# 抽象代数

作者：Dummit D. S. and Foote R.M.

版本：1.00

Wir müssen wissen, wir werden wissen. (我们必须知道，我们必将知道) - David.Hilbert

# 目录

# Preface

This book evolved out of notes by the authors from courses given at various universities over a period of about thirteen years. The backgrounds of students in these courses were

# Preliminaries

Some results and notation that are used throughout the text are collected in this chapter for convenience. Students may wish to review this chapter quickly at first and then read each section more carefully again as the concepts appear in the course of the text.

## 0.1 Basics

The basics of set theory: sets, $\cap$, $\cup$, $\in$, etc. should be familiar to the reader. Our notation for subsets of a given set $A$ will be

$$B = \{a \in A | \cdots (\text{conditions on a}) \cdots \}.$$

The order or cardinality of a set $A$ will be denoted by $|A|$. If $A$ is a finite set the order of $A$ is simply the number of elements of $A$.

It is important to understand how to test whether a particular $x \in A$ lies in a subset $B$ of $A$ (cf. Exercises 1 to 4). The Cartesian product of two sets $A$ and $B$ is the collection $A \times B = \{(a, b) | a \in A, b \in B\}$, of ordered pairs of elements from $A$ and $B$.

We shall use the following notation for some common sets of numbers:

(1) $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3 \cdots\}$ denotes the integers (the $\mathbb{Z}$ is for the German word for numbers: "Zahlen").

(2) $\mathbb{Q} = \{a/b | a, b \in \mathbb{Z}, b \neq 0\}$ denotes the rational numbers (or rationals).

(3) $\mathbb{R} = \{\text{all decimal expansions } \pm d_1 d_2 \cdots d_n . a_1 a_2 a_3 \cdots\}$ denotes the real numbers (or reals).

(4) $\mathbb{C} = \{a + bi | a, b \in \mathbb{R}, i^2 = -1\}$ denotes the complex numbers.

(5) $\mathbb{Z}^+$, $\mathbb{Q}^+$ and $\mathbb{R}^+$ will denote the positive (nonzero) elements in $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, respectively.

We shall use the notation $f : A \to B$ or $A \xrightarrow{f} B$ to denote a function $f$ from $a$ to $B$ and the value of $f$ at $a$ is denoted $f(a)$ (i.e. we shall apply our functions on the left). We use the words function and map interchangeably. The set $A$ is called the domain of $f$ and $B$ is called the codomain of $f$. The notation $f : a \mapsto b$ or $a \mapsto b$ if $f$ is understood indicates that $f(a) = b$, i.e. the function is being specified on elements.

If the function $f$ is not specified on elements it is important in general to check that $f$ is well defined, i.e. is unambiguously determined. For example, if the set $A$ is the union of two subsets $A_1$ and $A_2$ then one can try to specify a function from $A$ to the set $\{0, 1\}$ by declaring that $f$ is to map everything in $A_1$ to 0 and is to map everything in $A_2$ to 1. This unabiguously defines $f$ unless $A_1$ and $A_2$ have elements in common (in which case it is not clear whether these elements should map to 0 or to 1). Checking that this $f$ is well defined therefore amounts to checking that $A_1$ and $A_2$ have no intersection.

The set

$$f(A) = \{b \in B | b = f(a), \text{for some } a \in A\}$$

is a subset of $B$, called the range or image of $f$ (or the image of $A$ under $f$). For each subset $C$ of $B$ the set

$$f^{-1}(C) = \{a \in A | f(a) \in C\}$$

consisting of the elements of $A$ mapping into $C$ under $f$ is called the preimage or inverse image of $C$ under $f$. For each $b \in B$, the preimage of $\{b\}$ under $f$ is called the fiber of $f$ over $b$. Note that $f^{-1}$ is not in general a function and that the fibers of $f$ generally contain many elements since there may be many elements of $A$ mapping to the element $b$.

If $f : A \to B$ and $g : B \to C$, then the composite map $g \circ f : A \to C$ is defined by

$$(g \circ f)(a) = g(f(a)).$$

Let $f : A \to B$.

(1) $f$ is injective or is an injection if whenever $a_1 \neq a_2$, then $f(a_1) \neq f(a_2)$.

(2) $f$ is surjective or is a surjection if for all $b \in B$ there is some $a \in A$ such that $f(a) = b$, i.e. the image of $f$ is all of $B$. Note that since a function always maps onto its range (by definition) it is necessary to specify the codomain $B$ in order for the question of surjectivity to be meaningful.

(3) $f$ is bijective or is a bijection if it is both injective and surjective, If such a bijection $f$ exists from $A$ to $B$, we say $A$ and $B$ are in bijective correspondence.

(4) $f$ has a left inverse if there is a function $g : B \to A$ such that $g \circ f : A \to A$ is the identity map on $A$, i.e. $(g \circ f)(a) = a$, for all $a \in A$.

(5) $f$ has a right inverse if there is a function $h : B \to A$ such that $f \circ h : B \to B$ is the identity map on $B$.

**命题 0.1**

Let $f : A \to B$.

(1) The map $f$ is injective if and only if $f$ has a left inverse.

(2) The map $f$ is surjective if and only if $f$ has a right inverse.

(3) The map $f$ is bijective if and only if there exists $g : B \to A$ such that $f \circ g$ is the identity map on $B$ and $g \circ f$ is the identity map on $A$.

