A
Appendix

This appendix collects various properties used throughout the text: several formulations of the ascending and descending chain conditions; several formulations of the axiom of choice; basic properties of ordinal and cardinal numbers.

1. Chain Conditions

The conditions in question are two useful finiteness conditions: the ascending chain condition and the descending chain condition.

The ascending chain condition is a property of some partially ordered sets. Recall that a *partially ordered set*, $(X, \leqq)$ or just X, is an ordered pair of a set X and a binary relation $\leqq$ on X, the *partial order relation* on X, that is reflexive ($x \leqq x$), transitive ($x \leqq y$, $y \leqq z$ implies $x \leqq z$), and antisymmetric ($x \leqq y$, $y \leqq x$ implies $x = y$). (A *total* order relation also has $x \leqq y$ or $y \leqq x$, for every $x, y \in X$; then X is *totally ordered.*)

Proposition **1.1.** *For a partially ordered set X the following conditions are equivalent:*

(1) *every infinite ascending sequence $x_1 \leqq x_2 \leqq \cdots \leqq x_n \leqq x_{n+1} \leqq \cdots$ of elements of X* terminates (*is eventually stationary*): *there exists $N > 0$ such that $x_n = x_N$ for all $n \geqq N$;*

(2) *there is no infinite strictly ascending sequence $x_1 < x_2 < \cdots < x_n < x_{n+1} < \cdots$ of elements of X;*

(3) *every nonempty subset S of X has a* maximal *element* (*an element s of S such that there is no $s < x \in S$*).

Proof. (1) implies (2), since a strictly ascending infinite sequence cannot terminate.

(2) implies (3). If the nonempty set S in (c) has no maximal element, then one can choose $x_1 \in S$; since x_1 is not maximal in S one can choose $x_1 < x_2 \in S$; since x_2 is not maximal in S one can choose $x_1 < x_2 < x_3 \in S$; this continues indefinitely and, before you know it, you are saddled with an infinite strictly ascending sequence. (This argument implicitly uses the axiom of choice.)

(3) implies (1): some x_N must be maximal in the sequence $x_1 \leqq x_2 \leqq \cdots$ (actually, in the set $\{ x_n \mid n > 0 \}$), and then $x_N \leqq x_n$ implies $x_N = x_n$ when $n \geqq N$, since $x_N < x_n$ is impossible. □

A *chain* of a partially ordered set $(X, \leqq)$ is a subset of X that is totally ordered by $\leqq$. The infinite ascending sequences in (1) and (2) are traditionally called chains; this has been known to lure unwary readers into a deranged belief that all chains are ascending sequences.

Definition. The ascending chain condition *or* a.c.c. *is condition* (2) *in Proposition* 1.1.

The a.c.c. is a *finiteness condition*, meaning that it holds in every finite partially ordered set. Partially ordered sets that satisfy the a.c.c. are sometimes called *Noetherian*; this terminology is more often applied to bidules such as rings and modules whose ideals or submodules satisfy the a.c.c., when partially ordered by inclusion. In these cases the a.c.c. usually holds if and only if the subbidules are finitely generated. We prove this in the case of groups.

Proposition **1.2.** *The subgroups of a group G satisfy the ascending chain condition if and only if every subgroup of G is finitely generated.*

Proof. Assume that every subgroup of G is finitely generated, and let $H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n \subseteq H_{n+1} \subseteq \cdots$ be an infinite ascending sequence of subgroups of G. The union $H = \bigcup_{n>0} H_n$ is a subgroup, by I.3.9, and is generated by finitely many elements $x_1, \ldots, x_k$ of H. Then every x_i belongs to some H_{n_i}. If $N \geqq \max(n_1, \ldots, n_k)$, then H_N contains every x_i, $H \subseteq H_N$, and $H_n = H_N$ for all $n \geqq N$, since $H_N \subseteq H_n \subseteq H \subseteq H_N$. Thus the subgroups of G satisfy the ascending chain condition.

Conversely, assume that the subgroups of G satisfy the a.c.c. Let H be a subgroup of G. The set $\mathcal{S}$ of finitely generated subgroups of H is not empty, since, for instance, $\{1\} \in \mathcal{S}$. Therefore $\mathcal{S}$ has a maximal element M, which is generated by some $x_1, \ldots, x_k \in M$. For every $h \in H$, the subgroup K of H generated by $x_1, \ldots, x_k$ and h is finitely generated and contains M; hence $K = M$ and $h \in M$. Thus $H = M$, and H is finitely generated. □

Noetherian induction uses the a.c.c. to produce maximal elements, as in this last proof. Proposition 1.2 could be proved by ordinary induction: if H is not finitely generated, then H has a finitely generated subgroup $H_1 \subsetneqq H$; adding a generator $h \in H \setminus H_1$ to the generators of H_1 yields a finitely generated subgroup $H_1 \subsetneqq H_2 \subsetneqq H$, since H is not finitely generated; continuing thus contradicts the a.c.c. We recognize the proof that (2) implies (3) in Proposition 1.1. Noetherian induction is more elegant but not essentially different.

The descending chain condition is also a property of some partially ordered sets, which the next result shows is closely related to the a.c.c.

Proposition **1.3.** *If $\leqq$ is a partial order relation on a set X, then so is the opposite relation, $x \leqq^{\mathrm{op}} y$ if and only if $y \leqq x$.*

We omit the proof, to avoid insulting our readers.

Definition. If $X = (X, \leqq)$ *is a partially ordered set, then* $X^{\mathrm{op}} = (X, \leqq^{\mathrm{op}})$ *is its* opposite *partially ordered set.*

By Proposition 1.3, a theorem that holds in *every* partially ordered set X also holds in its opposite, and remains true when all inequalities are reversed. Thus Proposition 1.1 yields:

Proposition **1.4.** *For a partially ordered set* X *the following conditions are equivalent:*

(1) *every infinite descending sequence* $x_1 \geqq x_2 \geqq \cdots \geqq x_n \geqq x_{n+1} \geqq \cdots$ *of elements of* X terminates*: there exists* $N > 0$ *such that* $x_n = x_N$ *for all* $n \geqq N$*;*

(2) *there is no infinite strictly descending sequence* $x_1 > x_2 > \cdots > x_n > x_{n+1} > \cdots$ *of elements of* X*;*

(3) *every nonempty subset* S *of* X *has a* minimal *element* (*an element* s *of* S *such that there is no* $s > x \in S$).

Definition. The descending chain condition *or* d.c.c. *is condition* (2) *in Proposition* 1.4.

Like the a.c.c., the d.c.c. is a finiteness condition. Partially ordered sets that satisfy the d.c.c. are sometimes called *Artinian*; this terminology is more often applied to bidules such as rings and modules whose ideals or submodules satisfy the d.c.c., when partially ordered by inclusion.

Artinian induction uses the d.c.c. to produce minimal elements. This includes *strong induction* on a natural number n, in which the induction hypothesis is that the desired result holds for all smaller values of n. This works because the natural numbers satisfy the d.c.c.: if the desired result was false for some n, then it would be false for some minimal n, and true for all smaller values of n, which is precisely the situation ruled out by strong induction.

Exercises

1. Show that the subgroups of the additive group $\mathbb{Z}$ do not satisfy the d.c.c.

2. Show that the a.c.c. does not imply the d.c.c., and that the d.c.c. does not imply the a.c.c. (Hence neither condition implies finiteness.)

3. Prove the following: when a partially ordered set X satisfies the a.c.c. and the d.c.c., then every chain of elements of X is finite.

4. Construct a partially ordered set X that satisfies the a.c.c. and the d.c.c., and contains a finite chain with n elements for every positive integer n.

5. Show that a partially ordered set X satisfies the a.c.c. if and only if every nonempty chain C of X has a *greatest* element (an element m of C such that $x \leqq m$ for all $x \in C$).

6. Greatest elements are sometimes inaccurately called *unique maximal* elements. Construct a partially ordered set X with just one maximal element and no greatest element.

7. Let the partially ordered set X satisfy the d.c.c. You have just devised a proof that if a certain property of elements of X is true for every $y < x$ in X, then it is true for x (where $x \in X$ is arbitrary). Can you conclude that your property is true for all $x \in X$?

2. The Axiom of Choice

This section contains the axiom of choice (first formulated by Zermelo [1904]) and some of its useful consequences, including the most useful, Zorn's lemma.

Axiom of Choice: *Every set has a choice function.*

A *choice function* on a set S is a mapping c that assigns to every nonempty subset T of S an element $c(T)$ of T. (Thus c chooses one element $c(T)$ in each nonempty T.) Though less "intuitively obvious" than other axioms, the axiom of choice became one of the generally accepted axioms of set theory after Gödel [1938] proved that it is consistent with the other generally accepted axioms, and may therefore be assumed without generating contradictions.

In this section we give a number of useful statements that are equivalent to the axiom of choice (assuming the other axioms of set theory).

Proposition **2.1.** *The axiom of choice is equivalent to the following statement: when I is a nonempty set, and $(S_i)_{i\in I}$ is a family of nonempty sets, then $\prod_{i\in I} S_i$ is nonempty.*

Proof. Recall that $\prod_{i\in I} S_i$ is the set of all mappings (usually written as families) that assign to each $i \in I$ some element of S_i. If $I \neq \emptyset$ and $S_i \neq \emptyset$ for all i, and the axiom of choice holds, then $\bigcup_{i\in I} S_i$ has a choice function c, and then $\big(c(S_i)\big)_{i\in I} \in \prod_{i\in I} S_i$, so that $\prod_{i\in I} S_i \neq \emptyset$.

Conversely, assume that $\prod_{i\in I} S_i$ is nonempty whenever I is nonempty and $(S_i)_{i\in I}$ is a family of nonempty sets. Let S be any set. If $S = \emptyset$, then the empty mapping is a choice function on S. If $S \neq \emptyset$, then so is $\prod_{T\subseteq S,\, T\neq\emptyset} T$; an element of $\prod_{T\subseteq S,\, T\neq\emptyset} T$ is precisely a choice function on S. □

Zorn's lemma is due to Zorn [1935], though Hausdorff [1914] and Kuratowski [1922] had published closely related statements. Recall that a *chain* of a partially ordered set X is a subset C of X such that at least one of the statements $x \leqq y$, $y \leqq x$ holds for every $x, y \in C$. An *upper bound* of C in X is an element b of X such that $x \leqq b$ for all $x \in C$.

Zorn's Lemma: *when X is a nonempty partially ordered set, and every nonempty chain of X has an upper bound in X, then X has a maximal element.*

Theorem **2.2.** *The axiom of choice is equivalent to Zorn's lemma.*

We defer the proof. That Zorn's lemma implies the axiom of choice is shown later in this section, with Theorem 2.4. The converse is proved in Section 4.

Zorn's lemma provides a method of proof, *transfinite induction,* which is similar to integer induction and to Noetherian induction but is much more powerful. For instance, suppose that we want to prove that some nonempty partially ordered set X has a maximal element. Using ordinary induction we could argue as follows. Since X is not empty there exists $x_1 \in X$. If x_1 is not maximal, then $x_1 < x_2$ for some $x_2 \in X$. If x_2 is not maximal, then $x_2 < x_3$ for some $x_3 \in X$. Continuing in this fashion yields a strictly ascending sequence, which is sure to reach a maximal element only if X satisfies the ascending chain condition (equivalently, if every nonempty chain of X has a greatest element). Zorn's lemma yields a maximal element under the much weaker hypothesis that every nonempty chain of X has an upper bound. The proof in Section 4 reaches a maximal element by constructing a strictly ascending sequence that is indexed by ordinal numbers and can be as infinitely long as necessary.

Previous chapters contain numerous applications of Zorn's lemma. The author feels that this section should contain one; the exercises give more. Recall that a *cross section* of an equivalence relation on a set X is a subset S of X such that every equivalence class contains exactly one element of X.

Corollary **2.3.** *Every equivalence relation has a cross section.*

Proof. Let X be a set with an equivalence relation. Let $\mathcal{S}$ be the set of all subsets S of X such that every equivalence class contains at most one element of S. Then $\mathcal{S} \neq \emptyset$, since $\emptyset \in \mathcal{S}$. Partially order $\mathcal{S}$ by inclusion. We show that $S = \bigcup_{i \in I} S_i \in \mathcal{S}$ when $(S_i)_{i \in I}$ is a chain of elements of $\mathcal{S}$. If $x, y \in S$, then $x \in S_i$ and $y \in S_j$ for some $i, j \in I$, with $S_i \subseteq S_j$ or $S_j \subseteq S_i$, since $(S_i)_{i \in I}$ is a chain, so that, say, $x, y \in S_i$. If x and y are equivalent, then $x = y$, since $S_i \in \mathcal{S}$. Thus $S \in \mathcal{S}$: every chain of $\mathcal{S}$ has an upper bound in $\mathcal{S}$.

By Zorn's lemma, $\mathcal{S}$ has a maximal element S. Then every equivalence class C contains an element of S: otherwise, $S \cup \{c\} \in \mathcal{S}$ for any $c \in C$, in defiance of the maximality of S. Hence S is a cross section. □

Readers can also derive Corollary 2.3 directly from the axiom of choice.

Well ordered sets. A *well ordered* set is a partially ordered set X in which every nonempty subset S has a *least* element (an element s of S such that $s \leqq x$ for every $x \in S$).

For example, $\mathbb{N}$ is well ordered. A well ordered set is totally ordered (since every subset $\{x, y\}$ must have a least element) and satisfies the descending chain condition (since a least element of S is, in particular, a minimal element of S).

Theorem **2.4** (Zermelo [1904]). *The axiom of choice is equivalent to the* well-ordering principle: *every set can be well ordered.*

Proof. A well ordered set S has a choice function, which assigns to each nonempty subset of S its least element. Hence the well-ordering principle implies the axiom of choice. We show that Zorn's lemma implies the well-ordering

principle (hence implies the axiom of choice). That the axiom of choice implies Zorn's lemma is proved in Section 4.

Given a set S, let $\mathcal{W}$ be the set of all ordered pairs $(X, \leqq_X)$ such that $X \subseteq S$ and X is well ordered by $\leqq_X$. Then $\mathcal{W} \neq \emptyset$, since $\emptyset \subseteq S$ is well ordered by the empty order relation. Let $(X, \leqq_X) \leqq (Y, \leqq_Y)$ in $\mathcal{W}$ when

(a) $X \subseteq Y$;

(b) when $x', x'' \in X$, then $x' \leqq_X x''$ if and only if $x' \leqq_Y x''$; and

(c) if $y \in Y$ and $y \leqq_Y x \in X$, then $y \in X$;

equivalently, when $(X, \leqq_X)$ is the lower part of $(Y, \leqq_Y)$ with the induced order relation. It is immediate that this defines an order relation on $\mathcal{W}$.

Let $(X_i, \leqq_i)_{i \in I}$ be a chain of W. If $x, y \in X = \bigcup_{i \in I} X_i$, then let $x \leqq_X y$ if and only if $x, y \in X_i$ and $x \leqq_i y$, for some $i \in I$. If also $x, y \in X_j$ and $x \leqq_j y$ for some $j \in I$, then, say, $(X_i, \leqq_i) \leqq (X_j, \leqq_j)$, and $x \leqq_i y$ if and only if $x \leqq_j y$ by (b). Similarly, if $x \leqq_X y$ and $y \leqq_X x$, then $x, y \in X_i$, $x \leqq_i y$ and $x, y \in X_j$, $y \leqq_j x$ for some $i, j \in I$; if, say, $(X_i, \leqq_i) \leqq (X_j, \leqq_j)$, then $x \leqq_j y$ and $y \leqq_j x$, whence $x = y$. Thus $\leqq_X$ is antisymmetric. Similar arguments show that $\leqq_X$ is reflexive and transitive.

Let T be a nonempty subset of X. Then $T \cap X_i \neq \emptyset$ for some i, and $T \cap X_i$ has a least element t under $\leqq_i$. In fact, t is the least element of T. Indeed, let $u \in T$, $u \in X_j$ for some j. If $(X_i, \leqq_i) \leqq (X_j, \leqq_j)$, then $t \leqq_X u$, since $u <_j t \in X_i$ would imply $u \in X_i$ by (c) and $u <_i t$ by (b), so that t would not be the least element of $T \cap X_i$. If $(X_j, \leqq_j) \leqq (X_i, \leqq_i)$, then $u \in X_i$ and $t \leqq_X u$. Thus X is well ordered by $\leqq_X$, and $(X, \leqq_X) \in \mathcal{W}$.

If $x, y \in X_i$, then we saw at the beginning of the proof that $x \leqq_X y$ if and only if $x \leqq_i y$. Let $y \in X$ and $y \leqq_X x \in X_i$. Then $x, y \in X_j$ and $y \leqq_j x$ for some j. If $(X_i, \leqq_i) \leqq (X_j, \leqq_j)$, then $y \in X_i$ by (c). If $(X_j, \leqq_j) \leqq (X_i, \leqq_i)$, then again $y \in X_i$. Thus $(X_i, \leqq_i) \leqq (X, \leqq_X)$ for all i, and $(X, \leqq_X)$ is an upper bound of $(X_i, \leqq_i)_{i \in I}$ in $\mathcal{W}$.

