Chapter 5
The Axiom of Choice

Two terms occasionally used by musicians are "full" consonance and "pleasing" consonance. An interval is said to be "fuller" than another when it has greater power to satisfy the ear. Consonances are the more "pleasing" as they depart from simplicity, which does not delight our senses much.

GIOSEFFO ZARLINO
Le Istitutioni Harmoniche, 1558

Zermelo's Axiom of Choice and Its Consistency with ZF

In 1904, Zermelo published his first proof that every set can be well-ordered. The proof is based on the so-called Axiom of Choice, denoted AC, which, in Zermelo's words, states that *the product of an infinite totality of sets, each containing at least one element, itself differs from zero* (*i.e.*, the empty set). The full theory ZF + AC, denoted ZFC, is called *Set Theory*.

In order to state the Axiom of Choice we first define the notion of a choice function: If $\mathscr{F}$ is a family of non-empty sets (*i.e.*, $\emptyset \notin \mathscr{F}$), then a **choice function** for $\mathscr{F}$ is a function $f : \mathscr{F} \to \bigcup \mathscr{F}$ such that for each $x \in \mathscr{F}$, $f(x) \in x$.

The Axiom of Choice—which completes the axiom system of Set Theory and which is in our counting the ninth axiom of ZFC—states as follows:

9. The Axiom of Choice

$$\forall \mathscr{F}\Big(\emptyset \notin \mathscr{F} \to \exists f\Big(f \in {}^{\mathscr{F}}\bigcup \mathscr{F} \wedge \forall x \in \mathscr{F}\big(f(x) \in x\big)\Big)\Big).$$

Informally, every family of non-empty sets has a choice function, or equivalently, every Cartesian product of non-empty sets is non-empty.

Before we give some reformulations of the Axiom of Choice and show some of its consequences, we should address the question whether AC is consistent relative to the other axioms of Set Theory (*i.e.*, relative to ZF), which is indeed the case.

L.J. Halbeisen, *Combinatorial Set Theory*, Springer Monographs in Mathematics,
DOI 10.1007/978-1-4471-2173-2_5,

Assume that ZF is consistent, then, by PROPOSITION 3.5, ZF has a model, say $\mathbf{V}$. To obtain the relative consistency of AC with ZF, we have to show that also ZF + AC has a model. In 1935, Gödel informed von Neumann at the Institute for Advanced Study in Princeton that he had found such a model. In fact he showed that there exists a smallest transitive subclass of $\mathbf{V}$ which contains all ordinals (*i.e.*, contains Ω as a subclass) in which AC as well as ZF holds. This unique submodel of $\mathbf{V}$ is called the **constructible universe** and is denoted by $\mathbf{L}$, where "L" stands for the following "law" by which the constructible universe is built. Roughly speaking, the model $\mathbf{L}$ consists of all "mathematically constructible" sets, or in other words, all sets which are "constructible" or "describable", but nothing else. To be more precise, let us give the following definitions:

Let M be a set and $\varphi(x_0,\dots,x_n)$ be a first-order formula in the language $\{\in\}$. Then φ^M denotes the formula we obtain by replacing all occurrences of "$\exists x$" and "$\forall x$" by "$\exists x \in M$" and "$\forall x \in M$", respectively. A subset $y \subseteq M$ is **definable over** M if there is a first-order formula $\varphi(x_0,\dots,x_n)$ in the language $\{\in\}$, and parameters $a_1,\dots,a_n$ in M, such that $\{z : \varphi^M(z,a_1,\dots,a_n)\} = y$. Finally, for any set M:

$$\operatorname{def}(M) = \{y \subseteq M : y \text{ is definable over } M\}.$$

Notice that for any set M, $\operatorname{def}(M)$ is a set being itself a subset of $\mathscr{P}(M)$. Now, by induction on $\alpha \in \Omega$, define the following sets (compare with the cumulative hierarchy defined in Chapter 3):

$$\begin{aligned}
\mathrm{L}_0 &= \emptyset, \\
\mathrm{L}_\alpha &= \bigcup_{\beta\in\alpha} \mathrm{L}_\beta \quad \text{if } \alpha \text{ is a limit ordinal,} \\
\mathrm{L}_{\alpha+1} &= \operatorname{def}(\mathrm{L}_\alpha)
\end{aligned}$$

and let

$$\mathbf{L} = \bigcup_{\alpha\in\Omega} \mathrm{L}_\alpha .$$

Like for the cumulative hierarchy one can show that for each $\alpha \in \Omega$, L_α is a transitive set, $\alpha \subseteq \mathrm{L}_\alpha$ and $\alpha \in \mathrm{L}_{\alpha+1}$, and that $\alpha \in \beta$ implies $\mathrm{L}_\alpha \subsetneq \mathrm{L}_\beta$.

Moreover, Gödel showed that $\mathbf{L} \vDash \mathsf{ZF} + \mathsf{AC}$, and that $\mathbf{L}$ is the smallest transitive class containing Ω as a subclass such that $\mathbf{L} \vDash \mathsf{ZFC}$. Thus, by starting with any model $\mathbf{V}$ of ZF we find a subclass $\mathbf{L}$ of $\mathbf{V}$ such that $\mathbf{L} \vDash \mathsf{ZFC}$. In other words we find that if ZF is consistent then so is ZFC (roughly speaking, if ZFC is inconsistent, then AC cannot be blamed for it).

Equivalent Forms of the Axiom of Choice

There are dozens of hypotheses which are equivalent to the Axiom of Choice, but among the best known and most popular ones are surely the Well-Ordering Principle, the Kuratowski–Zorn Lemma, Kurepa's Principle, and Teichmüller's Principle—sometimes called Tukey's Lemma. Since the first three deal with orderings, we have to introduce first the corresponding definitions before we can state these—and some other—so-called *choice principles*.

A binary relation "$\leq$" on a set P is a **partial ordering** of P if it is transitive (*i.e.*, $p \leq q$ and $q \leq r$ implies $p \leq r$), reflexive (*i.e.*, $p \leq p$ for every $p \in P$), and anti-symmetric (*i.e.*, $p \leq q$ and $q \leq p$ implies $p = q$). If "$\leq$" is a partial ordering on P, then $(P, \leq)$ is called a **partially ordered set**.

If $(P, \leq)$ is a partially ordered set, then we define

$$p < q \quad \iff \quad p \leq q \wedge p \neq q,$$

and call $(P, <)$ a partially ordered in the **strict sense** (replacing reflexivity by $p \not< p$ for every $p \in P$).

Two distinct elements $p, q \in P$, where $(P, <)$ is a partially ordered set, are said to be **comparable** if either $p < q$ or $q < p$; otherwise, they are called **incomparable**. Notice that for $p, q \in P$ we could have $p \not\leq q$ as well as $p \not\geq q$. However, if for any elements p and q of a partially ordered set $(P, <)$ we have $p < q$ or $p = q$ or $p > q$ (where these three cases are mutually exclusive), then P is said to be **linearly ordered** by the **linear ordering** "$<$". Two elements p_1 and p_2 of P are called **compatible** if there exists a $q \in P$ such that $p_1 \leq q \geq p_2$; otherwise they are called **incompatible**, denoted $p_1 \perp p_2$.

We would like to mention that in the context of forcing, elements of partially ordered sets are called *conditions*. Furthermore, it is worth mentioning that the definition of "compatible" given above incorporates a convention, namely the so-called *Jerusalem convention for forcing*—with respect to the American convention of forcing, p_1 and p_2 are compatible if there exists a q such that $p_1 \geq q \leq p_2$.

Let $(P, <)$ be a partially ordered set. Then $p \in P$ is called **maximal** (or more precisely $<$-maximal) in P if there is no $x \in P$ such that $p < x$. Similarly, $q \in P$ is called **minimal** (or more precisely $<$-minimal) in P if there is no $x \in P$ such that $x < q$. Furthermore, for a non-empty subset $C \subseteq P$, an element $p' \in P$ is said to be an **upper bound** of C if for all $x \in C$, $x \leq p'$.

A non-empty set $C \subseteq P$, where $(P, <)$ is a partially ordered set, is a **chain** in P if C is linearly ordered by "$<$" (*i.e.*, for any distinct members $p, q \in C$ we have either $p < q$ or $p > q$). Conversely, if $A \subseteq P$ is such that any two distinct elements of A are incomparable (*i.e.*, neither $p < q$ nor $p > q$), then in Order Theory, A is called an anti-chain. However, in the context of forcing we say that a subset $A \subseteq P$ is an **anti-chain** in P if any two distinct elements of A are *incompatible*. Furthermore, $A \subseteq P$ is a **maximal anti-chain** in P if A is an anti-chain in P and A is maximal with this property. Notice that if $A \subseteq P$ is a maximal anti-chain, then for every $p \in P \setminus A$ there is a $q \in A$ such p and q are compatible.

Recall that a binary relation R on a set P is a *well-ordering* on P, if there is an ordinal $\alpha \in \Omega$ and a bijection $f : P \to \alpha$ such that $R(x, y)$ *iff* $f(x) \in f(y)$. This leads to the following equivalent definition of a well-ordering, where the equivalence follows from the proof of THEOREM 5.1 (the details are left to the reader): Let $(P, <)$ be a linearly ordered set. Then "$<$" is a **well-ordering** on P if every non-empty subset of P has a $<$-minimal element. Furthermore, a set P is said to be **well-orderable** (or equivalently, P can be well-ordered) if there exists a well-ordering on P.

In general, it is not possible to define a well-ordering by a first-order formula on a given set (*e.g.*, on $\mathbb{R}$). However, the existence of well-ordering is guaranteed by the following principle:

Well-Ordering Principle. Every set can be well-ordered.

To some extent, the Well-Ordering Principle—like the Axiom of Choice—postulates the existence of certain sets whose existence in general (*i.e.*, without any further assumptions like $\mathbf{V} = \mathbf{L}$), cannot be proved within ZF.

In particular, the Well-Ordering Principle postulates the existence of well-orderings of $\mathbb{Q}$ and of $\mathbb{R}$. Obviously, both sets are linearly ordered by "$<$". However, since for any elements x and y with $x < y$ there exists a z such that $x < z < y$, the ordering "$<$" is far away from being a well-ordering—consider for example the set of all positive elements. Even though $(\mathbb{Q}, <)$ and $(\mathbb{R}, <)$ have similar properties (at least from an order-theoretical point of view), when we try to well-order these sets they behave very differently. Firstly, by FACT 4.1 we know that $\mathbb{Q}$ is countable and the bijection $f : \mathbb{Q} \to \omega$ allows us to define a well-ordering "$\prec$" on $\mathbb{Q}$ by stipulating $q \prec p \iff f(q) < f(p)$. Now, let us consider the set $\mathbb{R}$. For example we could first well-order the rational numbers, or even the algebraic numbers, and then try to extend this well-ordering to all real numbers. However, this attempt—as well as all other attempts—to construct explicitly a well-ordering of the reals will end in failure (the reader is invited to verify this claim by writing down explicitly some orderings of $\mathbb{R}$).

As mentioned above, Zermelo proved in 1904 that the Axiom of Choice implies the Well-Ordering Principle. In the proof of this result presented here we shall use the ideas of Zermelo's original proof.

THEOREM 5.1. *The* Well-Ordering Principle *is equivalent to the* Axiom of Choice.

Proof. ($\Leftarrow$) Let M be a set. If $M = \emptyset$, then M is already well-ordered. So, assume that $M \neq \emptyset$ and let $\mathscr{P}^*(M) := \mathscr{P}(M) \setminus \{\emptyset\}$. Further, let $f : \mathscr{P}^*(M) \to M$ be an arbitrary but fixed choice function for $\mathscr{P}^*(M)$ (which exists by AC).

A one-to-one function $w_\alpha : \alpha \hookrightarrow M$, where $\alpha \in \Omega$, is an f-set if for all $\gamma \in \alpha$:

$$w_\alpha(\gamma) = f\big(M \setminus \{w_\alpha(\delta) : \delta \in \gamma\}\big).$$

For example $w_1(0) = f(M)$ is an f-set, in fact, w_1 is the unique f-set with domain $\{0\}$. Further, by HARTOGS' THEOREM 3.27, the collection of all f-sets is a *set*, say S. Define the ordering "$\prec$" on S as follows: For two distinct f-sets w_α and w_β let $w_\alpha \prec w_\beta$ if $\alpha \neq \beta$ and $w_\beta|_\alpha = w_\alpha$. Notice that $w_\alpha \prec w_\beta$ implies $\alpha \in \beta$.

CLAIM. *The set S of all f-sets is well-ordered by "$\prec$".*

Proof of Claim. Let w_α and w_β be any two f-sets and let

$$\Gamma = \big\{\gamma \in (\alpha \cap \beta) : w_\alpha(\gamma) \neq w_\beta(\gamma)\big\}.$$

If $\Gamma \neq \emptyset$, then, for $\gamma_0 = \bigcap \Gamma$, we have $w_\alpha(\gamma_0) \neq w_\beta(\gamma_0)$. On the other hand, for all $\delta \in \gamma_0$ we have $w_\alpha(\delta) = w_\beta(\delta)$, thus, by the definition of f-sets, we get $w_\alpha(\gamma_0) = w_\beta(\gamma_0)$. Hence, $\Gamma = \emptyset$, and consequently we are in exactly one of the following three cases:

- $w_\alpha \prec w_\beta$ *iff* $\alpha \in \beta$.
- $w_\alpha = w_\beta$ *iff* $\alpha = \beta$.
- $w_\beta \prec w_\alpha$ *iff* $\beta \in \alpha$.

Thus, the ordering "$\prec$" on S corresponds to the ordering of the ordinals by "$\in$", and since the latter relation is a well-ordering on Ω, the ordering "$\prec$" is a well-ordering, too. $\dashv_{\text{Claim}}$

Now, let $w := \bigcup S$ and let $M' := \{x \in M : \exists \gamma \in \mathrm{dom}(w)(w(\gamma) = x)\}$. Then $w \in S$ and $M' = M$; otherwise, w can be extended to the f-set

$$w \cup \left\{\left\langle \mathrm{dom}(w), f(M \setminus M')\right\rangle\right\}.$$

Thus, the one-to-one function $w : \mathrm{dom}(w) \to M$ is onto, or in other words, M is well-orderable.

($\Rightarrow$) Let $\mathscr{F}$ be any family of non-empty sets and let "$<$" be any well-ordering on $\bigcup \mathscr{F}$. Define $f : \mathscr{F} \to \bigcup \mathscr{F}$ by stipulating $f(x)$ being the $<$-minimal element of x. $\dashv$

It turns out that in many cases, the Well-Ordering Principle—mostly in combination with transfinite induction—is easier to apply than the Axiom of Choice. For example in order to prove that every vector space has an algebraic basis, we would first well-order the set of vectors and then build a basis by transfinite induction (*i.e.*, for every vector v_α we check whether it is in the linear span of the vectors $\{v_\beta : \beta \in \alpha\}$, and if it is not, we mark it as a vector of the basis). However, similarly to the well-ordering of $\mathbb{R}$, in many cases it is not possible to write down explicitly an algebraic basis of a vector space. For example consider the real vector space of all countably infinite sequences of real numbers, or any infinite dimensional Banach space.

The following three principles, which will be shown to be equivalent to the Axiom of Choice, are quite popular in Algebra and Topology. Even though these principles look rather different, all state that certain sets have maximal elements or subsets (with respect to some partial ordering), and so they are usually called *maximality principles*. Let us first state the Kuratowski–Zorn Lemma and Kurepa's Principle.

Kuratowski–Zorn Lemma. If $(P, \leq)$ is a non-empty partially ordered set such that every chain in P has an upper bound, then P has a maximal element.

Kurepa's Principle. Each partially ordered set has a maximal subset of pairwise incomparable elements.

In order to state Teichmüller's Principle we have to introduce one more notion: A family $\mathscr{F}$ of sets is said to have **finite character** if for each set x, $x \in \mathscr{F}$ *iff* $\operatorname{fin}(x) \subseteq \mathscr{F}$ (*i.e.*, every finite subset of x belongs to $\mathscr{F}$).

Teichmüller's Principle. Let $\mathscr{F}$ be a non-empty family of sets. If $\mathscr{F}$ has finite character, then $\mathscr{F}$ has a maximal element (maximal with respect to inclusion "$\subseteq$").

Below we shall see that the three maximality principles are all equivalent to the Axiom of Choice. However, in order to prove directly that the Axiom of Choice implies the Kuratowski–Zorn Lemma (*i.e.*, without using the Well-Ordering Principle), we have to show first the following interesting lemma—whose proof does not rely on any choice principles.

LEMMA 5.2. *Let $(P, \leq)$ be a non-empty partially ordered set. If there is a function $b : \mathscr{P}(P) \to P$ which assigns to every chain C an upper bound $b(C)$, and if $f : P \to P$ is a function such that for all $x \in P$ we have $x \leq f(x)$, then there is a $p_0 \in P$ such that $p_0 = f(p_0)$.*

Proof. Notice that because every well-ordered set is a chain, it is enough to require the existence of an upper bound $b(W)$ just for every set $W \subseteq P$ which is *well-ordered* by "$<$". If $W \subseteq P$ is a well-ordered subset of P and $x \in W$, then $W_x := \{y \in W : y < x\}$. A well-ordered set $W \subseteq P$ is called an f-chain, if for all $x \in W$ we have $x = f(b(W_x))$. Notice that since $\emptyset \subseteq P$ is well-ordered by "$<$", the set $\{f(b(\emptyset))\}$ is an f-chain.

We leave it as an exercise to the reader to verify that the set of f-chains is well-ordered by proper inclusion "$\subsetneq$". Hence, the set

$$U = \bigcup \bigl\{W \subseteq P : W \text{ is an } f\text{-chain}\bigr\}$$

is itself an f-chain. Consider $p_0 := f(b(U))$ and notice that $U \cup \{p_0\}$ is an f-chain. By the definition of U we find that $p_0 \in U$, and consequently we have $f(b(U_{p_0})) = p_0$. Now, since $f(b(U_{p_0})) \geq b(U_{p_0}) \geq p_0$, we must have $b(U_{p_0}) = p_0$, and therefore $f(p_0) = p_0$. ⊣

Now we are ready to prove that the Kuratowski–Zorn Lemma and Teichmüller's Principle are both equivalent to the Axiom of Choice.

THEOREM 5.3. *The following statements are equivalent:*

(a) Axiom of Choice.
(b) Kuratowski–Zorn Lemma.
(c) Teichmüller's Principle.