(4) If $A$ and $B$ are finite sets with the same number of elements (i.e. $|A| = |B|$). then $f : A \to B$ is bijective if and only if $f$ is injective if and only if $f$ is surjective.

证明 Exercise.

In the situation fo part (3) of the proposition above the map $g$ is necessarily unique and we shall say $g$ is the 2-sided iverse (or simply the inverse) of $f$.

A permutation of a set $A$ is simply a bijection from $A$ to itself.

If $A \subset B$ and $f : B \to C$, we denote the restriction of $f$ to $A$ by $f|_A$. When the domain we

are considering is understood we shall occasionally denote $f|_A$ again simply as $f$ even though these are formally different functions (their domains are different).

If $A \subset B$ and $g : A \to C$ and there is a function $f : B \to C$ such that $f|_A = g$, we shall say $f$ is an extension of $g$ to $B$ (such a map $f$ need not exist nor be unique).

Let $A$ be a nonempty set.

(1) A binary relation on a set $A$ is a subset $R$ of $A \times A$ and we write $a \sim b$ if $(a, b) \in R$.

(2) The relation $\sim$ on $A$ is said to be:

  (a) reflexive if $a \sim a$, for all $a \in A$,

  (b) symmetric if $a \sim b$ implies $b \sim a$ for all $a, b \in A$,

  (c) transitive if $a \sim b$ and $b \sim c$ implies $a \sim c$ for all $a, b, c \in A$.

  A relation is an equivalence relation if it is reflexive, symmetric and transitive.

(3) If $\sim$ defined an equivalence relation on $A$, then the equivalence class of $a \in A$ is defined to be $\{x \in A | x \sim a\}$. Elements of the equivalence class of $a$ are said to be equivalent to $a$. If $C$ is an equivalence class, any element of $C$ is called a representative of the class $C$.

(4) A partition of $A$ is any collection $\{A_i | i \in I\}$ of nonempty subsets of $A$ ($I$ some indexing set) such that

  (a) $A = \cup_{i \in I} A_i$, and

  (b) $A_i \cap A_j = \emptyset$, for all $i, j \in I$ with $i \neq j$.

  i.e. $A$ is the disjoint union of the sets in the partition.

The notions of an equivalence relation on $A$ and a partition of $A$ are the same:

**命题 0.2**

Let $A$ be an nonempty set.

(1) If $\sim$ defines an equivalece relation on $A$ then the set of equivalence classes of $\sim$ form a partition of $A$.

(2) If $\{A_i | i \in I\}$ is a partition of $A$ then there is an eqivalence relation on $A$ whose equivalence classes are precisely the sets $A_i$, $i \in I$.

♠

证明 Omitted.

Finally, we shall assume the reader is familiar with proofs by induction.

In Exercises 1 to 4 let $\mathcal{A}$ be the set of $2 \times 2$ matrices with real numbers entries. Recall that matrix multiplication is defined by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}$$

Let

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and let

$$\mathcal{B} = \{X \in \mathcal{A} | MX = XM\}.$$

### 第零章习题

1. Determine which of the following elements of $\mathcal{A}$ lie in $\mathcal{B}$:
$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$
2. Prove that if $P, Q \in \mathcal{B}$, then $P+Q \in \mathcal{B}$ (where $+$ denotes the usual sum of two matrices).
3. Prove that if $P, Q \in \mathcal{B}$, then $P \cdot Q \in \mathcal{B}$ (where $\cdot$ denotes the usual product of two matrices).
4. Find conditions on $p, q, r, s$ which determine precisely when $\begin{pmatrix}p & q\\ r & s\end{pmatrix} \in \mathcal{B}$.
5. Determine whether the following functions $f$ are well defined:
   (a) $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(a/b) = a$.
   (b) $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$.
6. Determine whether the function $f : \mathbb{R}^+ \to \mathbb{Z}$ defined by mapping a real number $r$ to the first digit to the right of the decimal point in a decimal expansion of $r$ is well defined.
7. Let $f : A \to B$ be a surjective map of sets. Prove that the relation
$$a \sim b \text{ if and only if } f(a) = f(b)$$
is an equivalence relation whose equivalence classes are the fibers of $f$.

## 0.2 Properties of the integers

The following properties of the integers $\mathbb{Z}$ (many familiar from elementary arithmetic) will be proved in a more general context in the ring theory of Chapter 3, but it will be necessary to use them in Part I (of course, none of the ring theory proofs of these properties will rely on the group theory).

(1) (Well Ordering of $\mathbb{Z}$) If $A$ is any nonempty subset of $\mathbb{Z}^+$, there is some element $m \in A$ such that $m \leq a$, for all $a \in A$ ($m$ is called a minimal element of $A$).

(2) If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say $a$ divides $b$ if there is an element $c \in \mathbb{Z}$ such that $b = ac$. In this case we write $a \mid b$; if $a$ does not divide $b$ we write $a \nmid b$.

(3) If $a, b \in \mathbb{Z} - \{0\}$, there is a unique positive integer $d$, called the greatest common divisor of $a$ and $b$ (or g.c.d. of $a$ and $b$), satisfying:
   (a) $d \mid a$ and $d \mid b$ (so $d$ is a common divisor of $a$ and $b$), and
   (b) if $e \mid a$ and $e \mid b$, then $e \mid d$ (so $d$ is the greatest such divisor).
   The g.c.d. of $a$ and $b$ will be denoted by $(a, b)$. If $(a, b) = 1$, we say that $a$ and $b$ are relatively prime.

