Отображение (или функция) $f\colon A \to B$ называется:

инъективным, если различные элементы переходят в различные (т.е. из $a_1 \neq a_2$ следует $f(a_1) \neq f(a_2)$);

сюръективным, если у каждой точки множества B есть прообраз (т.е. из $b \in B$ следует, что $y = f(a)$ для некоторого $a \in A$);

биективным, или *взаимно однозначным*, если оно инъективно и сюръективно.

Два множества A и B называются *равномощными* и пишут $|A| = |B|$, если существует взаимно однозначное отображение между ними. Если множество A инъективно вкладывается в множество B, то пишут $|A| \leq |B|$. Логически возможны 4 случая:

(Сл1) A равномощно B;

(Сл2) A равномощно подмножеству B, B не равномощно никакому подмножеству A;

(Сл3) A равномощно подмножеству B, B равномощно подмножеству A;

(Сл4) A не равномощно никакому подмножеству B, B не равномощно никакому подмножеству A.

Следующая теорема исключает случай (Сл3):

Теорема 1 (Кантора – Бернштейна). *Из (Сл3) следует (Сл1).*

Доказательство Пусть A равномощно подмножеству B_1 множества B, а B равномощно подмножеству A_1 множества A (см. рис. 1).

Рис. 1:

При взаимно однозначном соответствии между B и A_1 подмножество $B_1 \subseteq B$ переходит в некоторое подмножество $A_2 \subseteq A_1$. При этом все три множества A, B_1 и A_2 равномощны, и нужно доказать, что они равномощны множеству B, или, что то же самое, A_1.

Теперь мы можем забыть про множество B и его подмножества и доказывать такой факт: если $A_2 \subseteq A_1 \subseteq A_0$ и A_2 равномощно A_0, то все три множества равномощны.

Пусть f – функция, осуществляющая взаимно однозначное соответствие $A_0 \to A_2$. Когда A_0 переходит в A_2, меньшее множество A_1 переходит в какое-то множество $A_3 \subseteq A_2$ (см. рис. 2). Аналогичным образом само A_2 переходит в некоторое множество $A_4 \subseteq A_2$. При этом $A_4 \subseteq A_3$, так как $A_1 \subseteq A_2$.

Рис. 2:

Продолжая эту конструкцию, мы получаем убывающую последовательность множеств

$$A_0 \supseteq A_1 \supseteq A_2 \supseteq A_3 \supseteq A_4 \supseteq \ldots$$

и взаимно однозначное соответствие $f\colon A_0 \to A_2$, при котором A_i соответствует A_{i+2}. Теперь можно сказать так: множество A_0 мы разбили на непересекающиеся слои $C_i = A_i \setminus A_{i+1}$ и на сердцевину $C = \bigcap_i A_i$.

Слои $C_0, C_2, C_4, \ldots$ равномощны (функция f осуществляет взаимно однозначное соответствие между C_0 и C_2, между C_2 и C_4 и т.д.):

$$C_0 \xrightarrow{f} C_2 \xrightarrow{f} C_4 \xrightarrow{f} \ldots$$

То же самое можно сказать про слои с нечетными номерами:

$$C_1 \xrightarrow{f} C_3 \xrightarrow{f} C_5 \xrightarrow{f} \ldots$$

Теперь легко понять, как построить взаимно однозначное соответствие g между A_0 и A_1. Пусть $x \in A_0$. Тогда соответствующий ему элемент $g(x)$ строится так: $g(x) = f(x)$ при $x \in C_{2k}$ и

$g(x) = x$ при $x \in C_{2k+1}$ или $x \in C$ (см. диаграмму).

$$\begin{tikzcd}
C_0 \arrow[drrrr] & + & C_1 \arrow[d] & + & C_2 \arrow[drrrr] & + & C_3 \arrow[d] & + & C_4 & + & \dots & + & C \arrow[d] \\
 & & C_1 & + & C_2 & + & C_3 & + & C_4 & + & \dots & + & C
\end{tikzcd}$$

$\square$

Множество $(A, \leq)$ называется *частично упорядоченным*, если выполнены следующие свойства:

1. для любого $a \in A$ выполнено $a \leq a$ (*рефлексивность*);
2. для любых $a, b \in A$ если $a \leq b$ и $b \leq a$, то $a = b$ (*симметрия*);
3. для любых $a, b, c \in A$ если $a \leq b$ и $b \leq c$, то $a \leq c$ (*транзитивность*).

