество всех функций $f : \mathbb{N} \to \{0,1\}$.

1.3 Область определения и область значений

Областью определения функции $f : A \to B$ называется множество A (обозначается $\mathrm{dom}(f)$). *Областью значений* функции f называется множество $\{y \in B : \exists x \in A\, f(x) = y\}$, обозначаемое $\mathrm{rng}(f)$.

Если $X \subseteq A$, то множество $\{y \in B : \exists x \in X\, y = f(x)\}$ (*образ* множества X при отображении f) обозначается $f(X)$. (То же множество можно записать и как $\{f(x) : x \in X\}$).

Если $Y \subseteq B$, то множество $\{x \in A : f(x) \in Y\}$ обозначается $f^{-1}(Y)$ и называется *прообразом* множества Y при функции f.

Аналогичные обозначения применяются и для произвольных бинарных отношений R между A и B:

$$\begin{aligned} R(X) &:= \{y \in B : \exists x \in X\, xRy\} \\ R^{-1}(Y) &:= \{x \in A : \exists y \in Y\, xRy\} \\ \mathrm{dom}(R) &:= R^{-1}(B) \\ \mathrm{rng}(R) &:= R(A). \end{aligned}$$

Упражнение 1.13 Убедитесь, что для любой функции $f : A \to B$ и множества $X \subseteq A$ имеет место $X \subseteq f^{-1}(f(X))$. Приведите пример функции f и множества $X \subseteq A$ таких, что $f^{-1}(f(X)) \neq X$.

Упражнение 1.14 То же утверждение верно и для произвольных бинарных отношений между A и B.

1.4 Обозначения и способы задания функций

Определить функцию $f : A \to B$ означает задать множества A, B и соответствие между элементами A и B, то есть подмножество $A \times B$. Обычно применяются следующие способы задания (записи) функций:

- С помощью формул. Например, функция $f : \mathbb{R}^2 \to \mathbb{R}$ может быть задана формулой $f(x, y) = x^2 + y^2$. С формальной точки зрения это означает, что f есть множество пар вида $\langle\langle x, y\rangle, x^2 + y^2\rangle$ для всех $x, y \in \mathbb{R}$.

  Заметим, что в этом случае $\mathrm{rng}(f) = \{x \in \mathbb{R} : x \geq 0\}$, поскольку каждое неотрицательное действительное число есть квадрат; $\mathrm{dom}(f) = \mathbb{R}^2$.

  То же самое соответствие иногда записывают как $\langle x, y\rangle \longmapsto x^2 + y^2$ или даже $x, y \longmapsto x^2 + y^2$ (произносится «x, y переходит в $x^2 + y^2$»).

- С помощью более сложных инструкций, например

$$f(x) = \begin{cases} x^2, & \text{если } x > 0, \\ 0, & \text{если } x \leq 0. \end{cases}$$

  Проверка того, что данная инструкция корректно определяет функцию $f : A \to B$ обычно требует доказательства двух вещей: 1) того, что значение $y \in B$ определено *для каждого* значения $x \in A$; 2) того, что каждому $x \in A$ соответствует *не более одного* значения $y \in B$.

- Конечные функции могут быть заданы таблицами своих значений. Например, функция $f : \{0, 1, 2\} \to \{0, 1\}$ может быть задана следующей таблицей:

$$\begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 0 \end{pmatrix}$$

  Это означает, что $f(0) = 0$, $f(1) = 1$ and $f(2) = 0$.

1.5 Композиция отношений и функций

Пусть $R \subset A \times B$ и $S \subset B \times C$ — бинарные отношения. *Композицией* отношений R и S называется отношение

$$\{\langle x, z\rangle \in A \times C : \exists y \in B\, (xRy \wedge yRz)\}.$$

Композиция бинарных отношений R и S обычно обозначается $R \cdot S$ или RS. *Обратным отношением к* R называется отношение

$$R^{-1} := \{\langle y, x\rangle \in B \times A : xRy\}.$$

Отметим следующие очевидные свойства.

1. $Q(RS) = (QR)S$, если хотя бы одна из частей равенства определена;
2. $R^{-1}R \subset \mathrm{id}_B$, $RR^{-1} \subset \mathrm{id}_A$;
3. $(R^{-1})^{-1} = R$;
4. R тотально, если и только если R^{-1} сюръективно;
5. R функционально, если и только если R^{-1} инъективно;
6. если отношения R и S функциональны, то таково и RS;
7. если отношения R и S тотальны, то таково и RS;
8. $R(X \cup Y) = R(X) \cup R(Y)$;
9. $R(X \cap Y) \subset R(X) \cap R(Y)$.

Упражнение 1.15 Приведите пример, показывающий, что в последнем случае включение может быть строгим.

Функции являются частным случаем бинарных отношений. Легко видеть, что композицией функций $f : A \to B$ и $g : B \to C$ является функция $h : A \to C$ такая, что $h(x) = g(f(x))$ для всех $x \in A$. Для композиции функций принято обозначение $h = g \circ f$, то есть в этих обозначениях

$$(g \circ f)(x) = g(f(x)). \tag{5}$$

Так же, как и для произвольных бинарных отношений, операция композиции функций ассоциативна.