At this point we invoke Zorn's lemma and are rewarded with a maximal element $(M, \leqq_M)$ of $\mathcal{W}$. We show that $M = S$. Suppose that $(X, \leqq_X) \in \mathcal{W}$ and $X \subsetneqq S$. Let $s \in S \backslash X$. Extend $\leqq_X$ to $Y = X \cup \{s\}$ so that s is the greatest element of Y. Then Y is well ordered: when $T \subseteq Y$, $T \neq \emptyset$, then s is the least element of T if $T = \{s\}$: otherwise, the least element of $T \cap X$ is also the least element of T. Hence $(X, \leqq_X) < (Y, \leqq_Y)$ and $(X, \leqq_X)$ is not maximal. Therefore $M = S$, and then S is well ordered by $\leqq_M$. □

Exercises

1. Prove that every equivalence relation on a set has a cross section, using the axiom of choice but not Zorn's lemma.

2. The *domain* of a binary relation R is the set $\{ x \mid (x, y) \in R \text{ for some } y \}$. Show that the axiom of choice is equivalent to the following statement: every binary relation contains a mapping that has the same domain.

3. Show that a partially ordered set is well ordered if and only if it is totally ordered and satisfies the descending chain condition.

4. Let G be a group and let $a \in G$, $a \neq 1$. Use Zorn's lemma to prove that there is a subgroup M of G that is maximal such that $a \notin M$ (that is, $a \notin M$, and $M < H \leqq G$ implies $a \in H$).

5. Let G be a group and let A be a subgroup of G. Use Zorn's lemma to prove that there is a subgroup M of G that is maximal such that $M \cap A = 1$ (that is, $M \cap A = 1$, and $M < H \leqq G$ implies $H \cap A \neq 1$).

6. Use Zorn's lemma to prove that every vector space has a maximal linearly independent subset; then show that the latter is a basis.

7. Use Zorn's lemma to prove that every order relation is an intersection of total order relations.

3. Ordinal Numbers

This section contains basic general properties of ordinal numbers.

Definition. Ordinal numbers are most naturally defined as isomorphy classes of well ordered sets. Unfortunately, isomorphy classes of well ordered sets are very large, and embarrassing contradictions arise when such large classes are collected into sets or classes. The most famous is *Russell's paradox*: Let R be the "set" of all sets X such that $X \notin X$. If $R \notin R$, then R is one of the sets X such that $X \notin X$; therefore $R \in R$. But then R is not one of the sets X such that $X \notin X$; therefore $R \notin R$.

Contradictions can be avoided if "large" collections like R are not allowed among sets, and are denied all rights and privileges enjoyed by sets: in this case, the right to belong to a set or collection. Modern ordinal numbers are well ordered sets, chosen so that there is only one in each isomorphy class (as, for instance, in Jech [1978]).

Definition. A set X is transitive *when $x \in X$ and $t \in x$ implies $t \in X$; equivalently, when every element of X is a subset of X.*

The empty set is transitive. Since X transitive implies $X \cup \{X\}$ transitive, the sets $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, etc., are transitive.

Definition. An ordinal number *is a well ordered transitive set in which $x < y$ if and only if $x \in y$.*

The first ordinals are readily found. The empty set is an ordinal. A nonempty ordinal σ has a least element α, which must be empty since $t \in \alpha$ would imply $t \in \sigma$ and $t < \alpha$. If σ has no other element, then $\sigma = \{\emptyset\}$. Otherwise, there is a least $\beta > \alpha$ in σ. Then $\alpha \in \beta$; conversely, $x \in \beta$ implies $x \in \sigma$,

$\alpha \leqq x < \beta$, and $x = \alpha$; hence $\beta = \{\alpha\} = \{\emptyset\}$. If σ has no other element, then $\sigma = \{\alpha, \beta\} = \{\emptyset, \{\emptyset\}\}$. Continuing this process yields the first ordinals, which are generally identified with nonnegative integers:

$$0 = \emptyset, \quad 1 = \{\emptyset\}, \quad 2 = \{\emptyset, \{\emptyset\}\}, \quad 3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \text{etc.}$$

We see that $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, etc.

Readers may prove the following:

Proposition **3.1.** *Every element of an ordinal number is an ordinal number.*

Ordering. Ordinal numbers are ordered by inclusion:

Proposition **3.2.** *If α and β are ordinal numbers, then $\alpha \in \beta$ if and only $\alpha \subsetneqq \beta$. Hence the class Ord of all ordinal numbers is totally ordered, with $\alpha < \beta$ if and only if $\alpha \in \beta$.*

Proof. Since β is transitive, $\alpha \in \beta$ implies $\alpha \subseteq \beta$; moreover, $\alpha \notin \alpha$ (otherwise, $\alpha < \alpha$ in β), whence $\alpha \subsetneqq \beta$. Conversely, assume $\alpha \subsetneqq \beta$. Then $\beta \backslash \alpha$ has a least element γ. If $x \in \gamma$, then $x \in \alpha$: otherwise, γ would not be least. Conversely, $x \in \alpha$ implies $x \neq \gamma$, since $\gamma \notin \alpha$, and $\gamma \notin x$, otherwise, $\gamma \in \alpha$; in the totally ordered set β this implies $x \in \gamma$. Thus $\alpha = \gamma \in \beta$.

Now, let α and β be any ordinal numbers. Then $\delta = \alpha \cap \beta$ is transitive, since α and β are transitive, and is well ordered (as a subset of α) with $x < y$ in δ if and only if $x \in y$. In other words, δ is an ordinal. If $\delta \neq \alpha, \beta$, then $\delta \subsetneqq \alpha, \beta$, $\delta \in \alpha, \beta$ by the above, and $\delta \in \delta$, a contradiction. Therefore $\delta = \alpha$ or $\delta = \beta$; hence $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$. Thus *Ord* is totally ordered by inclusion. □

Propositions 3.1 and 3.2 imply $\alpha = \{\, \beta \in \mathit{Ord} \mid \beta < \alpha \,\}$ for every ordinal α.

Proposition **3.3.** *Every nonempty class of ordinal numbers has a least element.*

Proof. Let $\mathcal{C}$ be a nonempty class of ordinals. Let $\alpha \in \mathcal{C}$. We may assume that α is not the least element of $\mathcal{C}$. Then $\mathcal{C} \cap \alpha \neq \emptyset$ and $\mathcal{C} \cap \alpha \subseteq \alpha$ has a least element γ. In fact, γ is the least element of $\mathcal{C}$: if $\beta \in \mathcal{C}$, then, by 3.2, either $\gamma < \alpha \leqq \beta$, or $\beta \in \alpha \cap \mathcal{C}$ and $\beta \geqq \gamma$. □

Thus *Ord* is a well ordered class.

Proposition **3.4.** *The union of a set of ordinal numbers is an ordinal number.*

Proof. Let S be a set of ordinal numbers. Then $\upsilon = \bigcup_{\sigma \in S} \sigma$ is a set. By 3.2, S is a chain, and any two elements of S are elements of some $\sigma \in S$. It follows that υ is transitive, and is totally ordered, with $x < y$ in υ if and only if $x < y$ in some $\sigma \in S$, if and only if $x \in y$.

Let T be a nonempty subset of υ. Then $T \cap \sigma \neq \emptyset$ for some $\sigma \in S$, and $T \cap \sigma$ has a least element γ. As in the proof of 3.3, γ is the least element of T: if $\tau \in T$, then either $\gamma < \sigma \leqq \tau$, or $\tau \in \sigma \cap T$ and $\tau \geqq \gamma$. □

Corollary **3.5.** *The class Ord of all ordinal numbers is not a set.*

Proof. Let α be an ordinal. The *successor* $\beta = \alpha \cup \{\alpha\}$ of α is also an ordinal, as readers will verify. The result follows from this and 3.4. If *Ord* were a set, then $\bigcup_{\alpha \in Ord} \alpha$ would be an ordinal number, and would be the greatest ordinal number, in particular, would be greater than his successor, a feat easily achieved by King Louis XIV of France but not possible for ordinal numbers. □

Well ordered sets. Now, we show that there is one ordinal number in every isomorphy class of well ordered sets. First, a *lower section* (or *order ideal*) of a partially ordered set X is a subset S of X such that $x \leqq s \in S$ implies $x \in S$. Then X is a lower section of itself; for every $a \in X$ there is a lower section $X(a) = \{ x \in X \mid x < a \}$.

Lemma **3.6.** *A subset S of a well ordered set X is a lower section of X if and only if either $S = X$ or $S = X(a)$ for some $a \in X$.*

Proof. Let $S \neq X$ be a lower section. Then $X \backslash S$ has a least element a. If $x < a$, then $x \in S$: otherwise, a would not be the least element of $X \backslash S$. If $x \in S$, then $x < a$: otherwise, $a \leqq x \in S$ and $a \in S$. Thus $S = X(a)$. □

In general, an *isomorphism* of a partially ordered set X onto a partially ordered set Y is a bijection $\theta : X \longrightarrow Y$ such that $x' \leqq x''$ in X if and only if $\theta(x') \leqq \theta(x'')$ in Y. If X and Y are totally ordered, one needs only the implication "$x' \leqq x''$ implies $\theta(x') \leqq \theta(x'')$": then $\theta(x') \leqq \theta(x'')$ implies $x' \leqq x''$, since $x' > x''$ would imply $\theta(x') > \theta(x'')$.

Lemma **3.7.** *Let S and T be lower sections of a well ordered set X. If $S \cong T$, then $S = T$.*

Proof. Let $S \neq T$ and let $\theta : S \longrightarrow T$ be an isomorphism. By 3.6, $S \subseteq T$ or $T \subseteq S$, and we may exchange S and T if necessary and assume that $S \nsubseteq T$. Then we cannot have $\theta(x) = x$ for all $x \in S$, and the set $\{ x \in S \mid \theta(x) \neq x \}$ has a least element a. Then $\theta(x) = x$ when $x \in S$ and $x < a$, but $\theta(a) \neq a$. If $a < \theta(a) \in T$, then $a \in T$, $a = \theta(x)$ for some $x \in S$, and $\theta(x) < \theta(a)$ implies $x < a$ and $\theta(x) = x < a$, a contradiction. Therefore $\theta(a) < a \in S$, but then $\theta(a) \in S$, $\theta\big(\theta(a)\big) = \theta(a)$, and $\theta(a) = a$, another contradiction. □

Proposition **3.8.** *Every well ordered set is isomorphic to a unique ordinal number.*

Proof. Uniqueness follows from 3.7: if, say, $\alpha < \beta$ in *Ord*, then $\alpha = \{ \gamma \in \beta \mid \gamma < \alpha \}$ is a lower section of β, and $\alpha \ncong \beta$.

Now, let X be a well ordered set. Let φ be the set of all ordered pairs (a, α) such that $a \in X$, $\alpha \in Ord$, and $X(a) \cong \alpha$. Then φ is a mapping: if (a, α), $(b, \beta) \in \varphi$ and $a = b$, then $\alpha \cong X(a) \cong \beta$ and $\alpha = \beta$. Similarly, φ is injective: if (a, α), $(b, \beta) \in \varphi$ and $\alpha = \beta$, then $X(a) \cong X(b)$, $X(a) = X(b)$ by 3.7, and $a = b$ since a is the least element of $X \backslash X(a)$ and similarly for b.

Assume that (a, α), $(b, \beta) \in \varphi$ and $a < b$. Let $\theta : X(b) \longrightarrow \beta$ be an isomorphism. Then $\theta(a) < \beta$ and θ induces an isomorphism of $X(a)$ onto

$\{\gamma \in \beta \mid \gamma < \theta(a)\} = \theta(a)$. (This argument also shows that the domain $\operatorname{dom}\varphi$ of φ is a lower section of X.) Therefore $(a, \theta(a)) \in \varphi$. Hence $\alpha = \theta(a) < \beta$.

Similarly, assume that $(a, \alpha), (b, \beta) \in \varphi$ and $\alpha < \beta$. Let $\zeta : \beta \longrightarrow X(b)$ be an isomorphism. Then $\zeta(\alpha) < b$ and ζ induces an isomorphism of α onto $X(\zeta(\alpha))$. Therefore $(\zeta(\alpha), \alpha) \in \varphi$. (This argument also shows that the range $\operatorname{ran}\varphi$ of φ is a lower section of *Ord*.) Hence $a = \zeta(\alpha) < b$, since φ is injective. Thus φ is an isomorphism of $\operatorname{dom}\varphi$ onto $\operatorname{ran}\varphi$.

Since *Ord* is not a set, $\operatorname{ran}\varphi$ cannot be all of *Ord*, and there is a least ordinal $\gamma \notin \operatorname{ran}\varphi$. Then, as in the proof of 3.6, $\operatorname{ran}\varphi = \{\alpha \in \mathit{Ord} \mid \alpha < \gamma\} = \gamma$. If $\operatorname{dom}\varphi$ is not all of X, then $\operatorname{dom}\varphi = X(c)$ for some $c \in X$ by 3.6, φ is an isomorphism of $X(c)$ onto γ, $(c, \gamma) \in \varphi$, and $c \in \operatorname{dom}\varphi$, a contradiction; therefore $\operatorname{dom}\varphi = X$ and $X \cong \gamma$. □

Successor and limit ordinals. We show that all ordinals are generated by two constructions: unions from Proposition 3.4, and successors, whose definition follows.

Proposition **3.9.** *If α is an ordinal number, then so is $\alpha \cup \{\alpha\}$; in fact, $\alpha \cup \{\alpha\}$ is the least ordinal $\beta > \alpha$.*

The proof is an exercise for our avid readers.

Definition. The successor *of an ordinal number α is the ordinal number $\alpha \cup \{\alpha\}$.*

The successor $\alpha \cup \{\alpha\}$ of α is normally denoted by $\alpha + 1$. (The sum of any two ordinals is defined in the exercises.) It *covers* α: there is no ordinal $\alpha < \beta < \alpha + 1$, since there is no set $\alpha \subsetneqq S \subsetneqq \alpha \cup \{\alpha\}$.

Proposition **3.10.** *An ordinal number α is a successor if and only if it has a greatest element; then the greatest element of α is $\bigcup_{\gamma<\alpha}\gamma < \alpha$ and α is its successor. Otherwise, $\bigcup_{\gamma<\alpha}\gamma = \alpha$.*

Proof. A successor $\alpha = \beta \cup \{\beta\}$ has a greatest element β. Conversely, assume that α has a greatest element β. Then $\bigcup_{\gamma<\alpha}\gamma = \beta < \alpha$, and $\beta < \delta$ implies $\delta \geqq \alpha$, since $\delta < \alpha$ implies $\delta \leqq \beta$. Hence α is the successor of β.

The inclusion $\bigcup_{\gamma<\alpha}\gamma \subseteq \alpha$ holds for every ordinal α. If $\beta = \bigcup_{\gamma<\alpha}\gamma \subsetneqq \alpha$, then $\beta \in \mathit{Ord}$ by 3.4 and $\beta < \alpha$, so that β is the greatest element of α. Therefore $\bigcup_{\gamma<\alpha}\gamma = \alpha$ when α does not have a greatest element. □

Definition. A limit ordinal *is an ordinal $\alpha \neq 0$ such that $\alpha = \bigcup_{\gamma<\alpha}\gamma$.*

Thus, a nonzero ordinal is either 0 or a successor or a limit ordinal (a union or "limit" of lesser ordinals). We can now form a clearer picture of *Ord*. An ordinal α and its successors constitute a sequence $\alpha < \alpha+1 < \alpha+2 < \cdots < \alpha+n < \cdots$ whose union is a limit ordinal. Thus *Ord* is made of sequences

$$0 < 1 < 2 < \cdots < \omega < \omega+1 < \omega+2 < \cdots < \omega+\omega < \omega+\omega+1 < \cdots$$

that begin with 0 and with limit ordinals $\omega = \bigcup_{n<\omega} n$, $\omega + \omega = \bigcup_{n>0} (\omega + n)$, ... The limit ordinals themselves are arranged into similar sequences

$$\omega < \omega + \omega < \cdots < \omega^2 < \omega^2 + \omega < \cdots < \omega^2 + \omega^2 < \omega^2 + \omega^2 + \omega < \cdots$$

that begin with ω and with unions of lesser limit ordinals; these sequences extend indefinitely, with no end in sight.

Exercises

1. Prove the following: when the well ordered sets X and Y are isomorphic, then there is only one isomorphism of X onto Y.

2. Prove the following: when α is an ordinal number, then so is $\alpha \cup \{\alpha\}$; in fact, $\alpha \cup \{\alpha\}$ is the least ordinal $\beta > \alpha$.

3. Let X and Y be disjoint well ordered sets. Order $Z = X \cup Y$ so that $x \leqq y$ in Z if and only if either $x \leqq y$ in X, or $x \leqq y$ in Y, or $x \in X$ and $y \in Y$. Show that Z is well ordered. Show that $X \cong X'$, $Y \cong Y'$ implies $Z \cong Z'$.

The *sum* of two ordinal numbers α and β is the ordinal number $\alpha + \beta \cong Z$, where Z is constructed as in the previous exercise from $X \cong \alpha$ and $Y \cong \beta$.

4. Show that ordinal addition is associative.

5. Show that $\omega + 1 \neq 1 + \omega$. ($\omega$ is the least infinite ordinal.)

6. Prove that every ordinal can be written uniquely as a sum $\alpha + n$, where α is 0 or a limit ordinal, and n is a finite ordinal.

7. Let X and Y be well ordered sets. Order $Z = X \times Y$ so that $(x', y') < (x'', y'')$ in Z if and only if either $y' < y''$, or $y' = y''$ and $x' < x''$. (Thus Z consists of $|Y|$ copies of X placed end to end.) Show that Z is well ordered. Show that $X \cong X'$, $Y \cong Y'$ implies $Z \cong Z'$.

The *product* $\alpha\beta$ of two ordinal numbers α and β is the ordinal number $\alpha\beta \cong Z$, where Z is constructed as in the previous exercise from $X \cong \alpha$ and $Y \cong \beta$.