(4) If $a, b \in \mathbb{Z} - \{0\}$, there is q unique positive integer $l$, called least common multiple of $a$ and $b$ (or l.e.m. of $a$ and $b$), satisfying:
   (a) $a \mid l$ and $b \mid l$ (so $l$ is a common multiple of $a$ and $b$), and
   (b) if $a \mid m$ and $b \mid m$, then $l \mid m$ (so $l$ is the least such multiple).

The connection between the greatest common divisor $d$ and the least common multiple $l$ of two integers $a$ and $b$ is given by $dl = ab$.

(5) The Division Algorithm: if $a, b \in \mathbb{Z} - \{0\}$, then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \quad \text{and} \quad 0 \leq r < |b|,$$

where $q$ is the quotient and $r$ the remainder, This is the usual "long division" familiar from elementary arithmetic.

(6) The Euclidean Algorithm is an important procedure which produces a greatest common divisor of two integers $a$ and $b$ by iterating the Division Algorithm: if $a, b \in \mathbb{Z} - \{0\}$, then we obtain a sequence of quotients and remainders

$$a = q_0 b + r_0 \tag{0}$$

$$b = q_1 r_0 + r_1 \tag{1}$$

$$r_0 = q_2 r_1 + r_2 \tag{2}$$

$$r_1 = q_3 r_2 + r_3 \tag{3}$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \tag{n}$$

$$r_{n-1} = q_{n+1} r_n \tag{n+1}$$

where $r_n$ is the last nonzero remainder. Such an $r_n$ exists since $|b| > |r_0| > |r_1| > \cdots > |r_n|$ is a decreasing sequence of strictly positive integers if the remainders are nonzero and such a sequence cannot continue indefinitely. Then $r_n$ is the g.c.d. (a, b) of $a$ and $b$.

**例 0.1** Suppose $a = 57970$ and $b = 10353$. Then applying the Euclidean Algorithm we obtain:

$$57970 = (5)10353 + 6205$$

$$10353 = (1)6205 + 4148$$

$$6205 = (1)4148 + 2057$$

$$4148 = (2)2057 + 34$$

$$2057 = (60)34 + 17$$

$$34 = (2)17$$

which shows that $(57970, 10353) = 17$.

(7) One consequence of the Euclidean Algorithm which we shall use regularly is the following: if $a, b, \in \mathbb{Z} - \{0\}$, then there exist $x, y \in \mathbb{Z}$ such that

$$(a, b) = ax + by$$

that is, the g.c.d. of $a$ and $b$ is a $\mathbb{Z}$-linear combination of $a$ and $b$. This follows by recursively writing the element $r_n$ in the Euclidean Algorithm in terms of the previous remainders (namely, use equation (n) above to solve for $r_n = r_{n-2} - q_n r_{n-1}$ in terms of the remainders $r_{n-1}$ and $r_{n-2}$, then use equation (n-1) to write $r_n$ in terms of the remainders $r_{n-2}$ and

$r_{n-3}$, etc. eventually writing $r_n$ in terms of $a$ and $b$).

**例 0.2** Suppose $a = 57970$ and $b = 10353$, whose greatest common divisor we computed above to be 17. From the fifth equation (the next to last equation) in the Euclidean Algorithm applied to these two integers we solve for their greatest common divisor: $17 = 2057 - (60)34$. The fourth equation then shows that $34 = 4148 - (2)2057$, so substituting this expression for the previous remainder 34 gives the equation $17 = 2057 - (60)[4148-(2)2057]$, i.e. $17 = (121)2057-(60)4148$. Solving the third equation for 2057 and substituting gives $17 = (121)[6205-(1)4148]-(60)4148 = (121)6205-(181)4148$. Using the second equation to solve for 4148 and then the first equation to solve for 6205 we finally obtain

$$17 = (302)57970 - (1691)10353$$

as can easily be checked directly. Hence the equation $ax + by = (a, b)$ for the geatest common divisor of $a$ and $b$ in this example has the solution $x = 302$ and $y = -1691$. Note that it is relatively unlikely that this relation would have been found simply by guessing.

The integers $x$ and $y$ in (7) above are not unique. In the example with $a = 57970$ and $b = 10353$ we determined one solution to be $x = 302$ and $y = -1691$, for instance, and it is relatively simple to check that $x = -307$ and $y = 1719$ also satisfy $57970x+10353y = 17$. The general solution for $x$ and $y$ is known (cf. the exercises below and in Chapter 3).

(8) An element $p$ of $\mathbb{Z}^+$ is called a prime if $p > 1$ and the only positive divisors of $p$ are 1 and $p$ (initially, the word prime will refer only to positive integers). An integer $n > 1$ which is not prime is called composite. For example, $2, 3, 5, 7, 11, 13, 17, 19, \cdots$ are primes and $4, 6, 8, 9, 12, 14, 15, 16, 18, \cdots$ are composite.

An important property of primes (which in fact can be used to define the primes (cf. Exercise 3)) is the following: if $p$ is a prime and $p \mid ab$, for some $a, b \in \mathbb{Z}$, then either $p \mid a$ or $p \mid b$.