Всегда ли бинарное отношение, обратное к данной функции f, является функцией? Из свойств 4 и 5 мы видим, что отношение f^{-1} тотально и функционально в том и только том случае, когда функция f инъективна и сюръективна. Такие функции называются *взаимно однозначными* или *биекциями*. Таким образом мы получаем следующее утверждение.

Теорема 1.16 *Функция $f : A \to B$ является биекцией тогда и только тогда, когда существует обратная к ней функция f^{-1}.*

2 Натуральные числа и индукция

Понятие натурального числа является в математике столь же, а может быть и более, фундаментальным, чем понятие множества. Существуют аксиоматические системы, в которых неопределяемым понятием является натуральное число, а также некоторые операции над натуральными числами (такие как прибавление единицы, сложение и умножение). В рамках этих аксиоматических систем можно не только развить элементарную арифметику, но и намного более широкую часть математики, которую принято называть «финитарной», математикой конечных объектов. Первые аксиоматические системы арифметики натуральных чисел были предложены Дедекиндом и Пеано и в настоящее время активно изучаются в математической логике.

Однако, понятие множества является более общим, чем понятие натурального числа, и именно оно необходимо для построения развитой аксиоматической системы математического анализа. В аксиоматической теории множеств натуральные числа можно определить (то есть отождествить с определённого вида множествами) и установить для этих объектов основные свойства натуральных чисел, принимаемые в формальной арифметике за аксиомы. Таким образом, в теории множеств нет необходимости вводить новое неопределимое понятие натурального числа или конечного множества. Здесь мы приведём набросок того, как это делается.

Первые пять аксиом теории множеств позволяют определить индивидуальные натуральные числа. По определению, число 0 отождествляется с пустым множеством $\varnothing$, число 1 с $\{\varnothing\}$, число 2 с $\{\varnothing, \{\varnothing\}\}$ и так далее.[2] Однако мы пока не знаем, что такое совокупность *всех* натуральных чисел и, в частности, является ли она множеством. Для этой цели нам

[2] Данная интерпретация натуральных чисел в теории множеств предложена Дж. фон Нейманом.

необходимо привлечь дополнительную аксиому, называемую аксиомой бесконечности (аксиома 6). Только лишь на основе первых пяти аксиом мы не сможем доказать, что существует хотя бы одно бесконечное множество.

Как сформулировать аксиому бесконечности? Вопрос упирается в то, каким образом определить понятие конечного множества, не опираясь на натуральные числа. Чтобы избежать порочного круга мы заменяем понятие «бесконечное» на более сильное свойство множеств, заведомо гарантирующее их бесконечность. Затем мы постулируем существование таких множеств.

Определение 2.1 Множество S называется *индуктивным*, если $\varnothing \in S$ и $\forall x \in S\, x \cup \{x\} \in S$.

Аксиома бесконечности утверждает, что существует хотя бы одно индуктивное множество. Следующая лемма проверяется непосредственно.

Лемма 2.2 *Пересечение непустого множества индуктивных множеств индуктивно.*

Пусть S — некоторое индуктивное множество, существующее по аксиоме 6. Рассмотрим множество $\mathcal{I}$ всех индуктивных подмножеств S. Обозначим через ω его пересечение: $\omega := \bigcap \mathcal{I}$. Из леммы 2.2 получаем, что ω индуктивно. Кроме того, ω содержится в любом индуктивном множестве: если S' индуктивно, то таковым является $S \cap S'$, откуда $S \cap S' \in \mathcal{I}$ и следовательно $\omega \subset S \cap S'$. Таким образом, мы показали, что ω есть наименьшее (по включению) индуктивное множество. Такое множество единственно по аксиоме объёмности.

Определение 2.3 Наименьшее по включению индуктивное множество называется множеством натуральных чисел (обозначение $\mathbb{N}$ или ω).

Отметим, что $0 := \varnothing \in \mathbb{N}$ и из того, что $n \in \mathbb{N}$ следует $n \cup \{n\} \in \mathbb{N}$. Натуральное число $n \cup \{n\}$ назовём *следующим за* n и будем обозначать $n + 1$. Функция $n \mapsto n + 1$ действует из $\mathbb{N}$ в $\mathbb{N}$. Для $n \in \mathbb{N}$ и любого m определим $m < n$, если и только если $m \in n$. (Ниже мы докажем, что из $m \in n \in \mathbb{N}$ следует $m \in \mathbb{N}$.) Из этого определения мы видим, что для всех $m, n \in \mathbb{N}$

$$m < n + 1 \leftrightarrow (m < n \vee m = n).$$

Принцип математической индукции. Из определения множества натуральных чисел как *наименьшего* индуктивного множества мы выводим следующее фундаментальное свойство.

Теорема 2.4 (принцип индукции) *Допустим, что некоторое множество A удовлетворяет условиям: $0 \in A$ и $\forall n \in \mathbb{N}(n \in A \to n+1 \in A)$. Тогда $\forall n \in \mathbb{N}\, n \in A$.*

Доказательство. По условию теоремы множество $A \cap \mathbb{N}$ индуктивно. Поскольку $\mathbb{N}$ — наименьшее индуктивное, мы имеем $\mathbb{N} \subset A$. $\dashv$

Вместо множества A мы можем говорить о произвольном классе или свойстве φ натуральных чисел. Такая более общая форма индукции сводится к принципу индукции для множеств, поскольку $\{n \in \mathbb{N} : \varphi(n)\}$ есть множество по аксиоме выделения (и теореме о том, что $\mathbb{N}$ есть множество).