8. Show that ordinal multiplication is associative.

9. Show that $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ for all ordinals α, β, γ.

10. Show that $2\omega \neq \omega 2$.

11. Show that $(1 + 1)\omega \neq 1\omega + 1\omega$.

4. Ordinal Induction

Ordinal numbers can be used instead of integers in inductive proofs and constructions. This method of proof, known as ordinal induction, is as powerful as Zorn's lemma, and sometimes more convenient or more natural.

Ordinary induction is based on the following property of natural numbers: if S is a subset of $\mathbb{N} = \{1, 2, \ldots\}$ such that $1 \in S$ and that $n \in S$ implies $n + 1 \in S$, then $S = \mathbb{N}$. Ordinal numbers have a similar property:

Proposition **4.1.** *Let* $\mathcal{C}$ *be a class of ordinal numbers such that*

(1) $0 \in \mathcal{C}$;

(2) $\alpha \in \mathcal{C}$ *implies* $\alpha + 1 \in \mathcal{C}$;

(3) *if* α *is a limit ordinal and* $\beta \in \mathcal{C}$ *for all* $\beta < \alpha$, *then* $\alpha \in \mathcal{C}$.

Then $\mathcal{C} = Ord$.

Proof. If $\mathcal{C} \neq Ord$, then $Ord \setminus \mathcal{C}$ has a least element α, by 3.3. Then $\mathcal{C}$ contains every $\beta < \alpha$. But $\alpha \neq 0$, by (1); α is not a successor ordinal, by (2); and α is not a limit ordinal, by (3). Therefore $\mathcal{C} = Ord$. □

Ordinal induction is a method of proof based on Proposition 4.1. It resembles ordinary induction, except for (3). There are some variants, which readers will easily establish. Induction can be limited to a given ordinal σ:

Proposition **4.2.** *Let* σ *be an ordinal number and let* $\mathcal{C}$ *be a class of ordinal numbers such that*

(1) $0 \in \mathcal{C}$;

(2) *if* $\alpha \in \mathcal{C}$ *and* $\alpha + 1 < \sigma$, *then* $\alpha + 1 \in \mathcal{C}$;

(3) *if* $\alpha < \sigma$ *is a limit ordinal and* $\beta \in \mathcal{C}$ *for all* $\beta < \alpha$, *then* $\alpha \in \mathcal{C}$.

Then $\mathcal{C}$ *contains every ordinal number* $\alpha < \sigma$.

There are also "strong" versions of Propositions 4.1 and 4.2, which follow from Proposition 3.3:

Proposition **4.3.** *Let* $\mathcal{C}$ *be a class of ordinal numbers such that* $\beta \in \mathcal{C}$ *for all* $\beta < \alpha$ *implies* $\alpha \in \mathcal{C}$. *Then* $\mathcal{C} = Ord$.

Let σ *be an ordinal number and let* $\mathcal{C}$ *be a class of ordinal numbers such that* $\beta \in \mathcal{C}$ *for all* $\beta < \alpha$ *implies* $\alpha \in \mathcal{C}$ *when* $\alpha < \sigma$. *Then* $\mathcal{C}$ *contains every ordinal number* $\alpha < \sigma$.

Recursion. A *transfinite sequence* is a family $(x_\alpha)_{\alpha \in Ord}$ or $(x_\alpha)_{\alpha < \sigma}$ indexed by Ord or indexed by an ordinal number σ. By the well ordering principle, the elements of every set can be arranged into a transfinite sequence: well order X, so that X is isomorphic to some ordinal σ, and let $x_\alpha = \theta(\alpha)$, where $\theta : \sigma \longrightarrow X$ is the isomorphism. On the other hand, we have:

Lemma **4.4.** *No set can contain a transfinite sequence* $(x_\alpha)_{\alpha \in Ord}$ *indexed by all ordinals, such that* $x_\alpha \neq x_\beta$ *whenever* $\alpha \neq \beta$.

Proof. In the next section we shall see that such a sequence would force the poor set to have entirely too many elements. For now we argue as follows. Let X be the subset of all x_α. Order X so that $x_\alpha < x_\beta$ if and only if $\alpha < \beta$. Then X is well ordered, by 3.3; in fact, X is isomorphic to Ord. By 3.9, X is isomorphic to an ordinal number σ. The isomorphism $Ord \cong X \cong \sigma$ sends the lower section σ of Ord to a lower section $\tau < \sigma$ of σ, contradicting 3.7. □

As a rather complicated first example of ordinal induction we show that transfinite sequences can be constructed recursively.

Proposition **4.5** (Recursion). *Let S be a set and let $F : 2^S \longrightarrow S$ be a mapping, where 2^S is the set of all subsets of S. There exists a unique transfinite sequence $(x_\alpha)_{\alpha\in Ord}$ indexed by all ordinals, such that*

$$x_\alpha \;=\; F\big(\{\, x_\gamma \;\big|\; \gamma < \alpha \,\}\big) \qquad (*)$$

holds for all $\alpha \in Ord$.

Informally we say that $(*)$ "defines x_α by induction". The exercises give more general forms of recursion.

Proof. First we show by induction on $\sigma \in Ord$ that there is at most one sequence $(x_\alpha)_{\alpha<\sigma}$ indexed by σ such that $(*)$ holds for all $\alpha < \sigma$. Assume this uniqueness for every $\tau < \sigma$. Let $(x'_\alpha)_{\alpha<\sigma}$ and $(x''_\alpha)_{\alpha<\sigma}$ satisfy $(*)$ for all $\alpha < \sigma$. If $\sigma = 0$, then $x'_\alpha = x''_\alpha$ for all $\alpha < \sigma$, vacuously. If $\sigma = \tau + 1$ is a successor ordinal, then $x'_\alpha = x''_\alpha$ for all $\alpha < \tau$ by the induction hypothesis and

$$x'_\tau \;=\; F\big(\{\, x'_\gamma \;\big|\; \gamma < \tau \,\}\big) \;=\; F\big(\{\, x''_\gamma \;\big|\; \gamma < \tau \,\}\big) \;=\; x''_\tau\,;$$

hence $x'_\alpha = x''_\alpha$ for all $\alpha < \sigma$. If σ is a limit ordinal, then $x'_\alpha = x''_\alpha$ for every $\alpha < \tau < \sigma$ by the induction hypothesis, and for every $\alpha < \sigma = \bigcup_{\tau<\sigma} \tau$.

Next we show by induction on $\sigma \in Ord$ that there exists a sequence $(x_\alpha)_{\alpha<\sigma}$ indexed by σ such that $(*)$ holds for all $\alpha < \sigma$. Assume that such a sequence exists for all $\tau < \sigma$. The empty sequence serves if $\sigma = 0$. If $\sigma = \tau + 1$, then by the induction hypothesis there is a sequence $(x_\alpha)_{\alpha<\tau}$ indexed by τ such that $(*)$ holds for all $\alpha < \tau$; define $x_\tau \;=\; F\big(\{\, x_\gamma \;\big|\; \gamma < \tau \,\}\big)$; then $(*)$ holds for all $\alpha < \sigma$. Now, let σ be a limit ordinal. For every $\tau < \sigma$ the induction hypothesis provides a sequence $(x^\tau_\alpha)_{\alpha<\tau}$ indexed by τ such that $(*)$ holds for all $\alpha < \tau$. By the first part of the proof, $x^\tau_\alpha = x^\upsilon_\alpha$ whenever $\alpha < \tau, \upsilon < \sigma$. Since $\sigma = \bigcup_{\tau<\sigma} \tau$, a sequence $(x^\sigma_\alpha)_{\alpha<\sigma}$ indexed by σ is well defined by $x^\sigma_\alpha = x^\tau_\alpha$ whenever $\alpha < \tau < \sigma$. Then x^σ satisfies $(*)$ for all $\alpha < \sigma$.

We now have for every ordinal σ a sequence $(x^\sigma_\alpha)_{\alpha<\sigma}$ indexed by σ such that $(*)$ holds for all $\alpha < \sigma$. As above, the first part of the proof implies $x^\sigma_\alpha = x^\tau_\alpha$ whenever $\alpha < \sigma, \tau$. Hence a sequence $(x_\alpha)_{\alpha\in Ord}$ indexed by Ord is well defined by $x_\alpha = x^\sigma_\alpha$ whenever $\alpha < \sigma$; this sequence satisfies $(*)$ for all α, and is unique by the first part of the proof. □

Zorn's lemma. We use recursion to show that the axiom of choice implies Zorn's lemma. This completes the proofs of Theorems 2.2 and 2.4. Readers will make sure that the author did not pull a fast one and invoked Zorn in proofs, in either this section or Section 3.

Let X be a nonempty partially ordered set in which every nonempty chain has an upper bound. Assume that X has a choice function c but no maximal element. For every subset S of X let

$$u(S) \;=\; \{\, x \in X \;\big|\; s < x \text{ for all } s \in S \,\}$$

be the set of all (strict) upper bounds of S. Choose some $a \in X$ and let

$$F(S) = \begin{cases} c\big(u(S)\big) & \text{if } u(S) \neq \emptyset, \\ a & \text{if } u(S) = \emptyset. \end{cases}$$

By 4.5 there is a transfinite sequence $(x_\alpha)_{\alpha \in Ord}$ indexed by all ordinals, such that $x_\alpha = F\big(\{\, x_\gamma \mid \gamma < \alpha \,\}\big)$ for all $\alpha \in Ord$. We prove by induction on α that $x_\gamma < x_\alpha$ for all $\gamma < \alpha$; this contradicts 4.4. There is nothing to prove if $\alpha = 0$. Let $\alpha > 0$; assume that $x_\gamma < x_\beta$ whenever $\gamma < \beta < \alpha$. Let

$$S_\alpha = \{\, x_\gamma \mid \gamma < \alpha \,\}.$$

If $\alpha = \beta + 1$ is a successor, then S_α is a chain. We have $x_\beta < t$ for some $t \in X$, since x_β is not a maximal element of X. Then $x_\gamma \leqq x_\beta < t$ for all $\gamma < \alpha$ and $u(S_\alpha) \neq \emptyset$. Hence $x_\alpha \in u(S_\alpha)$ and $x_\gamma < x_\alpha$ for all $\gamma < \alpha$. If α is a limit ordinal, then the nonempty chain S_α has an upper bound t in X. Since α is a limit ordinal, $\gamma < \alpha$ implies $\gamma + 1 < \alpha$, so that $x_\gamma < x_{\gamma+1} \leqq t$ for all $\gamma < \alpha$; hence again $u(S_\alpha) \neq \emptyset$, $x_\alpha \in u(S_\alpha)$, and $x_\gamma < x_\alpha$ for all $\gamma < \alpha$.

The sequence $(x_\alpha)_{\alpha \in Ord}$ in this proof is normally constructed more informally, as follows. Assume that x_γ has been constructed for all $\gamma < \alpha$, so that $x_\gamma < x_\beta$ for all $\gamma < \beta < \alpha$. Choose any $x_0 \in X$. If $\alpha = \beta + 1$ is a successor, we can choose some $x_\alpha > x_\beta$, since x_β is not a maximal element of X; then $x_\gamma \leqq x_\beta < x_\alpha$ for all $\gamma < \alpha$. If α is a limit ordinal, we can choose an upper bound $x_\alpha \in X$ of the nonempty chain $\{\, x_\gamma \mid \gamma < \alpha \,\}$, and then $x_\gamma < x_{\gamma+1} \leqq x_\alpha$ for all $\gamma < \alpha$. We now have $x_\beta < x_\alpha$ whenever $\beta < \alpha$, blatantly contradicting 4.4. In this argument it is understood that x_α is constructed by ordinal recursion, and that a choice function provides all required choices.

Exercises

1. Let σ be an ordinal number and let $\mathcal{C}$ be a class of ordinal numbers such that (1) $0 \in \mathcal{C}$; (2) if $\alpha \in \mathcal{C}$ and $\alpha + 1 < \sigma$, then $\alpha + 1 \in \mathcal{C}$; and (3) if $\alpha < \sigma$ is a limit ordinal and $\beta \in \mathcal{C}$ for all $\beta < \alpha$, then $\alpha \in \mathcal{C}$. Prove that $\mathcal{C}$ contains every ordinal number $\alpha < \sigma$.

2. Let S be a set and let $F : D \longrightarrow S$ be a mapping, where D is a set of subsets of S. Prove that there exists a unique transfinite sequence (x_α), indexed by all ordinals or by some ordinal σ, such that $x_\alpha = F\big(\{\, x_\gamma \mid \gamma < \alpha \,\}\big)$ whenever $F\big(\{\, x_\gamma \mid \gamma < \alpha \,\}\big)$ is defined (whenever x_γ is defined for all $\gamma < \alpha$, and $\{\, x_\gamma \mid \gamma < \alpha \,\} \in D$).

3. Let G be a group and let $a \in G$, $a \neq 1$. Use ordinal induction to prove that there is a subgroup M of G that is maximal such that $a \notin M$.

4. Let G be a group and let A be a subgroup of G. Use ordinal induction to prove that there is a subgroup M of G that is maximal such that $M \cap A = 1$.

5. Use ordinal induction to prove that every vector space has a maximal linearly independent subset.

6. Given a field K, use ordinal induction to construct a field $F \supseteq K$ in which every

irreducible polynomial $q \in K[X]$ has a root. (First, arrange these polynomials into a transfinite sequence.)

7. Let G be a group. Construct a transfinite sequence of subgroups of G (the transfinite ascending central series),

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \cdots \trianglelefteq Z_\alpha(G) \trianglelefteq Z_{\alpha+1}(G) \trianglelefteq \cdots,$$

in which $Z_{\alpha+1}(G) / Z_\alpha(G) = Z\big(G/Z_\alpha(G)\big)$ for every ordinal α.

5. Cardinal Numbers

Cardinal numbers, introduced by Cantor [1873], are used to assign a number of elements to every set. This section contains a number of notable properties.

Number of elements. Deciding when one set has fewer elements than another, or has as many elements, is easier than actually counting its elements.

Definitions. A set X has as many elements as *a set Y when there exists a bijection of X onto Y. A set X* has at most as many elements as *a set Y when there exists an injection of X into Y. A set X* has fewer elements than *a set Y when there exists an injection of X into Y but no bijection of X onto Y.*

Thus, X has at most as many elements as Y if and only if X has as many elements as a subset of Y. For example, we have:

Proposition **5.1.** *Let $I_n = \{1, 2, \ldots, n\}$. If $m < n$, then I_m has fewer elements than I_n; in fact, there is no injection $I_n \longrightarrow I_m$.*

Proof. This is not obvious since we have not established that we can count elements as usual. What is obvious is that $I_m \subseteq I_n$ has at most as many elements as I_n. We prove by induction on m that there is no injection $f : I_n \longrightarrow I_m$.

If $m = 0 < n$, then there is no injection of I_n into $I_0 = \emptyset$. Let $m > 0$ and let $f : I_n \longrightarrow I_m$ be any mapping. If $f(n) = f(i)$ for some $i < n$, then f is not injective. Assume that $f(n) \neq f(i)$ for all $i < n$. Let σ be a permutation of I_m such that $\sigma\,(f(n)) = m$. Let $g = \sigma \circ f : I_n \longrightarrow I_m$. Then $g(n) = m$ and $g(i) \neq g(n) = m$ for all $i < n$. Hence $g(I_{n-1}) \subseteq I_{m-1}$. By the induction hypothesis, the restriction of g to I_{n-1} is not injective. Hence neither is g. □

Proposition **5.2** (Cantor [1883]). *Every set X has fewer elements than the set 2^X of all its subsets.*

Proof. There is an injection $x \longmapsto \{x\}$ of X into 2^X. To show that X has fewer elements than 2^X we prove that there is no bijection of X onto 2^X. Let $f : X \longrightarrow 2^X$ be any mapping. Then $S = \{\, x \in X \mid x \notin f(x) \,\} \in 2^X$. But $x \in X$ implies either $x \in S$ and $x \notin f(x)$, or $x \notin S$ and $x \in f(x)$; therefore $S \neq f(x)$ for all $x \in X$, and f is not surjective. □

The next result will fully establish that our terminology is sensible.

Theorem **5.3** (Cantor-Bernstein). *Let X and Y be sets. If there exist an injection of X into Y and an injection of Y into X, then there exists a bijection of X onto Y.*

Proof. We may assume that X and Y are disjoint. Let $f : X \longrightarrow Y$ and $g : Y \longrightarrow X$ be injections. Arrange $X \cup Y$ into disjoint families in which every element of one set begets (all by itself) one child in the other set. This imagery is due to Halmos. The *child* of $x \in X$ is $f(x) \in Y$, and x is the *parent* of $f(x)$ (the sole parent, since f is injective); similarly, the *child* of $y \in Y$ is $g(y) \in X$, and y is the sole *parent* of $g(y)$. The *descendants* of $x \in X$ are $f(x)$, $g(f(x))$, $f(g(f(x)))$, ...; the *descendants* of $y \in Y$ are $g(y)$, $f(g(y))$, $g(f(g(y)))$, ... The elements of $f(X)$ or $g(Y)$ have a parent, but the elements of $Y \backslash f(X)$, and the elements of $X \backslash g(Y)$, are *orphans*.

The ancestry of an element of $X \cup Y$ either extends indefinitely upward or ends, or rather begins, with an orphan. Thus, an element of X either descends from an orphan of X (or is an orphan itself), or descends from an orphan in Y, or has infinite ancestry; these constitute disjoint sets X_X, X_Y, X_∞ whose union is X. Similarly, an element of Y either descends from an orphan in X, or descends from an orphan of Y (or is an orphan itself), or has infinite ancestry; these constitute disjoint sets Y_X, Y_Y, Y_∞ whose union is Y.

