Введение в математическую логику и теорию алгоритмов

Лекция 11. Теория множеств Цермело – Френкеля

1. Предварительные замечания

Мы приступаем к знакомству с системой аксиом (теорией) **ZF**. Эта теория претендует на то, что любое математическое утверждение естественно записывается в виде замкнутой формулы в сигнатуре **ZF**, а доказательство утверждения может быть записано как (синтаксический) вывод в данной теории. Теория **ZF** называется *теорией множеств Цермело — Френкеля.* Имеются разные системы аксиом теории множеств, **ZF**, по-видимому, наиболее распространённая.

Теория **ZF** предназначена для того, чтобы на формальном языке описать понятие «множества». Поэтому естественно называть элементы моделей данной теории множествами. Это приводит к некоторой двусмысленности, поскольку термин «множество» используется нами и в неформальном смысле: «множество четных чисел» и пр. Аналогичная проблема возникала, например, и в случае моделей арифметики: мы называли натуральными числами и элементы моделей и «обычные» натуральные числа. В данной лекции, чтобы избежать двусмысленности, мы используем термины множество, подмножество, функция и пр. только в формальном смысле — в смысле элементов рассматриваемой модели **ZF**. Для содержательных неформальных понятий мы будем использовать термины класс, набор, совокупность, подкласс, отображение и пр. Например, обычный натуральный ряд мы будем называть «совокупностью натуральных чисел».

Теория **ZF** является теорией с равенством. Кроме знака $=$ сигнатура теории содержит ещё только имя $\in$ двуместного отношения, следуя традиции мы будем использовать запись $a \in b$, а не $\in (a, b)$.[1]

<u>Неформальное замечание</u>: структура, которую мы пытаемся описать с помощью **ZF**, — это класс всех «чистых» множеств, то есть множеств, элементами которых являются только множества. Так, у нас будет пустое множество; будет множество, единственным элементом которого является пустое множество; будет множество из двух элементов: один элемент — пустое множество, второй — одноэлементное множество, содержащее пустое множество, и т. д. Кажется, для целей математики достаточно таких множеств.

[1]Для достижения поставленной выше цели избежать двусмысленности, мы будем стараться не использовать знак $\in$ для классов, наборов, совокупностей, то есть не для *множеств.*

Но фигурные скобки мы будем использовать как для обозначения наборов, так и для обозначения множеств. Говоря «набор $\{a, b\}$», будем подразумевать набор, состоящий из двух (если $a \neq b$) элементов модели **ZF**: a и b. Говоря «множество $\{a, b\}$», будем подразумевать один конкретный элемент c модели **ZF**, такой, что $a \in c$, $b \in c$, и ни для какого другого элемента x модели отношение $x \in c$ не является истинным. Если встретится обозначение «$\{a, b\}$» без уточняющего слова «набор» или «множество», значит, будет предполагаться, что такое уточнение очевидно.

См. также ниже пояснение к парадоксу Рассела и примечание к аксиоме подмножеств.

2. Аксиомы ZF

1) ***Аксиома объёмности:***

$$\forall u\, \forall v\, (\forall w\, (w \in u \equiv w \in v) \to u = v).$$

Аксиома объёмности утверждает, что если два множества u и v имеют одни и те же элементы, то эти множества равны.

Хочется для каждой формулы $\Phi(x)$ добавить аксиому $\exists u\, (\forall v\, (v \in u \equiv \Phi(v)))$, но теория станет противоречивой (рассмотрите формулу $\Phi(x) = x \notin x$) — парадокс Рассела.

Мы скажем, что набор элементов $\{x \mid x \notin x\}$ «не является множеством», имея в виду, что, хотя элементы с таким свойством могут существовать в описываемой структуре, однако в ней нет такого элемента a, что $\{x \mid x \in a\} = \{x \mid x \notin x\}$.

Далее перечислим четыре вида аксиом существования множеств (2 – 5).

2) ***Аксиомы подмножеств:***

$$\forall \overline{t}\ \forall u\, \exists s\, \forall v\, (v \in s\ \equiv\ (v \in u \wedge \Phi(\overline{t}, v))) \qquad \text{для всех формул} \quad \Phi(\overline{x}, y).$$

Здесь и далее $\overline{x}$ обозначает список переменных.

