20. Well-orderings

There is an obvious counterpart to (18.2).

Conjecture 20.1. *Let $f\colon A \longrightarrow B$ and $g\colon B \longrightarrow A$ be two surjective functions.*

Then $|A| = |B|$.

Axiom 20.2 (Axiom of choice)**.** *If A_i, $i \in I$, is a set of non-empty sets then we can pick an element of each A_i.*

Theorem 20.3 (Kurt Gödel)**.** *There is a model of set theory in which the axiom of choice holds.*

Theorem 20.4 (Paul Cohen)**.** *There is a model of set theory in which the axiom of choice is false.*

It turns out that the axiom of choice is equivalent to many other reasonable looking axioms of set theory, such as (20.1). In practice, mathematicians assume the axiom of choice holds. The resulting model of set theory is called ZFC (Zermelo-Fraenkel, plus the axiom of choice). For example, the axiom of choice is equivalent to the statement that every surjective function $f\colon A \longrightarrow B$ has a right inverse, a function $g\colon B \longrightarrow A$ such that $f \circ g = \mathrm{id}_B$. In fact this right inverse is automatically injective, so the existence of surjective functions both ways, plus the axiom of choice, implies the existence of injective functions both ways and by (18.2) this implies there is a bijection.

Definition 20.5. *Let X be a set. A **relation** $\mathcal{R}$ on X, is a subset of $X \times X$.*

It is customary to write $x\mathcal{R}y$, which reads x is related to y, if $(x, y) \in \mathcal{R} \subset X \times X$.

Definition 20.6. *A relation $\leq$ on X is called a **partial order** if $\leq$ is*

*(1) **reflexive**, that is, $x \leq x$ for every $x \in X$,*
*(2) **anti-symmetric**, that is, if $x \leq y$ and $y \leq x$ then $x = y$, for every x and y, and*
*(3) $\leq$ is **transitive**, that is, if $x \leq y$ and $y \leq z$ then $x \leq z$.*

*A partial order is called a **total order**, if in addition either $x \leq y$ or $y \leq x$ for every pair of elements of X.*

Example 20.7. *The usual ordering of the real numbers is a total order.*

Example 20.8. *Let A be a set and let X be the powerset of A. Define a relation on the elements of X, that is, the subsets of A, by the rule*

$$B \leq C \qquad \textit{if and only if} \qquad B \subset C.$$

This relation is a partial order of X. It is almost never a total ordering. For example if

$$A = \{\, b, c \,\}$$

then $B = \{b\}$ and $C = \{c\}$ are not comparable.

Definition 20.9. *We say that a total order $(X, \leq)$ is a* ***well-ordering*** *if every non-empty subset $Y \subset X$ has a minimal element.*

Principle 20.10 (Well-ordering principle)**.** *The natural numbers are well-ordered, under the usual ordering.*

We accept the well-ordering principle. In fact, much more is true:

Theorem 20.11. *The well-ordering principle and the principle of mathematical induction are equivalent.*

Proof. We first check that the well-ordering principle implies the principle of mathematical induction.

Let $P(n)$ be a statement about the natural numbers, such that

(1) $P(0)$ holds.
(2) If $P(n)$ holds then $P(n+1)$ holds.

We have to check that $P(n)$ holds for all natural numbers. Let

$$A = \{\, n \in \mathbb{N} \mid P(n) \text{ does not hold} \,\}.$$

Suppose A is not empty. By the well-ordering principle, A contains a minimal element m. $m \neq 0$ as $P(0)$ holds by assumption. Thus $m = n + 1$, for some natural number n. As $n < m$, and m is the smallest element of A, $n \notin A$, so that $P(n)$ holds. Therefore $P(n+1)$ holds. Therefore $P(m)$ holds. Therefore $m \notin A$, a contradiction.

Thus A is empty and so $P(n)$ holds for every n. Thus the well-ordering principle implies the principle of mathematical induction.

Now we check the other direction. We suppose that the principle of mathematical induction holds and we need to check the well-ordering principle holds.

Let $P(n)$ be the statement that if $A \subset \mathbb{N}$ contains $m \leq n$ then A contains a minimal element. We want to prove that $P(n)$ holds for all natural numbers n.

Suppose that $n = 0$. Then A contains a natural number $m \leq 0$. In this case $m = 0$ and m is clearly a minimal element of A. Thus $P(0)$ holds.

Suppose that $P(k)$ holds. We check that $P(k+1)$ holds. Suppose that $A \subset \mathbb{N}$ contains $m \leq k+1$. There are two cases. Suppose that $m \leq k$. As $P(k)$ holds, it follows that A contains a minimal element. Otherwise $m = k+1$. If there is no smaller element of A then m is the minimal element. If there is a smaller element l then $l < m \leq k+1$ so that $l \leq k$. As $P(k)$ holds, A contains a minimal element.

As we checked that $P(0)$ holds and that $P(k) \implies P(k+1)$ for every integer k, it follows that $P(n)$ holds for every n, by the principle of mathematical induction.

