

Table of Contents.

1. Introduction.	1
1. Overview.	1
2. General notation.	2
3. Functions and relations.	3
4. The number systems.	4
5. Set theory.	5
2. Universal algebra.	8
3. Orders.	15
4. Groups.	21
1. Basic definitions.	21
2. Normal Subgroups.	23
3. An example of a group.	23
4. Homomorphism theorems.	24
5. Product of groups.	25
5. Permutation groups.	27
6. Rings.	31
1. Basic definitions.	31
2. Ideals.	31
3. Commutative rings.	32
4. Fractions.	35
5. Ordered commutative rings.	37
6. Chinese remainder theorem.	37
7. Möbius inversion.	38
7. Polynomials.	42
1. Single variable polynomials.	42
2. Interpolation.	45
3. Multi-variable polynomials.	47
8. Modules.	52
1. Basic definitions.	52
2. Multilinear maps.	54
3. Algebras.	55
4. Generation of modules.	55
5. Noetherian modules.	56
6. Module of fractions.	56
7. Linear algebra of modules.	57
8. Modules over principal ideal domains.	58
9. Fields.	62
1. Basic definitions.	62
2. Algebraic extensions.	62
3. Splitting fields.	63
4. Galois extensions.	63
5. Galois theory.	64
6. Finite fields.	65
10. Linear algebra.	68

1. Basic definitions.	68
2. Dual space.	70
3. Representations.	71
4. Rational canonical form.	71
5. Jordan canonical form.	72
6. Invariants.	74
7. Bilinear forms.	74
8. Orthogonal sums.	76
9. Witt's theorem.	78
10. Forms and operators.	79
11. Projection operators.	81
12. Factorizations.	82
13. Compound matrices.	85
11. Model theory.	88
1. Syntax and semantics.	88
2. Validity.	91
3. Basic definitions.	95
4. Ideals and filters.	97
5. Ultraproducts.	99
12. Computability.	101
1. Introduction.	101
2. Equivalence of three models.	102
3. Basic definitions.	105
4. Undecidability.	106
5. Subrecursion.	107
6. Decidability of theories.	110
7. \mathcal{NP} completeness of satisfiability.	117
8. Hilbert's tenth problem.	118
9. Word problem for groups.	122
10. Details for goto step simulation.	123
11. Details for Turing machine step simulation.	124
12. Details for a universal Turing machine.	124
13. Proof sketch for theorem 13.	124
13. Category theory.	126
1. Basic definitions.	126
2. Natural transformations.	129
3. Universal arrows.	130
4. Adjoint functors.	132
5. Limits.	135
6. Monics and Epics.	139
7. Preservation of limits.	140
8. Galois adjunctions.	141
9. Normals and conormals.	142
10. Images and coimages.	142
11. Biproducts.	144
12. Abelian categories.	144

14. Conjugacy.	149
1. Basic definitions.	149
2. Double cosets.	149
3. Sylow subgroups.	150
4. Primitivity and regular normal subgroups.	151
5. Simple groups.	152
6. Cyclotomic polynomials.	153
7. Wedderburn's theorem.	154
15. Characters.	156
1. Characters of commutative groups.	156
2. Norm and trace.	157
3. Characters on finite fields.	159
4. Dirichlet characters.	160
5. Matrices over noncommutative rings.	161
6. Semisimple modules and rings.	162
7. Group representation.	165
16. Series.	172
1. Basic definitions.	172
2. Modular lattices.	174
3. Solvable groups.	176
4. Regular rings.	179
5. The radical of a ring.	180
6. Artinian rings.	181
17. Topological spaces.	183
1. Basic definitions.	183
2. Induced and coinduced topologies.	184
3. The coherent topology.	186
4. Properties of topological spaces.	187
5. Connectedness.	191
6. Tychanoff's theorem.	193
7. Metric spaces.	193
8. Completion.	196
9. Manifolds.	198
18. Tensor algebra.	202
1. Adjunction with a parameter.	202
2. Cartesian closure.	203
3. The tensor product.	203
4. Non-commutative rings.	205
5. Graded modules.	206
6. The tensor algebra.	208
7. Tensor product of algebras.	211
19. Homology.	213
1. Limits in functor categories.	213
2. Diagram lemmas.	214
3. Chain complexes.	218
4. Abstract simplicial complexes.	221