Следующий вариант принципа индукции носит название *порядковой индукции.*

Теорема 2.5 *Пусть множество A удовлетворяет условию $\forall n \in \mathbb{N}\, (\forall m < n\, m \in A \to n \in A)$. Тогда $\forall n \in \mathbb{N}\, n \in A$.*

Доказательство. Предположим, что A удовлетворяет условию теоремы. Рассмотрим множество

$$A' := \{x \in \mathbb{N} : \forall y < x\, y \in A\}.$$

Тогда $0 \in A$, поскольку $\neg\exists y\, y < 0$, то есть условие $\forall y < 0\, y \in A$ выполняется тривиально. Допустим $n \in \mathbb{N}$ и $n \in A'$, тогда $\forall m < n\, m \in A$. По условию теоремы отсюда следует $n \in A$. Мы утверждаем, что $\forall m < n+1\, m \in A$, то есть $n \in A'$. В самом деле, если $m < n+1$, то $m < n$ или $m = n$. В каждом из этих случаев мы уже знаем, что $m \in A$. По теореме 2.4 мы заключаем $\forall n \in \mathbb{N}\, n \in A'$.

Осталось вывести отсюда $\forall n \in \mathbb{N}\, n \in A$. Рассмотрим любое $n \in \mathbb{N}$, тогда $n+1 \in \mathbb{N}$ и по доказанному $n+1 \in A'$. Поскольку $n < n+1$, по определению A' отсюда следует $n \in A$. $\dashv$

Двойственная форма принципа порядковой индукции называется *принципом наименьшего числа* или *принципом минимального элемента.* Говорим, что $n \in \mathbb{N}$ есть *минимальный элемент* множества $A \subset \mathbb{N}$, если $n \in A$ и $\forall m < n\, m \notin A$.

Теорема 2.6 (принцип минимального элемента) *Всякое непустое подмножество $A \subset \mathbb{N}$ имеет минимальный элемент.*

Доказательство. Допустим противное, то есть $A \neq \varnothing$ и

$$\neg\exists n \in A\, \forall m < n\, m \notin A. \tag{6}$$

Рассмотрим $B := \mathbb{N} \setminus A$. Докажем

$$\forall n \in \mathbb{N}\, (\forall m < n\, m \in B \to n \in B).$$

Допустим $n \in \mathbb{N}$ и $\forall m < n\, m \in B$. Тогда $\forall m < n\, m \notin A$. Значит $n \notin A$ в силу (6), то есть $n \in B$. По теореме 2.5 заключаем, что $\forall n \in \mathbb{N}\, n \in B$. Отсюда следует $A = \varnothing$, противоречие. $\dashv$

Следствие 2.7 $\forall n \in \mathbb{N}\, n \not< n$.

Доказательство. Применим порядковую индукцию. Допустим $\forall m < n m \not< m$. Если $n < n$, то в качестве m можно взять само n, тогда получим $n \not< n$, противоречие. Следовательно, $n \not< n$. $\dashv$

Следствие 2.8 $\forall n \in \mathbb{N}\, \forall x < n\, x \in \mathbb{N}$.

Доказательство. Применим индукцию. $\forall m < 0\, m \in \mathbb{N}$ тривиально. Допустим $n \in \mathbb{N}$ и $\forall x < n\, x \in \mathbb{N}$. Тогда очевидно $\forall x < n+1\, x \in \mathbb{N}$. $\dashv$

Следствие 2.9 $\forall k, m, n \in \mathbb{N}\, (k < m < n \to k < n)$.

Доказательство. Индукция по n. Случай $n = 0$ тривиален. Допустим, что утверждение верно для n и имеет место $k < m < n+1$. Тогда $m < n$ или $m = n$. В первом случае по предположению индукции $k < n$. Во втором случае мы уже знаем, что $k < n = m$. Из $k < n$ следует и $k < n + 1$. $\dashv$

Следствие 2.10 $\forall m, n \in \mathbb{N}\, \neg(n < m \wedge m < n)$.

Доказательство. Если $n < m < n$, то $n < n$, что противоречит следствию 2.7. $\dashv$

Лемма 2.11 *Для любых $m, n \in \mathbb{N}$*

(i) $n + 1 \neq 0$;

(ii) $n = 0 \vee \exists x \in \mathbb{N}\, n = x + 1$;

(iii) $n + 1 = m + 1 \leftrightarrow n = m$.

Доказательство. Утверждение (i) очевидно, так как множество $n + 1$ непусто. Утверждение (ii) легко доказывается индукцией по n.

Докажем (iii). Достаточно доказать импликацию слева направо. Допустим $n \cup \{n\} = m \cup \{m\}$. Так как $m \in n \cup \{n\}$ имеем $m \in n$ или $m = n$. Во втором случае утверждение доказано. Допустим $m \in n$. Так как $n \in m \cup \{m\}$ имеем $n \in m$ или $n = m$. Первый случай невозможен по следствию 2.10. Остаётся второй. $\dashv$

Тем самым, у любого натурального $n \neq 0$ найдётся единственный предшественник m такой, что $n = m + 1$ (такое m обозначаем $n - 1$).

Теория мощностей конечных множеств базируется на еще одном фундаментальном принципе, касающемся натуральных чисел.