We see that $f(X_X) = Y_X$, $g(Y_Y) = X_Y$, and $f(X_\infty) = Y_\infty$ (also, $g(Y_\infty) = X_\infty$). Hence f and g induce bijections $X_X \longrightarrow Y_X$, $X_Y \longrightarrow Y_Y$, and $X_\infty \longrightarrow Y_\infty$, which can be pasted together into a bijection $X \longrightarrow Y$. □

Cardinal numbers. The *equipotence* relation "X has as many elements as Y" is reflexive, symmetric, and transitive. Cardinal numbers are most naturally defined as equivalence classes of equipotent sets. Unfortunately, as was the case with ordinals, equipotence classes are too large to be allowed membership in a set or collection. Modern cardinal numbers are sets, chosen so that there is only one in each equipotence class (as in Jech [1978], for instance).

Definition. A cardinal number *is an ordinal number κ such that every ordinal number $\alpha < \kappa$ has fewer elements than κ.* □

For example, every finite ordinal number $0 = \emptyset$, $1 = \{0\}$, $2 = \{0, 1\}$, ... is a cardinal number, by Proposition 5.1. These are the *finite* cardinals; the remaining cardinals are *infinite*. The first limit ordinal ω is a cardinal: indeed, every finite ordinal $n < \omega$ has fewer elements than ω: if there were a bijection $\omega \longrightarrow n$, then there would be an injection $n + 1 \longrightarrow n$, in defiance of 5.1. Readers will verify that infinite cardinals are limit ordinals and can be arranged into a transfinite sequence, traditionally denoted by

$$\aleph_0 < \aleph_1 < \cdots < \aleph_\alpha < \aleph_{\alpha+1} < \cdots,$$

indexed by all ordinals. (Thus, $\aleph_0$ is another name for ω.)

We show that there is one cardinal number in every equipotence class of sets.

Proposition **5.4.** *For every set X there exists a unique cardinal number $|X|$ such that there is a bijection of X onto $|X|$.*

Proof. By the axiom of choice, every set X can be well ordered (Theorem 2.4) and has the same number of elements as an ordinal number, by 3.9. The least ordinal number κ with this property is a cardinal number (since all ordinals $\alpha < \kappa$ have fewer elements). Moreover, κ is the only cardinal number with a bijection $X \longrightarrow \kappa$: there is no bijection $\kappa \longrightarrow \lambda$ between cardinal numbers $\kappa < \lambda$, since κ has fewer elements than λ. □

Definition. In Proposition 5.4, $|X|$ *is the* cardinality *or* number of elements *of* X.

Then X has as many elements as Y, as defined earlier, if and only if $|X| = |Y|$; readers will show that X has at most as many elements as Y if and only if $|X| \leqq |Y|$.

Countable sets. A set X is *finite* when its cardinality $|X|$ is finite; equivalently, when there is a bijection of X onto some $I_n = \{1, 2, \ldots, n\}$. Then $n = |X|$; in particular, n is unique (by Proposition 5.1 or 5.4). Otherwise, X is *infinite*.

Definition. A set X is countable *when* $|X| \leqq \aleph_0$.

Countable sets are often defined by the stricter condition $|X| = \aleph_0$; then a set X such that $|X| \leqq \aleph_0$ is *finite or countable*.

Readers will verify that $0 < |X| \leqq \aleph_0 = |\mathbb{N}|$ if and only if there is a surjection of $\mathbb{N}$ onto X; hence a nonempty set X is countable if and only if all the elements of X can be arranged into a finite or infinite sequence $x_1, \ldots, x_n, \ldots$ (indexed by natural numbers). For example, $\mathbb{N}$ and every $I_n = \{1, 2, \ldots, n\}$ are countable. The next result yields more examples.

Proposition **5.5.** *A direct product of finitely many countable sets is countable. A union of countably many countable sets is countable.*

Proof. The elements of $\mathbb{N} \times \mathbb{N}$ can be arranged by increasing sums into a sequence $(1, 1)$; $(1, 2)$, $(2, 1)$; $(1, 3)$, $(2, 2)$, $(3, 1)$; ... Thus $\mathbb{N} \times \mathbb{N}$ is countable. If now X and Y are countable, there are injections $X \longrightarrow \mathbb{N}$, $Y \longrightarrow \mathbb{N}$, and $X \times Y \longrightarrow \mathbb{N} \times \mathbb{N}$, and $X \times Y$ is countable. It follows, by induction on n, that the direct product of n countable sets is countable (for every $n \in \mathbb{N}$).

A countable family of sets can be arranged into a finite or infinite sequence $X_1, \ldots, X_n, \ldots$. Its union $X = \bigcup_{n>0} X_n$ is also the disjoint union of the countable sets $X'_n = X_n \backslash (X_1 \cup \cdots \cup X_{n-1})$. Injections $X'_n \longrightarrow \mathbb{N} \longrightarrow \mathbb{N} \times \{n\}$ then combine into an injection $X \longrightarrow \mathbb{N} \times \mathbb{N}$. Hence X is countable. □

By Proposition 5.5, $\mathbb{Z} = \{0\} \cup \mathbb{N} \cup -\mathbb{N}$ and $\mathbb{Q} = \bigcup_{n \in \mathbb{N}} \{ a/n \mid a \in \mathbb{Z} \}$ are countable. But not every set is countable.

Proposition **5.6** (Cantor [1873]). $\mathbb{R}$ *is not countable.*

Proof. Let X be the set of all real numbers with a decimal expansion $0\,.\,d_1\,d_2\,\ldots\,d_n\,\ldots$ in which every digit d_n is either 0 or 1. Every such $0\,.\,d_1\,d_2\,\ldots\,d_n\,\ldots$ is determined by a subset $\{\,n \in \mathbb{N} \mid d_n = 1\,\}$ of $\mathbb{N}$. This constructs a bijection $X \longrightarrow 2^{\mathbb{N}}$. By 5.2, $|\mathbb{R}| \geqq |X| = |2^{\mathbb{N}}| > |\mathbb{N}| = \aleph_0$. □

Readers can now follow in Cantor's footsteps and show that there are only countably many real numbers that are algebraic over $\mathbb{Q}$; this leaves uncountably many real numbers that are transcendental over $\mathbb{Q}$.

Operations. Readers will verify that the union of a set of cardinals is a cardinal (not a pope). Hence the next result is proved like Corollary 3.5 (but using Proposition 5.2):

Proposition **5.7.** *The class Card of all cardinal numbers is not a set.*

In particular, sets do not constitute a set: if they did, then the smaller classes *Ord* and *Card* would be sets, contradicting 3.5 and 5.7.

Addition, multiplication, and *exponentiation* of cardinal numbers are defined as follows. If κ and λ are cardinals, then

$$\kappa + \lambda = |X \cup Y|,\ \kappa\lambda = |X \times Y|, \text{ and } \kappa^{\lambda} = |X^{Y}|,$$

where $|X| = \kappa$, $|Y| = \lambda$, $X \cap Y = \emptyset$, and X^Y denotes the set of all mappings of Y into X. The exercises also define infinite sums and products. Readers will verify that these operations are well defined and have good properties. They also have amusing little quirks.

Proposition **5.8.** *Let κ and λ be cardinal numbers. If κ or λ is infinite, then* $\kappa + \lambda = \max(\kappa, \lambda)$.

Proof. We show that $\kappa + \kappa = \kappa$ when κ is infinite. Then $\lambda \leqq \kappa$ implies $\kappa \leqq \kappa + \lambda \leqq \kappa + \kappa = \kappa$ and $\kappa + \lambda = \kappa$, and 5.8 holds.

For every set X, $|X| + |X| = |2 \times X|$, since $2 \times X = \{0, 1\} \times X$ is the disjoint union of $\{0\} \times X$ and $\{1\} \times X$. Let A be an infinite set. Let $\mathcal{S}$ be the set of all ordered pairs (X, f) such that $X \subseteq A$ and f is a bijection of X onto $2 \times X$. Since $|A| \geqq \aleph_0$ there exists an injection $\mathbb{N} \longrightarrow A$, A contains an infinite countable subset X, $2 \times X$ is countable by 5.5, and there is a bijection of X onto $2 \times X$; hence $\mathcal{S} \neq \emptyset$. Partially order $\mathcal{S}$ by $(X, f) \leqq (Y, g)$ if and only if $X \subseteq Y$ and $f = g_{|X}$. It is immediate that every nonempty chain of $\mathcal{S}$ has an upper bound in $\mathcal{S}$. By Zorn's lemma, $\mathcal{S}$ has a maximal element (M, m). Then $|M| + |M| = |M|$; we show that $|M| = |A|$.

If $A \backslash M$ is infinite, then $A \backslash M$ contains an infinite countable subset X, and any bijection $f : X \longrightarrow 2 \times X$ can be combined with $m : M \longrightarrow 2 \times M$ into a bijection $M \cup X \longrightarrow 2 \times (M \cup X)$ that extends m, contradicting the maximality of M. Therefore $A \backslash M$ is finite. Hence M is infinite and contains an infinite countable subset Y. Then $|Y \cup (A \backslash M)| = |Y|$ by 5.5 and

$$|A| \;=\; |Y \cup (A \backslash M)| + |M \backslash Y| \;=\; |Y| + |M \backslash Y| \;=\; |M|. \;\square$$

Proposition **5.9.** *Let κ and λ be nonzero cardinal numbers. If κ or λ is infinite, then $\kappa\lambda = \max(\kappa, \lambda)$.*

Proof. We show that $\kappa\kappa = \kappa$ when κ is infinite. Then $1 \leqq \lambda \leqq \kappa$ implies $\kappa \leqq \kappa\lambda \leqq \kappa\kappa = \kappa$ and $\kappa\lambda = \kappa$, and 5.9 holds.

Let A be an infinite set. As in the proof of 5.8, let $\mathcal{S}$ be the set of all ordered pairs (X, f) such that $X \subseteq A$ and f is a bijection of X onto $X \times X$. Since A is infinite, A contains an infinite countable subset X, $X \times X$ is countable by 5.5, and there is a bijection of X onto $X \times X$; hence $\mathcal{S} \neq \emptyset$. Partially order $\mathcal{S}$ by $(X, f) \leqq (Y, g)$ if and only if $X \subseteq Y$ and $f = g_{|X}$. It is immediate that every nonempty chain of $\mathcal{S}$ has an upper bound in $\mathcal{S}$. By Zorn's lemma, $\mathcal{S}$ has a maximal element (M, m). Then $|M|\,|M| = |M|$; we show that $|M| = |A|$.

Assume $|M| < |A|$. Then $|A \backslash M| = |A|$ by 5.8, since $|A| = |M| + |M \backslash A|$. Hence there is an injection $M \longrightarrow A \backslash M$ and $A \backslash M$ contains a subset X such that $|X| = |M|$. Then there is a bijection $f : X \longrightarrow M \longrightarrow M \times M \longrightarrow X \times X$, which can be combined with $m : M \longrightarrow M \times M$ into a bijection $M \cup X \longrightarrow (M \cup X) \times (M \cup X)$ that extends m, in utter disregard of the maximality of M. □

Corollary **5.10.** *An infinite set X has $|X|$ finite subsets; moreover, there are $|X|$ finite sequences of elements of X.*

Proof. The set X has at least $|X|$ finite subsets, since it has $|X|$ subsets with one element. On the other hand, X has $1 \leqq |X|$ empty subset, $|X|$ subsets with one element, at most $|X|\,|X| = |X|$ subsets with two elements, and generally at most $|X|\,|X| \cdots |X| = |X|^n = |X|$ subsets with n elements. Hence X has at most $|X| + |X| + \cdots = \aleph_0 |X| = |X|$ finite subsets, and $\aleph_0 |X| = |X|$ by 5.9. Subsets can be replaced by sequences in this argument. □

Readers will use Propositions 5.8, 5.9 to show that there are groups of arbitrary cardinality, and that for every ring R there are R-modules of arbitrary infinite cardinality $\kappa \geqq |R|$; hence groups do not constitute a set, and modules over a given ring R do not constitute a set.

Exercises

1. Given two sets X and Y, show that there exists an injection of X into Y if and only if there exists a surjection of Y onto X.

2. Show that the union of a set of cardinal numbers is a cardinal number.

3. Show that every infinite cardinal number is a limit ordinal.

4. Show that all infinite cardinals can be arranged into a transfinite sequence $\aleph_0 < \aleph_1 < \cdots < \aleph_\alpha < \aleph_{\alpha+1} < \cdots$ indexed by all ordinals.

5. Prove the following: there exists an injection $X \longrightarrow Y$ if and only if $|X| \leqq |Y|$.

6. Prove that there are countably many real numbers that are algebraic over $\mathbb{Q}$ and uncountably many real numbers that are transcendental over $\mathbb{Q}$.

7. Prove that there are uncountably many mappings of $\mathbb{N}$ into $\mathbb{N}$.

8. For every cardinal $\kappa > 0$, prove that sets of cardinality κ do not constitute a set.

Readers are warned that the sum and product of two cardinals are usually not the same as their sum and product as ordinals.

9. Show that the addition of cardinals is commutative and associative.

10. Show that the multiplication of cardinals is commutative and associative.

11. Show that $(\kappa + \lambda)\,\mu = \kappa\mu + \lambda\mu$ for all cardinals $\kappa,\ \lambda,\ \mu$.

12. Show that $\kappa^{\lambda+\mu} = \kappa^{\lambda}\,\kappa^{\mu}$ for all cardinals $\kappa,\ \lambda,\ \mu$.

13. Show that $\kappa^{\lambda\mu} = (\kappa^{\lambda})^{\mu}$ for all cardinals $\kappa,\ \lambda,\ \mu$.

14. Verify that infinite sums and products of cardinals $(\kappa_i)_{i\in I}$ are well defined by $\sum_{i\in I}\kappa_i = \left|\bigcup_{i\in I} X_i\right|$ and $\prod_{i\in I}\kappa_i = \left|\prod_{i\in I} X_i\right|$, where $|X_i| = \kappa_i$ for all i and the sets X_i are pairwise disjoint.

15. Show that $\sum_{i\in I}\kappa_i = \sum_{j\in J}\left(\sum_{i\in I_j}\kappa_i\right)$ when $I = \bigcup_{j\in J} I_j$ is a partition of I.

16. Show that $\prod_{i\in I}\kappa_i = \prod_{j\in J}\left(\prod_{i\in I_j}\kappa_i\right)$ when $I = \bigcup_{j\in J} I_j$ is a partition of I.

17. Show that $\prod_{i\in I}\kappa^{\lambda_i} = \kappa^{\sum_{i\in I}\lambda_i}$.

18. Show that $\left(\prod_{i\in I}\kappa_i\right)^{\lambda} = \prod_{i\in I}\kappa_i^{\lambda}$.

19. Show that every cardinal number is the cardinality of a group.

20. Let R be a ring. Show that every infinite cardinal number $\kappa \geqq |R|$ is the cardinality of an R-module.

References

The following are books and papers cited in the text.

[1824] Abel, N., *Mémoire sur les équations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré*, Christiana, 1824; published in J. reine angew. Math. 1 (1826), and in Oeuvres complètes, vol. I, Christiana, 1881, 28–33, 66–87.

[1926] Artin, E. and Schreier, O., *Algebraische Konstruktion reeller Körper*, Abh. Math. Sem. Hamburg 5 (1926), 83–115.

[1927] Artin, E., *Zur Theorie der hyperkomplexen Zahlen*, Abh. Math. Sem. Hamburg 5 (1927), 251–260.

[1940] Baer, R., *Abelian groups that are direct summands of every containing abelian group*, Bull. Amer. Math. Soc. 46 (1940), 800–806.

[1966] Beck, J., According to MacLane [1971], Beck's theorem was "unpublished, but presented at a conference in 1966"; it is likely that MacLane was there.

[1933] Birkhoff, G., *On the combination of subalgebras*, Proc. Cambridge Philos. Soc. 29 (1933), 441–464.

[1934] Birkhoff, G., *On the lattice theory of ideals*, Bull. Amer. Math. Soc. 40 (1934), 613–619.

[1935] Birkhoff, G., *On the structure of abstract algebras*, Proc. Cambridge Philos. Soc. 31 (1935), 433–454.

[1940] Birkhoff, G., *Lattice Theory*, Amer. Math. Soc., 1940.

[1944] Birkhoff, G., *Subdirect unions in universal algebra*, Bull. Amer. Math. Soc. 50 (1944), 764–768.

[1847] Boole, R., *The Mathematical Analysis of Logic*, 1847.

[1965] Buchberger, B., Doctoral Dissertation, Innsbrück, 1965; see also *A theoretical basis for the reduction of polynomials to canonical forms*, ACM SIGSAM Bull. 39 (1976), 19–29.

[1897] Burnside, W., *Theory of groups of finite order*, Cambridge Univ. Press, 1897.

[1905] Burnside, W., *On the condition of reducibility of any group of linear substitutions*, Proc. London Math. Soc. (2) 3 (1905), 430–434.

[1873] Cantor, G., *Über eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen*, J. reine angew. Math. 77 (1873), 258–263.

[1883] Cantor, G., *Fondements d'une théorie générale des ensembles*, Acta Math 2 (1883), 381–408.

[1545] Cardano, G., *Ars Magna*, 1545.

[1956] Cartan, H. and Eilenberg, S., *Homological Algebra*, Princeton, 1956.

[1815] Cauchy, A., *Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme*, J. Ecole Polytechn. X (1815), 1–28.

[1961] Chase, S., *Direct products of modules*, Trans. Amer. Math. Soc. 97 (1961), 457–473.