5. Projectives and injectives.	222
6. Derived functors.	225
7. Ext.	229
8. Flat modules and Tor.	232
9. Cohomology of groups.	234
20. Further topics in rings and fields.	238
1. Algebraic closure.	238
2. Transcendence bases.	238
3. Local rings.	239
4. Absolute values.	240
5. Valuations.	242
6. Integral extensions.	243
7. Ring homomorphisms and ideals.	245
8. The radical of an ideal.	247
9. Primary decomposition.	248
10. The Nullstellensatz.	249
11. Dedekind domains.	250
12. Complete fields.	252
13. Real algebras.	254
14. Lagrange's four square theorem.	257
21. Lattice orders.	261
1. Varieties of lattices.	261
2. Complete lattices.	265
3. Algebraic lattices.	267
4. Stone Duality.	269
5. Continuous lattices.	274
6. Exponential correspondence.	278
22. Convexity.	282
1. Basic facts.	282
2. Polyhedra and linear inequalities.	285
3. Linear programming.	287
4. Polytopes.	290
5. Krein-Rutman theorem in Euclidean space.	291
23. Point lattices.	294
1. Basic facts.	294
2. Lebesgue measure.	295
3. Minkowski's theorem.	298
4. Hermite and Smith normal form.	299
5. Reduced bases.	301
6. Root systems.	303
7. The wallpaper groups.	309
8. Continued Fractions.	313
24. Algebra and Topology.	318
1. Topological structures.	318
2. Topological groups.	320
3. Topological vector spaces.	321

4. Additional facts about metric spaces.	323
5. Normed linear spaces.	324
6. Complete normed linear spaces.	328
7. Inner product spaces.	331
8. Hilbert spaces.	332
9. Bundles.	333
10. Sheaves.	337
11. General manifolds.	339
12. Tensors on manifolds.	340
13. Homotopy.	341
14. Homology of simplicial complexes.	344
25. Algebraic geometry.	354
1. Introduction.	354
2. Noetherian topological spaces.	354
3. Affine algebraic sets.	356
4. Noether normalization.	359
5. Dimension.	359
6. Projective algebraic sets.	362
7. Hilbert functions.	365
8. Bezout's theorem.	368
9. Prime spectrum of a ring.	369
10. Schemes.	370
11. Groebner bases.	372
26. Algebraic number theory.	377
1. Basic facts.	377
2. Discriminant.	378
3. Extensions of real valuations.	379
4. Valuations on Dedekind Domains.	381
5. Decomposition and inertia groups.	383
6. Ideal norm.	384
7. Ideal class group.	385
8. Gauss' lemma.	386
27. Lie groups.	388
1. Definition.	388
2. Differentiation on manifolds.	389
3. Zariski closed subgroups of $GL(n)$	390
4. Lie algebras.	391
5. Lie algebra of a Lie group.	393
6. Covering projections.	395
28. Some algorithms.	399
1. Gaussian elimination.	399
2. Coset enumeration.	399
3. The Schreier-Sims algorithm.	401
4. Decision procedure for Presburger arithmetic.	402
5. Basic algorithms for polynomials.	404
6. Completeness of real closed fields.	408

7. Factoring polynomials over \mathcal{F}_p .	411
8. Factoring integer polynomials.	412
Appendix 1. Set theory.	416
Appendix 2. Basic linear algebra.	419
Appendix 3. Basic graph theory.	429
Bibliography	432
Index.	436

1. Introduction.

1. Overview. Abstract algebra is a subject whose scope and applicability continue to increase. Physical theories and engineering methods have come to make use of concepts from algebra to simplify their developments, and in some cases make essential use of them. Algebra has become indispensable throughout mathematics, and an increasingly rich subject in its own right. In the last twenty years, algebra has become increasingly relevant to computer science.