Теорема 2.12 (принцип Дирихле) *Не существует инъективного отображения $f : n + 1 \to n$.*

Отметим, что в формулировке теоремы (как и ранее) мы отождествляем натуральное число n с множеством $n = \{0, \ldots, n - 1\}$.

Доказательство. Доказательство проведём (порядковой) индукцией по n. Для $n = 0$ отображение f должно действовать из $\{\varnothing\}$ в $\varnothing$. В этом случае мы должны иметь $f(\varnothing) \in \varnothing$, что невозможно.

Допустим, что $n \neq 0$ и утверждение верно для любого $k < n$, установим его для n. Рассмотрим произвольную инъективную функцию $f : n + 1 \to n$. Обозначим $m := f(n)$, имеем $m < n$. Обозначим через $g : n \to n$ следующую функцию:

$$g(x) = \begin{cases} n - 1, & \text{если } x = m; \\ m, & \text{если } x = n - 1; \\ x, & \text{иначе.} \end{cases}$$

Очевидно, $g : n \to n$ — биекция, поэтому $g \circ f : n + 1 \to n$ — инъекция. Кроме того, $g(f(n)) = g(m) = n - 1$. Обозначим через h ограничение функции $g \circ f$ на n. По построению, h есть инъективная функция из n в $n - 1$. По предположению индукции (для $k = n - 1$), такой функции не существует. Противоречие. $\dashv$

Следствие 2.13 *Если $m < n$, то не существует инъекции $f : n \to m$.*

Доказательство. Индукция по n. Для $n = 0$ утверждение тривиально. Допустим $m < n + 1$, тогда $m < n$ или $m = n$. Во втором случае применяем теорему 2.12. В первом случае рассматриваем ограничение f на n и применяем предположение индукции. $\dashv$

Следствие 2.14 *Множества $n, m \in \mathbb{N}$ равномощны, если и только если $m = n$.*

Рекурсивные (индуктивные) определения. Функции натурального аргумента часто определяются по индукции (рекурсии). Для того, чтобы определить значение функции на аргументе $n+1$ предполагается известным значение функции на предыдущем аргументе n. Простейшая схема рекурсивного определения функции $f : \mathbb{N} \to Y$ сводится к следующей теореме.

Теорема 2.15 *Пусть Y — множество, $y_0 \in Y$ и $h : Y \to Y$ — любая функция. Тогда существует единственная функция $f : \mathbb{N} \to Y$ такая, что для всех $n \in \mathbb{N}$*

$$\begin{cases} f(0) = y_0 \\ f(n+1) = h(f(n)). \end{cases} \tag{7}$$

Доказательство. Пусть даны Y, y_0 и h как в условии теоремы. Рассмотрим множество F всех тех функций $f : m \to Y$, где $m \in \mathbb{N}$, для которых выполнены условия (7) для любого $n \in m$. Это множество непусто, поскольку содержит пустую функцию, а также функцию, состоящую из пары $\langle 0, y_0 \rangle$.

Утверждается, что любые две функции $f, g \in F$ совпадают на пересечении своих областей определения. В противном случае рассмотрим минимальный $k \in \mathbb{N}$ такой, что $f(k) \neq g(k)$. Мы имеем $k \neq 0$, поскольку $f(0) = y_0 = g(0)$. Следовательно $k = s + 1$, причем $f(s) = g(s)$, поскольку k — минимальный. Отсюда $f(k) = f(s+1) = h(f(s)) = h(g(s)) = g(s+1) = g(k)$, противоречие.

Каждая $g : m \to Y$ есть подмножество $m \times Y \subset \mathbb{N} \times Y$. Рассмотрим множество $\bigcup F \subset \mathbb{N} \times Y$. Утверждается, что $f := \bigcup F$ есть функция $\mathbb{N} \to Y$. Отношение $\bigcup F$ функционально, поскольку любые два элемента F совпадают на общей области определения. Докажем тотальность, рассуждая от противного. Рассмотрим минимальное m такое, что $m \notin \mathrm{dom}(f)$. Тогда $f : m \to Y$ и можно продолжить f до функции $f' : m + 1 \to Y$, определив $f'(m) := h(f(m))$. Очевидно, $f' \in F$, поэтому

$m \in \mathrm{dom}(\bigcup F)$, противоречие. Свойства (7) очевидно выполняются для f, тем самым существование f доказано.

Единственность f, как в рассуждении выше, легко следует по принципу наименьшего числа. $\dashv$

Применяя эту теорему мы доказываем, например, существование и единственность функции $f(x) = 2^x$ (предполагая известным определение сложения). Действительно, f рекурсивно определяется равенствами $f(0) = 1$ и $f(n+1) = f(n) + f(n)$.

Заметим, что на натуральных числах уже определена функция последователя $s(n) = n + 1$. Сложение и умножение можно определить рекурсией по второму аргументу. Сложение удовлетворяет равенствам

$$\begin{cases} m + 0 = m \\ m + (n+1) = (m+n) + 1 \end{cases} \tag{8}$$

Чтобы уложить эту схему в рамки теоремы 2.15 заметим, что функции $f : \mathbb{N} \times X \to Y$ можно отождествить с функциями $\mathbb{N} \to Y^X$, то есть с последовательностями функций $f_n : X \to Y$. Таким образом, с помощью теоремы 2.15 надо построить последовательность функций $f_n : \mathbb{N} \to \mathbb{N}$ такую, что

$$\begin{cases} f_0 = id_{\mathbb{N}} \\ f_{n+1} = s \circ f_n. \end{cases}$$

Тогда $f_0(m) = m$ и $f_{n+1}(m) = (s \circ f_n)(m) = s(f_n(m)) = f_n(m) + 1$. То есть, если положить $m + n := f_n(m)$, то выполняются равенства (8).