(9) The Fundamental Theorem of Arithmetic says: if $n \in \mathbb{Z}$, $n > 1$, then $n$ can be factored uniquely into the product of primes, i.e. there are distinct primes $p_1, p_2, \cdots, p_s$ and positive integers $\alpha_1, \alpha_2, \cdots, \alpha_s$ such that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s},$$

This factorization is unique in the sense that if $q_1, q_2, \cdots, q_t$ are any distinct primes and $\beta_1, \beta_2, \cdots, \beta_t$ positive integers such that

$$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t},$$

then $s = t$ and if we arrange the two sets of primes in increasing order, then $q_i = p_i$ and $\alpha_i = \beta_i$, $1 \le i \le s$. For example, $n = 1852423848 = 2^3 3^2 11^2 19^3 31$ and this decomposition into the product of primes is unique.

Suppose the positive integers $a$ and $b$ are expressed as products of prime powers:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$$

where $p_1, p_2, \cdots, p_s$ are distinct and the exponents are $\geq 0$ (we allow the exponents to be 0 here so that the products are taken over the same set of primes - the exponent will be 0 if that prime is not actually a divisor). Then the greatest common divisor of $a$ and $b$ is

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_s^{\min(\alpha_s, \beta_s)}$$

(and the least common multiple is obtained by instead taking the maximum of the $\alpha_i$ and $\beta_i$ instead of the minimum).

**例 0.3** In the example above, $a = 57970$ and $b = 10353$ can be factored as $a = 2{\cdot}5{\cdot}11{\cdot}17{\cdot}31$ and $b = 3 \cdot 7 \cdot 17 \cdot 29$, from which we can immediately conclude that their greatest common divisor is 17. Note, however, that for large integers it is extremely difficult to determine their prime factorizations (several common codes in current use are based on this difficulty, in fact), so that this is not an effective method to determine greatest common divisor in general. The Euclidean Algorithm will produce greatest common divisors quite rapidly without the need for the prime factorization of $a$ and $b$.

(10) The Euler $\varphi-$function is defined as follows: for $n \in \mathbb{Z}^+$ let $\varphi(n)$ be the number of positive integers $a \leq n$ with $a$ relatively prime to $n$, i.e. $(a, n) = 1$. For example, $\varphi(12) = 4$ since $1, 5, 7$ and $11$ are the only positive integers less than or equal to 12 which have no factors in common with 12. Similarly, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, etc. For primes $p$, $\varphi(p) = p - 1$, nd, more generally, for all $a \geq 1$ we have the formula

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1).$$

The function $\varphi$ is *multiplication* in the sense that

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{if } (a, b) = 1$$

(note that it is important here that $a$ and $b$ be relatively prime). Together with the formula above this gives a general formula for the values of $\varphi$: if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, then

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s}) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 2}(p_2 - 1) \cdots p_s^{\alpha_s - 1}(p_s - 1). \end{aligned}$$

For example, $\varphi(12) = \varphi(2^2)\varphi(3) = 2^1(2-1)3^0(3-1) = 4$. The reader should note that we shall use the letter $\varphi$ for many different functions throughout the text so we want this letter to denote Euler's function we shall be careful to indicate this explicitly.

## 第零章习题

1. For each of the following pairs of integers $a$ and $b$, determine their greatest common divisor, their least common multiple, and write their greatest common divisor on the form $ax + by$ for some integers $x$ and $y$.

(a) $a = 20, b = 13$.

(b) $a = 69, b = 372$.

(c) $a = 792, b = 275$.

(d) $a = 11391, b = 5673$.

(e) $a = 1761, b = 1567$.

(f) $a = 507885, b = 60808$.

2. Prove that if the integer $k$ divides the integers $a$ and $b$ then $k$ divides $as + bt$ for every pair of integers $s$ and $t$.
3. Prove that if $n$ is composite then there are integers $a$ and $b$ such that $n$ divides $ab$ but $n$ does not divide either $a$ or $b$.
4. Let $a$, $b$ and $N$ be fixed integers with $a$ and $b$ nonzero and let $d = (a, b)$ be the greatest common divisor of $a$ and $b$. Suppose $x_0$ and $y_0$ are particular solutions to $ax + by = N$ (i.e. $ax_0 + by_0 = N$). Prove for any integer $t$ that the integers
$$x = x_0 + \frac{b}{d}t \quad \text{and} \quad y = y_0 - \frac{a}{d}t$$
are also solutions to $ax + by = N$ (this is in fact the general solution).
5. Determine the value $\varphi(n)$ for each integer $n \leq 30$ where $\varphi$ denotes the Euler $\varphi-$function.
6. Prove the Well Ordering Property of $\mathbb{Z}$ by induction and prove the minimal element is unique.
7. If $p$ is a prime prove that there do not exist nonzero integers $a$ and $b$ such that $a^2 = pb^2$(i.e. $\sqrt{p}$ is not a rational number).
8. Let $p$ be a prime, $n \in \mathbb{Z}^+$. Find a formular for the largest power of $p$ which divides $n! = n(n-1)(n-2)\cdots 2 \cdot 1$ (it involves the greatest integer function).
9. Write a computer program to determine the greatest common divisor $(a, b)$ of two integers $a$ and $b$ and to express $(a, b)$ in the form $ax + by$ for some integers $x$ and $y$.
10. Prove for any given positive integer $N$ there exist only finitely many integers $n$ with $\varphi(n) = N$ where $\varphi$ denotes Euler's $\varphi-$function. Conclude in particular that $\varphi(n)$ tends to infinity as $n$ tends to infinity.
11. Prove that if $d$ divides $n$ then $\varphi(d)$ divides $\varphi(n)$ where $\varphi$ denotes Euler's $\varphi-$function.