This text is intended as an introduction to abstract algebra for advanced undergraduates. Much of it is accessible to advanced third year students, and the first nine chapters can be covered even earlier. There are many introductions to abstract algebra, so a new one should have some distinguishing characteristics. The main distinguishing characteristics of this text are the coverage of universal algebra and category theory, and their use in the introductory presentation of topics in algebra; and the coverage of various topics outside the main line of classical abstract algebra, which are of interest. These include topological spaces, model theory, computability theory, point lattices, and some algorithms.

The prerequisites of the text are high school mathematics, and a willingness to read. Familiarity with the usual “fundamentals”, namely sets, relations, functions, the axiomatic method, and fundamental properties of the integers and rational, real, and complex numbers is assumed. Occasionally a theorem from elementary calculus will be needed, including basic properties of infinite sequences and series. Various background facts will be summarized below, following a description of the contents.

Chapter 2 presents the basic definitions and theorems of universal algebra. This “quantifies” the observation that the basic theories of the basic structures considered in abstract algebra involve various analogous facts. Indeed, basic facts about a particular type of structure can be proved as corollaries of facts proved in chapter 2. This serves to better organize the material, and make its presentation shorter. Further, the student is introduced as soon as possible to unifying themes that have been discovered among the branches of mathematics.

Chapter 3 is also a preliminary chapter, covering the basic theory of orders. In addition to its use throughout mathematics, the study of orders is a branch in its own right. Basic facts about algebraic structures can be better understood in terms of concepts from order theory.

Chapters 4 to 9 cover the classic introductory topics of abstract algebra, namely groups, permutation groups, rings, polynomials, modules, and fields. Results from chapters 2 and 3 are used to put various facts in a general perspective.

Chapter 10 begins the “second half” of the text, which attempts to build on the first 9 chapters to cover further topics in abstract algebra in an advanced undergraduate course. It presents a comprehensive introduction to linear algebra.

Chapter 11 covers model theory. This has various uses in algebra, indeed a “type of algebraic structure” is usually the models of some set of axioms. The material covered is sufficient to consider many of these uses. For similar reasons, chapter 12 covers basic computability theory; this allows giving formal discussions not only of decidability, but also of various algorithms which have been devised in the last twenty-five years by algebraists and computer scientists. Hilbert’s tenth problem is also covered.

Chapter 13 gives a thorough treatment of basic category theory, which has been the medium of much unification in mathematical thought since its introduction in the 1940’s. Students of algebra should master basic category theory as early as possible, and chapter 13 is intended to facilitate this. Later chapters assume that the student has mastered it. Material covered includes the basic facts concerning Abelian categories.

Chapters 14 to 16 return to traditional topics in abstract algebra, covering a variety of topics including solvability and representation of groups, and general topics such as decomposition in modular lattices.

Chapter 17 covers topological spaces. Topology and algebra are intertwined throughout mathematics,

and a self-contained introduction to topology is useful in an algebra text. Using category theory, a robust introduction can be kept brief.

Chapters 18 and 19 cover tensor algebra and homology, adding to the student's mastery of category theoretic machinery. Chapter 20 covers further topics in rings and fields. Some basic topics from "commutative algebra" are covered, for example the Nullstellensatz. Chapters 21 to 23 cover topics which are not usually included in introductions to algebra, and consequently not introduced as early as their utility warrants, namely lattice orders, convexity, and point lattices.

Chapters 24 to 26 provide brief introductions to topics in advanced branches of mathematics (algebra and topology, algebraic geometry, algebraic number theory), giving examples of how basic algebra is used. Chapter 27 gives an introduction to Lie group theory, which has applications throughout the sciences. Finally, Chapter 28 contains some algorithms for solving computational problems in algebra.

Appendix 1 covers some topics from basic set theory needed for some proofs. Appendix 2 covers the basic linear algebra of finite dimensional vector spaces over a field, including determinants; this is assumed in chapter 10, and sometimes in earlier sections. Appendix 3 covers basic facts about graphs, which are occasionally useful in algebra.

This book was typeset using the "tetex" release of TeX, which includes various files such as eplain, psfig, and AMS fonts. There are various online books which cover material as in chapters 19, 20, 24, and 26, and other chapters, [Ash] and [Milne] for example.