Пусть $\Phi(\overline{x}, y)$ — произвольная формула, имеющая $k+1$ свободных переменных, из которых k переменных мы выделили в список $\overline{x}$. Аксиома подмножеств для формулы $\Phi(\overline{x}, y)$ гарантирует, что для любых элементов $b_0, \ldots, b_{k-1}, a$ нашей структуры набор $\{y \mid y \in a \wedge \Phi(\overline{b}, y)\}$ является множеством[2].

3) ***Аксиомы замены:***

$$\forall \overline{t}\ \Big(\forall u\, \exists v\, \forall w\, \big(w \in v \equiv \Phi(\overline{t}, u, w)\big) \to$$
$$\to \forall v\, \exists s\, \forall w\, \big(\exists u\, (u \in v \wedge \Phi(\overline{t}, u, w)) \equiv w \in s\big)\Big) \ \text{для всех формул}\ \Phi(\overline{x}, y, z).$$

Пусть список $\overline{x}$ состоит из k элементов и пусть $b_0, \ldots, b_{k-1}$ — некоторые элементы нашей структуры, тогда «формуле» $\Phi(\overline{b}, y, z)$ соответствует некоторое отображение: каждому элементу a соответствует набор $\{z \mid \Phi(\overline{b}, a, z)\}$. Предположим, что каждый такой набор является множеством. Даже в этом случае объединение семейства таких наборов может не быть множеством. Но если мы выбираем a из некоторого множества c, то аксиома замены гарантирует, что объединение таких наборов, то есть набор $\{z \mid \exists u\, (u \in c \wedge \Phi(\overline{b}, u, z))\}$, является множеством.

4) ***Аксиома степени:***

$$\forall u\, \exists s\, \forall v\, (\forall w\, (w \in v \to w \in u)\ \equiv\ v \in s).$$

Мы будем использовать выражение $x \subset y$ как сокращение для формулы $\forall u(u \in x \to u \in y)$. Используя это сокращение, можно сказать, что аксиома степени гарантирует, что для любого элемента a набор $\{x \mid x \subset a\}$ является множеством.

[2] Выше мы уже отметили, что *множествами* называем только элементы модели теории **ZF**. Никакой *набор* элементов модели сам не является элементом модели. Поэтому никакой набор элементов модели, строго говоря, не является множеством. Когда же мы, всё-таки, допуская вольность речи, говорим, что некоторый набор M элементов модели является множеством, то имеем в виду, что в модели есть такой элемент a, что набор элементов модели $\{x \mid x \in a\}$ — это в точности набор M.

Другими словами, аксиома степени гарантирует, что для любого множества существует множество всех его подмножеств.

5) *Аксиома бесконечности*:

$$\exists s \left(\exists u \left(u \in s \ \wedge \ \forall v \, (v \notin u) \right) \wedge \right.$$
$$\left. \wedge \, \forall u \left(u \in s \to \exists v \left(v \in s \wedge \forall w \, \left(w \in v \equiv (w \in u \vee w = u) \right) \right) \right) \right).$$

Словесная формулировка аксиомы бесконечности: существует такое множество s, что оно содержит пустое множество и вместе с каждым элементом u содержит элемент $v = u \cup \{u\}$ (каждый элемент v либо совпадает с u, либо является элементом u).

Заметим, что аксиома бесконечности безусловно гарантирует существование множества с некоторыми специальными свойствами. Это отличает её от аксиом подмножеств, замены и степени, которые позволяли строить множества лишь исходя из существования некоторых других множеств.

Дальнейшее обсуждение аксиомы бесконечности мы отложим до того момента, когда будем исследовать множество ω.

6) *Аксиома регулярности (фундирования)*:

$$\forall u \left(\exists v \, (v \in u) \to \exists v \left(v \in u \wedge \neg \exists w \, (w \in v \wedge w \in u) \right) \right).$$

Эта аксиома утверждает, что в любом непустом множестве a есть такой элемент b, что пересечение наборов $\{x \mid x \in a\}$ и $\{x \mid x \in b\}$ пусто. Такой элемент b можно называть *минимальным элементом* множества a (множество a не содержит элементов, «меньших», чем b, если «меньше» понимать в смысле отношения $\in$).

Следующие два утверждения выводятся из предыдущих аксиом, но, чтобы не загромождать изложение их выводом, мы включим их в теорию.