## 0.3 $\mathbb{Z}/n\mathbb{Z}$: The integers Modulo $n$

Let $n$ be a fixed positive integer. Define a relation on $\mathbb{Z}$ by

$$a \sim b \text{ if and only if } n \mid (b - a).$$

Clearly $a \sim a$, and $a \sim b$ implies $b \sim a$ for any integers $a$ and $b$, so this relation is trivially reflexive and symmetric. If $a \sim b$ and $b \sim c$ then $n$ divides $a - b$ and $n$ divides $b - c$ so $n$ also divides the sum of these two integers, i.e. $n$ divides $(a - b) + (b - c) = a - c$, so $a \sim c$ and the relation is transitive. Hence this is an equivalence relation. Write $a \equiv b \pmod{n}$ (read: $a$

is congruent to $b \bmod n$) if $a \sim b$. For any $k \in \mathbb{Z}$ we shall denote the equivalence class of $a$ by $\bar{a}$ - this is called the congruence class or residue class of $a \bmod n$ and consists of the integers which differ from $a$ by an integeral multiple of $n$, i.e.

$$\begin{aligned}\bar{a} &= \{a + kn | k \in \mathbb{Z}\} \\ &= \{a, a \pm n, a \pm 2n, a \pm 3n, \cdots\}.\end{aligned}$$

There are precisely $n$ distinct equivalence classes $\bmod n$, namely

$$\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}$$

determined by the possible remainders after division by $n$ and these residue classes partition the integers $\mathbb{Z}$. The set of equivalence classes under this equivalence relation will be denoted by $\mathbb{Z}/n\mathbb{Z}$ and called the integers modulo $n$ (or the integers $\bmod n$). The motivation for this notation will become clearer when we discuss quotient groups and quotient rings. Note that for different $n$'s the equivalence relation and equivalence classes are different so we shall always be careful to fix $n$ first before using the bar notation. The process of finding the equivalence class $\bmod n$ of some integer $a$ is often referred to as reducing $a \bmod n$. This terminology also frequently refers to finding the smallest nonnegative integer congruent to $a \bmod n$ (the least residue of $a \bmod n$).

We can define an addition and a multiplication for the elements of $\mathbb{Z}/n\mathbb{Z}$, defining modular arithmetic as follows: for $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$, define their sum and product by

$$\bar{a} + \bar{b} = \overline{a+b} \quad \text{and} \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

What this means is the following: given any two elements $\bar{a}$ and $\bar{b}$ in $\mathbb{Z}/n\mathbb{Z}$, to compute their sum (respectively, their product) take any representative integer $a$ in the class $\bar{a}$ and any representative integer $b$ in the class $\bar{b}$ and add (respectively, multiply) the integers $a$ and $b$ as usual in $\mathbb{Z}$ and then take the equivalence class containing the result. The following Theorem 3 asserts that this is well defined, i.e. does not depend on the choice of representatives taken for the elements $\bar{a}$ and $\bar{b}$ of $\mathbb{Z}/n\mathbb{Z}$.

**例 0.4** Suppose $n = 12$ and consider $\mathbb{Z}/12\mathbb{Z}$, which consists of the twelve residue classes

$$\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{11}$$

determined by the twelve possible remainders of an integer after division by 12. The elements in the residue class $\bar{5}$, for example, are the integers which leave a remainder of 5 when divided by 12 (the integers congruent to $5 \bmod 12$). Any integer congruent to $5 \bmod 12$ (such as $5, 17, 29, \cdots$ or $-7, -19, \cdots$) will serve as a representative for the residue class $\bar{5}$. Note that $\mathbb{Z}/12\mathbb{Z}$ consists of the twelve elements above (and each of these elements of $\mathbb{Z}/12\mathbb{Z}$ consists of an infinite number of usual integers).

Suppose now that $\bar{a} = \bar{5}$ and $\bar{b} = \bar{8}$. The most obvious representative for $\bar{a}$ is the integer 5 and similarly 8 is the most obvious representative for $\bar{b}$. Using these representatives for the residue classes we obtain $\bar{5} = \bar{8} = \overline{13} = \bar{1}$ since 13 and 1 lie in the same class modulo $n = 12$. Had we instead taken the representative 17, say, for $\bar{a}$ (note that 5 and 17 do lie in the same residue class

modulo 12) and the representative $-28$, say, for $\bar{b}$, we would obtain $\bar{5}+\bar{8}=\overline{17-28}=\overline{-11}=\bar{1}$ and as we mentioned the result does not depend on the choice of representatives chosen. The product of these two classes is $\bar{a}\cdot\bar{b}=\overline{5\cdot 8}=\overline{40}=\bar{4}$, also independent of the representatives chosen.