2. General notation. The abbreviations "iff" for "if and only if", and "w.l.g." for "without loss of generality" are used in the text. The propositional connectives $\neg, \wedge, \vee, \Rightarrow$ (not, and, or, implies) are used; and the quantifiers \forall, \exists (for all, there exists). These are discussed in chapter 11. The notation used for sets is as follows.

- $x \in S$ denotes that x is an element of the set S .
- $x \notin S$ denotes that x is not an element of S .
- $\{x : \dots x \dots\}$ denotes the set of x such that $\dots x \dots$ is true; this has some common variations, such as $\{x \in S : \dots x \dots\}$ to denote $\{x : x \in S \wedge \dots x \dots\}$, or $\{f(x) : \dots x \dots\}$ to denote $\{x : \exists y(y = f(x) \wedge \dots x \dots)\}$.
- $S = T$ denotes that the sets S and T are equal, that is, contain the same elements.
- \emptyset denotes the empty set, the set containing no elements. A set is called empty or nonempty according to whether it equals \emptyset .
- $S \subseteq T$, or $T \supseteq S$, denotes that $x \in S \Rightarrow x \in T$; we say S is a subset of T , or T is a superset of S .
- $S \subset T$, or $T \supset S$, denotes that $S \subseteq T$ but $S \neq T$; we say S is a proper subset of T .
- $S \cup T$ denotes $\{x : x \in S \vee x \in T\}$, the union of S and T . More generally if C is a collection of sets, $\bigcup C$ denotes $\{x : \exists S \in C : x \in S\}$; note that $\bigcup \emptyset = \emptyset$.
- $S \cap T$ denotes $\{x : x \in S \wedge x \in T\}$, the intersection of S and T . More generally if C is a nonempty collection of sets, $\bigcap C$ denotes $\{x : \forall S \in C : x \in S\}$. If there is a "universe" U such that for all sets under consideration $S \subseteq U$, then $\bigcap \emptyset$ can be taken as U .
- If there is a universe U such that for all sets under consideration $S \subseteq U$, then the complement S^c of S equals $\{x \in U : x \notin S\}$.
- Sets S and T are called disjoint if $S \cap T = \emptyset$.

A collection of sets may be denoted $\{S_\alpha\}$ where α ranges over an "index set"; this is sometimes more convenient than using $\{S\}$ to denote it. As an example of its use, given $\{S_\alpha\}$ the disjoint union is defined to be the set of pairs $\langle \alpha, x \rangle$ such that $x \in S_\alpha$. Thus, each element in the union is "tagged" by the set from which it came (by the index of the set, although the set itself could equally well be used).

An ordered n -tuple $\langle x_1, \dots, x_n \rangle$ is a list of n elements, in order, with repetitions allowed; x_i is called

the i th component. Two ordered n -tuples are equal exactly if their i th components are equal for all i . Given sets S_1, \dots, S_n , the set $\{\langle x_1, \dots, x_n \rangle : x_i \in S_i, 1 \leq i \leq n\}$ is called the Cartesian product of S_1, \dots, S_n , and denoted $S_1 \times \dots \times S_n$. If the S_i are all the same set S we write S^n for the Cartesian product.

3. Functions and relations. An n -ary relation or predicate on a set S is a subset of S^n . If R is an n -ary relation we write $R(x_1, \dots, x_n)$ as a synonym for $\langle x_1, \dots, x_n \rangle \in R$. An n -ary function from S to T is a subset $f \subseteq S^n \times T$ such that for each $\langle x_1, \dots, x_n \rangle \in S^n$ there is a unique y such that $\langle x_1, \dots, x_n, y \rangle \in f$; we write $f(x_1, \dots, x_n) = y$ for this y , which is called the value of f at x_1, \dots, x_n .

Although set-theoretically an n -ary function is always a set of $n + 1$ -tuples, to emphasize the fact the set of pairs is sometimes called the “graph” of the function.