Proof. (a) ⇒ (b) Let $(P, \leq)$ be a non-empty partially ordered set such that every chain in P, (in particular every well-ordered chain), has an upper bound. Then, for every non-empty well-ordered subset $W \subseteq P$, the set of upper bounds $B_W := \{p \in P : \forall x \in W(x \leq p)\}$ is non-empty. Thus, the family

$$\mathscr{F} = \{B_W : W \text{ is a well-ordered, non-empty subset of } P\}$$

is a family of non-empty sets and therefore, by the Axiom of Choice, for each $W \in \mathscr{F}$ we can pick an element $b(W) \in B_W$. Now, for every $x \in P$ let

$$M_x = \begin{cases} \{x\} & \text{if } x \text{ is maximal in } P, \\ \{y \in P : y > x\} & \text{otherwise.} \end{cases}$$

Then $\{M_x : x \in P\}$ is a family of non-empty sets and again by the Axiom of Choice, there is a function $f : P \to P$ such that

$$f(x) = \begin{cases} x & \text{if } x \text{ is maximal in } P, \\ y & \text{where } y > x. \end{cases}$$

Since $f(x) \geq x$ (for all $x \in P$) and every non-empty well-ordered subset $W \subseteq P$ has an upper bound $b(W)$, we can apply LEMMA 5.2 and get an element $p_0 \in P$ such that $f(p_0) = p_0$, hence, P has a maximal element.

(b) ⇒ (c) Let $\mathscr{F}$ be a non-empty family of sets and assume that $\mathscr{F}$ has finite character. Obviously, $\mathscr{F}$ is partially ordered by inclusion "$\subseteq$". For every chain $\mathscr{C}$ in $\mathscr{F}$ let $U_{\mathscr{C}} = \bigcup \mathscr{C}$. Then every finite subset of $U_{\mathscr{C}}$ belongs to $\mathscr{F}$, thus, $U_{\mathscr{C}}$ belongs to $\mathscr{F}$. On the other hand, $U_{\mathscr{C}}$ is obviously an upper bound of $\mathscr{C}$. Hence, every chain has an upper bound and we may apply the Kuratowski–Zorn Lemma and get a maximal element of the family $\mathscr{F}$.

(c) ⇒ (a) Given a family $\mathscr{F}$ of non-empty sets. We have to find a choice function for $\mathscr{F}$. Consider the family

$$\mathscr{E} = \{f : f \text{ is a choice function for some subfamily } \mathscr{F}' \subseteq \mathscr{F}\}.$$

Notice that f is a choice function if and only if every finite subfunction of f is a choice function. Hence, $\mathscr{E}$ has finite character. Thus, by Teichmüller's Principle, the family $\mathscr{E}$ has a maximal element, say f_0. Since f_0 is maximal, $\text{dom}(f_0) = \mathscr{F}$, and therefore f_0 is a choice function for $\mathscr{F}$. ⊣

In order to prove that also Kurepa's Principle is equivalent to the Axiom of Choice, we have to change the setting a little bit: In the proof of THEOREM 5.3, as well as in Zermelo's proof of THEOREM 5.1, the Axiom of Foundation was not involved (in fact, the proofs can be carried out in Cantor's Set Theory). However, without the aid of the Axiom of Foundation it is not possible to prove that Kurepa's Principle implies the Axiom of Choice, whereas the converse implication is evident (compare the following theorem with Chapter 7 | RELATED RESULT 46).

THEOREM 5.4. *The following statements are equivalent in* ZF*:*

(a) Axiom of Choice.
(b) *Every vector space has an algebraic basis.*

(c) Multiple Choice*: For every family* $\mathscr{F}$ *of non-empty sets, there exists a function* $f : \mathscr{F} \to \mathscr{P}(\bigcup \mathscr{F})$ *such that for each* $X \in \mathscr{F}$, $f(X)$ *is a non-empty finite subset of* X.
(d) Kurepa's Principle.

Proof. (a) $\Rightarrow$ (b) Let V be a vector space and let $\mathscr{F}$ be the family of all sets of linearly independent vectors of V. Obviously, $\mathscr{F}$ has finite character. So, by Teichmüller's Principle, which is, as we have seen in THEOREM 5.3 equivalent to the Axiom of Choice, $\mathscr{F}$ has a maximal element. In other words, there is a maximal set of linearly independent vectors, which must be of course a basis of V.

(b) $\Rightarrow$ (c) Let $\mathscr{F} = \{X_\iota : \iota \in I\}$ be a family of non-empty sets. We have to construct a function $f : \mathscr{F} \to \mathscr{P}(\bigcup \mathscr{F})$ such that for each $X_\iota \in \mathscr{F}$, $f(X_\iota)$ is a non-empty finite subset of X_ι. Without loss of generality we may assume that the members of $\mathscr{F}$ are pairwise disjoint (if necessary, consider the family $\{X_\iota \times \{X_\iota\} : \iota \in I\}$ instead of $\mathscr{F}$). Adjoin all the elements of $X := \bigcup \mathscr{F}$ as indeterminates to some arbitrary but fixed field $\mathbb{F}$ (*e.g.*, $\mathbb{F} = \mathbb{Q}$) and consider the field $\mathbb{F}(X)$ consisting of all rational functions of the "variables" in X with coefficients in $\mathbb{F}$. For each $\iota \in I$, we define the ι*-degree* of a monomial—*i.e.*, a term of the form $ax_1^{k_1} \cdots x_l^{k_l}$ where $a \in \mathbb{F}$ and $x_1, \ldots, x_l \in X$—to be the sum of the exponents of members of X_ι in that monomial. A rational function $q \in \mathbb{F}(X)$ is called ι*-homogeneous of degree* d if it is the quotient of two polynomials such that all monomials in the denominator have the same ι-degree n, while all those in the numerator have ι-degree $n + d$. The rational functions that are ι-homogeneous of degree 0 for all $\iota \in I$ form a subfield $\mathbb{F}_0$ of $\mathbb{F}(X)$. Thus, $\mathbb{F}(X)$ is a vector space over $\mathbb{F}_0$, and we let V be the subspace spanned by the set X.

By assumption, the $\mathbb{F}_0$-vector space V has an algebraic basis, say B. Below we use this basis B to explicitly define the desired function $f : \mathscr{F} \to \mathscr{P}(\bigcup \mathscr{F})$. For each $\iota \in I$ and each $x \in X_\iota$ we can express x as a finite linear combination of elements of B. Thus, every $x \in X_\iota$ can be written in the form

$$x = \sum_{b \in B(x)} a_b^x \cdot b,$$

where $B(x) \in \mathit{fin}(B)$ and for all $b \in B(x)$, $a_b^x \in \mathbb{F}_0 \setminus \{0\}$. If y is another element of the same X_ι as x, then we have on the one hand

$$y = \sum_{b' \in B(y)} a_{b'}^y \cdot b',$$

and on the other hand, after multiplying the above representation of x by the element $\frac{y}{x} \in \mathbb{F}_0$, we get

$$y = \sum_{b \in B(x)} \left(\tfrac{y}{x} \cdot a_b^x\right) \cdot b.$$

Comparing these two expressions for y and using the fact that B is a basis, *i.e.*, that the representation of y is unique, we must have

$$B(x) = B(y) \quad \text{and} \quad a_b^y = \tfrac{y}{x} \cdot a_b^x \quad \text{for all } b \in B(x).$$

Hence, the *finite* subset $B(x)$ of B as well as the elements $\frac{a_b^x}{x}$ of $\mathbb{F}(X)$ depend only on ι, not on the particular $x \in X_\iota$, and we therefore call them B_ι and a_b^ι, respectively. Notice that, since $a_b^x \in \mathbb{F}_0$, a_b^ι is ι-homogeneous of degree -1 (and ι'-homogeneous of degree 0 for $\iota' \neq \iota$). So, when a_b^ι is written as a quotient of polynomials in reduced form, some variables from X_ι must occur in the denominator. Define $f(X_\iota)$ to be the set of all those members of X_ι that occur in the denominator of a_b^ι (in reduced form) for some $b \in B_\iota$. Then $f(X_\iota)$ is a non-empty finite subset of X_ι, as required.

(c) $\Rightarrow$ (d) Let $(P, <)$ be a partially ordered set. By Multiple Choice, there is a function f such that for each non-empty set $X \subseteq P$, $f(X)$ is a non-empty finite subset of X. Let $g : \mathscr{P}(P) \to \mathit{fin}(P)$ be such that $g(\emptyset) := \emptyset$ and for each non-empty $X \subseteq P$, $g(X) := \{y \in f(X) : y \text{ is } <\text{-minimal in } f(X)\}$. Obviously, for every non-empty $X \subseteq P$, $g(X)$ is a non-empty finite set of pairwise incomparable elements. Using the function g we construct by transfinite induction a maximal subset of pairwise incomparable elements: Let $\mathscr{A}_0 := g(P)$, and for $\alpha \in \Omega$ let $\mathscr{A}_\alpha := g(X_\alpha)$, where

$$X_\alpha := \left\{x \in P : x \text{ is incomparable with each } a \in \bigcup\{\mathscr{A}_\beta : \beta \in \alpha\}\right\}.$$

By construction, the $\mathscr{A}_\alpha$'s are pairwise disjoint and any union of $\mathscr{A}_\alpha$'s is a set of pairwise incomparable elements. Again by construction there must be an $\alpha_0 \in \Omega$ such that $X_{\alpha_0} = \emptyset$. Thus, $\bigcup\{\mathscr{A}_\beta : \beta \in \alpha_0\} \subseteq P$ is a maximal set of pairwise incomparable elements.

(d) $\Rightarrow$ (a) By the Axiom of Foundation, for every set x there exists an ordinal $\alpha \in \Omega$ such that $x \subseteq \mathrm{V}_\alpha$. Thus, since the Axiom of Choice is equivalent to the Well-Ordering Principle (see THEOREM 5.1), it is enough to show that Kurepa's Principle implies that for every $\alpha \in \Omega$, V_α can be well-ordered. The crucial point in that proof is to show that power sets of well-orderable sets are well-orderable.

The first step is quite straightforward: Let Q be a well-orderable set and let "$<_Q$" be a well-ordering on Q. We define a linear ordering "$\prec$" on $\mathscr{P}(Q)$ by stipulating $x \prec y$ *iff* the $<_Q$-minimal element of the symmetric difference $x \triangle y$ belongs to x. To see that "$\prec$" is a linear ordering, notice that "$\prec$" is just the lexicographic ordering on $\mathscr{P}(Q)$ induced by "$<_Q$". The following claim is where Kurepa's Principle comes in.

CLAIM. Kurepa's Principle *implies that linearly orderable sets are well-orderable.*

Proof of Claim. Let $(P, \prec)$ be a linearly ordered set. Consider the set W of all pairs (X, x) where $X \subseteq P$ and $x \in X$. On W we define a partial ordering "$<$" by stipulating

$$(X, x) < (Y, y) \quad \iff \quad X = Y \wedge x \prec y.$$

By Kurepa's Principle, $(W, <)$ has a maximal set of pairwise incomparable elements, say $\mathscr{A} \subseteq W$. For every non-empty set $X \subseteq P$ let $f(X)$ be the unique element of X such that $(X, f(X)) \in \mathscr{A}$. It is not hard to verify that f is a choice function for $\mathscr{P}(P) \setminus \{\emptyset\}$, and consequently, P can be well-ordered. $\dashv_{\text{Claim}}$

Now we are ready to show that Kurepa's Principle implies that every set V_α ($\alpha \in \Omega$) can be well-ordered. We consider the following two cases:

α successor ordinal: Let $\alpha = \beta_0 + 1$ and assume that V_{β_0} is well-orderable. Then $\mathrm{V}_\alpha = \mathscr{P}(\mathrm{V}_{\beta_0})$, and as the power set of a well-orderable set, V_α is well-orderable.

α limit ordinal: Assume that for each $\beta \in \alpha$, V_β is well-orderable, *i.e.*, for each $\beta \in \alpha$ there exists a well-ordering "$<_\beta$" on V_β. Let ξ be the least ordinal such that there is no injection from ξ into V_α. The ordinal ξ exists by HARTOGS' THEOREM 3.27 and since every V_β can be well-ordered. Since ξ is well-ordered by $\in$, $\mathscr{P}(\xi)$ can be well-ordered; let us fix a well-ordering $\prec_\xi \subseteq (\mathscr{P}(\xi) \times \mathscr{P}(\xi))$. For every $\beta \in \alpha$ we choose a well-ordering "$<_\beta$" on V_β as follows:

- If $\beta = 0$, then $<_0 = \emptyset$.
- If $\beta = \bigcup_{\delta \in \beta} \delta$ is a limit ordinal, then, for $x, y \in \mathrm{V}_\beta$, let
$$x <_\beta y \iff \rho(x) \in \rho(y) \vee \big(\rho(x) = \rho(y) \wedge x <_{\rho(x)} y\big),$$
where for any z, $\rho(z) := \bigcap\{\gamma \in \Omega : x \in \mathrm{V}_\gamma\}$.
- If $\beta = \delta + 1$ is a successor ordinal, then, by the choice of ξ, there is an injection $f : \mathrm{V}_\delta \hookrightarrow \xi$. Let $x = \mathrm{ran}(f)$; then $x \subseteq \xi$. Further, there exists a bijection between $\mathscr{P}(\mathrm{V}_\delta) = \mathrm{V}_\beta$ and $\mathscr{P}(x)$, and since $\mathscr{P}(x) \subseteq \mathscr{P}(\xi)$ and $\mathscr{P}(\xi)$ is well-ordered by "$\prec_\xi$", the restriction of "$\prec_\xi$" to $\mathscr{P}(x)$ induces a well-ordering on V_β.

Thus, for every $\beta \in \alpha$ we have a well-ordering "$<_\beta$" on V_β. Now, for $x, y \in \mathrm{V}_\alpha$ define
$$x <_\alpha y \iff \rho(x) \in \rho(y) \vee \big(\rho(x) = \rho(y) \wedge x <_{\rho(x)} y\big).$$
Then, by construction, "$<_\alpha$" is a well-ordering on V_α. ⊣

We conclude this section on equivalent forms of AC by giving three cardinal relations which are equivalent to the Well-Ordering Principle.

THEOREM 5.5. *Each of the following statements is equivalent to the* Well-Ordering Principle, *and consequently to the* Axiom of Choice*:*

(a) *Every cardinal $\mathfrak{m}$ is an aleph, i.e., contains a well-orderable set.*
(b) Trichotomy of Cardinals*: If $\mathfrak{n}$ and $\mathfrak{m}$ are any cardinals, then $\mathfrak{n} < \mathfrak{m}$ or $\mathfrak{n} = \mathfrak{m}$ or $\mathfrak{n} > \mathfrak{m}$, where these three cases are mutually exclusive.*
(c) *If $\mathfrak{n}$ and $\mathfrak{m}$ are any cardinals, then $\mathfrak{n} \leq^* \mathfrak{m}$ or $\mathfrak{m} \leq^* \mathfrak{n}$.*
(d) *If $\mathfrak{m}$ is any infinite cardinal, then $\mathfrak{m}^2 = \mathfrak{m}$.*

Proof. (a) If every set is well-orderable, then obviously every cardinal contains an well-orderable set and is therefore an aleph. On the other hand, for an arbitrary set x let $\mathfrak{m} = |x|$ and let $y_0 \in \mathfrak{m}$ be well-orderable. By definition of $\mathfrak{m}$ there exists a bijection between y_0 and x, and therefore, x is well-orderable as well.

(b) Firstly notice that any two alephs are comparable. Thus, by (a) we see that the Well-Ordering Principle implies the Trichotomy of Cardinals and consequently so does AC. On the other hand, by HARTOGS' THEOREM 3.27 we know that for every cardinal $\mathfrak{m}$ there is a smallest aleph, denoted $\aleph(\mathfrak{m})$, such that $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$. Now, if any two cardinals are comparable we must have $\mathfrak{m} < \aleph(\mathfrak{m})$, which implies that $\mathfrak{m}$ is an aleph.

(c) Notice that if every set can be well-ordered, then for any cardinals $\mathfrak{n}$ and $\mathfrak{m}$ we have $\mathfrak{n} \leq^* \mathfrak{m}$ *iff* $\mathfrak{n} \leq \mathfrak{m}$. For the other direction we first prove that for any cardinal $\mathfrak{m}$ there exists an aleph $\aleph'(\mathfrak{m})$ such that $\aleph'(\mathfrak{m}) \not\leq^* \mathfrak{m}$: Notice that if there exists a surjection from a set A onto a set B, then there exist an injection from B into $\mathscr{P}(A)$. So, by definition of $\aleph(2^{\mathfrak{m}})$ we have $\aleph(2^{\mathfrak{m}}) \not\leq^* \mathfrak{m}$. Let now $\mathfrak{m}$ be an arbitrary cardinal and let $\mathfrak{n} = \aleph(2^{\mathfrak{m}})$. If $\mathfrak{n} \leq^* \mathfrak{m}$ or $\mathfrak{n} \geq^* \mathfrak{m}$, then we must have $\mathfrak{n} \geq^* \mathfrak{m}$ (since $\mathfrak{n} \not\leq^* \mathfrak{m}$), which implies that $\mathfrak{m}$ is an aleph and completes the proof.

(d) Assume that for any infinite cardinal $\mathfrak{n}$ we have $\mathfrak{n}^2 = \mathfrak{n}$. Hence, we get $\mathfrak{m} + \aleph(\mathfrak{m}) = (\mathfrak{m} + \aleph(\mathfrak{m}))^2 = \mathfrak{m}^2 + (\mathfrak{m} + \mathfrak{m}) \cdot \aleph(\mathfrak{m}) + \aleph(\mathfrak{m})^2 = \mathfrak{m} + \aleph(\mathfrak{m}) + \mathfrak{m} \cdot \aleph(\mathfrak{m})$, and since $\mathfrak{m} + \aleph(\mathfrak{m}) \leq \mathfrak{m} \cdot \aleph(\mathfrak{m})$ we have

$$\mathfrak{m} + \aleph(\mathfrak{m}) = \mathfrak{m} \cdot \aleph(\mathfrak{m}).$$

Now, let $x \in \mathfrak{m}$ and let $y_0 \in \aleph(\mathfrak{m})$ be a set which is well-ordered by "$<_{y_0}$". Without loss of generality we may assume that x and y_0 are disjoint. Since $|x \cup y_0| = |x \times y_0|$, there exists a bijection $f : x \cup y_0 \to x \times y_0$. Using the bijection f we define $\tilde{x} := \{a \in x : \exists b \in y_0\,(\langle a, b\rangle \in f[y_0])\} \subseteq x$. Firstly notice that $\tilde{x} = x$. Indeed, if there would be an $a_0 \in x \setminus \tilde{x}$, then for all $b \in y_0$ we have $f^{-1}(\langle a_0, b\rangle) \notin y_0$, *i.e.*, $f^{-1}(\langle a_0, b\rangle) \in x$. Thus, since f is bijective, $f^{-1}[\{a_0\} \times y_0] \subseteq x$ is a set of cardinality $\aleph(\mathfrak{m})$, contradicting the fact that $\aleph(\mathfrak{m}) \not\leq \mathfrak{m}$. So, for every $a \in x$, the set

$$u_a := \big\{b \in y_0 : \exists b' \in y_0 \big(f(b) = \langle a, b'\rangle\big)\big\}$$

is a non-empty subset of y_0, and—since y_0 is well-ordered by "$<_{y_0}$"—has a $<_{y_0}$-minimal element, say μ_a. Finally, define an ordering "$<$" on x by stipulating $a < a'$ *iff* $\mu_a <_{y_0} \mu_{a'}$. It is easily checked that "$<$" is a well-ordering on x, and therefore, $\mathfrak{m}$ is an aleph.