Аналогично определяется умножение, как единственная функция $\mathbb{N}^2 \to \mathbb{N}$ для которой

$$\begin{cases} m \cdot 0 = m \\ m \cdot (n+1) = (m \cdot n) + m. \end{cases} \tag{9}$$

3 Вполне упорядоченные множества и аксиома выбора

3.1 Упорядоченные множества

Строгим частичным порядком на множестве X называем бинарное отношение $<$ на X, удовлетворяющее свойствам:

- $x < y$ и $y < z \Rightarrow x < z$ (транзитивность);

- $x \not< x$ (иррефлексивность).

Пару $(X, <)$ называем *частично упорядоченным множеством*.

Элементы $x, y \in X$ называются *сравнимыми*, если $x < y$, или $x = y$, или $y < x$. Частично упорядоченное множество $(X, <)$ называется *линейно упорядоченным*, или просто *упорядоченным*, если любые $x, y \in X$ сравнимы.

Примеры частично упорядоченных множеств:

- $(\mathbb{R}, <)$, $(\mathbb{Q}, <)$, $(\mathbb{N}, <)$,
- $\mathbb{N}$ с отношением *x есть собственный делитель y*;
- $(\mathcal{P}(X), \subsetneq)$;
- $\mathbb{N}^*$ с отношением *последовательность x есть собственное начало последовательности y*.

Первые три примера — линейно упорядоченные множества, а последние три — нет.

Упражнение 3.1 (i) Если $<$ — строгий частичный порядок на X, то отношение

$$x \leq y \iff (x < y \text{ или } x = y)$$

является транзитивным, рефлексивным и *антисимметричным*, то есть

$$x \leq y \text{ и } y \leq x \Rightarrow x = y.$$

Такое отношение называют *(нестрогим) частичным порядком*.

(ii) Если $\leq$ — рефлексивное, транзитивное, антисимметричное отношение на X, то отношение

$$x < y \iff (x \leq y \text{ и } x \neq y)$$

есть строгий частичный порядок.

3.2 Терминология

Пусть $(X, <)$ — частично упорядоченное множество и $Y \subset X$.

- Элемент $y \in Y$ *максимальный в Y*, если $\forall x \in Y\ y \not< x$.
- Элемент $y \in Y$ *наибольший в Y*, если $\forall x \in Y\ x \leq y$.

- Элемент $x \in X$ есть *верхняя грань* Y, если $\forall y \in Y\ y \leq x$.

Определения минимального и наименьшего элементов и нижней грани Y аналогичны.

Всякое подмножество $Y \subset X$ частично упорядоченного множества $(X, <)$ можно также рассматривать как частично упорядоченное множество по отношению $<'$ на Y:

$$x <' y \iff (x, y \in Y \text{ и } x < y).$$

(Формально, можно было бы определить $<'$ как $< \cap Y^2$.) В этом случае говорят, что порядок $<'$ является *ограничением* порядка $<$ на множество Y или *индуцирован* на Y с X.

Множество $Y \subset X$ называется *цепью*, если любые два элемента Y сравнимы. Другими словами, Y — цепь, если Y линейно упорядочено в смысле индуцированного отношения порядка. Множество $Y \subset X$ называется *антицепью*, если любые два элемента Y *несравнимы*.

3.3 Сохраняющие порядок отображения

Пусть $(X, <_X)$ и $(Y, <_Y)$ — линейно упорядоченные множества. Отображение $f : X \to Y$ называется *сохраняющим порядок* (или *возрастающим*), если

$$\forall x_1, x_2 \in X\ (x_1 <_X x_2 \Rightarrow f(x_1) <_Y f(x_2)).$$

Изоморфизмом упорядоченных множеств X и Y называется биекция $f : X \to Y$, для которой f и обратное отображение f^{-1} сохраняют порядок. $X \cong Y$ означает, что упорядоченные множества X и Y изоморфны, то есть между ними существует изоморфизм.

Пример 3.2 Множество натуральных чисел (с обычным отношением порядка) изоморфно упорядоченному множеству чётных чисел. Функция $f : n \mapsto 2n$ осуществляет этот изоморфизм.

Упражнение 3.3 Пусть $f : X \to Y$ сохраняет порядок. Тогда f — инъективно и

$$\forall x_1, x_2 \in X\ (x_1 <_X x_2 \iff f(x_1) <_Y f(x_2)).$$

Отметим, что в этом упражнении существенна линейность рассматриваемых упорядоченных множеств.

Следствие 3.4 *Для линейно упорядоченных множеств сохраняющая порядок сюръекция $f : X \to Y$ является изоморфизмом.*

3.4 Операции над линейно упорядоченными множествами

Всякое натуральное число n можно рассматривать как упорядоченное множество из n элементов.

Пример 3.5 Покажите, что любые два линейно упорядоченных множества конечной мощности n изоморфны.

Для произвольных упорядоченных множеств можно определить операции суммы и произведения, обобщающие эти операции на множестве натуральных чисел.