Infix notation may be used for binary relations and functions, that is, we may write xfy or xRy rather than $f(x, y)$ or $R(x, y)$. Parentheses may be used to indicate the order of evaluation of complex expressions involving infix function symbols. We mention one other point regarding symbols. The same symbol is often used for several different operations (in computer science terminology, the symbol is “overloaded”). This causes no confusion, because the operation in question is determined by what domains the arguments are from (their “types”). For example, 0 is used for the additive identity of a vector space, or of the field.

The notation $f : S \mapsto T$ denotes that f is a function from S to T ; S is called the domain of f , and T the codomain. Note that an n -ary function from S to T is essentially the same as a function from S^n to T . For $S' \subseteq S$ $f[S']$ denotes $\{y \in T : f(x) = y \text{ for some } x \in S'\}$; $f[S']$ is called the image of S' , and the image of S is called simply the image, or the range. The notation $f^{-1}[T']$ for $T' \subseteq T$ is used to denote $\{x \in S : f(x) \in T'\}$, which is called the inverse image of T' . We assume familiarity with the properties of these operations, which are given in exercise 1.

The arrow notation may be used to avoid giving a name to a function. We may write $x \mapsto E$ where E is some expression involving x , to denote the function f where $f(x) = E$ for all x .

Another notation for application of functions, the “exponential” notation, is occasionally used in the text. If $\sigma : S \mapsto T$ and $x \in S$, x^σ may be used to denote $\sigma(x)$; and for $R \subseteq S$ R^σ denotes $\sigma[R]$.

Functions or relations are said to be equal if they are equal as sets. If $f : S \mapsto T$ and $g : T \mapsto U$ their composition $g \circ f : S \mapsto U$ is the function such that $g \circ f(x) = g(f(x))$ for all $x \in S$. The requirement that the codomain of f be given and equal the domain of g can be relaxed; $f[S] \subseteq T$ suffices to define the composition. In algebra the codomain of a function is often given; further remarks on this point are made in chapter 13. Composition of functions is associative; that is, if $h : S_1 \mapsto S_2$, $g : S_2 \mapsto S_3$, and $f : S_3 \mapsto S_4$, then $f \circ (g \circ h) = (f \circ g) \circ h$. The identity function $\iota_S : S \mapsto S$ on S is defined by $\iota_S(x) = x$ for all $x \in S$. Clearly $f \circ \iota_S = \iota_T \circ f = f$.

The function $f : S \mapsto T$ is called injective if $f(x) = f(y)$ only if $x = y$; surjective if its image is T ; and bijective if it is both injective and surjective. The composition of injections is an injection; of surjections a surjection; and of bijections a bijection. A bijection is also called a one to one correspondence.

THEOREM 1. Suppose $f : S \mapsto T$; then the following are true.

- f is injective iff $S = \emptyset$ or there is a function $f^L : T \mapsto S$ such that $f^L \circ f = \iota_S$; such an f^L is called a left inverse of f .
- f is surjective iff there is a function $f^R : T \mapsto S$ such that $f \circ f^R = \iota_T$; such an f^R is called a right inverse of f .
- f is bijective iff there is a function $f^{-1} : T \mapsto S$ such that $f^{-1} \circ f = \iota_S$ and $f \circ f^{-1} = \iota_T$. In this case there is a unique such f^{-1} ; it is a bijection, and is called the inverse of f .

PROOF: For part a, suppose $S \neq \emptyset$. If f^L exists, suppose $f(x) = f(y)$ and apply f^L to both sides; this shows f is injective. If f is injective, for each y such that $f(x) = y$ for some x let $f^L(y) = x$ and define

$f^L(y)$ arbitrarily otherwise. For part b, if f^R exists, consider $f^R(y)$ for $y \in Y$; this shows f is surjective. If f is surjective, one may choose an arbitrary x with $f(x) = y$ for $f^R(y)$. To prove part c, observe that

$$f^L = f^L \circ \iota_T = f^L \circ f \circ f^R = \iota_S \circ f^R = f^R$$

if f^L, f^R are left and right inverses; in particular the inverse is unique (the case $S = \emptyset$ follows also).