The converse implication—namely that the Well-Ordering Principle implies that $\mathfrak{m}^2 = \mathfrak{m}$ for every infinite cardinal $\mathfrak{m}$—is postponed to the next section (see THEOREM 5.7). ⊣

Cardinal Arithmetic in the Presence of AC

In the presence of AC we are able to define cardinal numbers as ordinals: For any set A we define

$$|A| = \bigcap\{\alpha \in \Omega : \text{there is a bijection between } \alpha \text{ and } A\}.$$

Recall that AC implies that every set A is well-orderable and that every well-ordering of A corresponds to exactly one ordinal (which is the order type of the well-ordering).

For example we have $|n| = n$ for every $n \in \omega$, and $|\omega| = \omega$. However, for $\alpha \in \Omega$ we have in general $|\alpha| \neq \alpha$, *e.g.*, $|\omega + 1| = \omega$.

Ordinal numbers $\kappa \in \Omega$ such that $|\kappa| = \kappa$ are called **cardinal numbers**, or just **cardinals**, and are usually denoted by Greek letters like κ, λ, μ, *et cetera*.

A cardinal κ is infinite if $\kappa \notin \omega$, otherwise, it is finite. In other words, a cardinal is finite if and only if it is a natural number.

Since cardinal numbers are just a special kind of ordinal, they are well-ordered by "$\in$". However, for cardinal numbers κ and λ we usually write $\kappa < \lambda$ instead of $\kappa \in \lambda$, thus,

$$\kappa < \lambda \quad \Longleftrightarrow \quad \kappa \in \lambda.$$

Let κ be a cardinal. The smallest cardinal number which is greater than κ is denoted by κ^+, thus,

$$\kappa^+ = \bigcap \big\{ \alpha \in \Omega : \kappa < |\alpha| \big\}.$$

Notice that by CANTOR'S THEOREM 3.25, for every cardinal κ there is a cardinal $\lambda > \kappa$, in particular, for every cardinal κ, $\bigcap\{\alpha \in \Omega : \kappa < |\alpha|\}$ is non-empty and therefore κ^+ exists.

A cardinal μ is called a **successor cardinal** if there exists a cardinal κ such that $\mu = \kappa^+$; otherwise, it is called a **limit cardinal**. In particular, every positive number $n \in \omega$ is a successor cardinal and ω is the smallest non-zero limit cardinal. By induction on $\alpha \in \Omega$ we define $\omega_{\alpha+1} := \omega_\alpha^+$, where $\omega_0 := \omega$, and $\omega_\alpha := \bigcup_{\delta \in \alpha} \omega_\delta$ for limit ordinals α; notice that $\bigcup_{\delta \in \alpha} \omega_\delta$ is a cardinal. In particular, ω_ω is the smallest uncountable limit cardinal and $\omega_1 = \omega_0^+$ is the smallest uncountable cardinal. Further, the collection $\{\omega_\alpha : \alpha \in \Omega\}$ is the class of all infinite cardinals, *i.e.*, for every infinite cardinal κ there is an $\alpha \in \Omega$ such that $\kappa = \omega_\alpha$. Notice that the collection of cardinals is—like the collection of ordinals—a proper *class* and not a *set*.

Cardinal addition, multiplication, and exponentiation are defined as follows:

Cardinal addition: For cardinals κ and μ let $\kappa + \mu := |(\kappa \times \{0\}) \dot\cup (\mu \times \{1\})|$.
Cardinal multiplication: For cardinals κ and μ let $\kappa \cdot \mu := |\kappa \times \mu|$.
Cardinal exponentiation: For cardinals κ and μ let $\kappa^\mu := |{}^\mu\kappa|$.

Since for any set A, $|{}^A 2| = |\mathscr{P}(A)|$, the cardinality of the power set of a cardinal κ is usually denoted by 2^κ. However, because 2^ω is the cardinality of the so-called *continuum* $\mathbb{R}$, it is usually denoted by $\mathfrak{c}$. Notice that by CANTOR'S THEOREM 3.25 for all cardinals κ we have $\kappa < 2^\kappa$.

As a consequence of the definition we get the following

FACT 5.6. *Addition and multiplication of cardinals is associative and commutative and we have the distributive law for multiplication over addition, and for all cardinals* κ, λ, μ, *we have*

$$\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu, \quad \kappa^{\mu\cdot\lambda} = (\kappa^\lambda)^\mu, \quad (\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu.$$

Proof. It is obvious that addition and multiplication is associative and commutative and that we have the distributive law for multiplication over addition. Now, let κ, λ, μ, be any cardinal numbers. Firstly, for every function $f : (\lambda \times \{0\}) \cup (\mu \times \{1\}) \to \kappa$

let the functions $f_\lambda : (\lambda \times \{0\}) \to \kappa$ and $f_\mu : (\mu \times \{1\}) \to \kappa$ be such that for each $x \in (\lambda \times \{0\}) \cup (\mu \times \{1\})$,

$$f(x) = \begin{cases} f_\lambda(x) & \text{if } x \in \lambda \times \{0\}, \\ f_\mu(x) & \text{if } x \in \mu \times \{1\}. \end{cases}$$

It is easy to see that each function $f : (\lambda \times \{0\}) \cup (\mu \times \{1\}) \to \kappa$ corresponds to a unique pair $\langle f_\lambda, f_\mu\rangle$, and vice versa, each pair $\langle f_\lambda, f_\mu\rangle$ defines uniquely a function $f : (\lambda \times \{0\}) \cup (\mu \times \{1\}) \to \kappa$. Thus, we have a bijection between $\kappa^{\lambda+\mu}$ and $\kappa^\lambda \cdot \kappa^\mu$.

Secondly, for every function $f : \mu \to {}^\lambda\kappa$ let $\tilde{f} : \mu \times \lambda \to \kappa$ be such that for all $\alpha \in \mu$ and all $\beta \in \lambda$ we have

$$\tilde{f}\big(\langle \alpha, \beta\rangle\big) = f(\alpha)(\beta).$$

We leave it as an exercise to the reader to verify that the mapping

$$\begin{aligned} {}^\mu\big({}^\lambda\kappa\big) &\longrightarrow {}^{\mu\times\lambda}\kappa \\ f &\longmapsto \tilde{f} \end{aligned}$$

is bijective, and therefore we have $\kappa^{\mu\cdot\lambda} = (\kappa^\lambda)^\mu$.

Thirdly, for every function $f : \mu \to \kappa \times \lambda$ let the functions $f_\kappa : \mu \to \kappa$ and $f_\lambda : \mu \to \lambda$ be such that for each $\alpha \in \mu$, $f(\alpha) = \langle f_\kappa(\alpha), f_\lambda(\alpha)\rangle$. We leave it again as an exercise to the reader to show that the mapping

$$\begin{aligned} {}^\mu(\kappa \times \lambda) &\longrightarrow {}^\mu\kappa \times {}^\mu\lambda \\ f &\longmapsto \langle f_\kappa, f_\lambda\rangle \end{aligned}$$

is a bijection. $\dashv$

The next result completes the proof of THEOREM 5.5(d):

THEOREM 5.7. *For any ordinal numbers $\alpha, \beta \in \Omega$ we have*

$$\omega_\alpha + \omega_\beta = \omega_\alpha \cdot \omega_\beta = \omega_{\alpha\cup\beta} = \max\{\omega_\alpha, \omega_\beta\}.$$

In particular, for every infinite cardinal κ we have $\kappa^2 = \kappa$.

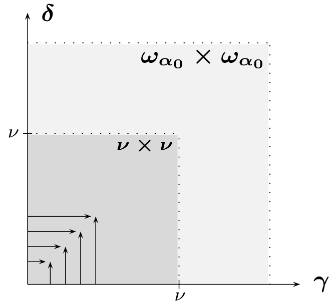
Proof. It is enough to show that for all $\alpha \in \Omega$ we have $\omega_\alpha \cdot \omega_\alpha = \omega_\alpha$. For $\alpha = 0$ we already know that $|\omega \times \omega| = \omega$, thus, $\omega_0 \cdot \omega_0 = \omega_0$. Assume towards a contradiction that there exists a $\beta_0 \in \Omega$ such that $\omega_{\beta_0} \cdot \omega_{\beta_0} > \omega_{\beta_0}$. Let

$$\alpha_0 = \bigcap\{\alpha \in \beta_0 + 1 : \omega_\alpha \cdot \omega_\alpha > \omega_\alpha\}.$$

On $\omega_{\alpha_0} \times \omega_{\alpha_0}$ we define an ordering "$<$" by stipulating

$$\langle \gamma_1, \delta_1\rangle < \langle \gamma_2, \delta_2\rangle \quad \iff \quad \begin{cases} \gamma_1 \cup \delta_1 \in \gamma_2 \cup \delta_2, \text{ or} \\ \gamma_1 \cup \delta_1 = \gamma_2 \cup \delta_2 \wedge \gamma_1 \in \gamma_2, \text{ or} \\ \gamma_1 \cup \delta_1 = \gamma_2 \cup \delta_2 \wedge \gamma_1 = \gamma_2 \wedge \delta_1 \in \delta_2. \end{cases}$$

This linear ordering can be visualised as follows:



It is easily verified that "<" is a well-ordering on $\omega_{\alpha_0} \times \omega_{\alpha_0}$. Now, let ρ be the order type of the well-ordering "<" and let $\Gamma : \omega_{\alpha_0} \times \omega_{\alpha_0} \to \rho$ be the unique order preserving bijection between $\omega_{\alpha_0} \times \omega_{\alpha_0}$ and ρ, *i.e.*, $\langle \gamma_1, \delta_1 \rangle < \langle \gamma_2, \delta_2 \rangle$ *iff* $\Gamma(\langle \gamma_1, \delta_1 \rangle) \in \Gamma(\langle \gamma_2, \delta_2 \rangle)$. Because $\omega_{\alpha_0} \cdot \omega_{\alpha_0} > \omega_{\alpha_0}$ we have $\omega_{\alpha_0} < |\rho|$. Now, by the definition of the well-ordering "<", there are $\gamma_0, \delta_0 \in \omega_{\alpha_0}$ such that $\Gamma(\langle \gamma_0, \delta_0 \rangle) = \omega_{\alpha_0}$ and for $\nu = \gamma_0 \cup \delta_0$ we have $|\nu \times \nu| \geq \omega_{\alpha_0}$. Thus, for $\omega_\beta = |\nu|$ we have $\omega_\beta < \omega_{\alpha_0}$ (since $\nu \in \omega_{\alpha_0}$) and $\omega_\beta \cdot \omega_\beta \geq \omega_{\alpha_0}$. In particular, $\omega_\beta \cdot \omega_\beta > \omega_\beta$, which is a contradiction to the choice of α_0. ⊣

As a consequence of THEOREM 5.7 we get the following

COROLLARY 5.8. *If* κ *is an infinite cardinal, then* $\mathrm{seq}(\kappa) = \kappa$ *and* $\kappa^\kappa = 2^\kappa$.

Proof. Firstly we have $\mathrm{seq}(\kappa) = |\bigcup_{n\in\omega} \kappa^n| = 1 + \kappa + \kappa^2 + \ldots = 1 + \kappa \cdot \omega = \kappa$. Secondly, by definition we have $\kappa^\kappa = |{}^\kappa\kappa|$. By identifying each function $f \in {}^\kappa\kappa$ by its graph, which is a subset of $\kappa \times \kappa$, we get $|{}^\kappa\kappa| \leq |\mathscr{P}(\kappa \times \kappa)|$, and since $|\kappa \times \kappa| = \kappa$ we finally have $\kappa^\kappa \leq |\mathscr{P}(\kappa)| = 2^\kappa$. ⊣

Let λ be an infinite limit ordinal. A subset C of λ is called **cofinal** in λ if $\bigcup C = \lambda$. The **cofinality** of λ, denoted $\mathrm{cf}(\lambda)$, is the cardinality of a smallest cofinal set $C \subseteq \lambda$. In other words,

$$\mathrm{cf}(\lambda) = \min\{|C| : C \text{ is cofinal in } \lambda\}.$$

Notice that by definition, $\mathrm{cf}(\lambda)$ is always a cardinal number.

Let again λ be an infinite limit ordinal and let $C = \{\beta_\xi : \xi \in \mathrm{cf}(\lambda)\} \subseteq \lambda$ be cofinal in λ. Now, for every $\nu \in \mathrm{cf}(\lambda)$ let $\alpha_\nu := \bigcup\{\beta_\xi : \xi \in \nu\}$ (notice that all the α_ν's belong to λ). Then $\langle \alpha_\nu : \nu \in \mathrm{cf}(\lambda) \rangle$ is an increasing sequence (not necessarily in the strict sense) of length $\mathrm{cf}(\lambda)$ with $\bigcup\{\alpha_\nu : \nu \in \mathrm{cf}(\lambda)\} = \lambda$. Thus, instead of cofinal *subsets* of λ we could equally well work with cofinal *sequences*.

Since every infinite cardinal is an infinite limit ordinal, $\mathrm{cf}(\kappa)$ is also defined for cardinals κ. An infinite *cardinal* κ is called **regular** if $\mathrm{cf}(\kappa) = \kappa$; otherwise, κ is called **singular**. For example ω is regular and ω_ω is singular (since $\{\omega_n : n \in \omega\}$ is cofinal in ω_ω). In general, for non-zero limit ordinals λ we have $\mathrm{cf}(\omega_\lambda) = \mathrm{cf}(\lambda)$. For example $\mathrm{cf}(\omega_\omega) = \mathrm{cf}(\omega_{\omega+\omega}) = \mathrm{cf}(\omega_{\omega_{\omega_\omega}}) = \omega$.

FACT 5.9. *For all infinite limit ordinals λ, the cardinal* $\mathrm{cf}(\lambda)$ *is regular.*

Proof. Let $\kappa = \mathrm{cf}(\lambda)$ and let $\langle \alpha_\xi : \xi \in \kappa \rangle$ be an increasing, cofinal sequence of λ. Further, let $\mathcal{C} \subseteq \kappa$ be cofinal in κ with $|\mathcal{C}| = \mathrm{cf}(\kappa)$. Now, $\langle \alpha_\nu : \nu \in \mathcal{C} \rangle$ is still a cofinal sequence of λ, which implies that $\mathrm{cf}(\lambda) \leq \mathrm{cf}(\kappa)$. On the other hand we have $\mathrm{cf}(\kappa) \leq \kappa = \mathrm{cf}(\lambda)$. Hence, $\mathrm{cf}(\kappa) = \kappa = \mathrm{cf}(\lambda)$, which shows that $\mathrm{cf}(\lambda)$ is regular. $\dashv$

The following result—which implicitly uses AC—shows that all infinite successor cardinals are regular.

PROPOSITION 5.10. *If κ is an infinite cardinal, then κ^+ is regular.*

Proof. Assume towards a contradiction that there exists a subset $\mathcal{C} \subseteq \kappa^+$ such that $\mathcal{C}$ is cofinal in κ^+ and $|\mathcal{C}| < \kappa^+$, *i.e.*, $|\mathcal{C}| \leq \kappa$. Since $\mathcal{C} \subseteq \kappa^+$, for every $\alpha \in \mathcal{C}$ we have $|\alpha| \leq \kappa$. Now, by AC, for each $\alpha \in \mathcal{C}$ we can choose a one-to-one mapping $f_\alpha : \alpha \hookrightarrow \kappa$ and further let g be a one-to-one mapping from $\mathcal{C}$ into κ. Then,

$$\big\{\big\langle g(\alpha), f_\alpha(\nu)\big\rangle : \alpha \in \mathcal{C} \wedge \nu \in \alpha\big\}$$

is a subset of $\kappa \times \kappa$ and consequently $|\bigcup \mathcal{C}| \leq |\kappa \times \kappa| = \kappa$. Thus, $\bigcup \mathcal{C} \neq \kappa^+$ which implies that $\mathcal{C}$ is not cofinal in κ^+. $\dashv$

For example, ω_1, ω_{17}, and $\omega_{\omega+5}$ are regular, since $\omega_1 = \omega_0^+$, $\omega_{17} = \omega_{16}^+$, and $\omega_{\omega+5} = \omega_{\omega+4}^+$.

We now consider arbitrary sums and products of cardinal numbers. For this, let I be a non-empty set and let $\{\kappa_\iota : \iota \in I\}$ be a family of cardinals. We define

$$\sum_{\iota \in I} \kappa_\iota = \Big|\bigcup_{\iota \in I} A_\iota\Big|$$

where $\{A_\iota : \iota \in I\}$ is a family of pairwise disjoint sets such that $|A_\iota| = \kappa_\iota$ for each $\iota \in I$, *e.g.*, $A_\iota = \kappa_\iota \times \{\iota\}$ will do.

Similarly we define

$$\prod_{\iota \in I} \kappa_\iota = \Big|\prod_{\iota \in I} A_\iota\Big|$$

where $\{A_\iota : \iota \in I\}$ is a family of sets such that $|A_\iota| = \kappa_\iota$ for each $\iota \in I$, *e.g.*, $A_\iota = \kappa_\iota$ will do.