[1871] Dedekind, R., Xth supplement to Dirichlet's *Vorlesungen über Zahlentheorie*, Braunschweig, 1871.

[1897] Dedekind, R., *Über Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler*, Festschr. Techn. Hoch. Braunschweig (1897), 1–40.

[1900] Dedekind, R., *Über die von drei Moduln erzeugte Dualgruppe*, Math. Ann. 53 (1900), 371–403.

[1837] Dirichlet, G., *Beweis des Satzes, dass jede unbegrentze arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält*, Abh. König. Akad. Wiss. Berlin, math. Abh. 1837, 45–71.

[1882] Dyck, W., *Gruppentheoretische Studien*, Math. Ann. 20 (1882), 1–45.

[1942] Eilenberg, S. and MacLane, S., *Group extensions and homology*, Ann. of Math. 43 (1942), 757–831.

[1945] Eilenberg, S. and MacLane, S., *General theory of natural equivalences*, Trans. Amer. Math. Soc. 58 (1945), 231–294.

[1965] Eilenberg, S. and Moore, J.C., *Adjoint functors and triples*, Illinois J. Math. 9 (1965), 381–398.

[1850] Eisenstein, G., *Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, J. reine angew. Math. 39 (1850), 160–179.

[1963] Feit, W. and Thompson, J.G., *Solvability of groups of odd order*, Pacific J. Math. 13 (1963), 775–1029.

[1964] Freyd, P., *Abelian Categories*, Harper and Row, New York, 1964.

[1877] Frobenius, G., *Über lineare Substitutionen und bilineare Formen*, J. reine angew. Math. 84 (1877), 1–63.

[1878] Frobenius, G. and Stickelberger, L., *Über Gruppen mit vertauschbaren Elementen*, J. reine angew. Math. 86 (1878), 217–262.

[1830] Galois, E., *Mémoire sur les conditions de résolubilité des équations par radicaux*, 1930; published in J. Math. Pures Appl. 11 (1846), 381–444, and in Oeuvres Mathématiques, Paris, 1897, 33–50.

[1799] Gauss, G., Doctoral dissertation, Helmstadt, 1799.

[1801] Gauss, G., *Disquisitiones arithmeticae*, Leipzig, 1801.

[1938] Gödel, K., *The consistency of the axiom of choice and of the generalized continuum hypothesis*, Proc. Nat. Acad. Sci. 24 (1938), 556–557.

[1994 up] Gorenstein, D., Lyons, R., Solomon, R., *The Classification of the Finite Simple Groups*, Amer. Math. Soc., Providence, RI, 1994, 1996, 1998, 1998, 2002, 2005.

[1844] Grassmann, H., *Grundzüge zu einer rein geometrischen Theorie der Curven, mit Anwendung einer rein geometrischen Analyse*, J. reine angew. Math. 31 (1844), 111–132.

[1927] Grell, H., *Beziehungen zwischen den Idealen verschiedener Ringe*, Math. Ann. 97 (1927), 490–523.

[1975] Grillet, P., *Primary semigroups*, Michigan Math. J. 22 (1975), 321–336.

[1939] Gröbner, W., *Über die algebraischen Eigenschaften der Integrale von linearen Differentialgleichungen mit konstanten Koeffizienten*, Monatsh. Math. Phys. 47 (1939), 247–284.

[1928] Hall, P., *A note on soluble groups*, J. London Math. Soc. 3 (1928), 98–105.

[1843] Hamilton, W.R., *On Quaternions; or on a new System of Imaginaries in Algebra* (letter to John T. Graves, dated October 17, 1843), Philos. Magazine 25, 489–495.

[1914] Hausdorff, F., *Grundzüge der Mengenlehre*, Leipzig, Veit & Co., 1914.

[1897] Hensel, K., *Über die Fundamentalgleichung und die ausserwesentlichen Diskriminantentheiler eines algebraischen Körpers*, Gött. Nachr. (1897), 254–260; see also *Theorie der algebraischen Zahlen*, Teubner, Lepzig, 1908.

[1904] Hensel, K., *Neue Grundlagen der Arithmetik*, J. Reine Angew. Math. 127 (1904), 51–84.

[1890] Hilbert, D., *Über die Theorie der algebraischen Formen*, Math. Ann. 36 (1890), 473–534.

[1893] Hilbert, D., *Über die vollen Invariantensysteme*, Math. Ann. 42 (1893), 313–373.

[1897] Hilbert, D., *Zahlbericht*, Jahresber. D.M.V., 4 (1897), 175–546.

[1889] Hölder, O., *Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen*, Math. Ann. 34 (1889), 26–56.

[1939] Hopkins, C., *Rings with minimal condition for left ideals*, Ann. Math. (2) 40 (1939), 712–730.

[1941] Hurewicz, W., *On duality theorems*, Abstract # 47-7-329, Bull. Amer. Math. Soc. 47 (1941), 562–563.

[1945a] Jacobson, N., *The radical and semi-simplicity for arbitrary rings*, Amer. J. Math. 67 (1945), 300–320.

[1945b] Jacobson, N., *Structure theory of simple rings without finiteness assumptions*, Trans. Amer. Math. Soc. 57 (1945), 228–245.

[1978] Jech, T., *Set Theory*, Academic Press, 1978.

[1869] Jordan, C., *Théorèmes sur les équations algébriques*, J. math. pures appl. (2) 14 (1869), 139–146; *Commentaires sur Galois*, Math. Ann. 1 (1869), 141–160.

[1870] Jordan, C., *Traité des substitutions et des équations algébriques*, Gauthier-Villars, Paris, 1870, 114–125.

[1872] Klein, F., Inaugural address, Erlangen Univ., 1872.

[1870] Kronecker, L., *Auseinandersetzungen einiger Eigenschaften der Klassenanzahl idealer complexer Zahlen*, Monatsh. Abh. Berlin (1870), 881.

[1887] Kronecker, L., *Ein Fundamentalsatz der allgemeinen Arithmetik*, J. reine angew. Math. 100 (1887), 490–510.

[1925] Krull, W., *Über verallgemeinerte endliche Abelsche Gruppen*, Math. Zeitschr. 23 (1925), 161–196.

[1928] Krull, W., *Primidealketten in allgemeinen Ringbereichen*, Sitz. Heidelberg Akad. Wiss. 1928, No. 7.

[1932] Krull, W., *Allgemeine Bewertungstheorie*, J. reine angew. Math. 167 (1932), 160–196.

[1922] Kuratowski, C., *Une méthode d'élimination des nombres transfinis des raisonnements mathématiques*, Fund. Math. 3 (1922), 76–108.

[1913] Kürschak, J., *Über Limesbildung und allgemeine Körpertheorie*, Proc. 5. Intern. Math. Congr. 1 (1913), 285–289.

[1770] Lagrange, J., *Réflexions sur la résolution algébrique des équations*, 1770; Oeuvres de Lagrange, 3, 205–421.

[1905] Lasker, E., *Zur Theorie der Moduln und Ideale*, Math. Ann. 60 (1905), 20–116.

[1969] Lazard, D., *Autour de la platitude*, Bull. Soc. Math. France 97 (1969), 81–128.

[1939] Levitzki, J., *On rings which satisfy the minimum condition for the right-hand ideals*, Compos. Math. 7 (1939), 214–222.

[1939] MacLane, S., *Modular fields (I)*, Duke Math. J. 5 (1939), 372–393.

[1963] MacLane, S., *Homology*, Springer, 1963.

[1971] MacLane, S., *Categories for the Working Mathematician*, Springer, 1971.

[1935] MacNeille, H., Doct. diss., Harvard, 1935; see also *Partially ordered sets*, Trans. Amer. Math. Soc. 42 (1937), 416–460.

[1958] Mal'cev, A.I., *On homomorphisms onto finite groups* [Russian], Uch. Zap. Ivanov. Gos. Ped. Inst. 18 (1958), 49–60.

[1898] Maschke, H., *Über den arithmetischen Charakter der Coefficienten der Substitutionen endlicher linearer Substitutionsgruppen*, Math. Ann. 50 (1898), 492–498.

[1966] McCarthy, P., *Algebraic Extensions of Fields*, Chelsea, 1966.

[1910] Moore, E., *Introduction to a Form of General Analysis*, The New Haven Math. Coll., Yale Univ. Press, New Haven, 1910.

[1962] Nagata, M., *Local Rings*, Wiley, 1962, p. 213.

[1924] Nielsen, J., *Die Isomorphismengruppe der freien Gruppen*, Math. Ann. 91 (1924), 169–209.

[1921] Noether, E., *Idealtheorie in Ringbereichen*, Math. Ann. 83 (1921), 24–66.

[1926] Noether, E., *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl und Funktionenkörpern*, Math. Ann. 96 (1926), 26–61.

[1929] Noether, E., *Hyperkomplexe Grössen und Darstellungstheorie*, Math. Z. 30 (1929), 641–692.

[1918] Ostrowski, A., *Über einige Lösungen der Funktionalgleichung* $\varphi(x)\,\varphi(y) = \varphi(xy)$, Acta Math. 41 (1918), 271–284.

[1934] Ostrowski, A., *Untersuchungen zur arithmetischen Theorie der Körper.* (*Die Theorie der Teilbarkeit in allgemeinen Körpern. I-III.*), Math. Z. 39 (1934), 296–404.

[1864] Peirce, B., *Linear Associative Algebra*, lecture to the American Association for the Advancement of Science; published in Amer. J. Math. 4 (1881), 97–229.

[1956] Rédei, L., *The Theory of Finitely Generated Commutative Semigroups*, Akad. Kiadó, Budapest, 1956; English translation, Pergamon Press, Oxford, 1963.

[1911] Remak, R., *Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren*, J. reine angew. Math. 139 (1911), 293–308.

[1930] Remak, R., *Über minimale invariante Untergruppen in der Theorie der endlichen Gruppen*, J. reine angew. Math. 162 (1930), 1–16.

[1868] Schering, E., *Der fundamental Classen der zusammengesetzbaren arithmetischen Formen*, Abh. Ges. Göttingen 14 (1868-69), 13.

[1912] Schmidt, O., *Über die Zerlegung endlicher Gruppen in direkte unzerlegbare Faktoren*, Izv. Kiev Univ. 1912, 1–6.

[1928] Schmidt, O., *Über unendlich Gruppen mit endlicher Kette*, Math. Z. 29 (1928), 34–41.

[1926] Schreier, O., *Über die Erweiterung von Gruppen, I*, Monatsh. Math. Phys. 34 (1926), 165–180; *Über die Erweiterung von Gruppen, II*, Abh. math. Sem. Hamburg 4 (1926), 321–346.

[1928] Schreier, O., *Über der Jordan-Hölderschen Satz*, Abh. math. Sem. Hamburg 6 (1928), 300–302.

[1980] Schreyer, F., *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass'schen Divisionsatz*, Diplom Thesis, Univ. of Hamburg, 1980; see also *A standard basis approach to syzygies of canonical curves*, J. Reine Angew. Math. 421 (1991), 83–123.

[1904] Schur, I., *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. reine angew. Math. 127 (1904), 20–50.

[1910] Steinitz, E., *Algebraische Theorie der Körper*, J. reine angew. Math. 137 (1910), 167–309.

[1934] Stone, M., *Boolean algebras and their applications to topology*, Proc. Nat. Acad. Sci. 20 (1934), 197–202.

[1935] Stone, M., *Subsumption of the theory of Boolean algebras under the theory of rings*, Proc. Nat. Acad. Sci. 21 (1935), 103–105.

[1872] Sylow, L., *Théorèmes sur les groupes de substitutions*, Math. Ann. 5 (1872), 584–594.

[1948] Uzkov, A.I., *On rings of quotients of commutative rings*, Mat. Sbornik (N.S.) 13 (1948), 71–78.

[1930] van der Waerden, B., *Moderne Algebra*, Springer, 1930 (vol. I), 1931 (vol. II).

[1905] Wedderburn, J., *A theorem on finite algebras*, Trans. Amer. Math. Soc. 6 (1905), 349–352.

[1907] Wedderburn, J., *Note on hypercomplex numbers*, Proc. Edinburgh Math. Soc. 25 (1907), 2–4.

[1952] Weil, A., *Fibre Spaces in Algebraic Geometry*, lectures at the University of Chicago, 1952.

[1898] Whitehead, A., *A Treatise on Universal Algebra*, Cambridge Univ. Press, 1898.

[1944] Zariski, O., *The compactness of the Riemann manifold of an abstract field of algebraic functions*, Bull. Amer. Math. Soc. 50 (1944), 683–691.

[1933] Zassenhaus, H., *Zum Satz von Jordan-Hölder-Schreier*, Abh. math. Sem. Hamburg 10 (1934), 106–108.

[1937] Zassenhaus, H., *Lehrbuch der Gruppentheorie*, vol. 1, Teubner, Lepizig, 1937.

[1904] Zermelo, E., *Beweis, dass jede Menge wohlgeordnet werden kann*, Math. Ann. 59 (1904), 514–516.

[1935] Zorn, M., *A remark on method in transfinite algebra*, Bull. Amer. Math. Soc. 41 (1935), 667–670.

Further Readings

The following are some historically important books, and some books I like. They do not constitute a complete bibliography.

General

van der Waerden, B.L., *Moderne Algebra, vol. I, vol. II*, Springer, 1930, 1931.

Lang, Serge, *Algebra*, Addison-Wesley, 1965.

Hungerford, Thomas W., *Algebra*, Springer, 1980.

Isaacs, I. Martin, *Algebra, a Graduate Course*, Brooks/Cole, 1994.

Kempf, George R., *Algebraic Structures*, Vieweg, 1995.

Groups

Burnside, W., *Theory of Groups of Finite Order*, Cambridge, 1897.

Suzuki, Michio, *Group Theory*, Springer, 1986.

Gorenstein, Daniel, *Finite Groups*, 2nd. ed., Chelsea, 1980.

Rings and modules

Jacobson, Nathan, *Structure of Rings*, American Mathematical Society, 1956.

Dauns, John, *Rings and Modules*, Cambridge, 1994.

Lam. T.Y., *A First Course in Noncommutative Rings*, Springer, 1991.

Commutative Algebra

Zariski, Oscar and Samuel, Pierre, *Commutative Algebra*, vol. I, vol. II, van Nostrand, 1958, 1960.

Eisenbud, David, *Commutative Algebra With a View to Algebraic Geometry*, Springer, 1994.

Homological Algebra

Cartan, Henri and Eilenberg, Samuel, *Homological Algebra*, Princeton, 1956.

MacLane, Saunders, *Homology*, Springer, 1963.

Rotman, Joseph J., *An Introduction to Homological Algebra*, Academic Press, 1979.

Lattices

Birkhoff, G., *Lattice Theory*, American Mathematical Society, 1940.

Grätzer, Goerge, *General Lattice Theory*, Birkhäuser, 1978.

Universal Algebra

Cohn, P.M., *Universal Algebra*, Harper and Row, 1965.

Grätzer, Goerge, *Universal Algebra*, van Nostrand, 1968.

Categories

MacLane, Saunders, *Categories for the Working Mathematician*, Springer, 1971.

Set Theory

Jech, T., *Set Theory*, Academic Press, 1978.

History

Lubos Nový, *Origins of Modern Algebra*, Noordhoff, Leyden 1973.