Пусть $(X, <_X)$ и $(Y, <_Y)$ — не пересекающиеся линейно упорядоченные множества. (Заменяя одно из множеств на его изоморфную копию можно всегда считать X и Y не пересекающимися.)

Суммой $X + Y$ назовём упорядоченное множество $(Z, <_Z)$, где $Z = X \sqcup Y$ и для любых $z_1, z_2 \in Z$ соотношение $z_1 <_Z z_2$ имеет место в одном из трех случаев:

- $z_1, z_2 \in X$ и $z_1 <_X z_2$,
- $z_1, z_2 \in Y$ и $z_1 <_Y z_2$,
- $z_1 \in X$ и $z_2 \in Y$.

Произведением $X \cdot Y$ назовём множество $(Z, <_Z)$, где $Z = Y \times X$ и для любых $z_1 = (y_1, x_1) \in Z$ и $z_2 = (y_2, x_2) \in Z$ соотношение $z_1 <_Z z_2$ имеет место, если и только если $y_1 <_Y y_2$ или же $y_1 = y_2$ и $x_1 < x_2$. (Сравнение сначала элементов множества Y, а потом уже X, выражает ту идею, что $X \cdot Y$ состоит из копий множества X, упорядоченных между собой как Y, а не наоборот.)

Упражнение 3.6 Нарисуйте множества $\omega + \omega$, $\omega \cdot 2$, $\omega \cdot \omega$, где ω — упорядоченное множество $(\mathbb{N}, <)$.

3.5 Вполне упорядоченные множества

Определение 3.7 Упорядоченное множество $(X, <)$ называем *вполне упорядоченным*, если любое непустое подмножество $Y \subset X$ имеет наименьший элемент $y \in Y$. Наименьший элемент Y — единственный и обозначается $\min(Y)$.

Пример 3.8 Множества ω, $\omega + \omega$, и $\omega \cdot \omega$ — вполне упорядочены. Объясните, почему. (В первом случае возможное объяснение состоит в том, что для натурального ряда это — аксиома.)

Отметим следующие простые свойства вполне упорядоченных множеств $(X, <)$.

1. $(X, <)$ имеет наименьший элемент (но может не иметь наибольшего).

2. Всякий элемент $x \in X$ (отличный от наибольшего) имеет непосредственного последователя, то есть $\exists y \in X \, \forall z \in X \, (x < z \Rightarrow y \leq z)$.

3. Всякое ограниченное сверху подмножество множества X имеет наименьшую верхнюю грань.

Определение 3.9 *Начальным отрезком множества* $(X, <)$ называем такое подмножество $Y \subset X$, для которого

$$\forall x, y \, (x \in Y, y < x \Rightarrow y \in Y).$$

В частности, начальными отрезками X считаем само X и пустое множество.

Упражнение 3.10 (i) Докажите, что любой собственный начальный отрезок $(X, <)$ имеет вид $\bar{a} = \{x \in X \mid x < a\}$ для некоторого $a \in X$.

(ii) Выведите отсюда, что множество всех начальных отрезков $(X, <)$ является вполне упорядоченным по включению.

Решение: (i) Пусть Y — собственный начальный отрезок X, и пусть $a = \min(X \setminus Y)$. Заметим, что $a \notin Y$ и $\forall x < a \, x \in Y$. Второе влечёт $\bar{a} \subset Y$. С другой стороны, если $\exists y \in Y \; a \leq y$, то мы имеем $a \in Y$, поскольку Y — начальный отрезок. Этого не может быть, значит $Y \subset \bar{a}$.

Лемма 3.11 *Пусть* $(X, <)$ *вполне упорядочено и* $f : X \to X$ *сохраняет порядок. Тогда* $\forall x \in X \; f(x) \geq x$.

Доказательство. В противном случае рассмотрим $a = \min Y$, где $Y = \{x \in X \mid f(x) < x\}$. Поскольку $a \in Y$ мы имеем $f(a) < a$. Отсюда следует $f(f(a)) < f(a)$ по монотонности f. Но тогда $f(x) < x$ для некоторого $x < a$ (возьмём $x = f(a)$), что противоречит минимальности a. $\dashv$

Теорема 3.12 (i) *Вполне упорядоченное множество не изоморфно никакому своему собственному начальному отрезку.*

(ii) *Для любых двух вполне упорядоченных множеств одно изоморфно начальному отрезку другого.*

Доказательство. (i) Пусть $Y \subset X$ — собственный начальный отрезок X, и $f : X \to Y$ — изоморфизм. Тогда по лемме 3.11 имеем $f(x) \geq x$ для всех $x \in X$. Но если $a \in X \setminus Y$, то $f(a) \in Y$ и тем самым $f(a) < a$, поскольку Y — начальный отрезок X. Противоречие.

(ii) Рассмотрим бинарное отношение $R \subset X \times Y$ такое, что

$$xRy \iff \bar{x} \cong \bar{y}.$$

Сначала докажем, что от отношения R, R^{-1} функциональны и сохраняют порядок.

Действительно, если xRy_1 и xRy_2, то $\bar{x} \cong \bar{y}_1$ и $\bar{x} \cong \bar{y}_2$, значит $\bar{y}_1 \cong \bar{y}_2$. Поскольку Y линейно упорядочено, мы имеем $y_1 < y_2$ или $y_2 < y_1$ или $y_1 = y_2$. Если $y_1 < y_2$, то $\bar{y}_1$ — собственный начальный отрезок $\bar{y}_2$, что противоречит (i). Аналогично, не может быть $y_2 < y_1$, поэтому $y_1 = y_2$.