THEOREM 5.11 (INEQUALITY OF KÖNIG–JOURDAIN–ZERMELO). *Let I be a non-empty set and let $\{\kappa_\iota : \iota \in I\}$ and $\{\lambda_\iota : \iota \in I\}$ be families of cardinal numbers such that $\kappa_\iota < \lambda_\iota$ for every $\iota \in I$. Then*

$$\sum_{\iota \in I} \kappa_\iota < \prod_{\iota \in I} \lambda_\iota .$$

Proof. Let $\{A_\iota : \iota \in I\}$ be a family of pairwise disjoint sets such that $|A_\iota| = \kappa_\iota$ for each $\iota \in I$. Firstly, for each $\iota \in I$ choose a injection $f_\iota : A_\iota \hookrightarrow \lambda_\iota$ and an element $y_\iota \in \lambda_\iota \setminus f_\iota[A_\iota]$ (notice that since $|A_\iota| < \lambda_\iota$, the set $\lambda_\iota \setminus f_\iota[A_\iota]$ is non-empty).

As a first step we show that $\sum_{\iota\in I} \kappa_\iota \leq \prod_{\iota\in I} \lambda_\iota$: For this, define $\bar{f} : \bigcup_{\iota\in I} A_\iota \to \prod_{\iota\in I} \lambda_\iota$ by stipulating $\bar{f}(x) := \langle \bar{f}_\iota(x) : \iota \in I\rangle$ where

$$\bar{f}_\iota(x) = \begin{cases} f_\iota(x) & \text{if } x \in A_\iota, \\ y_\iota & \text{otherwise.} \end{cases}$$

Then $\bar{f}$ is obviously a one-to-one function from $\bigcup_{\iota\in I} A_\iota$ into $\prod_{\iota\in I} \lambda_\iota$, which shows that $\sum_{\iota\in I} \kappa_\iota \leq \prod_{\iota\in I} \lambda_\iota$.

To see that $\sum_{\iota\in I} \kappa_\iota < \prod_{\iota\in I} \lambda_\iota$, take any function $g : \bigcup_{\iota\in I} A_\iota \to \prod_{\iota\in I} \lambda_\iota$. For every $\iota \in I$, let $P_\iota(g[A_\iota])$ be the projection of $g[A_\iota]$ on κ_ι. Then, for each $\iota \in I$ we can choose an element $z_\iota \in \lambda_\iota \setminus P_\iota(g[A_\iota])$. Evidently, the sequence $\langle z_\iota : \iota \in I\rangle$ does not belong to $g[\bigcup_{\iota\in I} A_\iota]$ which shows that g is not surjective, and consequently, g is not bijective. ⊣

As an immediate consequence we get the following

COROLLARY 5.12. *For every infinite cardinal κ we have*

$$\kappa < \kappa^{\mathrm{cf}(\kappa)} \quad \textit{and} \quad \mathrm{cf}(2^\kappa) > \kappa.$$

In particular we find that $\mathrm{cf}(\mathfrak{c}) > \omega$.

Proof. Let $\langle \alpha_\nu : \nu \in \mathrm{cf}(\kappa)\rangle$ be a cofinal sequence of κ. On the one hand we have

$$\kappa = \left| \bigcup_{\nu\in\mathrm{cf}(\kappa)} \alpha_\nu \right| \leq \sum_{\nu\in\mathrm{cf}(\kappa)} |\alpha_\nu| \leq \mathrm{cf}(\kappa)\cdot\kappa = \kappa,$$

and hence, $\kappa = \sum_{\nu\in\mathrm{cf}(\kappa)} |\alpha_\nu|$. On the other hand, for each $\nu \in \mathrm{cf}(\kappa)$ we have $|\alpha_\nu| < \kappa$, and therefore, by THEOREM 5.11, we have

$$\sum_{\nu\in\mathrm{cf}(\kappa)} |\alpha_\nu| < \prod_{\nu\in\mathrm{cf}(\kappa)} \kappa = \kappa^{\mathrm{cf}(\kappa)}.$$

Thus, we have $\kappa < \kappa^{\mathrm{cf}(\kappa)}$.

In order to see that $\mathrm{cf}(2^\kappa) > \kappa$, notice that $\mathrm{cf}(2^\kappa) \leq \kappa$ would imply that $(2^\kappa)^{\mathrm{cf}(2^\kappa)} \leq (2^\kappa)^\kappa = 2^{\kappa\cdot\kappa} = 2^\kappa$, which contradicts the fact that $2^\kappa < (2^\kappa)^{\mathrm{cf}(2^\kappa)}$. ⊣

Some Weaker Forms of the Axiom of Choice

The Prime Ideal Theorem and Related Statements

The following maximality principle—which is frequently used in areas like Algebra and Topology—is just slightly weaker than the Axiom of Choice. However, in order to formulate this choice principle we have to introduce the notion of *Boolean algebra* and *ideal*:

A **Boolean algebra** is an algebraic structure, say

$$(B, +, \cdot, -, \mathbf{0}, \mathbf{1})$$

where B is a non-empty set, "$+$" and "$\cdot$" are two binary operations (called *Boolean sum* and *product*), "$-$" is an unary operation (called *complement*), and $\mathbf{0}, \mathbf{1}$ are two constants. For all $u, v, w \in B$, the Boolean operations satisfy the following axioms:

$u + v = v + u$	$u \cdot v = v \cdot u$	(commutativity)
$u + (v + w) = (u + v) + w$	$u \cdot (v \cdot w) = (u \cdot v) \cdot w$	(associativity)
$u \cdot (v + w) = (u \cdot v) + (u \cdot w)$	$u + (v \cdot w) = (u + v) \cdot (u + w)$	(distributivity)
$u \cdot (u + v) = u$	$u + (u \cdot v) = u$	(absorption)
$u + (-u) = \mathbf{1}$	$u \cdot (-u) = \mathbf{0}$	(complementation)

An **algebra of sets** is a collection $\mathscr{S}$ of subsets of a given set S such that $S \in \mathscr{S}$ and whenever $X, Y \in \mathscr{S}$, then $S \setminus (X \cap Y) \in \mathscr{S}$ (*i.e.*, $\mathscr{S}$ is closed under unions, intersections and complements). An algebra of sets $\mathscr{S} \subseteq \mathscr{P}(S)$ is a Boolean algebra, with Boolean sum and product being $\cup$ and $\cap$, respectively, the complement $-X$ of a set $X \in \mathscr{S}$ being $S \setminus X$, and with $\emptyset$ and S being the constants $\mathbf{0}$ and $\mathbf{1}$, respectively. In particular, for any set S, $(\mathscr{P}(S), \cup, \cap, -, \emptyset, S)$ is a Boolean algebra. The case when $S = \omega$ plays an important role throughout this book and some combinatorial properties of the Boolean algebra $(\mathscr{P}(\omega), \cup, \cap, -, \emptyset, \omega)$ will be investigated in Chapters 8–10.

From the axioms above one can derive additional Boolean-algebraic rules that correspond to rules for the set operations $\cup$, $\cap$ and $-$. Among others we have

$$u + u = u \cdot u = -(-u) = u, \quad u + \mathbf{0} = u, \quad u \cdot \mathbf{0} = \mathbf{0}, \quad u + \mathbf{1} = \mathbf{1}, \quad u \cdot \mathbf{1} = u,$$

as well as the two **De Morgan laws**

$$-(u + v) = -u \cdot -v \quad \text{and} \quad -(u \cdot v) = -u + -v.$$

The De Morgan laws might be better recognised in set-theoretic notation as

$$S \setminus (X \cup Y) = (S \setminus X) \cap (S \setminus Y)$$

where $X, Y \in \mathscr{P}(S)$; or in Propositional Logic as

$$\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$$

where φ and ψ are any sentences formulated in a certain language.

This last formulation in the language of Propositional Logic shows the relation between Boolean algebra and Logic and provides other examples of Boolean algebras:

Let $\mathscr{L}$ be a first-order language and let S be the set of all $\mathscr{L}$-sentences. We define an equivalence relation "$\sim$" on S by stipulating

$$\varphi \sim \psi \iff \vdash \varphi \leftrightarrow \psi.$$

The set $B := S/\!\sim$ of all equivalence classes $[\varphi]$ is a Boolean algebra under the operations $[\varphi] + [\psi] := [\varphi \vee \psi]$, $[\varphi] \cdot [\psi] := [\varphi \wedge \psi]$, $-[\varphi] := [\neg\varphi]$, where $\mathbf{0} := [\varphi \wedge \neg\varphi]$ and $\mathbf{1} := [\varphi \vee \neg\varphi]$. This algebra is called the **Lindenbaum algebra**.

Let us define

$$u - v = u \cdot (-v)$$

and

$$u \leq v \quad \iff \quad u - v = \mathbf{0}.$$

We leave it as an exercise to the reader to verify that "$\leq$" is a partial ordering on B and that

$$u \leq v \quad \iff \quad u + v = v \quad \iff \quad u \cdot v = u.$$

Notice also that $[\varphi] \leq [\psi]$ is equivalent to $\vdash \varphi \to \psi$.

With respect to that ordering, $\mathbf{1}$ is the greatest element of B and $\mathbf{0}$ is the least element. Also, for any $u, v \in B$, $u + v$ is the least upper bound of $\{u, v\}$, and $u \cdot v$ is the greatest lower bound of $\{u, v\}$. Moreover, since $-u$ is the unique element v of B such that $u + v = \mathbf{1}$ and $u \cdot v = \mathbf{0}$ we see that all Boolean-algebraic operations can be defined in terms of the partial ordering "$\leq$" (*e.g.*, $-u$ is the least element v of B with the property that $u + v = \mathbf{1}$).

Now, let us define an additional operation "$\oplus$" on B by stipulating

$$u \oplus v = (u - v) + (v - u).$$

Notice that for every $u \in B$ we have $u \oplus u = \mathbf{0}$, thus, with respect to the operation "$\oplus$", every element of B is its own (and unique) inverse. We leave it as an exercise to the reader to show that B with the two binary operations $\oplus$ and $\cdot$ is a *ring* with zero $\mathbf{0}$ and unit $\mathbf{1}$.

Before we give the definition of ideals in Boolean algebras, let us briefly recall the *algebraic notion* of ideals in commutative rings: Let $\mathcal{R} = (R, +, \cdot, \mathbf{0})$ be an arbitrary commutative ring. An non-empty subset $\mathcal{I} \subseteq R$ is an *ideal* in R if and only if for all $x, y \in \mathcal{I}$ and all $r \in R$ we have $x - y \in \mathcal{I}$ and $r \cdot x \in \mathcal{I}$. The ideal $\{\mathbf{0}\}$ is called the *trivial ideal*. An ideal $I \subseteq R$ of a ring is called *maximal* if $I \neq R$ and the only ideals J in R for which $I \subseteq J$ are $J = I$ and $J = R$. If $\mathcal{R}$ is a commutative ring and $I \neq R$ is an ideal in R, then I is called a *prime ideal* if given any $r, s \in R$ with $r \cdot s \in I$ we always have $r \in I$ or $s \in I$. It is not hard to verify that in a commutative ring with $\mathbf{1}$, every maximal ideal is prime. Finally, if an ideal $J \subseteq R$ is generated by a single element of R, then J is so-called *principal ideal.*

With respect to the ring $(B, \oplus, \cdot, \mathbf{0}, \mathbf{1})$, this leads to the following definition of ideals in Boolean algebras.

Let $(B, +, \cdot, -, \mathbf{0}, \mathbf{1})$ be a Boolean algebra. An **ideal** I in B is a non-empty proper subset of B with the following properties:

- $\mathbf{0} \in I$ but $\mathbf{1} \notin I$.
- If $u \in I$ and $v \in I$, then $u + v \in I$.

- For all $w \in B$ and all $u \in I$, $w \cdot u \in I$ (or equivalently, if $w \in B$, $u \in I$ and $w \le u$, then $w \in I$).

Considering the Boolean algebra $(\mathscr{P}(\omega), \cup, \cap, -, \emptyset, \omega)$, one easily verifies that the set of all finite subsets of ω is an ideal *over* ω, *i.e.*, an ideal *on* $\mathscr{P}(\omega)$. This ideal is called the **Fréchet ideal**.

The dual notion of an ideal is a so-called filter. Thus, a **filter** F in B is a non-empty proper subset of B with the following properties:

- $\mathbf{0} \notin F$ but $\mathbf{1} \in F$.
- If $u \in F$ and $v \in F$, then $u \cdot v \in F$.
- For all $w \in B$ and all $u \in F$, $w + u \in I$ (or equivalently, if $w \in B$, $u \in F$ and $w \ge u$, then $w \in F$).

Moreover, if I is an ideal in B, then $I^* := \{-u : u \in I\}$ is a filter, called **dual filter**. Similarly, if F is a filter in B, then $F^* := \{-u : u \in F\}$ is an ideal, called **dual ideal**. The dual filter $I_0^* = \{x \subseteq \omega : \omega \setminus x \text{ is finite}\}$ of the Fréchet ideal I_0 on $\mathscr{P}(\omega)$ is called the **Fréchet filter**.

Let I be an ideal in B, and let F be a filter in B.

I is called

- **trivial** if $I = \{\mathbf{0}\}$;
- **principal** if there is an $u \in B$ such that $I = \{v : v \le u\}$;
- **prime** if for all $u \in B$, *either* $u \in I$ *or* $-u \in I$;

F is called

- **trivial** if $F = \{\mathbf{1}\}$;
- **principal** if there is an $u \in B$ such that $F = \{v : v \ge u\}$;
- an **ultrafilter** if for all $u \in B$, *either* $u \in F$ *or* $-u \in F$.

Let us consider a few ideals and filters over ω, *i.e.*, ideals and filters in the Boolean algebra $(\mathscr{P}(\omega), \cup, \cap, -, \emptyset, \omega)$: The trivial ideal is $\{\emptyset\}$, and the trivial filter is $\{\omega\}$. For any non-empty subset $x \subseteq \omega$, $F_x := \{y \in \mathscr{P}(\omega) : y \supseteq x\}$ is a principal filter, and the dual ideal $I_{\omega\setminus x} := (F_x)^* = \{z \in \mathscr{P}(\omega) : \omega \setminus z \in F_x\} = \{z \in \mathscr{P}(\omega) : z \cap x = \emptyset\}$ is also principal. In particular, if $x = \{a\}$ for some $a \in \omega$, then F_x is a principal ultrafilter and $I_{\omega\setminus x}$ is a principal prime ideal. We leave it as an exercise to the reader to show that every principal ultrafilter over ω is of the form $F_{\{a\}}$ for some $a \in \omega$, and that every principal prime ideal is of the form $I_{\omega\setminus\{a\}}$. Considering the Fréchet filter F on $\mathscr{P}(\omega)$, one easily verifies that F is a non-principal filter, but not an ultrafilter (notice that neither $x = \{2n : n \in \omega\}$ nor $\omega \setminus x$ belongs to F). Similarly, the Fréchet ideal is not prime but non-principal.

Let us now summarise a few basic properties of ultrafilters over sets (the proofs are left to the reader):

FACT 5.13. *Let U be an ultrafilter over a set S.*

(a) *If $\{x_0, \dots, x_{n-1}\} \subseteq \mathscr{P}(S)$ (for some $n \in \omega$) such that $x_0 \cup \ldots \cup x_{n-1} \in U$ and for any distinct $i, j \in n$ we have $x_i \cap x_j \notin U$, then there is a unique $k \in n$ such that $x_k \in U$.*

(b) *If* $x \in U$ *and* $|x| \geq 2$, *then there is a proper subset* $y \subsetneq x$ *such that* $y \in U$.
(c) *If* U *contains a finite set, then* U *is principal.*

On the one hand, prime ideals and ultrafilters in Boolean algebras are always maximal. On the other hand, one cannot prove in ZF that for example the Fréchet filter over ω can be extended to an ultrafilter. In particular, there are models of ZF in which every ultrafilter over ω is principal (*cf.* RELATED RESULT 38 and Chapter 17).

However, there is a choice principle which guarantees that every ideal in a Boolean algebra can be extended to a prime ideal, and consequently, that every filter can be extended to an ultrafilter.

Prime Ideal Theorem. If I is an ideal in a Boolean algebra, then I can be extended to a prime ideal.

In fact, the Prime Ideal Theorem, denoted PIT, is a choice principle which is just slightly weaker than the full Axiom of Choice. Below we shall present some equivalent formulations of the Prime Ideal Theorem, but first let us show that the Prime Ideal Theorem follows from the Axiom of Choice (for the fact that the converse implication does not hold see THEOREM 7.16).

PROPOSITION 5.14. AC $\Rightarrow$ PIT.

Proof. By THEOREM 5.3 it is enough to show that the Prime Ideal Theorem follows from Teichmüller's Principle. Let $(B, +, \cdot, -, \mathbf{0}, \mathbf{1})$ be a Boolean algebra and let $I_0 \subsetneq B$ be an ideal. Further, let $\mathscr{F}$ be the family of all sets $X \subseteq B \setminus I_0$ such that for every finite subset $\{u_0, \ldots, u_n\} \subseteq X \cup I_0$ we have

$$u_0 + \ldots + u_n \neq \mathbf{1}.$$

Obviously, $\mathscr{F}$ has finite character, and therefore, by Teichmüller's Principle, $\mathscr{F}$ has a maximal element. In other words, there is a maximal subset I_1 of B which has the property that whenever we pick finitely many elements $\{u_0, \ldots, u_n\}$ from $I := I_0 \cup I_1$ we have $u_0 + \ldots + u_n \neq \mathbf{1}$. Since I_1 is maximal we find that I is an *ideal* in B which extends I_0. Moreover, the ideal I has the property that for any element $v \in B \setminus I$ there is a $u \in I$ such that $u + v = \mathbf{1}$, *i.e.*, for any $v \in B$, $v \notin I$ implies $-v \in I$. Thus, I is a prime ideal in B which extends I_0. ⊣

A seemingly weaker version of PIT is the following statement.

Ultrafilter Theorem. If F is a filter over a set S, then F can be extended to an ultrafilter.

Notice that the Ultrafilter Theorem is the dual version of the Prime Ideal Theorem in the case when the Boolean algebra is an algebra of sets.

For the next version of the Prime Ideal Theorem we have to introduce first some terminology: Let S be a set and let $\mathcal{B}$ be a set of binary functions (*i.e.*, with values

0 or 1) defined on finite subsets of S. We say that $\mathcal{B}$ is a **binary mess** on S if $\mathcal{B}$ satisfies the following properties:

- For each finite set $P \subseteq S$, there is a function $g \in \mathcal{B}$ such that $\mathrm{dom}(g) = P$, *i.e.*, g is defined on P.
- For each $g \in \mathcal{B}$ and each finite set $P \subseteq S$, the restriction $g|_P$ belongs to $\mathcal{B}$.