7) *Аксиома пустого множества*:

$$\exists s \, \forall u \, (u \notin s).$$

8) *Аксиома пары*:

$$\forall u \, \forall v \, \exists s \, \forall w \, (w \in s \equiv (w = u \ \vee \ w = v)),$$

то есть $\{x \mid x = a \ \vee \ x = b\}$ является множеством для любых элементов a и b.

3. О содержательной теории множеств и о формальной теории множеств

Аналогично арифметике (теории чисел) и арифметике Пеано, теория множеств понимается и как содержательная теория (утверждения о некоторой структуре «настоящих» множеств), и как анализ формальной теории **ZF** (непротиворечивость, полнота, исследование всевозможных моделей и пр.). Мы, в основном, будем заниматься формальной теорией множеств.

Мы предположим, что у теории **ZF** есть модель, и постараемся понять, как она устроена, в частности, что в такой модели может соответствовать натуральным числам и другим обычным математическим объектам. Это похоже на рассмотрение нестандартных арифметик, с существенным отличием: в случае арифметики мы не предполагали, а были уверены, что модели существуют.

4. Некоторые определения и сокращения

4.1. Квантор $\exists!$

Чтобы избежать слишком длинных формул, мы будем использовать сокращения. Одно из них — квантор $\exists!$ — означает «существует единственное». Иными словами, запись $\exists!\, u\, \Phi(u)$ является сокращением для формулы $\exists\, u\ (\Phi(u) \wedge \forall\, v\ (\Phi(v) \to u = v))$.

4.2. Пустое множество

Из аксиомы пустого множества и аксиомы объёмности следует, что $\mathbf{ZF} \vDash \exists!\, s\, \forall\, u\ (u \notin s)$, то есть в модели существует единственный элемент a, удовлетворяющий «формуле» $\forall\, u\ (u \notin a)$. Этот элемент мы будем обозначать символом $\varnothing$. Этот символ мы будем использовать в атомных формулах так же, как имя предмета, однако это просто сокращение: выражение $\varnothing \in x$ является сокращением для $\exists\, u\ (\forall\, v\ (v \notin u) \wedge u \in x)$ или $\forall\, u\ (\forall\, v\ (v \notin u) \to u \in x)$ — эти формулы равносильны, поскольку $\exists!\, u\, \forall\, v\ (v \notin u)$. Аналогично, являются сокращениями выражения $\varnothing = x$, $x \in \varnothing$.

4.3. Добавление новых функциональных символов

В общем случае, пусть для некоторой формулы $\Phi(\overline{x}\,, y)$ выполнено $\mathbf{ZF} \vDash \forall\, \overline{u}\ \ \exists!\, v\, \Phi(\overline{u}\,, v)$, то есть $\Phi(\overline{x}\,, y)$, по существу, задаёт отображение. Тогда мы будем иногда добавлять новый функциональный символ $\varphi(\overline{x}\,)$ и использовать его в атомных формулах, имея в виду, что, например,

$$y \in \varphi(\overline{x}\,) \quad \text{является сокращением для} \quad \exists\, u\ (\Phi(\overline{x}\,, u) \wedge y \in u)$$
$$\text{или} \quad \forall\, u\ (\Phi(\overline{x}\,, u) \to y \in u),$$

$$y = \varphi(\overline{x}\,) \quad \text{является сокращением для} \quad \Phi(\overline{x}\,, y).$$

4.4. Множество всех подмножеств данного множества

Из аксиом степени и объёмности следует, что $\mathbf{ZF} \vDash \forall\, u\, \exists!\, s\, \forall\, v\ (v \subset u \equiv v \in s)$. Мы введём обозначение $\mathcal{P}(x)$ для соответствующего отображения, так что $\mathcal{P}(x) = y \ \Leftrightarrow\ \forall v (v \subset x \equiv v \in y)$, мы будем называть $\mathcal{P}(x)$ множеством подмножеств x.

4.5. Неупорядоченная пара множеств

Из аксиомы пары и объёмности следует, что

$$\mathbf{ZF} \ \vDash\ \forall\, u\, \forall\, v\, \exists!\, s\, \forall\, w\ (w \in s \equiv (w = u \vee w = v)).$$

Соответствующее отображение мы будем обозначать $\{x, y\}$ и называть (неупорядоченной) парой множеств x и y. Пару $\{x, x\}$ мы будем обозначать $\{x\}$.