Suppose $S' \subseteq S, T' \subseteq T$. Given a function $f : S \mapsto T$, its restriction to S' is defined to be $f \cap (S' \times T)$; we denote this $f \upharpoonright S'$. If $f' : S' \mapsto T$ is given and equals $f \upharpoonright S'$ we call f an extension to S of f' . If $f[S] \subseteq T'$ we call $f \cap (S \times T')$ the corestriction of f to T' .

A partial function from S to T is a set of pairs such that for each $s \in S$ there is at most one pair whose first element is s . It is thus a function (possibly empty) $f : S' \mapsto T$ where $S' \subseteq S$; S' is the domain of f . Considered as sets of pairs, the partial functions $\phi : S \mapsto T$ are partially ordered by inclusion; $\phi_1 \subseteq \phi_2$ iff $\text{Dom}(\phi_1) \subseteq \text{Dom}(\phi_2)$, and for $x \in \text{Dom}(\phi_1)$ $\phi_2(x) = \phi_1(x)$. This order on the partial functions is called the approximation order. The union of a chain of partial functions is readily verified to be a partial function.

The characteristic function of an n -ary relation R is the n -ary function whose value is 1 if R is true, and 0 if R is false. The codomain might be, for example, a ring where $0 \neq 1$. A useful binary function on S is the delta function, $\delta_S(x, y)$, or $\delta(x, y)$ if S is clear, which equals 1 if $x = y$, else 0. This is the characteristic function of the equality relation on S . It is also customarily denoted δ_{xy} , and called the ‘‘Kronecker delta function’’.

The transpose R^t of a binary relation R is defined to be the binary relation such that $R^t(x, y)$ iff $R(y, x)$. A binary relation R on a set S is called

- reflexive if xRx ;
- symmetric if yRx whenever xRy ;
- transitive if xRz whenever xRy and yRz ;
- an equivalence relation if it is reflexive, symmetric, and transitive.

If \equiv is an equivalence relation the set $\{y : y \equiv x\}$ is called the equivalence class of x , and denoted $[x]$. A partition of a nonempty set S is a collection of nonempty subsets P_α , called the parts of the partition, such that $S = \cup_\alpha P_\alpha$ and P_α, P_β are disjoint for all $\alpha \neq \beta$.

THEOREM 2. Suppose S is nonempty. The equivalence classes of an equivalence relation on S are the parts of a partition of S . Conversely given a partition of S , the relation of belonging to the same part is an equivalence relation. These maps between equivalence relations and partitions are inverse to each other.

PROOF: Exercise.

Given an equivalence relation on a set S , or equivalently a partition of S , by a system of representatives is meant a subset $R \subseteq S$ such that R contains exactly one element from each equivalence class, or part of the partition.

4. The number systems. We use $\mathcal{N}, \mathcal{Z}, \mathcal{Q}, \mathcal{R},$ and \mathcal{C} to denote the natural numbers or nonnegative integers, integers, rational numbers, real numbers, and complex numbers respectively. We assume familiarity with the basic properties of these structures. We also use \mathcal{R}^\neq for the nonzero reals, \mathcal{R}^\geq for the nonnegative reals, and so on. The notation R^\neq may be used in any ring (rings are defined in chapter 6; both \mathcal{Z} and \mathcal{R} are rings, so the notation \mathcal{Z}^\neq is another example). The notation R^* is often used, especially for a field, but the asterisk has so many uses in algebra that this notation is less confusing. R^\geq may be used in any ordered commutative ring.

The natural numbers have the property that any nonempty set of natural numbers contains a least element. A consequence of this is the principle of mathematical induction, which states that if $S \subseteq \mathcal{N}$,

$0 \in S$, and $n+1 \in S$ whenever $n \in S$, then $S = \mathcal{N}$. One may strengthen the induction hypothesis “whenever $n \in S$ ” to “whenever $k \in S$ for $k \leq n$ ”. Another way of stating induction is, if $n \in S$ whenever $k \in S$ for $k < n$ then $S = \mathcal{N}$, since for $n = 0$ the hypothesis is vacuously true.

A function $f : \mathcal{N} \times S \mapsto S$ may be defined “recursively” from functions $g : S \mapsto S$ and $h : \mathcal{N} \times S \times S \mapsto S$ by the equations $f(0, x) = g(x)$, $f(n+1, x) = h(n, x, f(x, n))$, in the sense that there is a unique such function satisfying these equations. This is a fact of elementary set theory, and we will assume it.