**定理 0.1**

The operations of addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ defined above are both well defined, that is, they do not depend on the choices of representatives for the classes involved. More precisely, if $a_1, a_2 \in \mathbb{Z}$ and $b_1, b_2 \in \mathbb{Z}$ with $\overline{a_1}=\overline{b_1}$ and $\overline{a_2}=\overline{b_2}$, then $\overline{a_1+a_2}=\overline{b_1+b_2}$ and $\overline{a_1a_2}=\overline{b_1b_2}$. i.e. if

$$a_1 \equiv b_1 \pmod{n} \quad \text{and} \quad a_2 \equiv b_2 \pmod{n}$$

then

$$a_1+a_2 \equiv b_1+b_2 \pmod{n} \quad \text{and} \quad a_1a_2 \equiv b_1b_2 \pmod{n}$$

♡

证明 Suppose $a_1 \equiv b_1 \pmod{n}$, i.e. $a_1-b_1$ is divisible by $n$. Then $a_1=b_1+sn$ for some integer $s$. Similarly, $a_2 \equiv b_2 \pmod{n}$ means $a_2=b_2+tn$ for some integer $t$. Then $a_1+a_2=(b_1+b_2)+(s+t)n$ so that $a_1+a_2 \equiv b_1+b_2 \pmod{n}$, which shows that the sum of the residue classes is independent of the representatives chosen. Similarly, $a_1a_2=(b_1+sn)(b_2+tn)=b_1b_2+(b_1t+b_2s+st)n$ shows that $a_1a_2 \equiv b_1b_2 \pmod{n}$ and so the product of the residue classes is also independent of the representatives chosen, completing the proof.

We shall see later that the process of adding equivalence classes by adding their representatives is a special case of a more general construction (the construction of a quotient). This notion of adding equivalence classes is already a familiar one in the context of adding rational numbers: each rational number $a/b$ is really a class of expressions: $a/b=2a/2b=-3a/-3b$ etc. and we often change representatives (for instance, take common denominators) in order to add two fractions (for example $1/2+1/3$ is computed by taking instead the equivalent representatives $3/6$ for $1/2$ and $2/6$ for $1/3$ to obtain $1/2+1/3=3/6+2/6=5/6$). The notion of modular arithmetic is also familiar: to find the hour of day after adding or subtracting some number of hours we reduce $\mathrm{mod}12$ and find the least residue.

It is important to be able to think of the equivalence classes of some equivalence relation as elements which can be manipulated (as we do, for example, with fractions) rather than as sets. Consistent with this attitude, we shall frequently denote the elements of $\mathbb{Z}/n\mathbb{Z}$ simply by $\{0,1,\cdots,n-1\}$ where addition and multiplication are reduced $\mathrm{mod}n$. It is important to remember, however, that the elements of $\mathbb{Z}/n\mathbb{Z}$ are not integers, but rather collections of usual integers, and the arithmetic is quite different. For example, $5+8$ is not 1 in the integers $\mathbb{Z}$ as it was in the example of $\mathbb{Z}/12\mathbb{Z}$ above.

The fact that one can define arithmetic in $\mathbb{Z}/n\mathbb{Z}$ has many important applications in elementary number theory. As one simply example we compute the last two digits in the

number $2^{1000}$. First observe that the last two digits give the remainder of $2^{1000}$ after we divide by 100 so we are interested in the residue class $\bmod 100$ containing $2^{1000}$. We compute $2^{10} = 1024 \equiv 24 \pmod{100}$, so then $2^{20} = (2^{10})^2 \equiv 24^2 = 576 \equiv 76 \pmod{100}$. Then $2^{40} = (2^{20})^2 \equiv 76^2 = 5776 \equiv 76 \pmod{100}$. Similarly $2^{80} \equiv 2^{160} \equiv 2^{320} \equiv 2^{640} \equiv 76 \pmod{100}$. Finally, $2^{1000} = 2^{640}2^{320}2^{40} \equiv 76 \cdot 76 \cdot 76 \equiv 76 \pmod{100}$ so the final two digits are 76.

An important subset $\mathbb{Z}/n\mathbb{Z}$ consists of the collection of residue classes which have a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} | \text{there exists } \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ with } \bar{a} \cdot \bar{c} = \bar{1}\}.$$

Some of the following exercises outline a proof that $(\mathbb{Z}/n\mathbb{Z})^\times$ is also the collection of residue classes whose representatives are relatively prime to $n$:

**命题 0.3**

$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} | (a, n) = 1\}$. ♠

It is easy to see that if any representative of $\bar{a}$ is relatively prime to $n$ then all representatives are relatively prime to $n$ so that the set on the right in the proposition is well defined.

**例 0.5** For $n = 9$ we obtain $(\mathbb{Z}/9\mathbb{Z})^\times = \{1, 2, 4, 5, 7, 8\}$ from the proposition. The multiplicative inverses of these elements are $\{1, 5, 7, 2, 4, 8\}$, respectively.

If $a$ is an integer relatively prime to $n$ then the Euclidean Algorithm produces integers $x$ and $y$ satisfying $ax + ny = 1$, hence $ax \equiv 1 \pmod{n}$, so that $\bar{x}$ is the multiplicative inverse of $\bar{a}$ in $\mathbb{Z}/n\mathbb{Z}$. This gives an efficient method for computing multiplicative inverses in $\mathbb{Z}/n\mathbb{Z}$.

**例 0.6** Suppose $n = 60$ and $a = 17$. Applying the Euclidean Algorithm we obtain

$$60 = (3)17 + 9$$
$$17 = (1)9 + 8$$
$$9 = (1)8 + 1$$

so that $a$ and $n$ are relatively prime, and $(-7)17+(2)60 = 1$. Hence $\overline{-1} = \overline{53}$ is the multiplicative inverse of $\overline{17}$ in $\mathbb{Z}/60\mathbb{Z}$.