4.6. Объединение множества

Класс $\mathsf{Un}(x) = \{y \mid \exists\, u\ (y \in u \land u \in x)\}$ называется объединением множества x. Мы хотим показать, что $\mathsf{Un}(x)$ является множеством и это множество определено однозначно. Мы можем воспользоваться аксиомой замены для формулы $\Phi(y,z) = z \in y$,[3] поскольку $\{z \mid z \in a\}$, очевидно, является множеством для любого a. Выпишем аксиому замены для данного случая:

$$\forall\, u\, \exists\, v\, \forall\, w\, \Big(w \in v \equiv \Phi(u,w)\Big) \to \forall\, v\, \exists\, s\, \forall\, w\, \Big(\exists\, u\ (u \in v \land \Phi(u,w)) \equiv w \in s\Big),$$

или

$$\forall\, u\, \exists\, v\, \forall\, w\, \Big(w \in v \equiv w \in u\Big) \to \forall\, v\, \exists\, s\, \forall\, w\, \Big(\exists\, u\ (u \in v \land w \in u) \equiv w \in s\Big).$$

Посылка импликации истинна (достаточно взять $v = u$). Следовательно, истинно заключение импликации:

$$\forall\, v\, \exists\, s\, \forall\, w\, \Big(\exists\, u\ (u \in v \land w \in u) \equiv w \in s\Big).$$

А это и есть утверждение о том, что объединение любого множества — множество. Здесь $s = \mathsf{Un}(v)$.

4.7. Объединение, пересечение и разность двух множеств

Множество $\mathsf{Un}(\{x,y\})$ мы будем обозначать $x \cup y$. Через $x \cap y$ мы будем обозначать *пересечение* множеств — множество $\{z \mid z \in x \land z \in y\}$, через $x \setminus y$ — *разность*: $\{z \mid z \in x \land z \notin y\}$. Из аксиомы подмножеств непосредственно следует, что пересечение и разность являются множествами и определены однозначно.

4.8. Упорядоченная пара множеств

Множество $\{\{x\},\{x,y\}\}$ мы назовём *упорядоченной парой* множеств x, y и будем обзначать $\langle x,y\rangle$. Нетрудно доказать основное свойство упорядоченных пар:

$$\langle x,y\rangle = \langle x',y'\rangle \quad\Leftrightarrow\quad x = x' \;\land\; y = y',$$

то есть, что $\{\{x\},\{x,y\}\} = \{\{x'\},\{x',y'\}\} \quad\Leftrightarrow\quad x = x' \;\land\; y = y'$. Постарайтесь сами провести доказательство, рассмотрев как случай $x = y$, так и $x \neq y$.

4.9. Упорядоченная тройка множеств и упорядоченная n-ка множеств

Упорядоченная тройка $\langle x,y,z\rangle$ определяется как $\langle x,\langle y,z\rangle\rangle$, аналогично определяется упорядоченная n-ка.

4.10. Декартово произведение

Декартово произведение $x \times y$ определяется как класс

$$\Big\{z \mid \exists\, u\, \exists\, v\, \big(u \in x \;\land\; v \in y \;\land\; z = \langle u,v\rangle\big)\Big\}.$$

Чтобы доказать, что $x \times y$ является множеством, нам достаточно показать, что все элементы класса содержатся в некотором множестве, и воспользоваться аксиомой подмножеств. Это сделать нетрудно, поскольку $a \in x \times y \;\Rightarrow\; a \in \mathcal{P}(\mathcal{P}(x \cup y))$.

---

[3] Когда мы выписывали аксиомы замены, мы использовали запись $\Phi(\overline{x}\,, y, z)$. Но в данном случае список $\overline{x}$ пуст, и мы используем более краткую запись $\Phi(y,z)$.

4.11. Функции

Множество f пар $\langle a, b\rangle$ мы будем называть *функцией*, если

$$\forall u \, \forall v \, \forall w \, \Big(\langle u, v\rangle \in f \;\wedge\; \langle u, w\rangle \in f \;\;\to\;\; v = w\Big).$$

Свойство множества f «быть функцией» будем записывать как $\mathsf{Func}(f)$. *Областью определения* функции f называется множество $\mathsf{Dom}(f) = \{z \mid \exists\, u\, (\langle z, u\rangle \in f)\}$. *Областью значений* функции f называется множество $\mathsf{Ra}(f) = \{z \mid \exists\, u\, (\langle u, z\rangle \in f)\}$. Покажите, воспользовавшись аксиомой замены, что это действительно множества. Ясно, как определить *инъективную* (*взаимно однозначную*) функцию. Свойство множества f «быть инъективной функцией» будем записывать как $\mathsf{IFunc}(f)$.