Let f be a binary function on S and let $\mathcal{B}$ be a binary mess on S. Then f is **consistent with** $\mathcal{B}$ if for every finite set $P \subseteq S$, $f|_P \in \mathcal{B}$.

Consistency Principle. For every binary mess $\mathcal{B}$ on a set S, there exists a binary function f on S which is consistent with $\mathcal{B}$.

In order to state the last version of the Prime Ideal Theorem we have to introduce first some terminology from **Propositional Logic**: The alphabet of Propositional Logic consists of an arbitrarily large but fixed set $\mathcal{P} := \{p_\lambda : \lambda \in \Lambda\}$ of so-called **propositional variables**, as well as of the logical operators "$\neg$", "$\wedge$", and "$\vee$". The formulae of Propositional Logic are defined recursively as follows:

- A single propositional variable $p \in \mathcal{P}$ by itself is a formula.
- If φ and ψ are formulae, then so are $\neg(\varphi)$, $(\varphi \wedge \psi)$, and $(\varphi \vee \psi)$; in Polish notation, the three composite formulae are $\neg\varphi$, $\wedge\varphi\psi$, and $\vee\varphi\psi$, respectively.

A **realisation** of Propositional Logic is a map of $\mathcal{P}$, the set of propositional variables, to the two element Boolean algebra $(\{\mathbf{0}, \mathbf{1}\}, +, \cdot, -, \mathbf{0}, \mathbf{1})$. Given a realisation f of Propositional Logic. By induction on the complexity of formulae we extend f to all formulae of Propositional Logic (compare with the definition of Lindenbaum's algebra): For any formulae φ and ψ, if $f(\varphi)$ and $f(\psi)$ have already been defined, then

$$f(\wedge\varphi\psi) = f(\varphi) \cdot f(\psi), \quad f(\vee\varphi\psi) = f(\varphi) + f(\psi),$$

and

$$f(\neg\varphi) = -f(\varphi).$$

Let φ be any formula of Propositional Logic. If the realisation f, extended in the way just described, maps the formula φ to $\mathbf{1}$, then we say that f **satisfies** φ. Finally, a set Σ of formulae of Propositional Logic is **satisfiable** if there is a realisation which simultaneously satisfies all the formulae in Σ.

Compactness Theorem for Propositional Logic. Let Σ be a set of formulae of Propositional Logic. If every finite subset of Σ is satisfiable, then also Σ is satisfiable.

Notice that the reverse implication of the Compactness Theorem for Propositional Logic is trivially satisfied.

Now we show that the above principles are all equivalent to the Prime Ideal Theorem.

THEOREM 5.15. *The following statements are equivalent:*

(a) Prime Ideal Theorem.
(b) Ultrafilter Theorem.
(c) Consistency Principle.
(d) Compactness Theorem for Propositional Logic.
(e) *Every Boolean algebra has a prime ideal.*

Proof. (a) ⇒ (b) The Ultrafilter Theorem is an immediate consequence of the dual form of the Prime Ideal Theorem.

(b) ⇒ (c) Let $\mathcal{B}$ be a binary mess on a non-empty set S. Assuming the Ultrafilter Theorem we show that there is a binary function f on S which is consistent with $\mathcal{B}$. Let $\mathrm{fin}(S)$ be the set of all finite subsets of S. For each $P \in \mathrm{fin}(S)$, let

$$A_P = \left\{g \in {}^S2 : g|_P \in \mathcal{B}\right\}.$$

Since $\mathcal{B}$ is a binary mess, the intersection of finitely many sets A_P is non-empty. Thus, the family $\mathscr{F}$ consisting of all supersets of intersections of finitely many sets A_P is a filter over ${}^S2$. By the Ultrafilter Theorem, $\mathscr{F}$ can be extended to an ultrafilter $\mathscr{U} \subseteq \mathscr{P}({}^S2)$. Since $\mathscr{U}$ is an ultrafilter, for each $s \in S$, either $\{g \in {}^S2 : g(s) = 0\}$ or $\{g \in {}^S2 : g(s) = 1\}$ belongs to $\mathscr{U}$, and we define the function $f \in {}^S2$ by stipulating that for each $s \in S$, the set $A_s = \{g \in {}^S2 : g(s) = f(s)\}$ belongs to $\mathscr{U}$. Now, for any finite set $P = \{s_0, \dots, s_n\} \subseteq S$, $\bigcap_{i \le n} A_{s_i} \in \mathscr{U}$, which shows that $f|_P \in \mathcal{B}$, *i.e.*, f is consistent with $\mathcal{B}$.

(c) ⇒ (d) Let Σ be a set of formulae of Propositional Logic and let $S \subseteq \mathcal{P}$ be the set of propositional variables which appear in formulae of Σ. Assume that every finite subset of Σ is satisfiable, *i.e.*, for every finite subset $\Sigma_0 \subseteq \Sigma$ there is a realisation $g_{\Sigma_0} : S_{\Sigma_0} \to \{\mathbf{0}, \mathbf{1}\}$ which satisfies Σ_0, where S_{Σ_0} denotes the set of propositional variables which appear in formulae of Σ_0. Let

$$\mathcal{B}_\Sigma := \left\{g_{\Sigma_0}|_P : \Sigma_0 \in \mathrm{fin}(\Sigma) \wedge P \subseteq S_{\Sigma_0}\right\}.$$

Then $\mathcal{B}_\Sigma$ is obviously a binary mess and by Consistency Principle there exists a binary function f on S which is consistent with $\mathcal{B}_\Sigma$. Now, f is a realisation of Σ and therefore Σ is satisfiable.

(d) ⇒ (e) Let $(B, +, \cdot, -, \mathbf{0}, \mathbf{1})$ be a Boolean algebra and let $\mathcal{P} := \{p_u : u \in B\}$ be a set of propositional variables. Further, let Σ_B be the following set of formulae of Propositional Logic:

- $p_{\mathbf{0}}, \neg p_{\mathbf{1}}$;
- $p_u \vee \neg p_{-u}$ (for each $u \in B$);
- $\neg(p_{u_1} \wedge \ldots \wedge p_{u_n}) \vee p_{u_1 + \ldots + u_n}$ (for each finite set $\{u_1, \dots, u_n\} \subseteq B$).
- $\neg(p_{u_1} \vee \ldots \vee p_{u_n}) \vee p_{u_1 \cdot \ldots \cdot u_n}$ (for each finite set $\{u_1, \dots, u_n\} \subseteq B$).

Notice that every finite subset of B generates a finite subalgebra of B and that every finite Boolean algebra has a prime ideal. Now, since every finite prime ideal in a finite subalgebra of B corresponds to a realisation of a finite subset of Σ_B, and vice versa, every finite subset of Σ_B is satisfiable. Thus, by the Compactness Theorem for Propositional Logic, Σ_B is satisfiable. Let f be a realisation of Σ_B and let $I = \{u \in B : f(p_u) = 1\}$. By definition of Σ_B and I, respectively, we get

- $f(p_{\mathbf{0}}) = 1$ and $f(p_{\mathbf{1}}) = 0$; thus, $\mathbf{0} \in I$ but $\mathbf{1} \notin I$.
- $f(p_u) = 1 - f(\neg p_u)$; thus, for all $u \in B$, either $u \in I$ or $-u \in I$.
- If $f(p_{u_1}) = f(p_{u_2}) = 1$, then $f(p_{u_1} \wedge p_{u_2}) = 1$; thus, for all $u_1, u_2 \in I$ we have $u_1 + u_2 \in I$.
- if $f(p_{u_1}) = 1$, then $f(p_{u_1} \vee p_{u_2}) = 1$; thus, for all $u_1 \in I$ and all $u_2 \in B$ we have $u_1 \cdot u_2 \in I$.

Thus, the set $I = \{u \in B : f(p_u) = 1\}$ is a prime ideal in B.

(e) $\Rightarrow$ (a) Let $(B, +, \cdot, -, \mathbf{0}, \mathbf{1})$ be a Boolean algebra and $I \subseteq B$ an ideal in B. Define the following equivalence relation on B:

$$u \sim v \quad \iff \quad (u - v) + (v - u) \in I.$$

Let C be the set of all equivalence classes $[u]\tilde{}$ and define the operations "$+$", "$\cdot$", and "$-$" on C as follows:

$$[u]\tilde{} + [v]\tilde{} = [u + v]\tilde{}, \quad [u]\tilde{} \cdot [v]\tilde{} = [u \cdot v]\tilde{}, \quad -[u]\tilde{} = [-u]\tilde{}.$$

Now,

$$(C, +, \cdot, -, [\mathbf{0}]\tilde{}, [\mathbf{1}]\tilde{})$$

is a Boolean algebra, the so-called *quotient of B modulo I*. By the Prime Ideal Theorem, C has a prime ideal J. We leave it as an exercise to the reader to verify that the set

$$\big\{u \in B : [u]\tilde{} \in J\big\}$$

is a prime ideal in B which extends I. $\dashv$

König's Lemma and Other Choice Principles

Let us begin by defining some choice principles:

- $\mathsf{C}(\aleph_0, \infty)$: Every countable family of non-empty sets has a choice function (this choice principle is usually called Countable Axiom of Choice).
- $\mathsf{C}(\aleph_0, \aleph_0)$: Every countable family of non-empty countable sets has a choice function.
- $\mathsf{C}(\aleph_0, < \aleph_0)$: Every countable family of non-empty finite sets has a choice function.
- $\mathsf{C}(\aleph_0, n)$: Every countable family of n-element sets, where $n \in \omega$, has a choice function.
- $\mathsf{C}(\infty, < \aleph_0)$: Every family of non-empty finite sets has a choice function (this choice principle is usually called Axiom of Choice for Finite Sets).
- $\mathsf{C}(\infty, n)$: Every family of n-element sets, where $n \in \omega$, has a choice function. This choice principle is usually denoted C_n.

Another—seemingly unrelated—choice principle is the Ramseyan Partition Principle, denoted RPP.

- RPP: If X is an infinite set and $[X]^2$ is 2-coloured, then there is an infinite subset Y of X such that $[Y]^2$ is monochromatic.

Below we show how these choice principles are related to each other, but first let us show that $\mathsf{C}(\aleph_0, < \aleph_0)$ and König's Lemma, denoted by KL, are equivalent.

PROPOSITION 5.16. $\mathsf{C}(\aleph_0, < \aleph_0) \iff \mathsf{KL}$.

Proof. ($\Rightarrow$) Let $T = (V, E)$ be an infinite, finitely branching tree with vertex set V, edge set E, and root say v_0. The edge set E can be considered as a subset of $V \times V$, *i.e.*, as a set of ordered pairs of vertices indicating the direction from the root to the top of the tree. Let $S_0 := \{v_0\}$, and for $n \in \omega$ let

$$S_{n+1} := \big\{v \in V : \exists u \in S_n\big(\langle u, v\rangle \in E\big)\big\}$$

and let $S := \bigcup_{n\in\omega} S_n$. Since T is infinite and finitely branching, S is infinite and for every $n \in \omega$, S_n is a non-empty finite set. Further, for every $v \in S$ let $S(v)$ be the set of all vertices $u \in S$ such that there exists a non-empty finite sequence $s \in \operatorname{seq}(S)$ of length $k + 1$ (for some $k \in \omega$) with $s(0) = v$ and $s(k) = u$, and for all $i \leq k$ we have $\langle s(i), s(i + 1)\rangle \in E$. In other words, $S(v)$ is the set of all vertices which can be reached from v. Notice that $(S(v), E|_{S(v)})$ is a subtree of T. Since S is infinite and for all $n \in \omega$, $\bigcup_{i\in n} S_i$ is finite, for each $n \in \omega$ there exists a vertex $v \in S_n$ such that $S(v)$ is infinite.

We now proceed as follows: By $\mathsf{C}(\aleph_0, < \aleph_0)$, for each $n \in \omega$ we can choose a well-ordering "$<_n$" on S_n and then construct a branch $v_0, v_1, \ldots, v_n, \ldots$ through T, where for all $n \in \omega$, v_{n+1} is the $<_{n+1}$-minimal element of the non-empty set $\{v \in S_{n+1} : \langle v_n, v\rangle \in E \wedge \text{“}S(v) \text{ is infinite”}\}$.

($\Leftarrow$) Let $\mathscr{F} = \{F_n : n \in \omega\}$ be a countable family of non-empty finite sets. Further, let $V = \bigcup_{k\in\omega}(\prod_{n\in k} F_n)$ and let $E \subseteq V \times V$ be the set of all ordered pairs $\langle s, t\rangle$ of the form $s = \langle x_0, \ldots, x_n\rangle$ and $t = \langle x_0, \ldots, x_n, x_{n+1}\rangle$, respectively, where for each $i \in n + 2$, $x_i \in F_i$ (*i.e.*, the sequence t is obtained by adding an element of F_{n+1} to s). Obviously, $T = (V, E)$ is an infinite, finitely branching tree and therefore, by KL, has an infinite branch, say $\langle a_n : n \in \omega\rangle$. Since, for all $n \in \omega$, a_n belongs to F_n, the function

$$\begin{aligned} f : \mathscr{F} &\longrightarrow \bigcup \mathscr{F} \\ F_n &\longmapsto a_n \end{aligned}$$

is a choice function for $\mathscr{F}$, and since the countable family of finite sets $\mathscr{F}$ was arbitrary, we get $\mathsf{C}(\aleph_0, < \aleph_0)$. ⊣

Obviously, $\mathsf{C}(\aleph_0, < \aleph_0) \Rightarrow \mathsf{C}(\aleph_0, n)$ for all positive integers $n \in \omega$. However, as a matter of fact we would like to mention that for each $n \geq 2$, $\mathsf{C}(\aleph_0, n)$ is a proper axiom, *i.e.*, not provable within ZF (for $n = 2$ see for example PROPOSITION 7.7).

The following result shows the strength of the choice principles RPP and KL compared to $\mathsf{C}(\aleph_0, \infty)$ and $\mathsf{C}(\aleph_0, n)$, respectively:

THEOREM 5.17. $\mathsf{C}(\aleph_0, \infty) \Longrightarrow \mathsf{RPP} \Longrightarrow \mathsf{KL} \Longrightarrow \mathsf{C}(\aleph_0, n)$.

Proof. $\mathsf{C}(\aleph_0, \infty) \Rightarrow \mathsf{RPP}$: Firstly we show that $\mathsf{C}(\aleph_0, \infty)$ implies that every infinite set X is transfinite, *i.e.*, there is an infinite sequence of elements of X in which no element appears twice: Let X be an infinite set and for every $n \in \omega$ let F_{n+1} be the set of all injections from $n + 1$ into X. Consider the family $\mathscr{F} = \{F_{n+1} : n \in \omega\}$. Since X is infinite, $\mathscr{F}$ is a countable family of non-empty sets. Thus, by $\mathsf{C}(\aleph_0, \infty)$, there is a choice function, say f, on $\mathscr{F}$. For every $n \in \omega$ let $g_n := f(F_{n+1})$. With the countably many injections g_n we can easily construct an injection from ω into X. In particular, we get an infinite sequence $\langle a_i : i \in \omega\rangle$ of elements of X in which no element appears twice. For $S := \{a_i : i \in \omega\} \subseteq X$, every 2-colouring of $[X]^2$ induces a 2-colouring of $[S]^2$. Now, by RAMSEY'S THEOREM 2.1, there exists an infinite subset Y of S such that $[Y]^2$ is monochromatic (notice that no choice is needed to establish RAMSEY'S THEOREM for countable sets).

$\mathsf{RPP} \Rightarrow \mathsf{KL}$: Let $T = (V, E)$ be an infinite, finitely branching tree and let the sets S_n (for $n \in \omega$) be as in the first part of the proof of PROPOSITION 5.16. Define the colouring $\pi : [V]^2 \to \{0, 1\}$ by stipulating $\pi(\{u, v\}) = 0 \iff \{u, v\} \subseteq S_n$ for some $n \in \omega$. By RPP there exists an infinite subset $X \subseteq V$ such that $[X]^2$ is monochromatic. Now, since T is finitely branching, we see that if $X \subseteq V$ is infinite and $[X]^2$ is monochromatic, then $[X]^2$ is of colour 1, *i.e.*, no two distinct elements of X are in the same set S_n. In order to construct an infinite branch through T, just proceed as in the first part of the proof of PROPOSITION 5.16.

$\mathsf{KL} \Rightarrow \mathsf{C}(\aleph_0, n)$: Because $\mathsf{C}(\aleph_0, < \aleph_0) \Rightarrow \mathsf{C}(\aleph_0, n)$, this is an immediate consequence of PROPOSITION 5.16. ⊣

The last result of this chapter deals with the relationship of the choice principles C_n (*i.e.*, $\mathsf{C}(\infty, n)$) for different natural numbers n. Before we can state the theorem we have to introduce the following number-theoretical condition: Let m, n be two positive integers. Then we say that m, n satisfy condition (S) if the following condition holds:

> There is no decomposition of n into a sum of primes, $n = p_1 + \ldots + p_s$, such that $p_i > m$ for all $1 \leq i \leq s$.

THEOREM 5.18. *If the positive integers m, n satisfy condition* (S) *and if C_k holds for every $k \leq m$, then also C_n holds.*

Proof. Firstly notice that C_1 is obviously true. Secondly notice that for $n \leq m$, the implication of the theorem is trivially true. So, without loss of generality we may assume that $n > m$.