Index

A
abelian group, 11, 44–46, 99, 315, 405–408, 456, 492, 493, 495, 576
  divisible, 406–408
  free, 330
  subdirectly irreducible, 576
  torsion-free, 452
  totally ordered, 251
Abel, N., 1, 191, 224
Abel's theorem, 224
Abs, 583
  See also *Pecs*
absolute value, 239, 239–266
  archimedean, 240, 241
  equivalent, 240
  extension of, 247–261
  nonarchimedean, 241
  p-adic, 241
  trivial, 239
a.c.c. *See* ascending chain condition
action
  See also group action
  by automorphisms, 92
  by inner automorphisms, 56
  by left multiplication, 54
  by permutations, 54
  in group extension, 96
  set, 96
  trivial, 501
addition, 2
adjoint functor theorem, 610, 609–612
adjunction, 606, 607, 608, 610, 613
$\aleph$, aleph, 641
$\aleph_0$, 641
algebra, vii
  commutative, 273
  homological, 463, 463–514
  universal, 559–580
algebra, 311, 381, 515, 515–538
  See also group ring
  See also universal algebra
  Artinian, 534
  associative, 515
  Boolean. *See* Boolean lattice
  central, 535
  central simple, 535–536
  division, 534, 537, 538
  exterior, 524, 523–527, 530
  free, 518, 520
  graded, 517
  group, 382, 381–386, 502
  nonassociative, 515
  quotient, 516, 517
  simple, 534, 534–538
  symmetric, 521, 521–524, 530
  T-, 614
  tensor, 519, 518–520, 530
  universal. *See* universal algebra
algebraic set, 275, 276, 304, 307, 307–310
  affine, 307
  irreducible, 309
  projective, 307
al-Kwowarizmi, vii, 188
almost all, 107
alphabet, 6
amalgam of groups, 41
A_n, 36
Ann, 317, 323, 324
annihilator
  of element, 324
  of ideal, 545
  of module, 317
arity, 559
arrow, 582, 583

Artin, E., vii, 37, 105, 155, 191, 198, 220, 228, 231, 236, 359
Artin-Rees lemma, 457
Artin-Schreier theorem, 236
Artin-Wedderburn theorem, 367, 370
associativity, 3, 566
  adjoint, 444
atom, 555
automorphism
  inner, 56
  of group, 20
axiom of choice, 628, 628–631
B
Baer, R., 403
Baer's criterion, 404
base, transcendence. *See* transcendence base
basis
  See also Gröbner basis
  dual, 448
  of ideal, 146
  of module, 330
  of vector space, 335
Bass, H., 407
Beck, J., 616, 618
Beck's theorem, 618
Belkhouche, B., vii
bidule, 8
bifunctor, 588, 589
bihomomorphism
  of bimodules, 438
  of modules, 435
bimodule, 417, 529
  of homomorphisms, 418
Bims, 588
binomial theorem, 107
biproduct, 601, 600
Birkhoff, G., vii, 539, 549, 552, 555, 558, 570, 574, 576
Birkhoff's theorem, 549; 552, 577; 555; 570; 576
Boole, R., 552
bound
  greatest lower, 539
  least upper, 540
  lower, 539
  upper, 628, 540
boundary, 463, 464
Buchberger, B., 148
Buchberger's algorithm, 152, 354
Buchberger's criterion, 151, 352
Burnside's theorem, 372; 391
Burnside, W., 1, 372, 380
butterfly lemma, 72
C
cancellation laws, 10, 12, 116
Cantor, G., 639, 641
Cantor-Bernstein theorem, 640
Card, 642
Cardano, G., 191, 206, 207
cardinal number, 640, 639–644
  finite, 640
  infinite, 640
cardinality, 641
Cartan, H., 401, 403, 463
Cartesian product, 43, 324, 592
  empty, 2
  of categories, 588
  of classes, 582
category, 582, 582–624
  abelian, 602, 602–604
  additive, 600, 600–604
  cocomplete, 598
  comma, 611
  complete, 596, 595–599
  dual, 585
  equivalent, 588, 590
  free, 584
  functor, 587, 600, 604
  isomorphic, 588
  locally small, 589
  of abelian groups, 583, 600, 602, 616, 620
  of bimodules, 588, 600, 602
  of groups, 583, 584, 596, 598, 599, 611, 617, 620
  of left R-modules, 583, 596, 598, 599, 600, 601, 602, 617, 620
  of partially ordered sets, 616
  of paths, 584
  of R-algebras, 584, 596
  of rings, 584, 585, 586, 596, 617, 620
  of sets, 583, 596, 598, 599, 609, 616
  of T-algebras, 615
  of topological spaces, 617, 620
  opposite, 584, 585, 588, 593, 598, 600
  small, 583
  tripleable, 616, 616–621, 623
Cats, 587

Cauchy, A., 1
Cauchy's theorem, 64
Cayley-Hamilton theorem, 345
Cayley's theorem, 54
center
  of algebra, 535
  of $GL(V)$, 78
  of group, 56
  of p-group, 57
  of $SL(V)$, 78
centralizer, 56, 537, 545
  of permutation, 63
chain, 626, 15, 111, 463, 464, 628
  maximal, 547, 553
  of subsets, 15
  singular, 463
chain condition
  ascending, 626, 146, 296, 346
  descending, 627, 300, 347
character, 386, 386–392
  complex, 389, 389–392
  irreducible, 386
  of group, 386
  of group representation, 386
  one-dimensional, 387
  regular, 387
  trivial, 387
characteristic
  of domain, 116
  of field, 116, 156
  of ring, 115
Chase, S., 407
Chinese remainder theorem, 289
class, 581, 582, 631
  associate, 133
  cohomology, 468
  conjugacy, 56, 65, 384
  homology, 464
  proper, 581
  small, 582
class equation, 57
classification theorem, 74
Clifford, A.H., 5
Clifford's theorem, 386
closure
  algebraic, 167, 165–168, 237, 238
  integral, 283
  real, 236
coboundary, 463, 467, 468, 501
cochain, 463, 467, 501
  singular, 463
cocone, 594
cocycle, 468, 501
codimension, 304
codomain, 582
coefficient
  leading, 121, 146, 351
coequalizer, 595
  absolute, 621
  split, 617
cohomology, 464
  of groups, 501, 500–507
  singular, 464
coimage, 603
Coker , 393
cokernel, 602
  of homomorphism, 393, 396, 594
colimit, 593, 594
  directed. *See* direct limit
combination, linear, 316
  infinite, 316
commutativity, 3, 567
commutator
  of two elements, 83
  series, 84
  subgroup, 83
comparison theorem, 472, 477
complement, 554
completion
  $\mathfrak{a}$-adic, 266, 301, 458
  MacNeille, 545
  of exact sequences, 460
  of field, 244, 243–246
  of module, 461, 456–462
  of partially ordered set, 544
  of ring, 266, 266–268, 461
complex
  bar, 503
  chain, 463, 464
  cochain, 464
  negative, 464
  positive, 464
  singular, 463, 464
component
  homogeneous, 517
  simple, 369
composite of fields, 158, 159, 164, 185
composition, 582

concatenation, 6
cone, 424, 430, 591, 594
  colimit, 593, 594, 610
  limit, 424, 430, 592, 610
  mapping, 470
congruence, 562, 564
  fully invariant, 572
  induced by ideal, 577
  on a group, 563
  on a ring, 564
  on a semigroup, 564
conjugate
  elements, 36, 56, 194, 216
  field extensions, 194
  permutations, 62
  subgroups, 65
connection, Galois. *See* Galois connection
constructible, 226, 226–230
construction
  by straightedge and compass, 226, 225–230
  standard. *See* triple
contraction, 286, 287
coordinates, 310, 330
coproduct, 594, 595
coset, 16, 15–17
  left, 15
  right, 15
  of normal subgroup, 19
cosyzygy, 476, 508, 510
cover, 547, 634
create
  coequalizers, 617
  everything, Gen:1:1
  limits, 599, 612, 616, 624
cross section, 629
  of group extension, 95
curve, algebraic, 271, 307
cycle, 60, 464
cylinder, mapping, 470

D

d.c.c. *See* descending chain condition
decomposition, subdirect, 575, 578
Dedekind, R., 104, 155, 273, 290, 539
Dedekind domain, 293, 295–297, 413–414, 497
degree
  of element, 162
  of field extension, 160
  of group representation, 380
  of monomial, 127
  of polynomial, 121, 127
  residual class, 254, 254–257
  separability, 170
  transcendence, 184, 311
derivative, 123
destination, 583
determinant, 526, 527
Diag , 591
diagram, 590
  commutative, 591
  constant, 592
dimension
  global, 510, 511, 510–514
  injective, 509
  Krull, 305, 306, 310
  of algebraic variety, 309, 312
  of group representation, 380
  of vector space, 336
  projective, 509, 507–510
direct limit, 424, 423–429, 433
  of complexes, 470
  of exact sequences, 428
  of modules, 424, 427, 447, 451, 453, 455, 497
  of sets, 424, 425
  of universal algebras, 573, 624
direct product
  of bimodules, 423
  of Boolean lattices, 557
  of complexes, 470
  of groups, 43, 48, 43–49, 592
  of homomorphisms, 325
  of modules, 325, 328, 420, 491, 592
  of injective modules, 404
  of projective modules, 403
  of rings, 364–366, 375
  of universal algebras, 568
direct sum
  external, 325
  internal, 327
  of complexes, 470
  of group representations, 380
  of groups, 44, 49
  of homomorphisms, 326
  of modules, 325, 325–329, 402, 421, 429, 433, 446, 451, 491, 494, 495,

508, 594
of injective modules, 407
of projective modules, 402
Dirichlet, G., 188, 214
Dirichlet's theorem, 214
discriminant, 179, 179–181, 206
distributivity, 105, 315, 548, 567
division
polynomial, 121, 149
divisor
greatest common, 135, 136, 142
domain, 116, 115–119, 582, 630
See also Dedekind domain
See also principal ideal domain
See also ring
See also unique factorization domain
of binary relation, 631
integral, 116
integrally closed, 283, 284, 287, 295, 296
normal, 283
valuation. *See* valuation ring
doohickey, 416
duality principle, 540, 541, 543, 546, 549, 553, 585
duplication of cube, 226
Dyck, W., 27, 31, 33
Dyck's theorem, 33
E
edge, 583
eigenspace, 345
eigenvalue, 345
Eilenberg, S., 401, 403, 463, 500, 613
Eisenstein, G., 144
Eisenstein's criterion, 144, 145, 262
element
See also elements
algebraic, 161, 162, 280
cancellative, 578
central, 382, 516
greatest, 627, 543
idempotent, 370
identity. *See* identity element
integral, 279, 280, 281
irreducible, 134, 142, 550
least, 629, 543
left quasiregular, 377
maximal, 625, 111, 145
minimal, 627
nilpotent, 112, 376, 377, 577
prime, 134, 142
primitive, 161
purely inseparable, 174
quasiregular, 377
radical, 218
representative, 133
separable, 171
torsion, 339
torsion-free, 339
transcendental, 161
unique maximal, 627
zero. *See* zero element
elementary
linear transformation, 77
matrix, 77
elements
See also element
associate, 133
algebraically dependent, 182
algebraically independent, 182
endomorphism
nilpotent, 51
normal, 50
of abelian group, 106
of group, 20
of module, 320
of vector space, 106
projection, 52
End_R, 332
$\mathrm{End}_R^{\mathrm{op}}$,
$\mathrm{End}_{\mathbb{Z}}$, 316
envelope, injective. *See* hull, injective
epimorphism, 19, 107, 584
of modules, 320, 393
split, 395, 402
equalizer, 593, 595
equipotence, 640
equivalence
of categories, 588, 609
of group extensions, 95, 98
Erlanger Programme, 1
Euclid, 138
evaluation
of polynomials, 122, 128
of rational fractions, 124, 129
exchange property, 50, 182, 335
expansion, 286, 287
exponentiation of cardinals, 642, 644

Ext, 490
extension
essential, 409, 408–410
of absolute values, 247–261
of fields. *See* field extension
of groups. *See* group extension
of rings. *See* ring extension
of valuations, 256–261
F
factor
of normal series, 71, 348
simple, 74
factor set, 96
factorization theorem
for algebras, 517
for groups, 23
for modules, 322
for rings, 114
for universal algebras, 562
family
algebraically dependent, 182
algebraically independent, 182
directed, 15, 423, 425, 568
linearly independent, 330
Feit, W., 83
Feit and Thompson theorem, 83
Fermat prime, 229
field, 116, 155–268, 569
See also field extension
algebraically closed, 166
archimedean, 232, 233
complete, 243, 249, 259, 264
cyclotomic, 212
finite, 192–193
fixed, 198, 202
formally real, 234, 234–239
Galois, 193
of fractions, 118, 119, 285
of rational fractions, 124, 128, 531
ordered, 231, 231–239
perfect, 196, 197, 237, 238
quotient. *See* field of fractions
real closed, 235, 235–239
residue class, 258, 258–261
skew, 334
splitting, 191, 192, 191–193
field extension, 159, 159–230, 530–534
algebraic, 164, 164–230
conjugate, 194, 199
cyclic, 219, 218–220
finite, 160, 164, 297
finitely generated, 161
Galois, 197, 197–225, 297–300
infinite, 160
infinite Galois, 200–204
linearly disjoint, 185, 186, 532
normal, 192, 191–197, 199, 225
purely inseparable, 173, 172–175, 192
purely transcendental, 181
quadratic, 283
radical, 221
separable, 171, 169–172, 189, 184–190, 195, 532
simple, 161, 162, 170
solvable by radicals, 221, 221–225
totally transcendental, 181
transcendental, 164, 181–190
filter, 462
filtration
$\mathfrak{a}$-, 456
$\mathfrak{a}$-adic, 266, 456
$\mathfrak{a}$-stable, 457, 458
on module, 456, 456–458
on ring, 266, 266–272
five lemma, 394
fixed point, 60
fraction, 118, 285
See also rational fraction
partial, 139
polynomial free, 139
reduced, 139
fractional ideal, 290, 291
finitely generated, 291
invertible, 291, 413
free product of groups, 40, 37–42, 594
with amalgamation, 41, 42, 584, 595
Freyd, P., 609
Frobenius, G., 45, 515, 538
Frobenius's theorem, 538
Func , 587
function
choice, 628
class, 387, 582
coordinate, 106, 310
Euler's, 46–47, 207
polynomial, 311
rational, 129, 311, 314
functor, 416, 586, 586–590

additive, 417, 603
adjoint, 606, 604–612
colimit, 599, 606
completion, 459, 460
contravariant, 416, 588
covariant, 416, 586
derived, 478–487
direct limit, 427–429
dual, 448
exact, 419, 420
Ext, 488–493, 507
forgetful, 586, 596, 604, 607, 611, 621, 622
free group, 586, 604
free module, 605, 613
Hom, 417, 418–423, 589, 597, 599
homology, 464
identity, 587
inverse limit, 432–434
left adjoint, 606, 622
left derived, 479, 479–484, 486
left exact, 419
limit, 598, 599, 606
representable, 612
right adjoint, 606
right derived, 484, 485, 486
right exact, 445
$\otimes$, 437, 438, 445–448, 607
Tor, 493, 493–496
tripleable, 616, 616–621, 623
fundamental theorem
of algebra, 137
of finitely generated abelian groups, 44, 339
of Galois theory, 198, 203

G

Galois, E., 1, 191, 192
Galois connection, 200, 544, 545
Galois group, 197, 204, 197–225, 224, 299–300
of polynomial, 204, 204–211
of extension of $\mathbb{Q}$, 214
Garibaldi, S., viii
Gauss, G., 105, 137, 142, 229, 262
Gauss integer, 109
Gauss's lemma, 143, 262
gcd , 135
geometry, algebraic, 271, 273, 275, 276, 307–314
GL, 76
g.l.b. *See* greatest lower bound
Gödel, K., 628
going up, 282
Gorenstein, D., 74
graph, 583
directed, 583
discrete, 592
finite, 598
square, 583
triangle, 583
Grassmann, H., 523
Grell, H., 285
Grillet, P.A., 579
Grillet's theorem, 579
Gröbner, W., 148
Gröbner basis
of ideal, 150, 148–154
of module, 352, 350–358
group, 8, 1–104
See also abelian group
See also Galois group
action. *See* group action
alternating, 36, 60, 74
amalgam, 41
classical, 76–83
cohomology, 100, 464, 468, 500–507
cyclic, 14, 21, 24, 25, 35, 46, 68, 94, 100, 507
defined by generators and relations. *See* presentation
derived, 83, 84
dihedral, 9, 14, 19, 20, 26, 34, 37, 68, 88
finite, 11, 13, 14, 16, 43–104
free, 29, 27–31, 505–506
fundamental, 8, 18, 20, 37, 43, 83
general linear, 76, 81
generated by a subset, 14
generated by ... subject to ..., 33
generator, 33
homology, 463, 464
indecomposable, 47, 49
isomorphic, 20
Klein four, 9, 13, 44
metabelian, 83
nilpotent, 89, 89–92
of automorphisms, 20, 55
of finite length, 49

of homomorphisms, 415–423
of isometries, 9
of rotations and symmetries, 9
p-, 45, 57, 64, 67, 84, 91
profinite, 204, 434
projective special linear, 78, 81, 82
quaternion, 35
quotient, 20, 20–23
simple, 73, 73–76, 81, 82
solvable, 83, 83–88, 219, 391
special linear, 77, 77–82
symmetric, 8, 58–64, 88
transitive, 75
value, 248
group action
left, 54, 55
right, 54
trivial, 501
group extension, 95, 95–104
equivalent, 95, 98
split, 99
Grps, 583
H
$\mathbb{H}$, quaternion algebra, 36, 37
Hall, P., 86
Hall theorems, 86–88
Halmos, P., 640
Hamilton, W.R., 37, 105, 515
Haupidealsatz, 303
Hausdorff, F., 628
height of prime ideal, 303, 304, 303–306
Hensel, K., 243, 261
Hensel's lemma, 263, 264, 270
Hilbert basis theorem, 147
Hilbert, D., 105, 147, 218, 307, 510, 511
Hilbert's Nullstellensatz, 307, 308
Hilbert's Theorem 90, 218
Hilbert theorem on syzygies, 511
Hölder, O., 74, 100
Hölder's theorem, 100
Hom, 415, 415–423, 433, 442, 589
homology, 463–471
singular, 463
homomorphism
boundary, 463, 464
central, 516
coboundary, 463, 467
connecting, 465, 466, 469, 478, 484, 485
evaluation, 122, 128, 448
inclusion, 18, 113, 156, 561
K-, 158
natural, 417
of algebras, 382, 516
of bimodules, 418
of direct systems, 423
of fields, 117, 156
of graded algebras, 517
of groups, 18, 18–25
of inverse system, 430
of lattices, 542
of modules, 320, 320–324
of rings, 107, 112–115
of rings with identity, 107
of T-algebras, 614
of universal algebras, 560
homomorphism theorem
for algebras, 516
for complexes, 470
for fields, 156
for graded algebras, 517
for groups, 23
for lattices, 542
for modules, 322
for rings, 114
for universal algebras, 562
in abelian category, 603
homotopic, 465
homotopy, 465, 470
Hopkins, C., 379
Hopkins-Levitski theorem, 379
Hopkins's theorem, 379
hull, injective, 410, 408–410
Hurewicz, W., 393
I
ideal, 110, 516, 552
associated prime, 276
fractional. *See* fractional ideal
generated by monomials, 149
generated by $1\frac{1}{2}$ elements, 293
generated by subset, 110
graded, 517
irreducible, 275
left, 318
maximal, 111, 117, 134, 282, 301, 308
membership problem, 150
minimal left, 360
nil, 377
nilpotent, 376

of quotient ring, 114
of semigroup, 578
of $\mathbb{Z}$, 110, 117
order, 632, 551
$\mathfrak{p}$-primary, 275
primary, 275, 287
prime, 117, 133, 274, 281–282, 287, 298, 302–306
principal, 110, 552
proper, 110
right, 318
semiprime, 275, 308
two-sided, 318, 516
idempotent, 370, 376, 377
central, 557
identity
See also identity element
of type T, 566
identity element, 2
left, 12
of ring, 106
Im , image, 19, 113, 321
image, 603
direct, 18, 113, 321, 563
homomorphic, 568
inverse, 18, 113, 321, 563
of homomorphism, 19, 113, 321
indeterminate, 120, 126, 130, 131
index, 16, 17
nilpotency, 90
of centralizer, 56
of normalizer, 65
of stabilizer, 55
ramification, 258, 258–261
induction
Artinian, 627
Noetherian, 626
ordinal, 635, 635–639
strong, 627, 636
transfinite, 629
infimum. *See* greatest lower bound
injection
to coproduct, 594
to direct sum, 325
to free group, 29
to free product, 40
to group extension, 95
to semidirect product, 93
integer, 1
algebraic, 109, 283, 297, 297–300
Gauss, 109, 137
modulo n, 21, 114
p-adic, 245, 246, 266
intersection
of congruences, 562
of ideals, 110
of primary ideals, 275–276
of subalgebras, 560
of subgroups, 15
of submodules, 318
reduced, 276
interval, 548, 557
inverse
left, 12
of element, 8
of product, 10
inverse limit, 431, 429–434
of exact sequences, 432
of modules, 431, 432
of sets, 433
of universal algebras, 574
Irr $(\alpha : K)$, 162
isometry, 9
isomorphism, 584, 602
K-, 160
natural, 587
of algebraic varieties, 313
of categories, 588
of fields, 156
of groups, 20
of lattices, 542, 543
of modules, 320, 393
of partially ordered sets, 633, 542
of rings, 107
of totally ordered abelian groups, 251
of universal algebras, 561
isomorphism theorems
first, 25
for groups, 23–26
for modules, 323
for rings, 115
for universal algebras, 563
second, 25
third, 25