Если f — функция, $x \in \mathsf{Dom}(f)$, то через $f(x)$ мы будем обозначать единственное множество y, такое, что $\langle x, y\rangle \in f$.

5. Натуральные числа (ω)

5.1. Натуральные числа и набор всех натуральных чисел

В нашей модели натуральным числам 0, 1, 2, 3, ... будут соответствовать множества $\varnothing$, $\{\varnothing\}$, $\{\varnothing, \{\varnothing\}\}$, $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$, ... Мы хотим понять, что при этом в нашей модели соответствует набору всех натуральных чисел.

Обозначим через $S(x)$ множество $x \cup \{x\}$. В этих обозначениях можно сказать, что $0 = \varnothing$, $1 = S(0)$, $2 = S(1)$, ..., а аксиому бесконечности

$$\exists\, s \,\Bigg(\exists\, u \,\Big(u \in s \;\wedge\; \forall\, v\, (v \notin u)\Big) \wedge \\ \wedge\, \forall\, u \,\Big(u \in s \to \exists\, v \,\Big(v \in s \wedge \forall\, w \,\big(w \in v \equiv (w \in u \vee w = u)\big)\Big)\Big)\Bigg)$$

можно записать в виде

$$\exists s(\varnothing \in s \;\;\wedge\;\; \forall\, u\, (u \in s \to S(u) \in s)),$$

то есть в нашей структуре существует элемент s, удовлетворяющий формуле

$$\varnothing \in s \;\wedge\; \forall u (u \in s \to S(u) \in s). \qquad (*)$$

Обозначим через ω пересечение всех множеств, удовлетворяющих $(*)$, то есть

$$\omega = \Big\{x \mid \forall\, s \,\Big(\Big(\varnothing \in s \;\wedge\; \forall\, u\, (u \in s \to S(u) \in s)\Big) \to x \in s\Big)\Big\}.$$

Из аксиомы бесконечности и аксиомы подмножеств следует, что ω является множеством, по аксиоме объёмности это множество определено однозначно.

Символами n, m, $k, \ldots$ мы будем в дальнейшем обозначать элементы ω. Так, вместо $\forall\, n\, (n \in \omega \to \ldots$ будем писать просто $\forall\, n\ \ldots$.

5.2. Граничный элемент подмножества множества ω. Теорема индукции

Если a — непустое подмножество ω, то *граничным элементом* множества a назовем такой элемент $b \in a$, что $b = 0$ или $b = S(c)$ для некоторого $c \in \omega$, $c \notin a$.[4]

[4] Граничный элемент может быть не единственным.

Теорема индукции. *В любом непустом подмножестве множества ω имеется граничный элемент, то есть*

$$\mathbf{ZF} \ \vDash \ \forall u\,(u \subset \omega \wedge u \neq \varnothing \ \rightarrow \ (0 \in u \vee \exists v\,(v \in \omega \ \wedge \ v \notin u \ \wedge \ S(v) \in u))).$$

Доказательство. Пусть $a \subset \omega$, $b = \omega \backslash a$. Предположим, что в a нет граничного элемента, то есть $\varnothing \in b$, $c \in b \rightarrow S(c) \in b$, значит, b удовлетворяет $(*)$. Тогда, по определению ω, выполнено $\omega \subset b$, и a пусто. $\square$

5.3. Порядок на множестве ω

Определим порядок на ω так, что $x < y \quad \Leftrightarrow \quad x \in y$. Ниже будут доказаны необходимые свойства порядка: транзитивность (утверждение 3), антирефлексивность (утверждение 4). Будет также доказано, что порядок линеен (утверждение 7) и полон (утверждение 8).

5.4. Несколько простых утверждений

Бо́льшая часть перечисленных ниже утверждений — это свойства порядка на ω. Некоторые утверждения, выбранные достаточно произвольно, мы докажем, остальные оставим в качестве упражнений.

