Chapter 0

Prerequisites

All topics listed in this chapter are covered in *A Primer of Abstract Mathematics* by Robert B. Ash, MAA 1998.

0.1 Elementary Number Theory

The greatest common divisor of two integers can be found by the Euclidean algorithm, which is reviewed in the exercises in Section 2.5. Among the important consequences of the algorithm are the following three results.

0.1.1

If d is the greatest common divisor of a and b, then there are integers s and t such that $sa + tb = d$. In particular, if a and b are relatively prime, there are integers s and t such that $sa + tb = 1$.

0.1.2

If a prime p divides a product $a_1 \cdots a_n$ of integers, then p divides at least one a_i

0.1.3 Unique Factorization Theorem

If a is an integer, not 0 or ± 1, then

(1) a can be written as a product $p_1 \cdots p_n$ of primes.

(2) If $a = p_1 \cdots p_n = q_1 \cdots q_m$, where the p_i and q_j are prime, then $n = m$ and, after renumbering, $p_i = \pm q_i$ for all i.

[We allow negative primes, so that, for example, -17 is prime. This is consistent with the general definition of prime element in an integral domain; see Section 2.6.]

0.1.4 The Integers Modulo m

If a and b are integers and m is a positive integer ≥ 2, we write $a \equiv b \bmod m$, and say that a is *congruent* to b modulo m, if $a - b$ is divisible by m. Congruence modulo m is an equivalence relation, and the resulting equivalence classes are called *residue classes* mod m. Residue classes can be added, subtracted and multiplied consistently by choosing a representative from each class, performing the appropriate operation, and calculating the residue class of the result. The collection $\mathbb{Z}_m$ of residue classes mod m forms a commutative ring under addition and multiplication. $\mathbb{Z}_m$ is a field if and only if m is prime. (The general definitions of ring, integral domain and field are given in Section 2.1.)

0.1.5

(1) The integer a is relatively prime to m if and only if a is a unit mod m, that is, a has a multiplicative inverse mod m.

(2) If c divides ab and a and c are relatively prime, then c divides b.

(3) If a and b are relatively prime to m, then ab is relatively prime to m.

(4) If $ax \equiv ay \bmod m$ and a is relatively prime to m, then $x \equiv y \bmod m$.

(5) If $d = \gcd(a, b)$, the greatest common divisor of a and b, then a/d and b/d are relatively prime.

(6) If $ax \equiv ay \bmod m$ and $d = \gcd(a, m)$, then $x \equiv y \bmod m/d$.

(7) If a_i divides b for $i = 1, \ldots, r$, and a_i and a_j are relatively prime whenever $i \neq j$, then the product $a_1 \cdots a_r$ divides b.

(8) The product of two integers is their greatest common divisor times their least common multiple.

0.1.6 Chinese Remainder Theorem

If $m_1, \ldots, m_r$ are relatively prime in pairs, then the system of simultaneous equations $x \equiv b_j \bmod m_j, j = 1, \ldots, r$, has a solution for arbitrary integers b_j. The set of solutions forms a single residue class mod m=$m_1 \cdots m_r$, so that there is a unique solution mod m.

This result can be derived from the abstract form of the Chinese remainder theorem; see Section 2.3.

0.1.7 Euler's Theorem

The *Euler phi function* is defined by $\varphi(n)$ = the number of integers in $\{1, \ldots, n\}$ that are relatively prime to n. For an explicit formula for $\varphi(n)$, see Section 1.1, Problem 13. Euler's theorem states that if $n \geq 2$ and a is relatively prime to n, then $a^{\varphi(n)} \equiv 1 \bmod n$.

0.1.8 Fermat's Little Theorem

If a is any integer and p is a prime not dividing a, then $a^{p-1} \equiv 1 \bmod p$. Thus for any integer a and prime p, whether or not p divides a, we have $a^p \equiv a \bmod p$.

For proofs of (0.1.7) and (0.1.8), see (1.3.4).

0.2 Set Theory

0.2.1

A *partial ordering* on a set S is a relation on S that is reflexive ($x \leq x$ for all $x \in S$), antisymmetric ($x \leq y$ and $y \leq x$ implies $x = y$), and transitive ($x \leq y$ and $y \leq z$ implies $x \leq z$). If for all $x, y \in S$, either $x \leq y$ or $y \leq x$, the ordering is *total*.

0.2.2

A *well-ordering* on S is a partial ordering such that every nonempty subset A of S has a smallest element a. (Thus $a \leq b$ for every $b \in A$).

0.2.3 Well-Ordering Principle

Every set can be well-ordered.