J

Jacobson, N., 370, 372, 376, 377
Jabobson density theorem, 371, 373
Jech, T., 581, 631, 640

join. *See* least upper bound
Jordan block, 345
Jordan, C., 74, 342
Jordan form, 345, 342–346
Jordan-Hölder theorem, 74, 348
K
K^{1/p^∞}, 173
Kempf, G., 166
ker, equivalence relation, 561
Ker, kernel, 19, 113, 321
kernel, 602
  of homomorphism, 19, 113, 321, 396, 593
Klein, F., 1
Kramer, D., viii
Kronecker, L., 45
Krull intersection theorem, 301
Krull-Schmidt theorem, 50, 349
Krull's Hauptidealsatz, 303, 305
Krull's theorem, 203; 305
Krull, W., vii, 48, 105, 203, 251, 300, 301, 303, 304, 305
Kuratowski, C., 628
Kürschak, J., 243
L
Lagrange, J., 1
Lagrange's theorem, 16
Lasker, E., 273
lattice, 541, 539–558, 573, 576, 624
  Boolean, 554, 553–558, 573, 624
  complete, 543, 543–545
  complete Boolean, 557
  distributive, 549, 549–553, 577, 624
  generalized Boolean, 557
  modular, 545, 545–548, 573, 624
  of normal subgroups, 548
  of submodules, 546
  of subgroups, 548, 552, 553
  of subsets, 539, 540, 549, 553, 554
  subdirectly irreducible, 576
Laurent series, 131, 131–133, 245, 254
laws, absorption, 542
Lazard, D., 450, 455
Lazard's theorem, 455
lcm, 135
length
  of module, 348
  of normal series, 70, 348
lift, 402, 471, 472, 477
Light's test, 5, 35
  fails, 5
  passes, 5
limit, 592, 591–593
  See also direct limit
  See also inverse limit
  directed. *See* inverse limit
  finite, 598
  inductive. *See* direct limit
  inverse. *See* inverse limit
  of sequence, 233, 243–245, 247–248, 268, 462
  projective. *See* inverse limit
  standard, 596
localization, 287, 285–290
Louis XIV, 633
l.u.b. *See* least upper bound
lying over, 281, 282
M
MacLane, S., vii, 184, 188, 393, 463, 490, 500, 532, 581, 609
MacLane's theorem, 188, 532
MacNeille, H., 544
MacNeille's theorem, 544
Mal'cev, A.I., 580
Malcev's theorem, 580
map
  See also mapping
  closure, 543
  tensor, 434, 436, 444
mapping, 582
  See also multilinear mapping
  biadditive balanced. *See* bihomomorphism
  bilinear, 434, 435
  middle linear. *See* bihomomorphism
  n-linear. *See* multilinear mapping
  order preserving, 542
  polynomial, 312
  regular, 312
Maschke, H., 383
Maschke's theorem, 383, 506
matrix
  column finitary, 334
  of homomorphism, 332, 450
McCarthy, P., 203
meet. *See* greatest lower bound
metatheorem, 540, 585
M_5, a lattice, 546, 549

M_n, 1, 332
module, 278, 279, 315–366, 615
  See also modules
  Artinian, 300, 348
  blown-up, 457
  completely reducible, 363
  complete, 458
  cyclic, 318, 323
  divisible, 405
  double dual, 448
  dual, 419, 448, 448–451
  faithful, 317
  finitely generated, 274, 318
  finitely presented, 453, 453–455
  flat, 450, 450–456, 461, 495, 496
  free, 330, 329–338
  homology, 464
  indecomposable, 349
  injective, 403, 403–410, 412, 414, 420, 422, 429, 452, 484, 491, 492
  left, 315
  Noetherian, 296, 347
  of finite length, 348, 379
  of fractions, 442, 456
  over a PID, 336–342
  over polynomial rings, 342, 350, 510–514
  projective, 402, 401–403, 411, 419, 448–451, 480, 486, 491, 492, 494
  quotient, 279
  right, 317
  semisimple, 363, 362–364, 371, 379
  simple, 359, 360
  torsion, 339
  torsion-free, 339
  unital, 315, 317
modules
  See also module
  injectively equivalent, 510
  isomorphic, 320
  projectively equivalent, 507
monad. *See* triple
monoid, 3, 614
  commutative, 3
  free, 6, 120
  free commutative, 7, 126
  of endomorphisms, 20
monomial, 6, 125
  leading, 149, 351
monomorphism, 19, 107, 584
  essential, 409
  of modules, 320, 393
  split, 395, 404
Moore, E., 543
Moore, J.C., 613
morphism, 582
  See also homomorphism
  codiagonal, 601
  diagonal, 601
  identity, 582
  natural, 587
  of algebraic varieties, 312
  of diagrams, 591
  of T-algebras, 614
  zero, 600
multihomomorphism, 443
multilinear mapping, 443
  alternating, 524, 525
  symmetric, 522
multiple
  integer, 4, 11, 106, 114–115
  least common, 135, 136, 142
multiplication, 2
multiplicity of root, 122, 125
N
$\mathbb{N}$, 1
Nagata, M., 376
Nakayama, I., 376
Nakayama's lemma, 302, 303, 376
N_5, a lattice, 546
Nielsen, J., 27
nilradical, 274
nilsemigroup, 577
nine lemma, 395, 397, 470
node, 583
Noether, E., vii, 105, 146, 273, 295, 529, 535, 534
Noether-Lasker theorem, 276
Noether's theorem, 535
norm
  of element, 215, 215–219
  on vector space, 247
normalization, 283
normalizer, 65, 67
normal series, 70, 72
  ascending central, 90, 639
  central, 89
  descending central, 89
  equivalent, 71, 348

notation
additive, 2, 4, 11, 13
multiplicative, 2
Nullstellensatz, 308
number
algebraic, 236
cardinal. *See* cardinal number
ordinal. *See* ordinal number
of elements, 639, 641
p-adic, 245, 246
O
object, 582
initial, 609, 612
terminal, 609, 612
zero, 600
ω, ordinal number, 634
$^{\mathrm{op}}$, opposite, 317, 540, 585, 627
operation
associative, 3
binary, 1, 559
commutative, 3
componentwise, 43
constant, 2, 559
idempotent, 540
n-ary, 2, 559
order preserving, 540
partial, 2, 559
unary, 2, 559
opposite
of element, 8
of sum, 11
orbit, 55
Ord, 632
order
degree lexicographic, 148
degree reverse lexicographic, 148
lexicographic, 148
monomial, 148, 351
of center, 57
of conjugacy class, 56
of element of a group, 24
of group, 16
of orbit, 55
of permutation, 62
of polynomial, 239
of power series, 130
of quotient group, 21
of subgroup, 16, 17
term, 148
order relation, 625, 631
opposite, 626
partial, 625
total, 625
ordered set
See also partially ordered set
See also preordered set
totally, 625, 423
well, 629, 633
ordinal number, 631, 631–639
limit, 634
successor, 633, 634
origin, 583
orthogonality of characters, 388, 389
Ostrowski, A., 241, 247
Ostrowski's theorem, 249
P
partially ordered set, 625, 423
See also preordered set
dual, 540
Noetherian, 626
opposite, 627, 540
partition, 16, 45, 55, 62
path, 583
empty, 583
Peirce, B., 104, 515
permutation, 9, 58–63
conjugate, 62
disjoint, 60
even, 59
fixed point of, 60
odd, 59
sign of, 60
support of, 60
place, 255
polygon, regular, 9, 226
polynomial, 120, 126, 119–130
See also polynomial equation
See also ring of polynomials
characteristic, 216, 345
constant, 120, 126
cyclotomic, 211, 211–215
elementary symmetric, 177, 224
general, 223
homogeneous, 129
in one variable, 120, 119–125
in several variables, 126, 125–130
irreducible, 136–138, 143–145, 233
minimal, 343, 345

monic, 121
of degree 2, 205
of degree 3, 205–207, 209, 210
of degree 4, 208–209, 210
primitive, 142, 258
separable, 169
splitting, 191
symmetric, 224
polynomial equation, vii, 1, 191
general, 223, 223–225
of degree 2, vii, 1, 191, 205
of degree 3, 191, 205–207
of degree 4, 191, 207–208
of degree 5, 191
POS, 616
power, 3, 10, 642
exterior, 525
symbolic, 298
symmetric, 523
tensor, 519
power series, 130, 130–133, 245, 254, 267–269
preimage. *See* inverse image
preordered set, 423, 428, 583, 585, 612, 616
See also partially ordered set
directed, 423
presentation, 34, 31–37
projective, 471
preserve colimits, 598, 608
preserve limits, 597, 608, 621
Preston, G.B., 5
primitive element theorem, 171
principal ideal domain, 133, 133–138, 254, 293, 294, 295, 336–342, 403, 405, 411, 497
product, 2, 592, 595
See also Cartesian product
See also direct product
See also free product
See also subdirect product
See also tensor product
balanced, 435, 443
empty, 2
of cardinal numbers, 642, 643, 644
of elements, 2
of ideals, 112, 269
of left ideal and submodule, 319, 320
of left ideals, 319
of morphisms, 582, 598
of ordinal numbers, 635
of subsets, 4
semidirect, 93, 92–94, 102
torsion. *See* Tor
projection
from direct product, 44, 325, 568
from group extension, 95
from product, 592
from semidirect product, 93
to quotient algebra, 561
to quotient group, 20
to quotient module, 321
to quotient ring, 113
to quotient set, 561
PSL, 79
pullback, 593, 604
of modules, 397, 398, 400, 423, 429, 433, 593
pushout, 595
of modules, 399, 398–401, 423, 429, 448
Q
Q, quaternion group, 35, 69
$\mathbb{Q}$, 1
$\widehat{\mathbb{Q}}_p$, 245
quadrature of circle, 229
quotient
universal algebra, 562
group, 20
module, 321–322
of ideals, 273
ring, 113
R
$\mathbb{R}$, 1
R^1, 108
Rad, 274
radical, 375
Jacobson, 375, 374–377
nil, 274
of ideal, 274
R-Algs, 584
range, 19, 113, 321
rank of module, 334, 335
rational fraction, 124, 129, 139–141
symmetric, 224
recursion, 637, 638
Rédei, L., 148, 580
Rédei's theorem, 148, 580
reduction, 27, 29, 38, 39
refinement of normal series, 71, 348

relation
See also order relation
defining, 33
equivalence, 561
group, 27, 32
of type T, 565
Remak, R., 48
representation of group, 380, 382, 380–392
complex, 389, 389–392
equivalent, 380, 382
irreducible, 381, 384
regular, 380
trivial, 380
resolution, 471–478
bar, 505, 502–505
flat, 496
free, 471, 504
injective, 476, 476–478, 491, 508
projective, 471, 471–476, 491, 494, 507, 508
resultant, 176, 176–178
ring, 105, 105–154, 273–318, 366–379
See also algebra
See also domain
affine, 311
associative, 106
blown-up, 457
Boolean, 554
change of, 440, 441, 461
commutative, 106, 115–119, 269–314, 318
complete, 267, 267–272
coordinate, 310, 310–314
division, 116, 209, 334, 336, 360, 384, 538
Euclidean, 138
free commutative, 129
group, 120, 382; *see also* group algebra
isomorphic, 107
Jacobson semisimple, 378, 377–379
left Artinian, 348, 349, 377–379
left hereditary, 411, 411–414, 497, 499, 510
left Noetherian, 347, 349, 407, 429
left primitive, 372, 372–374, 377
local, 287, 403
Noetherian, 146, 146–148, 287, 296
nonassociative, 106
of endomorphisms, 316, 332, 360, 364, 370–374
of fractions, 285, 285–290
of matrices, 106, 332, 360–362, 364, 370, 371, 377, 515
of polynomials, 119–130, 147, 142–144, 276, 305–306, 308, 309, 510–514, 515, 517, 522, 577
opposite, 317, 332, 361, 442
reduced, 532
regular, 109, 370, 379
right Artinian, 348
right Noetherian, 347
right primitive, 372
semigroup, 120, 124
semiprimitive, 378
semisimple, 359, 366, 366–370, 377, 383, 402, 404, 510
simple, 360
valuation. *See* valuation ring
von Neumann regular, 109, 370, 379
with identity, 105
with unity, 104
ring extension, 277, 277–284, 515
finitely generated, 278, 288
integral, 280, 280–282, 287, 288
Rings, 584
${}_R$*Mods*, 583
root, 122
See also root of unity
multiple, 122
simple, 122, 123
root of unity, 157
primitive, 157, 211
${}_RR$, 315
Russell's paradox, 631
$R[X]$, 120
$R(X)$, 124
$R[[X]]$, 130
$R((X))$, 131
$R[(X_i)_{i\in I}]$, $R[X_1, ..., X_n]$, 126
$R((X_i)_{i\in I})$, $R(X_1, ..., X_n)$, 128, 129
S
Schanuel's lemma, 507
Schering, E., 45
Schmidt, O., 48
Schreier, O., 41, 71, 97, 217, 231, 236
Schreier's theorem, 71, 348; 97
Schreyer, F., 355
Schreyer's theorem, 355

