Логика и Алгоритмы

Факультет математики ВШЭ, 1-й курс, осень 2013 г.

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 $\{1, 1, 2\} = \{1, 2\}$.

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

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

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

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 $\{a, a\}$.

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. Так же и число 5 есть элемент множества натуральных чисел $\mathbb{N}$, однако не является подмножеством $\mathbb{N}$. (Однако, подмножеством $\mathbb{N}$ является одноэлементное множество $\{5\}$.)

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 *формальноˊго 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.

Парадокс Рассела и «множество» всех множеств. 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.)

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

$$\langle x_1, y_1\rangle = \langle x_2, y_2\rangle \iff (x_1 = x_2 \text{ и } y_1 = y_2). \tag{1}$$

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 (1) заметим, что

$$\{x\} = \bigcap\langle x, y\rangle \tag{2}$$

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

Мы имеем $x = y$, если и только если $\{x\} = \{y\}$ (в силу определения $\{x\}$). Поэтому по паре $\langle x, y\rangle$ её первый и второй элементы однозначно восстанавливаются.

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 1.1. 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 1.2. *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 1.3. *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 1.4. *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 1.5. 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 1.6. 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

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

Пример 1.7. Если считать известным определение натурального ряда $\mathbb{N}$ (см. ниже), то множество целых чисел $\mathbb{Z}$ также 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:

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

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 $\langle x, y \rangle \in f$.

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

[Нужно дополнить, см. записи Functions and Relations.]

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 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 любого множества индуктивных множеств индуктивно.*

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

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 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 $\mathbb{N} \subset A$. $\boxtimes$

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 $n \in A$. ⊠

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

$$\neg\exists n \in A \, \forall m < n \, m \notin A. \tag{4}$$

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 (4), то есть $n \in B$. По теореме 2.5 заключаем, что $\forall n \in \mathbb{N} \, n \in B$. Отсюда следует $A = \varnothing$, противоречие. ⊠

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, $n \not< n$. ⊠

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 $\forall x < n+1\ x \in \mathbb{N}$. $\boxtimes$

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 $k < n + 1$. $\boxtimes$

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. $\boxtimes$

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. $\boxtimes$

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. ⊠

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. ⊠

Следствие 2.14. *Любые элементы $n, m \in \mathbb{N}$ попарно неравномощны.*

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 $n \in \mathbb{N}$*

$$\begin{cases} f(0) = y_0 \\ f(n+1) = h(f(n)). \end{cases} \tag{5}$$

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 (5) 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 (5) очевидно выполняются для f, тем самым существование f доказано.

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

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

$$\begin{cases} m + 0 = m \\ m + (n+1) = (m+n) + 1 \end{cases} \tag{6}$$

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 (6).

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

$$\begin{cases} m \cdot 0 = m \\ m \cdot (n+1) = (m \cdot n) + m. \end{cases} \tag{7}$$