## 第零章习题

1. Write down explicitly all the elements in the residue classes of $\mathbb{Z}/18\mathbb{Z}$.
2. Prove that the distinct equivalence classes in $\mathbb{Z}/n\mathbb{Z}$ are precisely $\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}$(use the Division Algorithm).
3. Prove that if $a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0$ is any positive integer then $a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod{9}$ (note that this is the usual arithmetic rule that the remainder after division by 9 is the same as the sum of the decimal digits $\bmod 9$ - in particular an integer is divisible by 9 if and only if the sum of its digits is divisible by 9)[note that $10 \equiv 1 \pmod{9}$].

4. Compute the remainder when $37^{100}$ is divided by 29.
5. Compute the last two digits of $9^{1500}$.
6. Prove that the squares of the elements in $\mathbb{Z}/4\mathbb{Z}$ are just $\bar{0}$ and $\bar{1}$.
7. Prove for any integers $a$ and $b$ that $a^2 + b^2$ never leaves a remainder of 3 when divided by 4 (use the previous exercise).
8. Prove that the equation $a^2 + b^2 = 3c^2$ has no solutions in nonzero integers $a$, $b$ and $c$.[Consider the equation $\mathrm{mod}4$ as in the previous two exercises and show that $a$, $b$ and $c$ would all have to be divisible by 2. Then each of $a^2$, $b^2$ and $c^2$ has a factor of 4 and by dividing through by 4 show that there would be a smaller set of solutions to the original equation. Iterate to reach a contradiction.]
9. Prove that the square of any odd integer always leaves a remainder of 1 when divided by 8.
10. Prove that the number of elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $\varphi(n)$ where $\varphi$ denotes the Euler $\varphi-$function.
11. Prove that if $\bar{a}, \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\bar{a} \cdot \bar{b} \in (\mathbb{Z}/n\mathbb{Z})^\times$.
12. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if $a$ and $n$ are not relatively prime, there exists an integer $b$ with $1 \leq b < n$ such that $ab \equiv 0 \pmod{n}$ and deduce that there cannot be an integer $c$ such that $ac \equiv 1 \pmod{n}$.
13. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove if $a$ and $n$ are relatively prime then there is an integer $c$ such that $ac \equiv 1 \pmod{n}$[use the fact that the g.c.d. of two integers is a $\mathbb{Z}-$linear combination of the integers].
14. Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition **??**. Verify this directly in the case $n = 12$.
15. For each of the following pairs of integers $a$ and $n$, show that $a$ is relatively prime to $n$ and determine the multiplicative inverse of $a$ in $\mathbb{Z}/n\mathbb{Z}$.
    (a) $a = 13$, $n = 20$.
    (b) $a = 69$, $n = 89$.
    (c) $a = 1891$, $n = 3797$.
    (d) $a = 6003722857$, $n = 77695236973$. [The Euclidean Algorithm requires only 3 steps for these integers.]
16. Write a computer program to add and multiply $\mathrm{mod}n$, for any $n$ given as input. The output of these operations should be the least residues of the sums and products of two integers. Also include the feature that if $(a, n) = 1$, an integer $c$ between 1 and $n - 1$ such that $\bar{a} \cdot \bar{c} = \bar{1}$ may be printed on request. (Your program should not, of course, simply quote "mod" functions already built into many systems).

# 第一部分

# Group Theory

The modern treatment of abstract algebra begins with the disarmingly simple abstract definition of a group. This simple definition qickly leads to difficult questions involving the structure of such objects. There are many specific examples of groups and the power of the abstract point of view becomes apparent when results for all of these examples are obtained by proving a single result for the abstract group.

The notion of a group did not simply spring into existence, however, but is rather the culmination of a long period of mathematical investigation, the first formal definition of an abstract group in the form in which we use it appearing in 1882.[1] The definition of an abstract group has its origins in extremely old problems in algebraic equations, number theory, and geometry, and arose because very similar techniques were found to be applicable in a variety of situations. As Otto Hölder (1859-1937) observed, one of the essential characteristics of mathematics is that after applying a certain algorithm or method of proof one then considers the scope and limits of the method. As a result, properties possessed by a number of interesting objects are frequently abstracted and the question raised: can one determine all the objects possessing these properties? Attempting to answer such a question also frequently adds considerable understanding of the original objects under consideration. It is in this fashion that the definition of an abstract group evolved into what is, for us, the starting point of abstract algebra.

We illustrate with a few of the disparate situstions in which the ideas later formalized into the notion of an abstract group were used:

1. In number theory the very object of study, the set of integers, is an example of a group. Consider for example what we refer to as "Euler's Theorem" (cf. Exercise 22 of Section 3.2), one extremely simple example of which is that $a^{40}$ has last two digits $01$ if $a$ is any integer not divisible by 2 nor by 5. This was proved in 1761 by Leonhard Euler (1707-1783) using "group-theoretic" ideas of Hoseph Louis Lagrange (1736-1813), long before the first formal definition of a group. From our perspective, one now proves "Lagrange's Theorem" (cf. Theorem 8 of Section 3.2), applying these techniques abstracted to an arbitary group, and then recovers Euler's Theorem (and many others) as a special case.