Утверждение 0. $\forall n\,(n = 0 \ \vee \ \exists m\,(n = S(m)))$.
Доказательство. Допустим противное, что не для всех n выполнено свойство $n = 0 \ \vee \ \exists m\,(n = S(m))$. Тогда множество

$$\{n \mid n \in \omega \ \wedge \ n \neq 0 \ \wedge \ \forall m\,(m \in \omega \rightarrow n \neq S(m)\}$$

не пусто, но не содержит граничного элемента, что противоречит теореме индукции. $\square$

Утверждение 1. $\forall n\,(n < S(n))$. (Следует из определений S и $<$.)

Утверждение 2. $\forall x\,\forall n\,(x \in n \rightarrow x \subset n)$.
Доказательство. Допустим противное. Тогда набор

$$\{y \ \mid \ y \in \omega \ \wedge \ \exists u\,(u \in y \wedge \neg(u \subset y))\}$$

не пуст. По аксиоме подмножеств этот набор является множеством, обозначим его a. По предположению $a \neq \varnothing$, следовательно, по теореме индукции, в нем есть граничный элемент — обозначим его n. По определению a выполнено $0 \notin a$, поэтому $n = S(m)$ для некоторого $m \in \omega \setminus a$. Если $x \in S(m)$, то, по определению операции S, имеет место $x = m$ или $x \in m$. Разберём оба случая.

Если $x = m$, то $x \subset S(m)$ по определению операции S. Если $x \in m$, то $x \subset m$, поскольку $m \notin a$. Тогда $x \subset m \subset S(m)$. В обоих случаях мы плучили, что из $x \in n$ следует $x \subset n$, что противоречит тому, что n — элемент множества a. $\square$

Утверждение 3. Порядок транзитивен: $(n < m) \wedge (m < k) \quad \rightarrow \quad (n < k)$. (Следует из утверждения 2.)

Утверждение 4. $\forall n\,(\neg(n < n))$. (Следует из теоремы индукции или из аксиомы регулярности.)

Утверждение 5. $\forall n\,(0 < S(n))$. (Следует из теоремы индукции.)

Утверждение 6. $\forall n\, \forall m\, \Big((n < m) \;\to\; \big((S(n) = m) \vee (S(n) < m) \big) \Big).$
(Доказывается индукцией по m.)

Утверждение 7. Порядок линеен, то есть любые два элемента сравнимы:

$$\forall n\, \forall m\, \big((n < m) \;\vee\; (n = m) \;\vee\; (m < n) \big).$$

Доказательство. Пусть есть несравнимые элементы. Пусть

$$a = \{ x \mid x \in \omega \;\wedge\; \exists w\, (w \in \omega \;\wedge\; (x \text{ и } w \text{ не сравнимы})) \}.$$

Пусть n — граничный элемент множества a. Из утверждения 5 следует, что $n \neq 0$, поэтому $n = S(m)$, $m \notin a$. Пусть n не сравним с k. Однако m сравним с k. Если $k < m$ или $k = m$, то $k < n$ из утверждения 3 (транзитивность порядка). Если $m < k$, то сравнимость n с k следует из утверждения 6. $\square$

Утверждение 8. Стандартная индукция: в любом непустом подмножестве множества ω есть наименьший элемент, то есть

$$\forall a\, \Big(a \subset \omega \wedge a \neq \varnothing \;\;\to\;\; \exists k\, (k \in a \wedge \forall m\, (m < k \to m \notin a)) \Big).$$

Доказательство. Пусть a — произвольное непустое подмножество множества ω. Рассмотрим множество b таких элементов ω, для каждого из которых в множестве a найдётся равный ему или меньший его элемент m:

$$b = \{ n \mid n \in \omega \;\wedge\; \exists m\, (m \in a \wedge m \leqslant n) \}.$$

Так как каждый элемент, принадлежащий множеству a, равен самому себе, то он принадлежит также и множеству b. Поэтому множество b не пусто. Граничный элемент k множества b — это и есть наименьший элемент множества a. Чтобы в этом убедиться, нужно рассмотреть два случая.

Первый случай: $k = 0$. Легко понять, что в этом случае число 0 обязано принадлежать не только множеству b, но и множеству a, и 0 при этом будет наименьшим элементом множества a.