Докажем, что R сохраняет порядок. Допустим, что $x_1 < x_2$, $\bar{x}_1 \cong \bar{y}_1$ и $\bar{x}_2 \cong \bar{y}_2$. Изоморфизм $f : \bar{x}_2 \to \bar{y}_2$ переводит $\bar{x}_1$ в некоторый собственный начальный отрезок $f(\bar{x}_1) \subset \bar{y}_2$. Если при этом $y_2 \leq y_1$, то получаем, что $\bar{y}_1$ изоморфно собственному начальному отрезку $f(\bar{x}_1) \cong \bar{x}_1$, что невозможно. Значит, $y_1 < y_2$.

Аналогично устанавливаем, что x_1Ry и x_2Ry влечёт $x_1 = x_2$, и что R^{-1} сохраняет порядок.

Осталось доказать, что хотя бы одна из функций R и R^{-1} определена на всём множестве X или на всём множестве Y, соответственно. Предположим противное и рассмотрим наименьший $a \in X$ такой, что $\nexists y \in Y\ aRy$ и наименьший $b \in Y$ такой, что $\nexists x \in X\ xRb$. Тогда R есть изоморфизм начального отрезка $\bar{a} \subset X$ на начальный отрезок $\bar{b} \subset Y$, поскольку на $\bar{a}$ функция R всюду определена, сохраняет порядок, и то же верно для обратной функции R^{-1}. Но тогда по определению R мы имеем aRb. Противоречие с минимальностью a и b. $\dashv$

3.6 Аксиома выбора

Пусть S — семейство непустых множеств. *Функцией выбора на* S называем функцию, сопоставляющую каждому множеству из S некоторый его элемент, то есть функцию $f : S \to \bigcup S$ такую, что $\forall x \in S\ f(x) \in x$.

Аксиома выбора. Для всякого S такого, что $\varnothing \notin S$, существует функция выбора на S.

Специфика этой аксиомы состоит в том, что функция f, существование которой постулируется, ни в каком смысле явно не определяется. Это открывает широкую дверь для так называемых «чистых теорем существования» в математике, доказывающих существование объектов без их явного описания или построения.

Аксиома выбора имеет несколько эквивалентных форм, которые удобны в математических рассуждениях.

Теорема Цермело. Всякое множество можно вполне упорядочить. (Более строго: для всякого множества X существует бинарное отношение $<$ на X такое, что $(X, <)$ — вполне упорядоченное множество.)

Лемма Цорна. Пусть $(X, <)$ — частично упорядоченное множество, в котором любая цепь $C \subset X$ имеет верхнюю грань. Тогда в $(X, <)$ найдётся максимальный элемент.

Мы докажем эквивалентность каждого из этих утверждений аксиоме выбора. Как важное следствие теоремы Цермело отметим такой факт.

Теорема 3.13 *Любые два множества сравнимы по мощности, то есть для любых множеств A, B найдётся инъекция из A в B или из B в A.*

Действительно, вполне упорядочим множества A и B. Тогда одно из них вложимо в другое как начальный отрезок.

Доказательство леммы Цорна. Допустим, что $(X, <)$ удовлетворяет условию леммы Цорна, но не имеет максимального элемента. Назовем *строгой верхней гранью цепи* $C \subset X$ такой элемент $x \in X$, что $c < x$ для всех $c \in C$. Тогда можно утверждать, что для всякой цепи C в X множество её строгих верхних граней $\psi(C)$ непусто. (Рассмотрим любую верхнюю грань x цепи C. Поскольку элемент x не максимален, найдётся $y > x$, он и будет строгой верхней гранью C.)

Рассмотрим теперь множество

$$S = \{\psi(C) \mid C \text{ — цепь в } X\}.$$

Заметим, что S будет множеством, поскольку $S \subset \mathcal{P}(X)$. Применяя аксиому выбора к множеству S мы можем заключить, что существует функция φ, сопоставляющая любой цепи C некоторую её строгую верхнюю

грань $\varphi(C)$. (Эта функция является композицией функции ψ и функции выбора для S.)

Теперь мы построим цепь, которая будет настолько велика, что должна выйти за пределы X (это и будет желаемым противоречием). Идея состоит в неограниченном удлиннении цепи путём применения функции φ.

Множество $S \subset X$ называем *корректным*, если выполняются условия:

1. $(S, <)$ вполне упорядочено (порядок индуцирован с X);
2. $\forall x \in S \;\; x = \varphi(S_x)$, где S_x означает $\{y \in S \mid y < x\}$.

Заметим, что корректными множествами являются

$$\varnothing; \;\; \{\varphi(\varnothing)\}; \;\; \{\varphi(\varnothing), \varphi(\{\varphi(\varnothing)\})\} \text{ и т.д.}$$

Докажем следующее вспомогательное утверждение.