The proof is now by induction on n: Let $m < n$ be a fixed positive integer such that m, n satisfy condition (S) and assume that the implication of the theorem is true for every $l < n$. Since n, m satisfy (S), n is not a prime and consequently n is divisible by some prime $p < n$. Necessarily, $p \leq m$, since otherwise we could write $n = p + \ldots + p$, contrary to (S). Let $\mathscr{F} = \{A_\lambda : \lambda \in \Lambda\}$ be a family of n-element sets. We have to describe a way to choose an element from each set A_λ $(\lambda \in \Lambda)$. Take an arbitrary $A \in \mathscr{F}$ and consider $[A]^p$ (*i.e.*, the set of all p-element subsets of A). Since $p \leq m$, by the premiss of the theorem there is a choice function g for $[A]^p$. In other words, for every $X \in [A]^p$, $g(X) \in X$, in particular, $g(X) \in A$. For every $a \in A$ let

$$q(a) = \left|\left\{X \in [A]^p : g(X) = a\right\}\right|$$

and let $q := \min\{q(a) : a \in A\}$. Further, let $B := \{a \in A : q(a) = q\}$. Obviously, the set B is non-empty and the set $[A]^p$ has $\binom{n}{p}$ elements. In order to prove that $A \setminus B$ is non-empty, we have to show that $\binom{n}{p}$ is not divisible by n. Indeed, because p divides n, there is a positive integer k which is not divisible by p such that $n = k \cdot p^{a+1}$ (for some $a \in \omega$). We have

$$\binom{n}{p} = \frac{k \cdot p^{a+1}}{p} \cdot \frac{(n-1) \cdot \cdots \cdot (n-p+1)}{(p-1) \cdot \cdots \cdot 1} = \frac{k \cdot p^{a+1}}{p} \cdot \binom{n-1}{p-1},$$

and since p does obviously not divide $\binom{n-1}{p-1}$, we find that $\binom{n}{p}$ is divisible by p^a, but not by p^{a+1}; in particular, $\binom{n}{p}$ is not divisible by $n = k \cdot p^{a+1}$. Thus, the sets B and $A \setminus B$ are both non-empty, and for $l_1 := |B|$ and $l_2 := |A \setminus B|$ we get that l_1 and l_2 are positive integers with $l_1 + l_2 = n$. Moreover, m, l_1 or m, l_2 satisfy condition (S), since otherwise we could write $l_1 = p_1 + \ldots + p_r$ and $l_2 = p_{r+1} + \ldots + p_s$, where $p_1, \ldots, p_s$ are primes bigger than m, which would imply that $n = p_1 + \ldots + p_s$, contrary to the assumption that m, n satisfy (S). Thus, by the induction hypothesis, either C_{l_1} holds and we choose an element in B, or, if C_{l_1} fails, C_{l_2} holds and we choose an element in $A \setminus B$. Finally, since $A \in \mathscr{F}$ was arbitrary, this completes the proof. ⊣

NOTES

The Axiom of Choice. Fraenkel writes in [26, p. 56 f.] that *the* Axiom of Choice *is probably the most interesting and, in spite of its late appearance, the most discussed axiom of Mathematics, second only to Euclid's axiom of parallels which was introduced more than two thousand years ago.* We would also like to mention a different view to choice functions, namely the view of Peano. In 1890, Peano published a proof in which he was constrained to choose a single element from each set in a certain infinite sequence $A_1, A_2, \ldots$ of infinite subsets of $\mathbb{R}$. In that proof, he remarked carefully (*cf.* [73, p. 210]): *But as one cannot apply infinitely many times an* arbitrary *rule by which one assigns to a class A an individual of this class, a* determinate *rule is stated here, by which, under suitable hypotheses, one assigns to each class A an individual of this class*. To obtain his rule, he employed least upper bounds. According to Moore [66, p. 76], Peano was the first mathematician who—while accepting infinite collections—categorically rejected the use of infinitely many arbitrary choices.

The difficulty is well illustrated by a Russellian anecdote (*cf.* Sierpiński [82, p. 125]): *A millionaire possesses an infinite number of pairs of shoes, and an infinite number of pairs of socks. One day, in a fit of eccentricity, he summons his valet and asks him to select one shoe from each pair. When the valet, accustomed to receiving precise instructions, asks for details as to how to perform the selection, the millionaire suggests that the left shoe be chosen from each pair. Next day the millionaire proposes to the valet that he select one sock from each pair. When asked as to how this operation is to be carried out, the millionaire is at a loss for a reply, since, unlike shoes, there is no intrinsic way of distinguishing one sock of a pair from the other. In other words, the selection of the socks cannot be carried out without the aid of some choice function*.

As long as the implicit and unconscious use of the Axiom of Choice by Cantor and others involved only generalised arithmetical concepts and properties well-known from finite numbers, nobody took offence. However, the situation changed drastically after Zermelo [107] published his first proof that every set can be well-ordered—which was one of the earliest assertions of Cantor. It is worth mentioning that, according to Zermelo [107, p. 514] & [108, footnote p. 118], it was in fact the idea of Erhard Schmidt to use the Axiom of Choice in order to build the f-sets. Zermelo considered the Axiom of Choice as a *logical principle*, that *cannot be reduced to a still simpler one, but is used everywhere in mathematical deductions without hesitation* (see [107, p. 516]). Even though in Zermelo's view the Axiom of Choice was "self-evident", which is not the same as "obvious" (see Shapiro [81, §5] for a detailed discussion of the meaning of "self-evidence"), not all mathematicians at that time shared Zermelo's opinion. Moreover, after the first proof of the Well-Ordering Principle was published in 1904, the mathematical journals (especially volume 60 of *Mathematische Annalen*) were flooded with critical notes rejecting the proof (see for example Moore [66, Chapter 2]), mostly arguing that the Axiom of Choice was either illegitimate or meaningless (*cf.* Fraenkel, Bar-Hillel, and Lévy [26, p. 82]). The reason for this was not only due to the non-constructive character of the Axiom of Choice, but also because it was not yet clear what a "set" should be. So, Zermelo decided to publish a more detailed proof, and at the same time taking the opportunity to reply to his critics. This resulted in [108], his second proof of the Well-Ordering Principle which was published in 1908, the same year as he presented his first axiomatisation of Set Theory in [108]. It seems that this was not a coincidence. Moore [66, p. 159] writes that *Zermelo's axiomatisation was primarily motivated by a desire to secure his demonstration of the* Well-Ordering Principle *and, in particular, to save his* Axiom of Choice. Moreover, Hallett [32, p. xvi] goes even further by trying to show *that the selection of the axioms themselves was guided by the demands of Zermelo's reconstructed [second] proof*. Hallett's statement is motivated by a remark on page 124 in Zermelo [108], where he emphasises that the proof is just based on certain fixed principles to *build initial sets* and to *derive new sets from given ones*—exactly what we would require for principles to form an axiomatic system of Set Theory.

We would like to mention that because of its different character (*cf.* Bernays [3]) and since he considered the Axiom of Choice as a general logical principle, he did not include the Axiom of Choice to his second axiomatic system of Set Theory.

For a comprehensive survey of Zermelo's Axiom of Choice, its origins, development, and influence, we refer the reader to Moore [66] (see also Kanamori [46], Jech [41], and Fraenkel, Bar-Hillel, and Lévy [26, Chapter II, §4]); and for a biography of Zermelo (including the history of AC and axiomatic Set Theory) we refer the reader to Ebbinghaus [17].

Gödel's Constructible Universe. According to Kanamori [45, p. 28 ff.], in October of 1935 Gödel informed von Neumann at the Institute for Advanced Study in Princeton that he had established the relative consistency of the Axiom of Choice. This he did by devising his constructible (not *constructive*!) hierarchy **L** (for "law") and verifying the Axiom of Choice and the rest of the ZF axioms there. Gödel conjectured that the Continuum Hypothesis would also hold in **L**, but he soon fell ill and only gave a proof of this and the Generalised Continuum Hypothesis (*i.e.*, for all $\alpha \in \Omega$, $2^{\omega_\alpha} = \omega_{\alpha+1}$) two years later. The crucial idea apparently came to him during the night of June 14/15, 1937 (see also [31, pp. 1–8]).

Gödel's article [28] was the first announcement of these results, in which he describes the model **L** as the class *of all "mathematically constructible" sets, where the term "constructible" is to be understood in the semi-intuitionistic sense which excludes impredicative procedures. This means "constructible" sets are defined to be those sets which can be obtained by Russell's ramified hierarchy of types, if extended to include transfinite orders*. In the succeeding article [29], Gödel provided more details in the context of ZF, and in his monograph [30]—based on lectures given at the Institute for Advanced Study during the winter of 1938/39—Gödel gave another presentation of **L**. This time he generated **L** set by set with a transfinite recursion in terms of eight elementary set generators, a sort of Gödel numbering into the transfinite (*cf.* Kanamori [45, p. 30], and for Gödel's work in Set Theory see Kanamori [47]).

Equivalent Forms of the Axiom of Choice. The literature gives numerous examples of theorems which are equivalent to the Axiom of Choice and a huge collection of such equivalent forms of the Axiom of Choice was accumulated by Rubin and Rubin [79, 80].

The most popular variants of the Axiom of Choice—and the most often used in mathematical proofs—are probably the Well-Ordering Principle (discussed above), the Kuratowski–Zorn Lemma, and Teichmüller's Principle.

The Kuratowski–Zorn Lemma was proved independently by Kuratowski [53] and more than a decade later by Zorn [106] (see Moore [66, p. 223] and also Campbell [13]). Usually, the Kuratowski–Zorn Lemma is deduced quite easily from the Well-Ordering Principle. The direct deduction from the Axiom of Choice presented above (THEOREM 5.3) is due to Kneser [51], who also proved LEMMA 5.2 which was stated without proof by Bourbaki [12, p. 37 (lemme fondamental)].

Teichmüller's Principle was formulated independently by Tukey [103] and slightly earlier by Teichmüller in [97], where he provides also some equivalent forms of this very useful principle. Teichmüller himself was a member of the Nazi party and joined the army in 1939. Fighting first in Norway and then at the Eastern Front, he eventually died in 1943.

Kurepa's Principle was introduced by Kurepa in [54], where he showed that Kurepa's Principle together with the Linear-Ordering Principle—which states that every set can be linearly ordered—implies the Axiom of Choice. The proof that—in the presence of the Axiom of Foundation—Kurepa's Principle implies the Axiom of Choice is due to Felgner [18] (see also Felgner and Jech [20] or Jech [40, Theorem 9.1(a)]).

The proof that "every vector space has an algebraic basis" implies Multiple Choice is taken from Blass [9], and the proof that Multiple Choice implies Kurepa's Principle is taken from Jech [40, Theorem 9.1(a)] (compare with Chapter 7 | RELATED RESULT 44).

Among the dozens of cardinal relations which are equivalent to the Axiom of Choice (see for example Lindenbaum and Tarski [60], Bachmann [1, §31], or Moore [66, p. 330 f.]), we just mentioned three.

In 1895, Cantor [14, §2] asserted the Trichotomy of Cardinals without proof, and in a letter of 28 July 1899 (*cf.* [16, pp. 443–447]) he wrote to Dedekind that the Trichotomy of Cardinals follows from the Well-Ordering Principle. However, their equivalence remained unproven until Hartogs [34] established it in 1915 (*cf.* also Moore [66, p. 10]). As a matter of fact we would like to mention that—according to Sierpiński [82, p. 99 f.]—Leśniewski showed that Trichotomy of Cardinals is equivalent to the statement that for any two cardinals $\mathfrak{n}$ and $\mathfrak{m}$, where at least one of these cardinals is infinite, we always have $\mathfrak{n}+\mathfrak{m}=\mathfrak{n}$ or $\mathfrak{n}+\mathfrak{m}=\mathfrak{m}$.

THEOREM 5.5(c)—which is to some extent a dualisation of the Trichotomy of Cardinals—was stated without proof by Lindenbaum [60, p. 312 (A_6)] and the proof given above is taken from Sierpiński [83, p. 426].

The fact that the cardinal equation $\mathfrak{m}^2=\mathfrak{m}$ implies the Axiom of Choice is due to Tarski [87] (see also Bachmann [1, V, p. 140 ff.]).

***Cardinal Arithmetic in the Presence of* AC.** The definition of cardinals given above can also be found for example in von Neumann [72, VII.2. p.731].

The first proof of THEOREM 5.7 appeared in Hessenberg [38, p. 593] (see also Jourdain [44]).

Regularity of cardinals was investigated by Hausdorff, who also raised the question of existence of regular limit cardinals (*cf.* [35, p. 131]).

The INEQUALITY OF KÖNIG–JOURDAIN–ZERMELO 5.11—also known as König's Theorem—was proven by König [52] (but only for countable sums and products), and independently by Jourdain [43] and by Zermelo [110] (for historical facts see Moore [66, p. 154] and Fraenkel [25, p. 98]). Obviously, the INEQUALITY OF KÖNIG–JOURDAIN–ZERMELO implies the Axiom of Choice (since it guarantees that every Cartesian product of non-empty sets is non-empty), and consequently we see that the INEQUALITY OF KÖNIG–JOURDAIN–ZERMELO is *equivalent* to the Axiom of Choice.

Algebras. Boolean algebra is named after George Boole who—according to Russell—discovered Pure Mathematics. Even though this might be an exaggeration, it is true that Boole was one of the first to view Mathematics as the study of abstract structures rather than as the science of magnitude, and he was the first who applied successfully mathematical techniques to Logic (*cf.* Boole [10, 11]) and his work evolved into the modern theory of Boolean algebras and algebraic Logic. In 1849, Boole was appointed at the newly founded Queen's College in Cork, where he died in 1864 as a result of pneumonia caused by walking to a lecture in a December downpour and lecturing all day in wet clothes (see also MacHale [61]).

Lindenbaum's algebra is named in memory of the Polish mathematician Adolf Lindenbaum, who was killed by the Gestapo at Nowa Wilejka in the summer of 1941. Lindenbaum and Tarski (see for example Tarski [89–91]) developed the idea of viewing the set of formulae as an algebra (with operations induced by the logical connectives) independently around 1935; however, Lindenbaum's results were not published (see Rasiowa and Sikorski [78, footnote to page 245]).

For the history of abstract algebraic Logic and Boolean algebras we refer the reader to Font, Jansana, and Pigozzi [22].

Prime Ideals. Ideals and prime ideals on algebras of sets where investigated for example by Tarski in [93].

The notion of Lindenbaum's algebra and the Compactness Theorem for Propositional Logic is taken from Bell and Slomson [2, Chapter 2]. The equivalent forms of the Prime Ideal Theorem are taken from Jech [40, Chapter 2, §3], and the corresponding references can be found in [40, Chapter 2, §7]. We would like to mention that the Ultrafilter Theorem, which is just the dual form of the Prime Ideal Theorem, is due to Tarski [88].

Ramsey's Theorem as a Choice Principle. RAMSEY'S ORIGINAL THEOREM (*cf.* Chapter 2) implies that every infinite set X has the following property: For every 2-colouring of $[X]^2$ there is an infinite subset Y of X such that $[Y]^2$ is monochromatic. As mentioned in Chapter 2, Ramsey [76] explicitly indicated that his proof of this theorem used the Axiom of Choice. Later, Kleinberg [50] showed that every proof of RAMSEY'S ORIGINAL THEOREM must use the Axiom of Choice, although rather weak forms of the Axiom of Choice like $\mathsf{C}(\aleph_0, \infty)$ suffice (see THEOREM 5.17). For the position of Ramsey's Original Theorem in the hierarchy of choice principles we refer the reader to Blass [8] (see also RELATED RESULT 31).

For the fact that none of the implications in THEOREM 5.17 is reversible we refer the reader to Howard and Rubin [39].

From Countable Choice to Choice for Finite Sets. The Countable Axiom of Choice asserts that every *countable* family of non-empty sets has a choice function, whereas the Axiom of Choice for Finite Sets asserts that every family of non-empty *finite* sets has a choice function. Replacing the finite sets in the latter choice principle by n-element sets (for natural numbers $n \geq 2$), we obtained the choice principles C_n

which assert that every family of n-element sets has a choice function. Combining these two choice principles we get in fact versions of König's Lemma, namely choice principles like $\mathsf{C}(\aleph_0, < \aleph_0)$ and $\mathsf{C}(\aleph_0, n)$ (for positive integers $n \geq 2$).

The proof of THEOREM 5.18 is taken from Jech [40, p. 111] and is optimal in the following sense: If the positive integers m, n do not satisfy condition (S), then there is a model of Set Theory in which C_k holds for every $k \leq m$ but C_n fails (see the proof of Theorem 7.16 in Jech [40]).

RELATED RESULTS

22. *Hausdorff's Principle*. Among the numerous maximality principles which are equivalent to the Axiom of Choice, we like to mention the one known as Hausdorff's Principle (*cf.* Hausdorff [35, VI, §1, p. 140]):

    Hausdorff's Principle. Every partially ordered set has a maximal chain (maximal with respect to inclusion "$\subseteq$").

    For the history of Hausdorff's Principle see Moore [66, Section 3.4, p. 167 ff.] and a proof of the equivalence with the Axiom of Choice can be found for example in Bernays [5, p. 142 ff.].

23. *Bases in vector spaces and the Axiom of Choice*. Relations between the existence or non-existence of bases in vector spaces and some weaker forms of the Axiom of Choice are investigated for example in Keremedis [48, 49], Läuchli [55], and Halpern [33].

24. *Cardinal relations which are equivalent to* AC. Below we list a few of the dozens of cardinal relations which are equivalent to the Axiom of Choice (mainly taken from Tarski [87]):
    (a) $\mathfrak{m} \cdot \mathfrak{n} = \mathfrak{m} + \mathfrak{n}$ for all infinite cardinals $\mathfrak{m}$ and $\mathfrak{n}$.
    (b) If $\mathfrak{m}^2 = \mathfrak{n}^2$, then $\mathfrak{m} = \mathfrak{n}$.
    (c) If $\mathfrak{m} < \mathfrak{n}$ and $\mathfrak{p} < \mathfrak{q}$, then $\mathfrak{m} + \mathfrak{p} < \mathfrak{n} + \mathfrak{q}$.
    (d) If $\mathfrak{m} < \mathfrak{n}$ and $\mathfrak{p} < \mathfrak{q}$, then $\mathfrak{m} \cdot \mathfrak{p} < \mathfrak{n} \cdot \mathfrak{q}$.
    (e) If $\mathfrak{m} + \mathfrak{p} < \mathfrak{n} + \mathfrak{p}$, then $\mathfrak{m} < \mathfrak{n}$.
    (f) If $\mathfrak{m} \cdot \mathfrak{p} < \mathfrak{n} \cdot \mathfrak{p}$, then $\mathfrak{m} < \mathfrak{n}$.
    (g) If $2\mathfrak{m} < \mathfrak{m} + \mathfrak{n}$, then $\mathfrak{m} < \mathfrak{n}$.
    For the proofs we refer the reader to Tarski [87] and Sierpiński [83, p. 421] (compare (g) with Chapter 4 | RELATED RESULT 17). More such cardinal relations can be found for example in Howard and Rubin [39, p. 82 ff.], Rubin and Rubin [80, p. 137 ff.], Moore [66, p. 330 f.], and Bachmann [1, §31]).