Элемент $a_0 \in A$ называется *максимальным* (*минимальным*), если из того, что $a_0 \leq a$ ($a \leq a_0$) следует, что $a = a_0$. Элемент $a_0 \in A$ называется *наибольшим* (*наименьшим*), если $a \leq a_0$ ($a_0 \leq a$) для любого $a \in A$. Элемент $a \in A$ называется *верхней гранью* (*нижней гранью*) подмножества $X \subseteq A$, если $x \leq a$ ($a \leq x$) для любого $x \in X$.

Частично упорядоченное множество $(A, \leq)$ называется *линейно упорядоченным* или *цепью*, если дополнительно выполнено свойство:

4. для любых $a, b \in A$ или $a \leq b$, или $b \leq a$.

Примером частично, но не линейно упорядоченного множества является, например, множество всех подмножеств $(2^A, \subseteq)$ множества A с отношением включения. Ясно, что в случае линейно упорядоченного множества понятия минимального (максимального) и наименьшего (наибольшего) элемента совпадают.

Линейно упорядоченное множество $(A, \leq)$ называется *вполне упорядоченным*, если дополнительно выполнено свойство:

5. всякое непустое подмножество $X \subseteq A$ имеет наименьший элемент.

Теорема Цермело утверждает:

(ТЦ) всякое множество можно вполне упорядочить.

В доказательстве теоремы Цермело будет использоваться, так называемая, аксиома выбора:

(АВ) для всякого семейства $\{X_s\}_{s \in S}$ непустых множеств существует функция f из S в $\bigcup_{s \in S} X_s$, такая, что $f(s) \in X_s$ при всех $s \in S$.

В дальнейшем нам понадобится лемма Цорна:

(ЛЦ) частично упорядоченное множество, в котором каждая цепь имеет верхнюю грань, обладает максимальным элементом.

Оказывается, что утверждения (ТЦ), (АВ) и (ЛЦ) эквивалентны. Докажем это в такой последовательности (АВ)$\Rightarrow$(ТЦ)$\Rightarrow$(ЛЦ)$\Rightarrow$(АВ).

Теорема 2. *Из (AB) следует (ТЦ).*

Доказательство. I. Пусть A обозначает рассматриваемое множество, B — множество всех его подмножеств, $\phi\colon B \setminus \{\emptyset\} \to A$ – функция выбора, сопоставляющая каждому непустому подмножеству X множества A, принадлежащую ему точку: $\phi(X) \in X$. Функция $\alpha(X) = \phi(A \setminus X)$ определена для всех подмножеств множества A за исключением самого множества A.

II. Подмножество P множества B назовем *правильным*, если

1) оно линейно упорядочено отношением $\subseteq$, то есть, если $p_1, p_2 \in P$, то либо $p_1 \subseteq p_2$, либо $p_2 \subseteq p_1$;

2) оно при этом вполне упорядочено отношением $\subseteq$, то есть, если $\gamma \subseteq P$, то в γ есть наименьший элемент относительно этого порядка (так как речь идет об отношении порядка $\subseteq$, то наименьший элемент есть $\bigcap \gamma$);

3) $\emptyset \in P$;

4) если множество $q \in P$ непусто, то $q = q_1 \cup \{\alpha(q_1)\}$, где $q_1 = \bigcup \{p : p \in P, p \subset q\}$.

Правильные множества существуют. Таковыми, например, являются множества $\{\emptyset\}$, $\{\emptyset, \{\alpha(\emptyset)\}\}$, $\{\emptyset, \{\alpha(\emptyset)\}, \{\alpha(\emptyset), \alpha(\{\alpha(\emptyset)\})\}\}$ и т.д. Заметим, что если $p \in P$ и $p + 1 \in P$, то $p + 1 = p \cup \{\alpha(p)\}$.