0.2.4 Maximum Principle

If T is any chain (totally ordered subset) of a partially ordered set S, then T is contained in a maximal chain M. (Maximal means that M is not properly contained in a larger chain.)

0.2.5 Zorn's Lemma

If S is a nonempty partially ordered set such that every chain of S has an upper bound in S, then S has a maximal element.

(The element x is an upper bound of the set A if $a \leq x$ for every $a \in A$. Note that x need not belong to A, but in the statement of Zorn's lemma, we require that if A is a chain of S, then A has an upper bound that actually belongs to S.)

0.2.6 Axiom of Choice

Given any family of nonempty sets S_i, $i \in I$, we can choose an element of each S_i. Formally, there is a function f whose domain is I such that $f(i) \in S_i$ for all $i \in I$.

The well-ordering principle, the maximum principle, Zorn's lemma, and the axiom of choice are equivalent in the sense that if any one of these statements is added to the basic axioms of set theory, all the others can be proved. The statements themselves cannot be proved from the basic axioms. Constructivist mathematics rejects the axiom of choice and its equivalents. In this philosophy, an assertion that we can choose an element from each S_i must be accompanied by an explicit algorithm. The idea is appealing, but its acceptance results in large areas of interesting and useful mathematics being tossed onto the scrap heap. So at present, the mathematical mainstream embraces the axiom of choice, Zorn's lemma et al.

0.2.7 Proof by Transfinite Induction

To prove that statement P_i holds for all i in the well-ordered set I, we do the following:

1. Prove the basis step P_0, where 0 is the smallest element of I.

2. If $i > 0$ and we assume that P_j holds for all $j < i$ (the transfinite induction hypothesis), prove P_i.

It follows that P_i is true for all i.

0.2.8

We say that the size of the set A is less than or equal to the size of B (notation $A \leq_s B$) if there is an injective map from A to B. We say that A and B have the same size ($A =_s B$) if there is a bijection between A and B.

0.2.9 Schröder-Bernstein Theorem

If $A \leq_s B$ and $B \leq_s A$, then $A =_s B$. (This can be proved without the axiom of choice.)

0.2.10

Using (0.2.9), one can show that if sets of the same size are called equivalent, then $\leq_s$ on equivalence classes is a partial ordering. It follows with the aid of Zorn's lemma that the ordering is total. The equivalence class of a set A, written $|A|$, is called the *cardinal number* or *cardinality* of A. In practice, we usually identify $|A|$ with any convenient member of the equivalence class, such as A itself.

0.2.11

For any set A, we can always produce a set of greater cardinality, namely the *power set* 2^A, that is, the collection of all subsets of A.

0.2.12

Define addition and multiplication of cardinal numbers by $|A|+|B| = |A \cup B|$ and $|A||B| = |A \times B|$. In defining addition, we assume that A and B are disjoint. (They can always be disjointized by replacing $a \in A$ by $(a, 0)$ and $b \in B$ by $(b, 1)$.)

0.2.13

If $\aleph_0$ is the cardinal number of a countably infinite set, then $\aleph_0 + \aleph_0 = \aleph_0\aleph_0 = \aleph_0$. More generally,

(a) If α and β are cardinals, with $\alpha \leq \beta$ and β infinite, then $\alpha + \beta = \beta$.

(b) If $\alpha \neq 0$ (i.e., α is nonempty), $\alpha \leq \beta$ and β is infinite, then $\alpha\beta = \beta$.

0.2.14

If A is an infinite set, then A and the set of all finite subsets of A have the same cardinality.

0.3 Linear Algebra

It is not feasible to list all results presented in an undergraduate course in linear algebra. Instead, here is a list of topics that are covered in a typical course.

1. Sums, products, transposes, inverses of matrices; symmetric matrices.
2. Elementary row and column operations; reduction to echelon form.
3. Determinants: evaluation by Laplace expansion and Cramer's rule.
4. Vector spaces over a field; subspaces, linear independence and bases.
5. Rank of a matrix; homogeneous and nonhomogeneous linear equations.
6. Null space and range of a matrix; the dimension theorem.
7. Linear transformations and their representation by matrices.
8. Coordinates and matrices under change of basis.
9. Inner product spaces and the projection theorem.
10. Eigenvalues and eigenvectors; diagonalization of matrices with distinct eigenvalues, symmetric and Hermitian matrices.
11. Quadratic forms.

A more advanced course might cover the following topics:

12. Generalized eigenvectors and the Jordan canonical form.
13. The minimal and characteristic polynomials of a matrix; Cayley-Hamilton theorem.
14. The adjoint of a linear operator.
15. Projection operators.
16. Normal operators and the spectral theorem.