A fundamental fact about \mathcal{Z} is the division law, which states that for $p, d \in \mathcal{Z}$, $d > 0$, there are unique integers q, r , the quotient and remainder respectively, such that $p = qd + r$ and $0 \leq r < d$. If $r = 0$ d is said to divide p , for which we write $d|p$. The remainder when p is divided by d will be denoted $p \bmod d$. The division law can be proved from a suitable set of axioms for \mathcal{Z} .

The factorial function is that mapping the nonnegative integer n to $n! = 1 \cdot 2 \cdots n$. In a ring we let the empty product equal 1; thus $0! = 1$. The quantities

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}$$

for nonnegative integers n, k with $0 \leq k \leq n$ are called the binomial coefficients. These are readily verified to satisfy

$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

where $0 < k < n$. From this, the binomial coefficients are readily seen to be positive integers.

A set S is called finite if there is a bijection from S to $\{1, 2, \dots, n\}$ for some n ; in this case n is unique, and is called the cardinality of S . Given finite sets S and T , $|S| \leq |T|$ iff there is an injection from S to T .

The real numbers are sometimes extended with symbols $\pm\infty$, which obey some algebraic rules as follows, where r denotes an ordinary real number.

- $-\infty < r < +\infty$.
- $r + \pm\infty = \pm\infty + r = \pm\infty$.
- if $r > 0$ then $r \cdot \pm\infty = \pm\infty \cdot r = \pm\infty$.
- if $r < 0$ then $r \cdot \pm\infty = \pm\infty \cdot r = \mp\infty$.
- $\pm\infty + \pm\infty = \pm\infty$.
- $\pm\infty \cdot \pm\infty = +\infty$.
- $\pm\infty \cdot \mp\infty = \mp\infty \cdot \pm\infty = -\infty$.

Other algebraic structures are sometimes extended in this way, such as an arbitrary field; in some cases only one of the two infinities is needed.

The function, floor “floor” function $\lfloor x \rfloor$ mapping \mathcal{R} to \mathcal{Z} maps x to the largest integer n such that $n \leq x$. The function, ceiling “ceiling” function $\lceil x \rceil$ maps x to the smallest integer n such that $n \geq x$. These functions obey various identities which follow immediately from the definitions; see [Knuth] for some of these.

5. Set theory. A set is called infinite if it is not finite. In algebra many facts about finite sets can be generalized to infinite sets. Introductory texts often omit the infinite case, to avoid appealing to the necessary set theory. However, this can be kept to a minimum, and we will frequently give the infinite generalizations, assuming the necessary facts from set theory. Some discussion of these is given here, and further discussion in appendix 1.

The notion of an infinite Cartesian product is an example. If I is a set, we can consider the notion of a sequence $\langle x_i \rangle$ of elements from some set S , indexed by (the index set) I ; x_i is called the i th component. Set theoretically this is just a function from I to S . Given a set S_i for each $i \in I$, the Cartesian product $\times_i S_i$ of the sets is the collection of sequences $\langle x_i \rangle$ where $x_i \in S_i$. Set theoretically, this is the collection of functions $f : I \mapsto \cup_i S_i$ such that $f(i) \in S_i$ for all $i \in I$. If $S_i = S$ for all i we write S^I for the Cartesian

product, or what is the same thing the set of functions from I to S . An n -tuple is the special case where I has n elements. Technically, the earlier characterization is not the same thing as a sequence on an n -element index set, but there is an obvious correspondence which can almost always be ignored.

It is intuitively clear that the Cartesian product of nonempty sets is nonempty. This may be shown using the principle of higher set theory known as the axiom of choice; in fact it is equivalent to it. The axiom of choice states that given any collection of nonempty sets there is a function (from the collection to its union) which selects one member from each set.

The collection of subsets of a set S is called the power set of S ; in this text it is denoted $\text{Pow}(S)$. Collections of subsets of S are often considered; these are just subsets of $\text{Pow}(S)$.