III. Пусть P_1 и P_2 — правильные множества.

Положим $P_3 = \{p : p \in P_1 \cap P_2, \{q : q \in P_1, q \subset p\} = \{q : q \in P_2, q \subset p\}\}$.

Покажем, что $(*)$ $P_3 = P_1$ или $P_3 = P_2$.

Так как в силу определения P_3 имеем: $P_3 \subseteq P_1 \cap P_2$, то, предположив невыполнение $(*)$, получаем непустоту множеств $P_1 \setminus P_3$ и $P_2 \setminus P_3$. Пусть r_1 — наименьший элемент множества $P_1 \setminus P_3$, r_2 — наименьший элемент множества $P_2 \setminus P_3$. Так как $\{p : p \in P_1, p \subset r_1\} = P_3 = \{p : p \in P_2, p \subset r_2\}$, то в силу 4) $r_1 = \bigcup P_3 \cup \{\alpha(\bigcup P_3)\} = r_2$. Следовательно, $r_1 \in P_3$, что невозможно ($r_1 \notin P_3$).

Таким образом, предположение о невыполнении $(*)$ приводит нас к противоречию.

Выполнение же $(*)$ означает, что либо P_1 является начальным отрезком P_2, либо P_2 является начальным отрезком P_1.

IV. Обозначим через Q объединение всех правильных множеств. При этом Q очевидным образом удовлетворяет условиям 1) и 3) из II.

Покажем выполнение условия 2).

Пусть $\gamma \subseteq Q$. Для некоторого правильного множества P пересечение $\gamma \cap P$ непусто. Пусть $m \in \gamma \cap P$. В силу правильности множества P множество $\{n : n \in \gamma, n \subseteq m\} \subseteq P$ имеет наименьший элемент. Обозначим его через g. Он не больше всех элементов γ, меньших m, по своему определению и не больше всех элементов γ, больших m, в силу того, что $g \subseteq m$.

Покажем выполнение условия 4).

Пусть множество $q \in Q$ непусто. В силу определения Q $q \in P$ для некоторого правильного множества P. Поэтому $q = q_1 \cup \{\alpha(q_1)\}$, где $q_1 = \bigcup\{p : p \in P, p \subset q\}$ в силу правильности множества P. Для любого множества $r \in Q \setminus P$ выполнено $q \subseteq r$, поэтому $q_1 = \bigcup\{p : p \in Q, p \subset q\}$.

Таким образом, множество Q правильно. Пусть $Z = \bigcup Q$.

Если при этом $Z \neq A$, то множество $\tilde{Q} = Q \cup \{Z \cup \{\alpha(Z)\}\}$ является правильным. Это противоречит определению Q как объединению всех правильных множеств, так как $\tilde{Q}$ содержит Q в качестве собственного подмножества.

Таким образом, $\bigcup Q = A$.

V. Рассмотрим α в качестве отображения из Q в A.

Покажем, что отображение α инъективно.

Пусть $q_1 \neq q_2$. Положим для определенности $q_1 \subset q_2$. Тогда $q_1 + 1 \subseteq q_2$. В силу правильности множества Q имеем $q_1 + 1 = q_1 \cup \{\alpha(q_1)\}$. Поэтому $\alpha(q_1) \in q_1 + 1 \subseteq q_2$, т. е. $\alpha(q_1) \in q_2$. Но $\alpha(q_2) \notin q_2$. Следовательно, $\alpha(q_1) \neq \alpha(q_2)$.

Покажем, что отображение α сюръективно.

В силу того, что $\bigcup Q = A$ для любого $a \in A$ множество $\{q : q \in Q, q \ni a\}$ непусто. Обозначим через r его наименьший элемент. Тогда в силу правильности множества Q имеем $r = r_1 \cup \{\alpha(r_1)\}$, где $r_1 = \bigcup\{q : q \in Q, q \subset r\}$. Так как r — наименьший элемент, содержащий точку a, то $a \notin r_1$. Следовательно, $\alpha(r_1) = a$.

