Chapter 1

Zermelo's well-ordering theorem

File: `set-theory/sections/05_well-ordering-theorem.ftl.tex`

[readtex `foundations/sections/13_equinumerosity.ftl.tex`]

[readtex `set-theory/sections/04_recursion.ftl.tex`]

SET_THEORY_05_4227480655233024

Theorem 1.1 (Zermelo). Every set is equinumerous to some ordinal.

Proof. Let x be a set.

[prover vampire] Every element of $(x \cup \{x\})^{<\infty}$ is a map. Define

$$G(F) = \begin{cases} \text{choose } u \in x \setminus \operatorname{range}(F) \text{ in } u & : x \setminus \operatorname{range}(F) \neq \emptyset \\ x & : x \setminus \operatorname{range}(F) = \emptyset \end{cases}$$

for $F \in (x \cup \{x\})^{<\infty}$. [prover eprover]

Then G is a map from $(x \cup \{x\})^{<\infty}$ to $x \cup \{x\}$. Indeed we can show that for any $F \in (x \cup \{x\})^{<\infty}$ we have $G(F) \in x \cup \{x\}$. Let $F \in (x \cup \{x\})^{<\infty}$. If $x \setminus \operatorname{range}(F) \neq \emptyset$ then $G(F) \in x \setminus \operatorname{range}(F)$. If $x \setminus \operatorname{range}(F) = \emptyset$ then $G(F) = x$. Hence $G(F) \in x \cup \{x\}$. End. Hence we can take a map F from **Ord** to $x \cup \{x\}$ that is recursive regarding G. For any ordinal α we have $F \restriction \alpha \in (x \cup \{x\})^{<\infty}$.

For any $\alpha \in \mathbf{Ord}$
$$x \setminus F[\alpha] \neq \emptyset \quad \text{implies} \quad F(\alpha) \in x \setminus F[\alpha]$$
and
$$x \setminus F[\alpha] = \emptyset \quad \text{implies} \quad F(\alpha) = x.$$

Proof. Let $\alpha \in \mathbf{Ord}$. We have $F[\alpha] = \{F(\beta) \mid \beta \in \alpha\}$. Hence $F[\alpha] = \{G(F \upharpoonright \beta) \mid \beta \in \alpha\}$. We have $\text{range}(F \upharpoonright \alpha) = \{F(\beta) \mid \beta \in \alpha\}$. Thus $\text{range}(F \upharpoonright \alpha) = F[\alpha]$.

Case $x \setminus F[\alpha] \neq \emptyset$. Then $x \setminus \text{range}(F \upharpoonright \alpha) \neq \emptyset$. Hence $F(\alpha) = G(F \upharpoonright \alpha) \in x \setminus \text{range}(F \upharpoonright \alpha) = x \setminus F[\alpha]$. End.

Case $x \setminus F[\alpha] \neq \emptyset$. Then $x \setminus \text{range}(F \upharpoonright \alpha) = \emptyset$. Hence $F(\alpha) = G(F \upharpoonright \alpha) = x$. End. Qed.

(1) For any ordinals α, β such that $\alpha < \beta$ and $F(\beta) \neq x$ we have $F(\alpha), F(\beta) \in x$ and $F(\alpha) \neq F(\beta)$.
Proof. Let $\alpha, \beta \in \mathbf{Ord}$. Assume $\alpha < \beta$ and $F(\beta) \neq x$. Then $x \setminus F[\beta] \neq \emptyset$. (a) Hence $F(\beta) \in x \setminus F[\beta]$. We have $F[\alpha] \subseteq F[\beta]$. Thus $x \setminus F[\alpha] \neq \emptyset$. (b) Therefore $F(\alpha) \in x \setminus F[\alpha]$. Consequently $F(\alpha), F(\beta) \in x$ (by a, b). We have $F(\alpha) \in F[\beta]$ and $F(\beta) \notin F[\beta]$. Thus $F(\alpha) \neq F(\beta)$. Qed.

(2) There exists an ordinal α such that $F(\alpha) = x$.
Proof. Assume the contrary. Then F is a map from $\mathbf{Ord}$ to x.

Let us show that F is injective. Let $\alpha, \beta \in \mathbf{Ord}$. Assume $\alpha \neq \beta$. Then $\alpha < \beta$ or $\beta < \alpha$. Hence $F(\alpha) \neq F(\beta)$ (by 1). Indeed $F(\alpha), F(\beta) \neq x$. End.

Thus F is an injective map from some proper class to some set. Contradiction. Qed.

Define $\Phi = \{\alpha \in \mathbf{Ord} \mid F(\alpha) = x\}$. Φ is nonempty. Hence we can take a least element α of Φ regarding $\in$. Take $f = F \upharpoonright \alpha$. Then f is a map from α to x. Indeed for no $\beta \in \alpha$ we have $F(\beta) = x$. Indeed for all $\beta \in \alpha$ we have $(\beta, \alpha) \in \in$.

(3) f is surjective onto x.
Proof. $x \setminus F[\alpha] = \emptyset$. Hence $\text{range}(f) = f[\alpha] = F[\alpha] = x$. Qed.

(4) f is injective.
Proof. Let $\beta, \gamma \in \alpha$. Assume $\beta \neq \gamma$. We have $f(\beta), f(\gamma) \neq x$. Hence $f(\beta) \neq f(\gamma)$ (by 1). Indeed $\beta < \gamma$ or $\gamma < \beta$. Qed.

Therefore f is a bijection between α and x. Consequently x and α are equinumerous. □

SET_THEORY_05_689384265351168

Corollary 1.2. For every set x there exists a strong wellorder on x.

Proof. Let x be a set. Choose an ordinal α that is equinumerous to x. Take a bijection f between x and α. Define $R = \{(u, v) \mid u, v \in x \text{ and } f(u) < f(v)\}$.

Let us show that R is a strong wellorder on x. $<$ is a strong wellorder on α. For all $u, v \in x$ we have $(u, v) \in R$ iff $f(u) < f(v)$.

(1) R is irreflexive on x. Indeed for all $u \in x$ we have $f(u) \not< f(u)$.

(2) R is transitive on x. Indeed for all $u, v, w \in x$ if $f(u) < f(v)$ and $f(v) < f(w)$ then $f(u) < f(w)$.

(3) R is connected on x.
Proof. Let $u, v \in x$. Assume $u \neq v$. Then $f(u) \neq f(v)$. Hence $f(u) < f(v)$ or $f(v) < f(u)$ (by **??**). Indeed $f(u), f(v)$ are ordinals. Qed.

Hence R is a strict linear order on x.

(4) R is wellfounded on x.
Proof. Let A be a nonempty subclass of x. Then we can take a least element β of $f[A]$ regarding $<$. Indeed $f[A]$ is a nonempty subclass of α. Then $f^{-1}(\beta)$ is a least element of A regarding R. Qed.

We can show that for all $v \in x$ there exists a set y such that $y = \{u \in x \mid (u, v) \in R\}$. Let $v \in x$. Define $y = \{u \in x \mid (u, v) \in R\}$. Then y is a set such that $y = \{u \in x \mid (u, v) \in R\}$. End. [prover vampire] Hence R is strongly wellfounded on x (by definition 11.18). Indeed R is a binary relation. Thus R is a strong wellorder on x. End. □