Let $A \subset \mathbb{N}$ be a non-empty subset. Then A contains a natural number n. As $P(n)$ holds, A contains a minimal element. Thus the principle of mathematical induction implies the well-ordering principle. $\square$

One can use (20.11) in practice. Instead of checking the hypothesis of mathematical induction sometimes it is more straightforward to consider a putative minimal counterexample and show it cannot exist.

It is interesting to consider which sets admit well-orderings. For example, consider the rational numbers. The rational numbers with the usual ordering is not a well-ordered set. Indeed,

$$\mathbb{Z} \subset \mathbb{Q}$$

does not contain a minimal element. It is more interesting to consider the non-negative rational numbers, but even this set is not well-ordered. Consider the set

$$(0, 1) \cap \mathbb{Q}.$$

This contains the numbers

$$1/2 \quad 1/3 \quad 1/4 \quad 1/5 \dots.$$

The infimum is zero but this is not an element of the set. So there is no minimal element.

On the other hand, the rationals are countable. The natural numbers are well-ordered under the usual ordering and we can transfer this ordering to the rational numbers, to get a well-ordering of the rational numbers.

In fact the problem of putting a well-ordering on a set, just depends on the cardinality of the set.

Axiom 20.12. *Every set can be well-ordered.*

In fact (20.12) is equivalent to the axiom of choice. Even finding a well-ordering of the reals seems hard.

Definition 20.13. *An* ***ordinal*** α *is a set whose elements are well-ordered by the relation*

$$x < y \qquad \textit{if and only if} \qquad x \in y.$$

Any natural number, considered as a set, is an ordinal. The set of all natural numbers, ω, is an ordinal. It is not hard to check two things. If α is an ordinal then so is α^+. The union of a set of ordinals, is an ordinal. It is natural to defined

$$\beta = \alpha + 1 = \alpha^+.$$

We call β a successor ordinal. By contrast ω is the union of all natural numbers. It is easy to see that ω is not a successor ordinal. We call any ordinal which is not a successor ordinal, a limite ordinal. Note that

$$\omega = \{ 0, 1, 2, 3, \dots, \}.$$

By contrast

$$\omega + 1 = \omega^+ = \{ 0, 1, 2, 3, \dots, \omega \}.$$

Clearly there is no reason to stop there,

$$\omega + 2 = (\omega + 1)^+ = \{ 0, 1, 2, 3, \dots, \omega, \omega + 1 \}.$$

It is interesting to note that

$$1 + \omega = \omega.$$

If you put 1 at the beginning then you don't change the ordinal type.

In general, we can construct $\omega + n$, for all natural numbers n. If we take the limit of all of these numbers we get a new limit ordinal

$$\omega 2 = \bigcup_{n \in \mathbb{N}} \omega + n.$$

As a set

$$\omega 2 = \{ 0, 1, 2, 3, \dots, \omega, \omega + 1, \omega + 2, \dots \}$$

Note that $2\omega = \omega$ has the same ordering type as ω.

We can keep going from here. We can construct

$$\omega 3, \omega 4, \dots, \omega n.$$

Taking the union we get

$$\omega^2 = \omega\omega.$$

We can keep going from here. We can construct

$$\omega^2, \omega^3, \omega^4, \dots, \omega^n.$$

Taking the union we get

$$\omega^\omega.$$

We can keep going from here. We can construct

$$\omega^\omega, \omega^{\omega^\omega}, \dots.$$

Taking the union we get

$$\omega^{\omega^{\omega^{\cdots}}}$$

Note that all of the infinite ordinals we have constructed so far are countable. If we look at the set of all countable ordinals, this is a new ordinal

$$\omega_1 = \{ \alpha \,|\, \alpha \text{ is a countable ordinal} \}.$$

ω_1 is not countable (by the axiom of foundation; if it were it would be an element of itself). The corresponding cardinal is called

$$\aleph_1.$$

In fact there is no reason to stop here. Given an ordinal α it is possible to construct

$$\omega_\alpha.$$

If $\alpha = \beta + 1$ is a successor ordinal then it is the set of all ordinals whose cardinality is the same as β,

$$\omega_\alpha = \{ \gamma \,|\, \gamma \text{ has cardinality } \aleph_\beta \}.$$

The axiom of choice says that every cardinal arises in this way.

Conjecture 20.14 (Generalised Continuum hypothesis)**.** *There are no cadinals*

$$\aleph_{\alpha+1} = 2^{\aleph_\alpha}.$$

Around sixty years after Cantor made this conjecture, the following was proved:

Theorem 20.15 (Kurt Gödel)**.** *There is a model of set theory in which the generalised continuum hypothesis is true.*

Theorem 20.16. *Let α be a successor ordinal.*

There is a model of set theory in which

$$2^{\aleph_0} = \aleph_\alpha$$

In other words, not only does the continuum hypothesis fail, it fails in every conceivable fashion.