Таким образом, функция α индуцирует полный порядок на A. $\square$

Теорема 3. *Из (ТЦ) следует (ЛЦ).*

Доказательство. Пусть дано частично упорядоченное множество $(Z, \leq)$ и произвольный элемент $a \in Z$. Вполне упорядочим множество Z с помощью теоремы Цермело. Этот порядок никак не связан с исходным порядком на Z; мы будем обозначать его символом $\prec$. Построим с помощью трансфинитной индукции функцию $f\colon Z \to Z$ с такими свойствами:

1) $a \leq f(z)$ для любого $z \in Z$;

2) f монотонна в следующем смысле: если $x \prec y$, то $f(x) \leq f(y)$;

3) $f(z)$ не может быть строго меньше z (в смысле исходного порядка $\leq$) ни при каком z.

Делается это так. Значение $f(z_0)$ для $\prec$-наименьшего элемента z_0 мы положим равным либо a, либо z_0 (последнее – если $z_0 > a$). Значение $f(z)$ для остальных z есть либо верхняя граница значений $f(z')$ при $z' \prec z$ (по предположению индукции множество таких значений линейно упорядочено и потому имеет некоторую верхнюю границу α), либо само z (последнее – если $z > \alpha$).

В силу монотонности множество значений функции f линейно упорядочено и имеет верхнюю границу. Эта граница (обозначим ее β) больше или равна a (которое есть $f(z_0)$) и является искомым максимальным элементом: если $\beta < z$ для некоторого z, то $f(z) \leq \beta < z$, что противоречит свойству 3). $\square$

Теорема 4. *Из (ЛЦ) следует (АВ).*

Доказательство. Пусть $\{X_s\}_{s\in S}$ – семейство непустых множеств. Обозначим через $\mathscr{X}$ множество всех пар (T, f), где $T \subseteq S$ и f – функция из T в $\bigcup_{s\in S} X_s$, такая, что $f(s) \in X_s$ для любого $s \in T$. Упорядочим множество $\mathscr{X}$, полагая:

$$(T_1, f_1) \leq (T_2, f_2) \text{ в том и только том случае, когда } T_1 \subseteq T_2 \text{ и } f_2(s) = f_1(s) \text{ для } s \in T_1.$$

Легко видеть, что для каждого линейно упорядоченного подмножества $\mathscr{A} = \{(T_w, f_w)\}_{w\in W}$ множества $\mathscr{X}$ формулы

$$T_0 = \bigcup_{w\in W} T_w \text{ и } f_0(s) = f_w(s) \text{ для } s \in T_w$$

определяют элемент (T_0, f_0) множества $\mathscr{X}$ и $(T_w, f_w) \leq (T_0, f_0)$ для каждого $w \in W$. По лемме Цорна в $\mathscr{X}$ существует максимальный элемент (T, f); мы покажем, что $T = S$, и тем завершим доказательство. В самом деле, допустим, что существует $s_0 \in S\backslash T$; выберем $x_0 \in X_{x_0}$ и положим

$$T' = T \cup \{s_0\},\ f'(s) = f(s) \text{ для } s \in T \text{ и } f'(s_0) = s_0.$$

Тем самым определена пара $(T', f') \in \mathscr{X}$, такая, что $(T, f) < (T', f')$; мы пришли к противоречию. $\square$

Рассмотрим два множества A и B. С помощью теоремы Цермело вполне упорядочим их и соответствующие порядки обозначим через $\prec_A$ и $\prec_B$. Построим с помощью трансфинитной индукции функцию $f\colon A \to B$ следующим образом:

(Ф1) значение $f(a_0)$ для наименьшего элемента a_0 множества A положим равным наименьшему элементу множества B;

(Ф2) значение $f(a)$ для остальных $a \in A$ положим равным наименьшему элементу множества $B \setminus \bigcup\{f(a')\colon a' \prec_A a\}$.

Такое определение функции f закончится в случае, когда исчерпается множество A или B. Но оба случая означают, что одно из множеств инъективно вкладывается в другое. Таким образом, случай (Сл4) исключается при выполнении теоремы Цермело.