Schur, I., 102, 360, 380
Schur's lemma, 360
Schur's theorem, 102, 493
Schur-Zassenhaus theorem, 102
section, lower, 632
  See also order ideal
semigroup, 3, 1–7
  cancellative, 577
  commutative, 3, 577–579
  determined by ideal, 577
  elementary, 579, 580
  free, 6
  free commutative, 7, 577
  nil. *See* nilsemigroup
  subelementary, 579, 580
semilattice, 539–541, 542
  lower, 539
  upper, 540
separate the elements, 575
sequence
  addible, 131, 268
  Cauchy, 233, 243–245, 247–248, 268, 462
  connected, 478, 484, 485
  empty, 6
  exact, 393, 393–397, 465, 604
  exact cohomology, 468, 504
  exact homology, 465
  Hom-Ext, 491
  Ker-Coker, 467, 471
  left exact, 394, 419, 420
  Mayer-Vietoris, 470
  null, 393
  right exact, 394, 420
  short exact, 394
  split exact, 395, 604
  summable, 130
  Tor, 494
  transfinite, 635
series
  See also Laurent series
  See also power series
  central, 89, 639
  commutator, 84
  composition, 73, 74
  normal. *See* normal series
  of submodules, 348
  subnormal, 71
set
  See also algebraic set
  See also ordered set
  See also preordered set
  countable, 641, 642
  finite, 641
  infinite, 641
  quasiordered. *See* preordered set
  quotient, 561
  transitive, 631
  underlying, 3, 8
  zero, 307
Sets, 583
sign of permutation, 60
simplex, 463
  singular, 463
  standard, 463
$\mathfrak{s}_k$, 176
skeleton, 590
Skolem-Noether theorem, 536
SL, 77
S_n, 58
$S^{-1}R$, 285
solution set condition, 610
space
  affine, 307
  projective, 79, 307
  Stone, 555, 556, 557
spectrum, 301
Spencer, M., viii
stabilizer, 55
Steinitz, E., 155
Stickelberger, L., 45
Stone, M., 539, 555, 556
Stone space, 556, 557, 558
Stone's theorem, 555; 556
structure
  cycle, 61
  module, 315, 316
subalgebra, 516, 560
  generated by a subset, 519, 564
  graded, 517
subdirect product, 574, 574–580
subfield, 155, 156, 157
  generated by subset, 158
subgroup, 12, 12–18
  characteristic, 58
  commutator, 83
  cyclic, 14
  Frattini, 17

fully invariant, 88, 91
generated by subset, 13
Hall, 86, 86–88
maximal, 17, 92
normal, 19
of quotient group, 21
of $\mathbb{Z}$, 14
subnormal, 71
Sylow, 65, 65–67, 85, 91
sublattice, 542
Boolean, 555
submodule, 278, 318
anticommutative, 524
cyclic, 318
essential, 329, 408
finitely generated, 278, 318
generated by monomials, 351
generated by subset, 278, 318
graded, 517
large, 408
membership problem, 351
of free module, 336, 337, 411
of quotient module, 322
pure, 448
syzygy, 354
subring, 109, 110
generated by subset, 112, 158
of field, 155
of quotient ring, 114
of ring extension, 278
subsemigroup, 578
subset
algebraically dependent, 182
algebraically independent, 182
cofinal, 429
cofinite, 557
dense, 372
linearly independent, 330
multiplicative, 281
proper multiplicative, 281
substitution
in polynomials, 122, 125
in power series, 132
subtraction, 106
successor, 633, 634
sum
See also direct sum
direct, 328
infinite, 107
of cardinal numbers, 642, 644
of elements, 4
of ideals, 111
of ordinal numbers, 635
of power series, 131
of submodules, 319
of subsets, 4
summand, direct, 328, 402, 404, 451
of free module, 402
support of permutation, 60
supremum. *See* least upper bound
surgery, 160
Sylow, L., 64, 65
Sylow theorems, 64–67
system
direct, 423
inverse, 430
syzygy, 354, 471, 507–508
T
T, a group, 36, 69
table, 4
Light's, 5
$\otimes$, 434, 436
tensor product, 435, 434–448
of algebras, 527, 527–530, 594
of bimodules, 438, 438–441, 444
of elements, 434, 436
of exact sequences, 445, 446
of fields, 530–534
of free modules, 439
of graded algebras, 530
of modules, 435, 444, 449–451
of vector spaces, 434
term, 148
leading, 149, 351
terminate, 624, 626, 145, 292, 296, 346, 347
Thompson, J.G., 83
topology
algebraic, 8, 18, 20, 37, 41, 43, 83, 463, 464, 465, 470, 497, 500
compact-open, 372
finite, 201, 203
Krull, 202, 201–204, 272, 462
on power series ring, 132
profinite, 27
Stone, 555
Zariski, 309, 310
Tops, 617
Tor, 493, 493–496

torsion, 339
tower
  of field extensions, 158
  property, 160, 164, 170, 172, 175, 183, 189, 195, 217, 281
trace
  of element, 215, 215–219
  of linear transformation, 215
transcendence base, 183
  separating, 187
transformation, 2
  chain, 464
  diagonalizable, 345
  linear, 320, 342–346
  natural, 417, 587
  nilpotent, 346
  projective, 79
  rational, 312
transporter, 273, 274
transposition, 58
trihomomorphism, 444
triple, 613, 613–620
trisection of angle, 226
2^X, 539, 540, 549, 553, 554
type of universal algebra, 560
U
union
  directed, 568
  of congruences, 562
  of ideals, 111
  of subalgebras, 560
  of subgroups, 15
  of submodules, 318
  of subrings, 112
unique factorization domain, 141, 141–145, 283, 304
unit
  of ring, 109
  of polynomial ring, 121, 127
  of power series ring, 131
universal algebra, 560, 559–580
  free, 569, 573, 622
  of type T, 560
  quotient, 561
  subdirectly irreducible, 575
  word, 565, 564–567
universal coefficient theorem, 497, 499
universal property, 610, 612
  of category of T-algebras, 616
  of coequalizer, 594
  of cokernel, 393, 394, 601
  of colimit, 594
  of completion, 244, 459
  of coproduct, 594
  of derived group, 84
  of direct limit, 425
  of direct product, 47, 325
  of direct sum, 326
  of exterior algebra, 524
  of exterior power, 525
  of field of fractions, 117
  of free category, 591
  of free group, 30
  of free module, 331
  of free product, 40
  of free product with amalgamation, 42
  of free universal algebra, 569
  of group algebra, 382
  of initial object, 609
  of inverse limit, 431
  of kernel, 393, 394, 601
  of left derived functor, 481
  of left exact sequence, 394
  of limit, 592
  of localization, 285
  of polynomial rings, 123, 128
  of power series rings, 269
  of presentation, 33
  of product, 592
  of pullback, 397, 593
  of pushout, 399, 595
  of quotient algebra, 517, 562
  of quotient group, 23
  of quotient module, 322
  of quotient ring, 114
  of $\mathbb{R}$, 233
  of R^1, 108
  of right derived functor, 484, 485
  of right exact sequence, 394
  of ring of fractions, 285
  of simple field extension, 163
  of symmetric algebra, 521
  of symmetric power, 522
  of tensor algebra, 520
  of tensor product, 434, 436, 529
  of terminal object, 609
  of word algebra, 565
  of $\mathbb{Z}$ (as a ring), 114

universe, 581
Uzkov, A.I., 285
V
valuation, 251, 251–261
  discrete, 254
  domain. *See* valuation ring
  induced by valuation ring, 253
  real, 239
valuation ring, 252, 253, 254, 256, 288
  discrete, 254, 255
  of field, 253
value, absolute. *See* absolute value
van der Waerden, B., 155
variety
  algebraic, 300, 309
  generated by a class, 571
  of type T, 567, 567–573, 575, 621–624
vector space, 315, 334, 334–336
  normed, 247
vertex, 583
W
Wedderburn, J., 209, 359
Wedderburn's theorem, 209, 534
Weil, A., 309
well defined, 23
Whitehead, A., 559
word, 6, 27, 38
  reduced, 27, 38, 41
Y
Yoneda's lemma, 590
Z
$\mathbb{Z}$, 1, 14, 110
Zassenhaus, H., 72, 102
Zassenhaus's lemma, 72
Zariski, O., 309
Zen Buddhism, 2
Zermelo, E., 628, 629
zero element
  of ring, 106
  of semigroup, 577
$\mathbb{Z}_n$, 21, 114, 116, 441
Zorn, M., 628
Zorn's lemma, 628, 111, 636
$\widehat{\mathbb{Z}}_p$, 245
$\mathbb{Z}_{p^\infty}$, 406, 425

Graduate Texts in Mathematics

(continued from page ii)

64 EDWARDS. Fourier Series. Vol. I. 2nd ed.
65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.
66 WATERHOUSE. Introduction to Affine Group Schemes.
67 SERRE. Local Fields.
68 WEIDMANN. Linear Operators in Hilbert Spaces.
69 LANG. Cyclotomic Fields II.
70 MASSEY. Singular Homology Theory.
71 FARKAS/KRA. Riemann Surfaces. 2nd ed.
72 STILLWELL. Classical Topology and Combinatorial Group Theory. 2nd ed.
73 HUNGERFORD. Algebra.
74 DAVENPORT. Multiplicative Number Theory. 3rd ed.
75 HOCHSCHILD. Basic Theory of Algebraic Groups and Lie Algebras.
76 IITAKA. Algebraic Geometry.
77 HECKE. Lectures on the Theory of Algebraic Numbers.
78 BURRIS/SANKAPPANAVAR. A Course in Universal Algebra.
79 WALTERS. An Introduction to Ergodic Theory.
80 ROBINSON. A Course in the Theory of Groups. 2nd ed.
81 FORSTER. Lectures on Riemann Surfaces.
82 BOTT/TU. Differential Forms in Algebraic Topology.
83 WASHINGTON. Introduction to Cyclotomic Fields. 2nd ed.
84 IRELAND/ROSEN. A Classical Introduction to Modern Number Theory. 2nd ed.
85 EDWARDS. Fourier Series. Vol. II. 2nd ed.
86 VAN LINT. Introduction to Coding Theory. 2nd ed.
87 BROWN. Cohomology of Groups.
88 PIERCE. Associative Algebras.
89 LANG. Introduction to Algebraic and Abelian Functions. 2nd ed.
90 BRØNDSTED. An Introduction to Convex Polytopes.
91 BEARDON. On the Geometry of Discrete Groups.
92 DIESTEL. Sequences and Series in Banach Spaces.
93 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part I. 2nd ed.
94 WARNER. Foundations of Differentiable Manifolds and Lie Groups.
95 SHIRYAEV. Probability. 2nd ed.
96 CONWAY. A Course in Functional Analysis. 2nd ed.
97 KOBLITZ. Introduction to Elliptic Curves and Modular Forms. 2nd ed.
98 BRÖCKER/TOM DIECK. Representations of Compact Lie Groups.
99 GROVE/BENSON. Finite Reflection Groups. 2nd ed.
100 BERG/CHRISTENSEN/RESSEL. Harmonic Analysis on Semigroups: Theory of Positive Definite and Related Functions.
101 EDWARDS. Galois Theory.
102 VARADARAJAN. Lie Groups, Lie Algebras and Their Representations.
103 LANG. Complex Analysis. 3rd ed.
104 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part II.
105 LANG. $SL_2(\mathbf{R})$.
106 SILVERMAN. The Arithmetic of Elliptic Curves.
107 OLVER. Applications of Lie Groups to Differential Equations. 2nd ed.
108 RANGE. Holomorphic Functions and Integral Representations in Several Complex Variables.
109 LEHTO. Univalent Functions and Teichmüller Spaces.
110 LANG. Algebraic Number Theory.
111 HUSEMÖLLER. Elliptic Curves. 2nd ed.
112 LANG. Elliptic Functions.
113 KARATZAS/SHREVE. Brownian Motion and Stochastic Calculus. 2nd ed.
114 KOBLITZ. A Course in Number Theory and Cryptography. 2nd ed.
115 BERGER/GOSTIAUX. Differential Geometry: Manifolds, Curves, and Surfaces.
116 KELLEY/SRINIVASAN. Measure and Integral. Vol. I.
117 J.-P. SERRE. Algebraic Groups and Class Fields.
118 PEDERSEN. Analysis Now.
119 ROTMAN. An Introduction to Algebraic Topology.
120 ZIEMER. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.

121 LANG. Cyclotomic Fields I and II. Combined 2nd ed.
122 REMMERT. Theory of Complex Functions. *Readings in Mathematics*
123 EBBINGHAUS/HERMES et al. Numbers. *Readings in Mathematics*
124 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications Part III.
125 BERENSTEIN/GAY. Complex Variables: An Introduction.
126 BOREL. Linear Algebraic Groups. 2nd ed.
127 MASSEY. A Basic Course in Algebraic Topology.
128 RAUCH. Partial Differential Equations.
129 FULTON/HARRIS. Representation Theory: A First Course. *Readings in Mathematics*
130 DODSON/POSTON. Tensor Geometry.
131 LAM. A First Course in Noncommutative Rings. 2nd ed.
132 BEARDON. Iteration of Rational Functions.
133 HARRIS. Algebraic Geometry: A First Course.
134 ROMAN. Coding and Information Theory.
135 ROMAN. Advanced Linear Algebra.2nd ed.
136 ADKINS/WEINTRAUB. Algebra: An Approach via Module Theory.
137 AXLER/BOURDON/RAMEY. Harmonic Function Theory. 2nd ed.
138 COHEN. A Course in Computational Algebraic Number Theory.
139 BREDON. Topology and Geometry.
140 AUBIN. Optima and Equilibria. An Introduction to Nonlinear Analysis.
141 BECKER/WEISPFENNING/KREDEL. Gröbner Bases. A Computational Approach to Commutative Algebra.
142 LANG. Real and Functional Analysis. 3rd ed.
143 DOOB. Measure Theory.
144 DENNIS/FARB. Noncommutative Algebra.
145 VICK. Homology Theory. An Introduction to Algebraic Topology. 2nd ed.
146 BRIDGES. Computability: A Mathematical Sketchbook.
147 ROSENBERG. Algebraic *K*-Theory and Its Applications.
148 ROTMAN. An Introduction to the Theory of Groups. 4th ed.
149 RATCLIFFE. Foundations of Hyperbolic Manifolds. 2nd ed.
150 EISENBUD. Commutative Algebra with a View Toward Algebraic Geometry.
151 SILVERMAN. Advanced Topics in the Arithmetic of Elliptic Curves.
152 ZIEGLER. Lectures on Polytopes.
153 FULTON. Algebraic Topology: A First Course.
154 BROWN/PEARCY. An Introduction to Analysis.
155 KASSEL. Quantum Groups.
156 KECHRIS. Classical Descriptive Set Theory.
157 MALLIAVIN. Integration and Probability.
158 ROMAN. Field Theory.
159 CONWAY. Functions of One Complex Variable II.
160 LANG. Differential and Riemannian Manifolds.
161 BORWEIN/ERDÉLYI. Polynomials and Polynomial Inequalities.
162 ALPERIN/BELL. Groups and Representations.
163 DIXON/MORTIMER. Permutation Groups.
164 NATHANSON. Additive Number Theory: The Classical Bases.
165 NATHANSON. Additive Number Theory: Inverse Problems and the Geometry of Sumsets.
166 SHARPE. Differential Geometry: Cartan's Generalization of Klein's Erlangen Program.
167 MORANDI. Field and Galois Theory.
168 EWALD. Combinatorial Convexity and Algebraic Geometry.
169 BHATIA. Matrix Analysis.
170 BREDON. Sheaf Theory. 2nd ed.
171 PETERSEN. Riemannian Geometry. 2nd ed.
172 REMMERT. Classical Topics in Complex Function Theory.
173 DIESTEL. Graph Theory. 2nd ed.
174 BRIDGES. Foundations of Real and Abstract Analysis.
175 LICKORISH. An Introduction to Knot Theory.
176 LEE. Riemannian Manifolds.
177 NEWMAN. Analytic Number Theory.
178 CLARKE/LEDYAEV/ STERN/WOLENSKI. Nonsmooth Analysis and Control Theory.
179 DOUGLAS. Banach Algebra Techniques in Operator Theory. 2nd ed.
180 SRIVASTAVA. A Course on Borel Sets.
181 KRESS. Numerical Analysis.

182 Walter. Ordinary Differential Equations.
183 Megginson. An Introduction to Banach Space Theory.
184 Bollobas. Modern Graph Theory.
185 Cox/Little/O'Shea. Using Algebraic Geometry. 2nd ed.
186 Ramakrishnan/Valenza. Fourier Analysis on Number Fields.
187 Harris/Morrison. Moduli of Curves.
188 Goldblatt. Lectures on the Hyperreals: An Introduction to Nonstandard Analysis.
189 Lam. Lectures on Modules and Rings.
190 Esmonde/Murty. Problems in Algebraic Number Theory. 2nd ed.
191 Lang. Fundamentals of Differential Geometry.
192 Hirsch/Lacombe. Elements of Functional Analysis.
193 Cohen. Advanced Topics in Computational Number Theory.
194 Engel/Nagel. One-Parameter Semigroups for Linear Evolution Equations.
195 Nathanson. Elementary Methods in Number Theory.
196 Osborne. Basic Homological Algebra.
197 Eisenbud/Harris. The Geometry of Schemes.
198 Robert. A Course in p-adic Analysis.
199 Hedenmalm/Korenblum/Zhu. Theory of Bergman Spaces.
200 Bao/Chern/Shen. An Introduction to Riemann–Finsler Geometry.
201 Hindry/Silverman. Diophantine Geometry: An Introduction.
202 Lee. Introduction to Topological Manifolds.
203 Sagan. The Symmetric Group: Representations, Combinatorial Algorithms, and Symmetric Functions.
204 Escofier. Galois Theory.
205 Félix/Halperin/Thomas. Rational Homotopy Theory. 2nd ed.
206 Murty. Problems in Analytic Number Theory.
Readings in Mathematics
207 Godsil/Royle. Algebraic Graph Theory.
208 Cheney. Analysis for Applied Mathematics.
209 Arveson. A Short Course on Spectral Theory.
210 Rosen. Number Theory in Function Fields.
211 Lang. Algebra. Revised 3rd ed.
212 Matoušek. Lectures on Discrete Geometry.
213 Fritzsche/Grauert. From Holomorphic Functions to Complex Manifolds.
214 Jost. Partial Differential Equations. 2nd ed.
215 Goldschmidt. Algebraic Functions and Projective Curves.
216 D. Serre. Matrices: Theory and Applications.
217 Marker. Model Theory: An Introduction.
218 Lee. Introduction to Smooth Manifolds.
219 Maclachlan/Reid. The Arithmetic of Hyperbolic 3-Manifolds.
220 Nestruev. Smooth Manifolds and Observables.
221 Grünbaum. Convex Polytopes. 2nd ed.
222 Hall. Lie Groups, Lie Algebras, and Representations: An Elementary Introduction.
223 Vretblad. Fourier Analysis and Its Applications.
224 Walschap. Metric Structures in Differential Geometry.
225 Bump. Lie Groups.
226 Zhu. Spaces of Holomorphic Functions in the Unit Ball.
227 Miller/Sturmfels. Combinatorial Commutative Algebra.
228 Diamond/Shurman. A First Course in Modular Forms.
229 Eisenbud. The Geometry of Syzygies.
230 Stroock. An Introduction to Markov Processes.
231 Björner/Brenti. Combinatorics of Coxeter Groups.
232 Everest/Ward. An Introduction to Number Theory.
233 Albiac/Kalton. Topics in Banach Space Theory.
234 Jorgenson. Analysis and Probability.
235 Sepanski. Compact Lie Groups.
236 Garnett. Bounded Analytic Functions.
237 Martínez-Avendaño/Rosenthal. An Introduction to Operators on the Hardy-Hilbert Space.
238 Aigner, A Course in Enumeration.
239 Cohen, Number Theory, Vol. I.
240 Cohen, Number Theory, Vol. II.
241 Silverman, Arithmetic of Dynamical Systems.
242 Grillet, Abstract Algebra, 2nd ed.