Второй случай: $k = S(m)$, $m \notin b$. Допустим, что k не является наименьшим элементом множества a. Это могло бы быть по двум причинам. Первая причина: в множестве a есть элемент l такой, что $l < k$. Тогда $l \leqslant m$, и, по определению множества b, множество b обязано было бы содержать m. Противоречие. Вторая причина: k не является элементом множества a. Но тогда, поскольку k является элементом множества b, в множестве a должен найтись элемент s такой, что $s < k$. Тогда $s \leqslant m$, и, по определению множества b, множество b обязано было бы содержать m. Противоречие. $\square$

5.5. Определение операции сложения на множестве натуральных чисел

Через $n+1$ мы будем обозначать $S(n)$, через $n-1$ — такое (единственное) m, что $n = S(m)$ (если такое m существует). Введём ещё обозначение:

$$[n, m] \;=\; \{ k \mid (k \in \omega) \;\wedge\; (n \leqslant k) \;\wedge\; (k \leqslant m) \}.$$

Теперь нетрудно рекурсивно определить сложение на элементах ω как функцию $\Sigma\colon \omega \times \omega \to \omega$, удовлетворяющую следующим рекурсивным соотношениям:

(0) $\Sigma\big(\langle n, 0 \rangle\big) = n,$

(1) $\Sigma\big(\langle n, m+1\rangle\big) = \Sigma\big(\langle n, m\rangle\big) + 1$.

Докажем стандартной индукцией, что такое единственное Σ существует и является всюду определённой функцией на $\omega \times \omega$.

Доказательство. Скажем, что элемент $k \in \omega$ *корректен*, если существует функция $\Sigma\colon \omega \times [0, k] \to \omega$, удовлетворяющая указанным рекурсивным соотношениям при $m \leqslant k$. Ясно, что набор некорректных элементов ω является множеством, предположим, что оно не пусто. Пусть k' — наименьший некорректный элемент. Из (1) следует, что $k' \neq 0$. Если $k' = l + 1$, то из корректности l можно доопределить Σ на k' в соответствии с (2). То есть, все элементы ω корректны. Единственность Σ доказываем так же, рассмотрев элементы, на которых функция $\Sigma\colon \omega \times [0, k] \to \omega$ не единственна.

Таким образом, для любого $k \in \omega$ существует единственная функция Σ_k, удовлетворяющая рекурсивным соотношениям на множестве $\omega \times [0, k]$. Нетрудно заметить, что $k < k' \Rightarrow \Sigma_k \subset \Sigma_{k'}$. По аксиоме замены $\mathsf{Un}\{\Sigma_k \mid k \in \omega\}$ является функцией. Эта функция и будет сложением. $\square$

Вместо $\Sigma\big(\langle n, m\rangle\big)$ мы будем использовать привычную запись $n + m$.

5.6. Определение операции умножения и других операций на множестве натуральных чисел

Теперь нетрудно определить умножение как функцию $\Pi\colon \omega \times \omega \to \omega$, удовлетворяющую рекурсивным соотношениям:

(0) $\Pi\big(\langle n, 0\rangle\big) = 0$,

(1) $\Pi\big(\langle n, m+1\rangle\big) = \Pi\big(\langle n, m\rangle\big) + n$.

Аналогично можно определить и все прочие нужные нам арифметические функции и отношения.

5.7. Определение множеств $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

Множество целых чисел $\mathbb{Z}$ можно определить как множество пар вида $\langle 0, n\rangle$ и $\langle 1, n\rangle$, $(n \in \omega)$, имея в виду, что $\langle 0, n\rangle$ соответствует положительному числу, а $\langle 1, n\rangle$ — отрицательному.[5] Множество рациональных чисел $\mathbb{Q}$ нетрудно определить как множество классов эквивалентности (подмножеств) множества $\mathbb{Z} \times \big(\omega \setminus \{0\}\big)$ с обычной эквивалентностью $\langle x_1, x_2\rangle \sim \langle y_1, y_2\rangle \Leftrightarrow x_1 y_2 = x_2 y_1$.

Множество действительных чисел $\mathbb{R}$ можно определить как множество сечений (пар подмножеств множества $\mathbb{Q}$ специального вида).

Вы уже и сами можете понять, как обычные математические утверждения переводятся в формулы теории **ZF**, и оценить, насколько сложно переформулировать обычные доказательства в следствия теории **ZF**.

[5] Другим способом множество целых чисел $\mathbb{Z}$ можно определить как множество классов эквивалентности множества $\omega \times \omega$ с эквивалентностью $\langle x_1, x_2\rangle \sim \langle y_1, y_2\rangle \Leftrightarrow x_1 + y_2 = x_2 + y_1$. Этот способ больше похож на способ, которым ниже определяется множество рациональных чисел $\mathbb{Q}$.