2. Investigations into the question of rational solutions to algebraic equations of the form $y^2 = x^3 - 2x$ (there are infinitely many, for example $(0,0)$,$(-1,1)$, $(2,2)$, $(9/4,-21/8)$, $(-1/169, 239/2197)$) showed that connecting any two solutions by a straight line and computing the intersection of this line with the curve $y^2 = x^3 - 2x$ produces another solution. Such"Diophantine equations", among others, were considered by Pierre de Fermat (1601-1655) (this one was solved by him in 1644), by Euler, by Lagrange around 1777, and others. In 1730 Euler raised the question of determining the indefinite integral $\int dx/\sqrt{1-x^4}$ of the "lemniscatic

[1]For most of the historical comments below, see the excellent book *A History of Algebra*, by B.L.vander Waerden. Springer-Verlag, 1980 and the references there, particularly *The Genesis of the Abstract Group Concept: A Contribution to the History of the Origin of Abstract Group Theory*(translated from the German by Abe Shenitzer), by H. Wussing, MIT Press, 1984. See also *Number Theory: An Approach Through History from Hammurapai to Legendre*, by A. Weil, Birkhäuser, 1984.

differential" $dx/\sqrt{1-x^4}$, used in determining the arc length along an ellipse (the question had also been considered by Gottfried Wilhelm Leibniz (1646-1716) and Johannes Bernoulli(1667-1748)). In 1752 Euler proved a "multiplication formula" for such elliptic integrals (using ideas of G.C. di Fagnano(1682-1766), received by Euler in 1751), which shows how two elliptic integrals give rise to a third , bringing into existence the theory of elliptic functions in analysis. In 1834 Carl Gustav Jacob Jacobi (1804-1851) observed that the work of Euler on solving certain Diophantine equations amounted to writing the multiplication formula for certain elliptic integrals. Today the curve above is referred to as an "elliptic curve" and these questions are viewed as two different aspects of the same thing — the fact that this geometric operation on points can be used to give the set of points on an elliptic curve the structure of a group. The study of the "arithmetic" of these groups is an active area of current research.[2]

3. By 1824 it was known that there are formulas giving the roots of quadratic, cubic and quartic equations (extending the familiar quadratic formula for the roots of $ax^2+bx+c=0$). In 1824, however, Niels Henrik Abel (1802-1829) proved that such a formula for the roots of a quintic is impossible (cf. Corollary 40 of Section 14.7). The proof is based on the idea of examining what happens when the roots are permuted amongst themselves (for example, interchanging two of the roots). The collection of such permutations has the structure of a group (called, naturally enough, a "permutation group"). This idea culminated in the beautiful work of Evariste Galois (1811-1832) in 1830-32, working with explicit groups of "substitutions". Today this work is referred to as Galois Theory (and is the subject of the fourth part of this text). Similar explicit groups were being used in geometry as collections of geometric transformations (translations, reflections, etc.) by Arthur Cayley (1821-1895) around 1850, Camille Jordan (1838-1922) around 1867, Felix Klein (1949-1925) around 1870, etc., and the application of groups to geometry is still extremely active in current research into the structure of 3-space, 4-space, etc. The same group arising in the study of the solvability of the quintic arises in the study of the rigid motions of an icosahedron in geometry and in the study of elliptic functions in analysis.

The precursors of today's abstract groups can be traced back many years, even before the groups of "substitutions" of Galois. The formal definition of an abstract group which is our starting point appeared in 1882 in the work of Walter Dyck (1856-1934), an assistant to Felix Klein, and also in the work of Heinrich Weber (1842-1913) in the same year.

It is frequently the case in mathematics research to find specific application of an idea before having that idea extracted and presented as an item of interest in its own right (for example, Galois used the notion of a "quotient group" implicitly in his investigations in 1830 and the definition of an abstract quotient group is due to Hölder in 1889). It is important to realize, with or without the historical context, that the reason the abstract definitions are made is because it is useful to isolate specific characteristics and consider what structure is imposed on an object having these

[2]See The Arithmetic of Elliptic Curves by J.Silverman, Springer-Verlag. 1986

characteristics. The notion of the structure of an algebraic object (which is made more precise by the concept of an isomorphsim — which considers when two apparently different objects are in some sense the same) is a major theme which will recur throughout the text.

# 第一章 Introduction to Groups

## 1.1 Basic Axioms and Examples

In this section the basic algebraic structure to be studied in Part I is introduced and some examples are given.

**定义 1.1**

(1) A binary operation $\star$ on a set $G$ is a function $\star$: $G \times G \to G$. For any $a, b \in G$ we shall write $a \star b$ for $\star(a, b)$.

(2) A binary operation $\star$ on a set $G$ is associative if for all $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.

(3) If $\star$ is a binary operation on a set $G$ we say elements $a$ and $b$ of $G$ commute if $a \star b = b \star a$. We say $\star$(or $G$) is commutative if for all $a, b \in G$, $a \star b = b \star a$. ♣

**例 1.1**

(1) $+$ (usual addition) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ respectively).

(2) $\times$ (usual multiplication) is a commutative binary operation on $\mathbb{Z}$ (or on $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ respectively).

## 1.2 Dihedral Groups

## 1.3 Symmetric Groups

## 1.4 Matrix Groups

## 1.5 The Quaternion Groups

## 1.6 Homomorphisms and Isomorphisms

## 1.7 Group Actions

# 第二章 Subgroups

## 2.1 Definition and Examples

# 第三章 Euclidean Domains, Principal Ideal Domains and Unique Factorization Domains