Let S be a collection of subsets of some set. A maximal set in S is one which is not properly contained in any other set in the collection. A chain in S is a collection C of sets from S , such that for any A and B in C , either $A \subseteq B$ or $B \subseteq A$. S is said to be inductive if for every chain C in S there is a set in S which contains every element of C (often in applications this is the union of the sets in C). The maximal principle states that an inductive collection of subsets contains a maximal element.

The maximal principle is quite useful in handling infinite sets in algebra. For example as we will see it can be used to show that every vector space has a basis, which need not be finite in the general case.

The maximal principle is another example of a principle of set theory which, given the other axioms of set theory, is equivalent to the axiom of choice. In chapter 3 a generalization, called Zorn's lemma, will be given. Many arguments in algebra involving infinite sets can be given using the maximal principle or Zorn's lemma, but occasionally a more general method, called transfinite induction, is required. A discussion of transfinite induction is given in appendix 1, together with proofs of some theorems from algebra.

The cardinality $|S|$ of an infinite set can be defined. Indeed, the proper handling of this notion was fundamental to Cantor's development of set theory. The cardinality of a set is something called a "cardinal number" in set theory. Basic algebra can often avoid having to consider these; we may define $|S| \leq |T|$ to hold if there is an injection from S to T , and $|S| = |T|$ if there is a bijection. The Bernstein-Cantor-Schröder theorem of set theory states that if $|S| \leq |T|$ and $|T| \leq |S|$ then $|S| = |T|$; a proof is given in appendix 1. If there is a surjection from S to T then $|S| \geq |T|$, because there is an injection from T to S . Note also that if $S \subseteq T$ and $|S| < |T|$ (i.e., $\neg(|S| \geq |T|)$), then $S \subset T$.

Occasionally a fact about cardinality is required which requires additional machinery to prove. For one example of such, if S is an infinite set then $|S| = |S \times S|$. Various additional facts can be proved using this. For example, if S is an infinite set and T is the set of finite subsets of S then $|T| = |S|$. Additional discussion can be found in appendix 1.

Exercises.

1. Suppose $f : S \mapsto T$; $S', S_1, S_2 \subseteq S$; and $T', T_1, T_2 \subseteq T$. Show the following.
 - a. If $S_1 \subseteq S_2$ then $f[S_1] \subseteq f[S_2]$, $f[\emptyset] = \emptyset$, $f[S_1 \cup S_2] = f[S_1] \cup f[S_2]$, and $f[S_1 \cap S_2] \subseteq f[S_1] \cap f[S_2]$.
 - b. If $T_1 \subseteq T_2$ then $f^{-1}[T_1] \subseteq f^{-1}[T_2]$, $f^{-1}[\emptyset] = \emptyset$, $f^{-1}[T] = S$, $f^{-1}[T_1 \cup T_2] = f^{-1}[T_1] \cup f^{-1}[T_2]$, and $f^{-1}[T_1 \cap T_2] = f^{-1}[T_1] \cap f^{-1}[T_2]$.
 - c. $f[S'] \subseteq T'$ iff $S' \subseteq f^{-1}[T']$.
 - d. $f[f^{-1}[T']] = f[S] \cap T'$; thus, $f[f^{-1}[T']] \subseteq T'$, and equality holds if f is surjective.
 - e. $S' \subseteq f^{-1}[f[S']]$, and equality holds if f is injective.
2. Show that two finite sets have the same cardinality iff there is a bijection between them. You may assume that there is no bijection between $\{0, \dots, m-1\}$ and $\{0, \dots, n-1\}$ for $m \neq n$.
3. Show that the divisibility relation on \mathcal{Z} has the following properties.
 - $x|y$ iff $x|(-y)$ iff $(-x)|y$ iff $(-x)|(-y)$
 - $x|x$

- if $x|y$ and $y|z$ then $x|z$
- if $x|y$ and $y|x$ then $y = \pm x$
- $x|0$
- $1|x$
- if $x|y$ and $x|z$ then $x|y + z$
- if $x|y$ and w is any integer than $x|wy$
- if $x, y > 0$ and $x|y$ then $x \leq y$