Лемма 3.14 (i) *Если множества S и T корректны, то одно из них есть начальный отрезок другого.*

(ii) *Объединение любого семейства корректных множеств корректно.*

Доказательство. (i) Допустим, что ни одно из множеств S и T не является начальным отрезком другого. *Общим началом S и T* назовём такое подмножество $J \subset S \cap T$, которое есть начальный отрезок как S, так и T. Заметим, что объединение I множества всех общих начал S и T само есть их общее начало. (В самом деле, если $x \in I$, то для некоторого общего начала J имеем $x \in J$, а тогда $\forall y \in S \, (y < x \Rightarrow y \in J \subset I)$ и аналогично для T.)

Если I совпадает с одним из множеств S или T, то (i) доказано. В противном случае рассмотрим $s = \min_S(S \setminus I)$ и $t = \min_T(T \setminus I)$, где min берётся по множествам S и T, соответственно. Тогда $S_s = I = T_t$. В силу корректности S и T получаем $s = \varphi(S_s) = \varphi(T_t) = t$, то есть $I \cup \{s\}$ есть общее начало T и S, расширяющее I, что не возможно.

(ii) Пусть Σ — семейство корректных множеств и $U = \bigcup \Sigma$.

Множество $(U, <)$ линейно упорядочено по утверждению (i). (В самом деле, если $x, y \in U$, то для некоторых корректных множеств $S, T \in \Sigma$ имеем $x \in S$ и $y \in T$. Возьмём из них большее и воспользуемся его линейной упорядоченностью.)

Каждое $S \in \Sigma$ есть начальный отрезок U. Иначе найдётся $x \in S$ и $y < x$ такой, что $y \in U \setminus S$. Тогда для некоторого корректного $T \in \Sigma$ имеем $y \in T \setminus S$, значит T не является начальным отрезком S. По свойству (i) множество S должно быть начальным отрезком T, что противоречит тому, что $y < x \in S$ и $y \notin S$.

Докажем, что $(U, <)$ вполне упорядочено. Пусть $Y \subset U$ непусто. Рассмотрим любой $y \in Y$ и корректное множество $S \in \Sigma$ такое, что $y \in S$. Поскольку $Y \cap S$ непусто и вполне упорядочено (как подмножество S), существует $x = \min_S(Y \cap S) \in S$. Поскольку S есть начальный отрезок U, x также будет наименьшим элементом Y в U.

Осталось проверить, что $x = \varphi(U_x)$ для любого $x \in U$. Выберем $S \in \Sigma$ такое, что $x \in S$. Заметим, что $U_x = S_x$, поскольку S есть начальный отрезок U. Следовательно, $x = \varphi(S_x) = \varphi(U_x)$. $\dashv$

Рассмотрим теперь множество Σ *всех* корректных подмножеств X и положим $U = \bigcup \Sigma$. Поскольку U вполне упорядочено и, в частности, является цепью, оно имеет строгую верхнюю грань $\varphi(U)$. Тогда $U \cup \{\varphi(U)\}$ есть собственное расширение U и является корректным множеством, что невозможно по определению Σ. Лемма Цорна доказана.

Заметим, что полученное противоречие сильно напоминает парадокс Кантора (а точнее, так называемый парадокс Бурали–Форти).

Вывод теоремы Цермело из леммы Цорна. Вполне упорядоченное множество $(S, <_S)$ назовём *вполне упорядоченным подмножеством* X, если $S \subset X$. Для данного множества X рассмотрим совокупность $W(X)$ всех его вполне упорядоченных подмножеств. На $W(X)$ определим отношение строгого частичного порядка $\prec$ следующим образом:

> $(S, <_S) \prec (T, <_T)$, *если и только если* $S \subset T$ *есть собственный начальный отрезок* $(T, <_T)$, *и* $<_S$ *совпадает с ограничением* $<_T$ *на* S.

Докажем, что $(W(X), \prec)$ удовлетворяет условию леммы Цорна. Рассмотрим любую цепь $C \subset W(X)$. Цепи C соответствует возрастающая по включению цепь подмножеств X и возрастающая по включению цепь бинарных отношений на этих множествах. Обозначим через U объединение этой цепи подмножеств X, а через $<_U$ — объединение соответствующей цепи отношений. Ясно, что $<_U$ есть отношение линейного порядка на U и каждое $(S, <_S) \in C$ есть начальный отрезок $(U, <_U)$. Отсюда получаем, что $(U, <_U)$ — вполне упорядоченное подмножество X. Таким образом, $(U, <_U)$ есть элемент $W(X)$ и верхняя грань цепи C.

Применяя лемму Цорна получаем, что в $(W(X), \prec)$ найдётся некоторый максимальный элемент $(M, <_M)$. Тогда M обязано совпадать со всем X: в противном случае мы можем взять $a \in X \setminus M$ и продолжить порядок $<_M$ на большее множество $N = M \cup \{a\}$ полагая $x <_N a$ для всех $x \in M$. (Формально, $<_N$ будет объединением $<_M$ и $\{\langle x, a\rangle \mid x \in M\}$.) Тогда $(N, <_N)$ будет вполне упорядоченным подмножеством X и $(M, <_M) \prec (N, <_N)$, что противоречит максимальности $(M, <_M)$.

Вывод аксиомы выбора из теоремы Цермело. Пусть S — данное семейство непустых множеств. По теореме Цермело множество $U = \bigcup S$ может быть вполне упорядочено. Для каждого $x \in S$ имеем $x \subset U$. Пусть $\min(x)$ означает наименьший элемент x в смысле порядка на U. Поскольку $\varnothing \notin S$, соответствие $x \mapsto \min(x)$ является функцией выбора на S.