25. *Successors of Cardinals*. In [96] Tarski investigated the following three types of successor of a cardinal number:

S_1. For every cardinal $\mathfrak{m}$ there is a cardinal $\mathfrak{n}$ such that $\mathfrak{m} < \mathfrak{n}$ and the formula $\mathfrak{m} < \mathfrak{p} < \mathfrak{n}$ does not hold for any cardinal $\mathfrak{p}$.
S_2. For every cardinal $\mathfrak{m}$ there is a cardinal $\mathfrak{n}$ such that $\mathfrak{m} < \mathfrak{n}$ and for every cardinal $\mathfrak{p}$ the formula $\mathfrak{m} < \mathfrak{p}$ implies $\mathfrak{n} \leq \mathfrak{p}$.
S_3. For every cardinal $\mathfrak{m}$ there is a cardinal $\mathfrak{n}$ such that $\mathfrak{m} < \mathfrak{n}$ and for every cardinal $\mathfrak{p}$ the formula $\mathfrak{p} < \mathfrak{n}$ implies $\mathfrak{p} \leq \mathfrak{m}$.

Tarski [96] showed that S_1 can be proved without the help of the Axiom of Choice, whereas S_2 is equivalent to this axiom. The relation of S_3 with the Axiom of Choice was further investigated by Sobociński [84] and Truss [100] (see also Bachmann [1, §31, p. 141]).

26. *A formulation by Sudan*. Sudan [85] showed that the following statement is equivalent to the Axiom of Choice: Let $\mathfrak{m}$, $\mathfrak{n}$, and $\mathfrak{p}$ be arbitrary infinite cardinals. If $\mathfrak{m}$ and $\mathfrak{n}$ are either equal or $\mathfrak{n}$ is a S_1-successor (*i.e.*, a successor in the in the sense of S_1) of $\mathfrak{m}$, then also $\mathfrak{p} \cdot \mathfrak{m}$ and $\mathfrak{p} \cdot \mathfrak{n}$ are either equal or $\mathfrak{p} \cdot \mathfrak{n}$ is an S_1-successor of $\mathfrak{p} \cdot \mathfrak{m}$. For the influence of Tarski [87] on Sudan see Moore [66, p. 218].

27. *A formulation by Tarski*. There are also some equivalents of the Axiom of Choice which seemingly are far away of being choice principles. The following formulation by Tarski [92] is surely of this type: For every set N there is a set M such that $X \in M$ if and only if $X \subseteq M$ and for all $Y \subseteq X$ we have $|Y| \neq |N|$. Similar statements can be found in Tarski [94, 95] (see also Bachmann [1, §31.3]).

28. *Singular Cardinal Hypothesis*. The Singular Cardinal Hypothesis states that for every singular cardinal κ, $2^{\mathrm{cf}(\kappa)} < \kappa$ implies $\kappa^{\mathrm{cf}(\kappa)} = \kappa^+$. Obviously, the SINGULAR CARDINAL HYPOTHESIS follows from the Generalised Continuum Hypothesis. On the other hand, the SINGULAR CARDINAL HYPOTHESIS is not provable within ZFC and in fact, the failure of the SINGULAR CARDINAL HYPOTHESIS is equiconsistent with the existence of a certain large cardinal (*cf.* Jech [42, p. 58 f. & Chapter 24]).

29. *Model Theory and the Prime Ideal Theorem*. Using Lindenbaum's algebra, Rasiowa and Sikorski [77] gave an alternative proof of GÖDEL'S COMPLETENESS THEOREM 3.4, and Henkin [36] proved that the Prime Ideal Theorem is equivalent to the COMPACTNESS THEOREM 3.7. Notice that by THEOREM 5.15 we just find that the Prime Ideal Theorem is equivalent to the Compactness Theorem for Propositional Logic, which is a seemingly weaker statement than the COMPACTNESS THEOREM 3.7.

30. *Colouring infinite graphs and the Prime Ideal Theorem**. For n a positive integer consider the following statement.

P_n: If G is a graph such that every finite subgraph of G is n-colourable, then G itself is n-colourable.

The following implications are provable in Set Theory without the Axiom of Choice (see Mycielski [69, 70]):

$$\mathsf{PIT} \quad\Rightarrow\quad \mathsf{P}_{n+1} \quad\Rightarrow\quad \mathsf{P}_n \quad\Rightarrow\quad \mathsf{C}(\infty, n), \qquad \mathsf{C}(\infty, 2) \quad\Rightarrow\quad \mathsf{P}_2.$$

On the other hand, Lévy [59] showed that for any n, $\mathsf{ZF} \nvdash \mathsf{C}(\infty, n) \Rightarrow \mathsf{P}_3$. Surprisingly, Läuchli showed in [57] that P_3 implies PIT, and consequently, for all $n \geq 3$, the equivalence $\mathsf{P}_n \Rightarrow \mathsf{PIT}$ is provable in Set Theory without the Axiom of Choice. However, the question whether there is a "direct" proof of $\mathsf{P}_3 \Rightarrow \mathsf{P}_4$ without involving PIT is still open.

31. *Ramsey's Theorem, König's Lemma, and countable choice*. Truss investigated in [102] versions of König's Lemma, where restrictions are placed on the degree of branching of the finitely branching tree. In particular, he investigated $\mathsf{C}(\aleph_0, n)$ for different $n \in \omega$. Later in [24], Forster and Truss considered the relation between versions of Ramsey's Original Theorem and these versions of König's Lemma.

    The choice principle $\mathsf{C}(\aleph_0, n)$ was also investigated by Wiśniewski [105], where it is compared with $\mathsf{C}(\infty, n)$ and other weak forms of the Axiom of Choice.

32. *Ramsey Choice**. Related to C_n are the following two choice principles: C_n^- states that every infinite family X of n-element sets has an infinite subfamily $Y \subseteq X$ with a choice function; and RC_n states that for every infinite set X there is an infinite subset $Y \subseteq X$ such that $[Y]^n$ has a choice function. These two choice principles are both strictly weaker than C_n (*cf.* Truss [99]). Montenegro investigated in [65] the relation between RC_n and C_n^- for some small values of n: It is not hard to see that $\mathsf{RC}_2 \Rightarrow \mathsf{C}_2^-$ and $\mathsf{RC}_3 \Rightarrow \mathsf{C}_3^-$ (*cf.* [65, Lemma]). However, it is quite tricky to prove that $\mathsf{RC}_4 \Rightarrow \mathsf{C}_4^-$ (*cf.* [65, Theorem]) and it is still open whether RC_5 implies C_5^-.

33. *Well-ordered and well-orderable subsets of a set*. For a set x, $s(x)$ is the set of all subsets of x which can be well-ordered, and $w(x)$ is the set of all well-orderings of subsets of x. Notice that $s(x) \subseteq \mathscr{P}(x)$, whereas $w(x) \subseteq \mathscr{P}(x \times x)$. Tarski [94] showed—without the help of the Axiom of Choice—that $|x| < |s(x)|$, for any set x, and his proof also yields $|x| < |w(x)|$. Later, Truss showed in [101] that for any infinite set x and for any $n \in \omega$ we have $|s(x)| \nleq |x^n|$ as well as $|x^n| < |w(x)|$. Furthermore, he showed that if there is a choice function for the set of finite subsets of x, then $|x^n| < |s(x)|$. According to Howard and Rubin [39, p. 371] it is not known whether $|x^n| < |s(x)|$ (form 283 of [39]) is provable in ZF. The cardinality of the set $w(x)$ was further investigated by Forster and Truss in [23].

34. *Axiom of Choice for families of n-element sets*. For different $n \in \omega$, C_n has been extensively studied by Mostowski in [67], and most of the following results—which are all provable without the help of the Axiom of Choice—can be found in that paper (see also Truss [99], Gauntt [27], or Jech [40, Chapter 7, §4]):

(a) If m, n satisfy condition (S), then $n < 8m^2$.
(b) $\mathsf{C}_2 \Rightarrow \mathsf{C}_n$ is provable if and only if $n \in \{1, 2, 4\}$.
(c) For a finite set $Z = \{m_1, \ldots, m_k\}$ of positive integers let C_Z denote the statement $\mathsf{C}_{m_1} \wedge \cdots \wedge \mathsf{C}_{m_k}$. We say that Z, n satisfy condition (S) if for every decomposition of n into a sum of primes, $n = p_1 + \ldots + p_s$, at least one prime p_i belongs to Z. Now, the following condition holds: *If Z, n satisfy condition* (S), *then C_Z implies C_n.*
(d) Let S_n be the group of all permutation of $\{1, \ldots, n\}$. A subgroup G of S_n is said to be *fixed point free* if for every $i \in \{1, \ldots, n\}$ there is a $\pi \in S_n$ such that $\pi(i) \neq i$. Let Z be again a finite set of positive integers. We say that Z, n satisfy condition (T) if for every fixed point free subgroup G of S_n there is a subgroup H of G and a finite sequence $H_1, \ldots, H_k$ of proper subgroups of H such that the sum of indices $[H : H_1] + \ldots + [H : H_k]$ is in Z. Now, the following condition holds: *If Z, n satisfy condition* (T), *then C_Z implies C_n.* Moreover we have: *If Z, n do not satisfy condition* (T), *then there is a model of* ZF *in which C_Z holds and C_n fails.*

We would also like to mention that the Axiom of Choice for Finite Sets $\mathsf{C}(\infty, < \aleph_0)$ is unprovable in ZF, even if we assume that C_n is true for each $n \in \omega$ (*cf.* Jech [40, Chapter 7, §4], or Lévy [58] and Pincus [75]).

35. *Ordering principles*. Among the numerous choice principles which deal with ordering we mention just two:

Ordering Principle. Every set can be linearly ordered.

If "$<$" and "$\prec$" are partial orderings of a set P, then we say that "$\prec$" **extends** "$<$" if for any $p, q \in P$, $p < q$ implies $p \prec q$.

Order-Extension Principle. Every partial ordering of a set P can be extended to a linear ordering of P.

Obviously, the Order-Extension Principle implies the Ordering Principle, but the other direction fails (see Mathias [62]). Thus, the Ordering Principle is slightly weaker than the Order-Extension Principle. Furthermore, Szpilrajn—who changed his name from Szpilrajn to Marczewski while hiding from the Nazi persecution—showed in [86] that the Order-Extension Principle follows from the Axiom of Choice, where one can even replace the Axiom of Choice by the Prime Ideal Theorem (see for example Jech [40, 2.3.2]). We leave it as an exercise to the reader to show that the Ordering Principle implies $\mathsf{C}(\infty, < \aleph_0)$. Thus, we get the following sequence of implications:

$$\text{PIT} \Rightarrow \text{Order-Extension Principle} \Rightarrow \text{Ordering Principle} \Rightarrow \mathsf{C}(\infty, < \aleph_0).$$

On the other hand, none of these implications is reversible (see Läuchli [56] and Pincus [74, §4B], Felgner and Truss [21, Lemma 2.1], Mathias [62], or Jech [40, Chapter 7]; compare also with Chapter 7 | RELATED RESULT 48).

36. *More ordering principles*. Mathias showed in [62] that the following assertion does not imply the Order-Extension Principle:

    If X is a set of well-orderable sets, then there is a function f such that for each $x \in X$, $f(x)$ is a well-ordering of x.

    On the other hand, Truss [98] showed that following assertion, apparently only slightly stronger than the ordering principle above, implies the Axiom of Choice:

    If X is a set and f a function on X such that for each $x \in X$, $f(x)$ is a non-empty set of well-orderings of x, then $\{f(x) : x \in X\}$ has a choice function.

37. *Principle of Dependent Choices*. Finally, let us mention a choice principle which is closely related to the Countable Axiom of Choice. Its meaning is that one is allowed to make a countable number of consecutive choices.

    Principle of Dependent Choices. If R is a binary relation on a non-empty set S, and if for every $x \in S$ there exists $y \in S$ with xRy, then there is a sequence $\langle x_n : n \in \omega \rangle$ of elements of S such that for all $n \in \omega$ we have $x_n R x_{n+1}$.

    The Principle of Dependent Choices, usually denoted DC, was formulated by Bernays in [4] and for example investigated by Mostowski [68] (see also Jech [40, Chapter 8]). Even though DC is significantly weaker than AC, it is stronger than $\mathsf{C}(\aleph_0, \infty)$ and (thus) implies for example that every Dedekind-finite set is finite (*i.e.*, every infinity set is transfinite). Thus, in the presence of DC, many propositions are still provable. On the other hand, having just DC instead of full AC, most of the somewhat paradoxical constructions (*e.g.*, making two balls from one) cannot be carried out anymore (see Herrlich [37] for some 'disasters' that happen with and without AC). In my opinion, DC reflects best our intuition, and consequently, ZF + DC would be a quite reasonable and smooth axiomatic system for Set Theory; however, it is not suitable for really exciting results.

38. *An alternative to the Axiom of Choice*. Let $\omega \to (\omega)^\omega$ be the statement that whenever the set $[\omega]^\omega$ is coloured with two colours, there exists an infinite subset of ω, all whose infinite subsets have the same colour (compare with the *Ramsey property* defined in Chapter 9). In Chapter 2 we have seen that $\omega \to (\omega)^\omega$ fails in the presence of the Axiom of Choice. On the other hand, Mathias proved that under the assumption of the existence of an *inaccessible cardinal* (defined on page 302), $\omega \to (\omega)^\omega$ is consistent with ZF + DC (see Mathias [64, Theorem 5.1]). The combinatorial statement $\omega \to (\omega)^\omega$ has many interesting consequences: For example Mathias [63] gave an elementary proof of the fact that if $\omega \to (\omega)^\omega$ holds, then there are no so-called *rare filters* and every ultrafilter over ω is principal (see Mathias [64, p. 91 ff.] for similar results).

39. *The Axiom of Determinacy*. Another alternative to the Axiom of Choice is the Axiom of Determinacy, which asserts that all games of a certain type are determined. In order to be more precise we have to introduce first some terminology:

With each subset A of ${}^{\omega}\omega$ we associate the following game $\mathcal{G}_A$, played by two players I and II. First I chooses a natural number a_0, then II chooses a natural number b_0, then I chooses a_1, then II chooses b_1, and so on. The game ends after ω steps: if the resulting sequence $\langle a_0, b_0, a_1, b_1, \ldots\rangle$ is in A, then I wins, otherwise II wins. A *strategy* (for I or II) is a rule that tells the player what move to make depending on the previous moves of both players; and a strategy is a *winning strategy* if the player who follows it always wins (for a more formal definition see Chapter 10). The game $\mathcal{G}_A$ is *determined* if one of the players has a winning strategy.

Axiom of Determinacy (AD). For every set $A \subseteq {}^{\omega}\omega$ the game $\mathcal{G}_A$ is determined, *i.e.*, either player I or player II has winning strategy.

An easy diagonal argument shows that AC is incompatible with AD, *i.e.*, assuming the Axiom of Choice there exists a set $A \subseteq {}^{\omega}\omega$ such that the game $\mathcal{G}_A$ is not determined (*cf.* Jech [42, Lemma 33.1]). In contrast we find that AD implies that every countable family of non-empty sets of reals has a choice function (*cf.* Jech [42, Lemma 33.2]). Moreover, one can show that Con(ZF + AD) implies Con(ZF + AD + DC), thus, even in the presence of AD we still can have DC. Furthermore, AD implies that sets of reals are well behaved, *e.g.*, every set of reals is *Lebesgue measurable*, has the *property of Baire*, and every uncountable set of reals contains a *perfect subset*, *i.e.*, a closed set without isolated points (*cf.* Jech [42, Lemma 33.3]); however, it also implies that every ultrafilter over ω is principal (*cf.* Kanamori [45, Proposition 28.1]) and that $\aleph_1$ and $\aleph_2$ are both measurable cardinals (*cf.* Jech [42, Theorem 33.12]). Because of its nice consequences for sets of reals, AD is a reasonable alternative to AC, especially for the investigation of the real line (for the beauty of ZF + AD see for example Herrlich [37, Section 7.2]). In 1962, when Mycielski and Steinhaus [71] introduced the Axiom of Determinacy, they did not claim this new axiom to be intuitively true, but stated that the purpose of their paper is *only to propose another theory which seems very interesting although its consistency is problematic*. Since AD implies the existence of large cardinals, the consistency of ZF + AD cannot be derived from that of ZF. Moreover, using very sophisticated techniques—far beyond the scope of this book—Woodin proved that ZF + AD is equiconsistent with ZFC + "There are infinitely many Woodin cardinals" (*cf.* Kanamori [45, Theorem 32.16] or Jech [42, Theorem 33.27]). Further results and the corresponding references can be found for example in Kanamori [45, Chapter 6] and Jech [42, Chapter 33].

