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 $y_2 \leqslant y_1$, 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. ⊠

1.6 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 1.13. *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 1.14. (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, $x = \varphi(S_x) = \varphi(U_x)$. $\boxtimes$

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.