REFERENCES

1. HEINZ BACHMANN: ***Transfinite Zahlen***. Springer, Berlin (1967)
2. JOHN L. BELL, ALAN B. SLOMSON: ***Models and Ultraproducts: An Introduction***. North-Holland, Amsterdam (1969)

3. PAUL BERNAYS: *Sur le platonisme dans les mathématiques*. ***Enseign. Math.*** 34, 52–69 (1935) (see [7]/[6] for a translation into English/German)
4. PAUL BERNAYS: *A system of axiomatic set theory. III: Infinity and enumerability. Analysis*. ***J. Symb. Log.*** 7, 65–89 (1942)
5. PAUL BERNAYS: ***Axiomatic Set Theory. With a Historical Introduction by Abraham A. Fraenkel***, 2nd edn. Studies in Logic and the Foundations of Mathematics. North-Holland, Amsterdam (1968) [reprint: Dover, New York (1991)]
6. PAUL BERNAYS: ***Abhandlungen zur Philosophie der Mathematik***. Wissenschaftliche Buchgesellschaft, Darmstadt (1976)
7. PAUL BERNAYS: *On platonism in mathematics*. In: ***Philosophy of Mathematics. Selected Readings***, 2nd edn., Paul Benacerraf, Hilary Putnam (eds.), pp. 258–271. Cambridge University Press, Cambridge (1983)
8. ANDREAS BLASS: *Ramsey's theorem in the hierarchy of choice principles*. ***J. Symb. Log.*** 42, 387–390 (1977)
9. ANDREAS BLASS: *Existence of bases implies the axiom of choice*. In: ***Axiomatic Set Theory***, James E. Baumgartner, Donald A. Martin, Saharon Shelah (eds.). Contemporary Mathematics, vol. 31, pp. 31–33. Am. Math. Soc., Providence (1984)
10. GEORGE BOOLE: *The calculus of logic*. ***The Cambridge and Dublin Math. J.*** 3, 183–198 (1848)
11. GEORGE BOOLE: ***An Investigation of the Laws of Thought, on Which Are Founded the Mathematical Theories of Logic and Probabilities***. Walton and Maberley, London (1854) [reprint: Prometheus Books, New York (2003)]
12. NICOLAS BOURBAKI: ***Éléments de mathématique. Première partie: Les structures fondamentales de l'analyse. Livre I. Théorie des ensembles (Fascicule de résultats)***. Hermann, Paris (1939)
13. PAUL J. CAMPBELL: *The origin of "Zorn's lemma"*. ***Hist. Math.*** 5, 77–89 (1978)
14. GEORG CANTOR: *Beiträge zur Begründung der transfiniten Mengenlehre. I./II*. ***Math. Ann.*** 46/49, 481–512 (1895/1897), 207–246 (see [15] for a translation into English)
15. GEORG CANTOR: ***Contributions to the Founding of the Theory of Transfinite Numbers*** (translation into English of [14]) [translated, and provided with an introduction and notes, by Philip E.B. Jourdain]. Open Court Publishing Company, Chicago (1915) [reprint: Dover, New York (1952)]
16. GEORG CANTOR: ***Gesammelte Abhandlungen mathematischen und philosophischen Inhalts***, Mit Erläuternden Anmerkungen sowie mit Ergänzungen aus dem Briefwechsel Cantor–Dedekind, edited by E. Zermelo. Julius Springer, Berlin (1932)
17. HEINZ-DIETER EBBINGHAUS (in cooperation with VOLKER PECKHAUS): ***Ernst Zermelo, An Approach to His Life and Work***. Springer, Berlin (2007)
18. ULRICH FELGNER: *Die Existenz wohlgeordneter, konfinaler Teilmengen in Ketten und das Auswahlaxiom*. ***Math. Z.*** 111, 221–232 (1969) (cf. also [19])
19. ULRICH FELGNER: *Berichtigung zu "Die Existenz wohlgeordneter, konfinaler Teilmengen in Ketten und das Auswahlaxiom"*. ***Math. Z.*** 115, 392 (1970)
20. ULRICH FELGNER, THOMAS JECH: *Variants of the axiom of choice in set theory with atoms*. ***Fundam. Math.*** 79, 79–85 (1973)
21. ULRICH FELGNER, JOHN K. TRUSS: *The independence of the prime ideal theorem from the order-extension principle*. ***J. Symb. Log.*** 64, 199–215 (1999)
22. JOSEP MARIA FONT, RAMON JANSANA, DON PIGOZZI: *A survey of abstract algebraic logic*. ***Stud. Log.*** 74, 13–97 (2003)
23. THOMAS E. FORSTER, JOHN K. TRUSS: *Non-well-foundedness of well-orderable power sets*. ***J. Symb. Log.*** 68, 879–884 (2003)
24. THOMAS E. FORSTER, JOHN K. TRUSS: *Ramsey's Theorem and König's Lemma*. ***Arch. Math. Log.*** 46, 37–42 (2007)
25. ABRAHAM A. FRAENKEL: ***Abstract Set Theory***. Studies in Logic and the Foundations of Mathematics. North-Holland, Amsterdam (1961)

26. ABRAHAM A. FRAENKEL, YEHOSHUA BAR-HILLEL, AZRIEL LEVY: ***Foundations of Set Theory***. Studies in Logic and the Foundations of Mathematics, vol. 67. North-Holland, Amsterdam (1973)
27. ROBERT. J. GAUNTT: *Axiom of choice for finite sets—A solution to a problem of Mostowski*. ***Not. Am. Math. Soc.*** 17, 454 (1970)
28. KURT GÖDEL: *The consistency of the axiom of choice and of the generalized continuum-hypothesis*. ***Proc. Natl. Acad. Sci. USA*** 24, 556–557 (1938) (reprinted in [31])
29. KURT GÖDEL: *Consistency-proof for the generalized continuum-hypothesis*. ***Proc. Natl. Acad. Sci. USA*** 25, 220–224 (1939) (reprinted in [31])
30. KURT GÖDEL: ***The Consistency of the Axiom of Choice and of the Generalized Continuum-Hypothesis with the Axioms of Set Theory***. Annals of Mathematics Studies, vol. 3. Princeton University Press, Princeton (1940) (reprinted in [31])
31. KURT GÖDEL: ***Collected Works, Volume II: Publications 1938–1974***, edited by S. Feferman (Editor-in-chief), J.W. Dawson Jr., S.C. Kleene, G.H. Moore, R.M. Solovay, J. van Heijenoort. Oxford University Press, New York (1990)
32. MICHAEL HALLETT: ***Cantorian Set Theory and Limitation of Size***. Oxford Logic Guides, vol. 10. The Clarendon Press Oxford University Press, New York (1984)
33. JAMES D. HALPERN: *Bases in vector spaces and the axiom of choice*. ***Proc. Am. Math. Soc.*** 17, 670–673 (1966)
34. FRIEDRICH HARTOGS: *Über das Problem der Wohlordnung*. ***Math. Ann.*** 76, 438–443 (1915)
35. FELIX HAUSDORFF: ***Grundzüge der Mengenlehre***. De Gruyter, Leipzig (1914) [reprint: Chelsea, New York (1965)]
36. LEON HENKIN: *Metamathematical theorems equivalent to the prime ideal theorems for Boolean algebras*. ***Bull. Am. Math. Soc.*** 60, 388 (1954)
37. HORST HERRLICH: ***Axiom of Choice***. Lecture Notes in Mathematics, vol. 1876. Springer, Berlin (2006)
38. GERHARD HESSENBERG: ***Grundbegriffe der Mengenlehre***. Vandenhoeck & Ruprecht, Göttingen (1906)
39. PAUL HOWARD, JEAN E. RUBIN: ***Consequences of the Axiom of Choice***. Mathematical Surveys and Monographs, vol. 59. Am. Math. Soc., Providence (1998)
40. THOMAS JECH: ***The Axiom of Choice***. Studies in Logic and the Foundations of Mathematics, vol. 75. North-Holland, Amsterdam (1973)
41. THOMAS JECH: *About the axiom of choice*. In: ***Handbook of Mathematical Logic***, J. Barwise (ed.), pp. 345–370. North-Holland, Amsterdam (1977)
42. THOMAS JECH: ***Set Theory***, *The Third Millennium Edition, Revised and Expanded*. Springer Monographs in Mathematics. Springer, Berlin (2003)
43. PHILIP E.B. JOURDAIN: *On infinite sums and products of cardinal numbers*. ***Q. J. Pure Appl. Math.*** 39, 375–384 (1907)
44. PHILIP E.B. JOURDAIN: *The multiplication of Alephs*. ***Math. Ann.*** 65, 506–512 (1908)
45. AKIHIRO KANAMORI: ***The Higher Infinite, Large Cardinals in Set Theory from Their Beginnings***. Perspectives in Mathematical Logic. Springer, Heidelberg (1994)
46. AKIHIRO KANAMORI: *The mathematical import of Zermelo's well-ordering theorem*. ***Bull. Symb. Log.*** 3, 281–311 (1997)
47. AKIHIRO KANAMORI: *Gödel and set theory*. ***Bull. Symb. Log.*** 13, 153–188 (2007)
48. KYRIAKOS KEREMEDIS: *Bases for vector spaces over the two-element field and the axiom of choice*. ***Proc. Am. Math. Soc.*** 124, 2527–2531 (1996)
49. KYRIAKOS KEREMEDIS: *Extending independent sets to bases and the axiom of choice*. ***Math. Log. Q.*** 44, 92–98 (1998)
50. EUGENE M. KLEINBERG: *The independence of Ramsey's theorem*. ***J. Symb. Log.*** 34, 205–206 (1969)
51. HELLMUTH KNESER: *Eine direkte Ableitung des Zornschen Lemmas aus dem Auswahlaxiom*. ***Math. Z.*** 53, 110–113 (1950)
52. JULIUS KÖNIG: *Zum Kontinuum-Problem*. ***Math. Ann.*** 60, 177–180 (1905)

53. CASIMIR KURATOWSKI: *Une méthode d'élimination des nombres transfinis des raisonnements mathématiques*. ***Fundam. Math.*** 3, 76–108 (1922)
54. DJURO (GEORGE) KUREPA: *Über das Auswahlaxiom*. ***Math. Ann.*** 126, 381–384 (1953)
55. HANS LÄUCHLI: *Auswahlaxiom in der Algebra*. ***Comment. Math. Helv.*** 37, 1–18 (1962)
56. HANS LÄUCHLI: *The independence of the ordering principle from a restricted axiom of choice*. ***Fundam. Math.*** 54, 31–43 (1964)
57. HANS LÄUCHLI: *Coloring infinite graphs and the Boolean prime ideal theorem*. ***Isr. J. Math.*** 9, 422–429 (1971)
58. AZRIEL LÉVY: *Axioms of multiple choice*. ***Fundam. Math.*** 50, 475–483 (1961)
59. AZRIEL LÉVY: *Remarks on a paper by J. Mycielski*. ***Acta Math. Acad. Sci. Hung.*** 14, 125–130 (1963)
60. ADOLF LINDENBAUM, ALFRED TARSKI: *Communication sur les recherches de la théorie des ensembles*. ***C. R. Séances Soc. Sci. et des Lettres de Varsovie, Classe III*** 19, 299–330 (1926)
61. DESMOND MACHALE: *George Boole 1815–64*. In: ***Creators of Mathematics: The Irish Connection***, K. Houston (ed.), pp. 27–32. University College Dublin Press, Dublin (2000)
62. ADRIAN RICHARD DAVID MATHIAS: *The order extension principle*. In: ***Axiomatic Set Theory***, Thomas J. Jech (ed.). Proceedings of Symposia in Pure Mathematics, vol. XIII, Part II, pp. 179–183. Am. Math. Soc., Providence (1974)
63. ADRIAN RICHARD DAVID MATHIAS: *A remark on rare filters*. In: ***Infinite and Finite Sets***, A. Hajnal, R. Rado, V. Sós (eds.). Colloquium Keszthely, Hungary, 1973; dedicated to P. Erdős on his 60th birthday. Colloquia Mathematica Societatis János Bolyai, vol. 10, pp. 1095–1097. North-Holland, Amsterdam (1975)
64. ADRIAN RICHARD DAVID MATHIAS: *Happy families*. ***Ann. Math. Log.*** 12, 59–111 (1977)
65. CARLOS H. MONTENEGRO: *Weak versions of the axiom of choice for families of finite sets*. In: ***Models, Algebras, and Proofs***, *Selected Papers of the X Latin American Symposium on Mathematical Logic*, Bogotá, Colombia, June 24–29, 1995, X. Caicedo, C. Montenegro (eds.). Lecture Notes in Pure and Applied Mathematics, vol. 203, pp. 57–60. Dekker, New York (1999)
66. GREGORY H. MOORE: ***Zermelo's Axiom of Choice. Its Origins, Development, and Influence***. Studies in the History of Mathematics and Physical Sciences, vol. 8. Springer, New York (1982)
67. ANDRZEJ MOSTOWSKI: *Axiom of choice for finite sets*. ***Fundam. Math.*** 33, 137–168 (1945)
68. ANDRZEJ MOSTOWSKI: *On the principle of dependent choices*. ***Fundam. Math.*** 35, 127–130 (1948)
69. JAN MYCIELSKI: *Some remarks and problems on the colouring of infinite graphs and the theorem of Kuratowski*. ***Acta Math. Acad. Sci. Hung.*** 12, 125–129 (1961)
70. JAN MYCIELSKI: *Correction to: "On the colouring of infinite graphs and the theorem of Kuratowski"*. ***Acta Math. Acad. Sci. Hung.*** 18, 339–340 (1967)
71. JAN MYCIELSKI, HUGO STEINHAUS: *A mathematical axiom contradicting the axiom of choice*. ***Bull. Acad. Pol. Sci., Sér. Sci. Math. Astron. Phys.*** 10, 1–3 (1962)
72. JOHN VON NEUMANN: *Die Axiomatisierung der Mengenlehre*. ***Math. Z.*** 27, 669–752 (1928)
73. GIUSEPPE PEANO: *Démonstration de l'intégrabilité des équations différentielles ordinaires*. ***Math. Ann.*** 37, 182–228 (1890)
74. DAVID PINCUS: *Zermelo–Fraenkel consistency results by Fraenkel–Mostowski methods*. ***J. Symb. Log.*** 37, 721–743 (1972)
75. DAVID PINCUS: *The strength of the Hahn–Banach theorem*. In: ***Victoria Symposium on Nonstandard Analysis*** (Univ. Victoria, Victoria, B.C., 1972). Lecture Notes in Mathematics, vol. 369, pp. 203–248. Springer, Berlin (1974)
76. FRANK P. RAMSEY: *On a problem of formal logic*. ***Proc. Lond. Math. Soc., Ser. II*** 30, 264–286 (1930)
77. HELENA RASIOWA, ROMAN SIKORSKI: *A proof of the completeness theorem of Gödel*. ***Fundam. Math.*** 37, 193–200 (1950)

78. HELENA RASIOWA, ROMAN SIKORSKI: ***The Mathematics of Metamathematics***. Monografie Matematyczne, vol. 41. Państwowe Wydawnictwo Naukowe, Warsaw (1963)
79. HERMAN RUBIN, JEAN E. RUBIN: ***Equivalents of the Axiom of Choice***. Studies in Logic and the Foundations of Mathematics. North-Holland, Amsterdam (1963)
80. HERMAN RUBIN, JEAN E. RUBIN: ***Equivalents of the Axiom of Choice, II***. Studies in Logic and the Foundations of Mathematics, vol. 116. North-Holland, Amsterdam (1985)
81. STEWART SHAPIRO: *We hold these truths to be self-evident: but what do we mean by that*? ***Rev. Symb. Log.*** 2, 175–207 (2009)
82. WACŁAW SIERPIŃSKI: ***Leçons sur les Nombres Transfinis***. Gauthier–Villars, Paris (1928)
83. WACŁAW SIERPIŃSKI: ***Cardinal and Ordinal Numbers***. Państwowe Wydawnictwo Naukowe, Warszawa (1958)
84. BOLESŁAW SOBOCIŃSKI: *A remark concerning the third theorem about the existence of successors of cardinals*. ***Notre Dame J. Form. Log.*** 3, 279–283 (1962)
85. GABRIEL SUDAN: *Sur une note de A. Tarski*. ***C. R. Séances Inst. Sci. Roum.*** 3, 7–8 (1939)
86. EDWARD SZPILRAJN: *Sur l'extension de l'ordre partiel*. ***Fundam. Math.*** 16, 386–389 (1930)
87. ALFRED TAJTELBAUM-TARSKI: *Sur quelques théorèmes qui équivalent à l'axiome du choix*. ***Fundam. Math.*** 5, 147–154 (1924)
88. ALFRED TARSKI: *Une contribution à la théorie de la mesure*. ***Fundam. Math.*** 15, 42–50 (1930)
89. ALFRED TARSKI: *Grundzüge des Systemenkalküls. I*. ***Fundam. Math.*** 25, 503–526 (1935)
90. ALFRED TARSKI: *Zur Grundlegung der Boole'schen Algebra I*. ***Fundam. Math.*** 24, 177–198 (1935)
91. ALFRED TARSKI: *Grundzüge des Systemenkalküls. II*. ***Fundam. Math.*** 26, 283–301 (1936)
92. ALFRED TARSKI: *Eine äquivalente Formulierung des Auswahlaxioms*. ***Fundam. Math.*** 30, 197–201 (1938)
93. ALFRED TARSKI: *Ideale in vollstandigen Mengenkorpern. I*. ***Fundam. Math.*** 32, 45–63 (1939)
94. ALFRED TARSKI: *On well-ordered subsets of any set*. ***Fundam. Math.*** 32, 176–183 (1939)
95. ALFRED TARSKI: *Axiomatic and algebraic aspects of two theorems on sums of cardinals*. ***Fundam. Math.*** 35, 79–104 (1948)
96. ALFRED TARSKI: *Theorems on the existence of successors of cardinals and the axiom of choice*. ***K. Ned. Akad. Wet., Proc. Sect. Sci., Ser. A*** 57, 26–32 (1954)
97. OSWALD TEICHMÜLLER: *Braucht der Algebraiker das Auswahlaxiom?* ***Dtsch. Math.*** 4, 567–577 (1939)
98. JOHN K. TRUSS: *Two equivalents of the axiom of choice*. ***J. Lond. Math. Soc. (2)*** 6, 175–176 (1972)
99. JOHN K. TRUSS: *Finite axioms of choice*. ***Ann. Math. Log.*** 6, 147–176 (1973)
100. JOHN K. TRUSS: *On successors in cardinal arithmetic*. ***Fundam. Math.*** 78, 7–21 (1973)
101. JOHN K. TRUSS: *The well-ordered and well-orderable subsets of a set*. ***Z. Math. Log. Grundl. Math.*** 19, 211–214 (1973)
102. JOHN K. TRUSS: *Some cases of König's lemma*. In: ***Set Theory and Hierarchy Theory***, W. Marek, M. Srebrny, A. Zarach (eds.). Lecture Notes in Mathematics, vol. 537, pp. 273–284. Springer, Berlin (1976)
103. JOHN W. TUKEY: ***Convergence and Uniformity in Topology***. Annals of Mathematics Studies, vol. 2. Princeton University Press, Princeton (1940)
104. JEAN VAN HEIJENOORT: ***From Frege to Gödel. A Source Book in Mathematical Logic, 1879–1931***. Source Books in the History of Science. Harvard University Press, Cambridge (1967)
105. KAZIMIERZ WIŚNIEWSKI: *On the axiom of choice for families of finite sets*. ***Fundam. Math.*** 73, 187–192 (1972)
106. MAX ZORN: *A remark on method in transfinite algebra*. ***Bull. Am. Math. Soc.*** 41, 667–670 (1935)
107. ERNST ZERMELO: *Beweis, dass jede Menge wohlgeordnet werden kann*. ***Math. Ann.*** 59, 514–516 (1904) (see [104, 109] for a translation into English)

108. ERNST ZERMELO: *Neuer Beweis für die Möglichkeit einer Wohlordnung*. ***Math. Ann.*** 65, 107–128 (1908) (see [104, 109] for a translation into English)
109. ERNST ZERMELO: ***Collected Works/Gesammelte Werke***, *Volume I: Set Theory, Miscellanea/Band I: Mengenlehre, Varia*, Heinz-Dieter Ebbinghaus, Craig G. Fraser, Akihiro Kanamori (eds.). Schriften der Mathematisch-naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften, Nr. 21 (2010). Springer, Berlin (2010)
110. ERNST ZERMELO: *Untersuchungen über die Grundlagen der Mengenlehre. I*. ***Math. Ann.*** 65, 261–281 (1908) (see [104, 109] for a translation into English)