Elementary Abstract Algebra

W. Edwin Clark
Department of Mathematics
University of South Florida

(Last revised: December 23, 2001)

Preface

This book is intended for a one semester introduction to *abstract algebra*. Most introductory textbooks on abstract algebra are written with a two semester course in mind. See, for example, the books listed in the Bibliography below. These books are listed in approximate order of increasing difficulty. A search of the library using the keywords *abstract algebra* or *modern algebra* will produce a much longer list of such books. Some will be readable by the beginner, some will be quite advanced and will be difficult to understand without extensive background. A search on the keywords *group* and *ring* will also produce a number of more specialized books on the subject matter of this course. If you wish to see what is going on at the frontier of the subject, you might take a look at some recent issues of the journals *Journal of Algebra* or *Communications in Algebra* which you will find in our library.

Instead of spending a lot of time going over background material, we go directly into the primary subject matter. We discuss proof methods and necessary background as the need arises. Nevertheless, you should at least skim the appendices where some of this material can be found so that you will know where to look if you need some fact or technique.

Since we only have one semester, we do not have time to discuss any of the many applications of abstract algebra. Students who are curious about applications will find some mentioned in Fraleigh [1] and Gallian [2]. Many more applications are discussed in Birkhoff and Bartee [5] and in Dornhoff and Horn [6].

Although abstract algebra has many applications in engineering, computer science and physics, the thought processes one learns in this course may be more valuable than specific subject matter. In this course, one learns, perhaps for the first time, how mathematics is organized in a rigorous manner. This approach, the *axiomatic method*, emphasizes examples, definitions, theorems and proofs. A great deal of importance is placed on *understanding*.

Every detail should be understood. Students should not expect to obtain this understanding without considerable effort. My advice is to learn each definition as soon as it is covered in class (if not earlier) and to make a real effort to solve each problem in the book *before* the solution is presented in class. Many problems require the construction of a proof. Even if you are not able to find a particular proof, the effort spent trying to do so will help to increase your understanding of the proof when you see it. With sufficient effort, your ability to successfully prove statements on your own will increase.

We assume that students have some familiarity with basic set theory, linear algebra and calculus. But very little of this nature will be needed. To a great extent, the course is self-contained, except for the requirement of a certain amount of mathematical maturity. And, hopefully, the student's level of mathematical maturity will increase as the course progresses.

I will often use the symbol ■ to indicate the end of a proof. Or, in some cases, ■ will indicate the fact that no more proof will be given. In such cases the proof will either be assigned in the problems or a reference will be provided where the proof may be located. This symbol was first used for this purpose by the mathematician Paul Halmos.

Note: when teaching this course I usually present in class lots of hints and/or outlines of solutions for the less routine problems.

This version includes a number of improvements and additions suggested by my colleague Milé Krajčevski.

Bibliography

[1] J. B. Fraleigh, *A First Course in Abstract Algebra*, (Fifth Edition), Addison-Wesley, 1994.

[2] J. A. Gallian, *Contemporary Abstract Algebra*, (Third Edition), D.C. Heath, 1994.

[3] G. Birkhoff and S. MacLane, *A Survey of Modern Algebra*, A. K. Peters Ltd., 1997.

[4] I. N. Herstein, *Topics in Algebra*, (Second Edition), Blaisdell, 1975.

[5] G. D. Birkhoff and T. C. Bartee, *Modern Applied Algebra*, McGraw-Hill Book Company, 1970.

[6] L. Dornhoff and F. Hohn, *Applied Modern Algebra*, Macmillan, 1978.

[7] B. L. Van der Waerden, *Modern Algebra*, (Seventh Edition, 2 vols), Fredrick Ungar Publishing Co., 1970.

[8] T. W. Hungerford, *Algebra*, Springer Verlag, 1980.

[9] N. Jacobson, *Basic Algebra I and II*, (Second Edition, 2 vols), W. H. Freeman and Company, 1989.

[10] S. Lang, *Algebra*, Addison-Wesley, (Third Edition), 1992.

Contents

Chapter 1

Binary Operations

The most basic definition in this course is the following:

Definition 1.1 *A* **binary operation** $*$ *on a set* S *is a function from* $S \times S$ *to* S. *If* $(a, b) \in S \times S$ *then we write* $a * b$ *to indicate the image of the element* (a, b) *under the function* $*$.

The following lemma explains in more detail exactly what this definition means.

Lemma 1.1 *A binary operation* $*$ *on a set* S *is a rule for combining two elements of* S *to produce a third element of* S. *This rule must satisfy the following conditions:*

(a) $a \in S$ *and* $b \in S \Longrightarrow a * b \in S$. [$S$ is closed under $*$.]

(b) *For all* a, b, c, d *in* S
$a = c$ *and* $b = d \Longrightarrow a * b = c * d$. [Substitution is permissible.]

(c) *For all* a, b, c, d *in* S
$a = b \Longrightarrow a * c = b * c$.

(d) *For all* a, b, c, d *in* S
$c = d \Longrightarrow a * c = a * d$.

Proof Recall that a function f from set A to set B is a rule which assigns to each element $x \in A$ an element, usually denoted by $f(x)$, in the set B. Moreover, this rule must satisfy the condition

$$x = y \Longrightarrow f(x) = f(y) \tag{1.1}$$

On the other hand, the Cartesian product $S \times S$ consists of the set of all ordered pairs (a, b) where $a, b \in S$. Equality of ordered pairs is defined by the rule

$$a = c \text{ and } b = d \Longleftrightarrow (a, b) = (c, d). \tag{1.2}$$

Now in this case we assume that $*$ is a function from the set $S \times S$ to the set S and instead of writing $*(a, b)$ we write $a * b$. Now, if $a, b \in S$ then $(a, b) \in S \times S$. So the rule $*$ assigns to (a, b) the element $a * b \in S$. This establishes **(a)**. Now implication (1.1) becomes

$$(a, b) = (c, d) \Longrightarrow a * b = c * d. \tag{1.3}$$

From (1.2) and (1.3) we obtain

$$a = c \text{ and } b = d \Longrightarrow a * b = c * d. \tag{1.4}$$

This establishes **(b)**.

To prove **(c)** we assume that $a = b$. By reflexivity of equality, we have for all $c \in S$ that $c = c$. Thus we have $a = b$ and $c = c$ and it follows from part **(b)** that $a * c = b * c$, as desired. The proof of **(d)** is similar. ■

Remarks In part **(a)** the order of a and b is important. We do not assume that $a * b$ is the same as $b * a$. Although sometimes it may be true that $a * b = b * a$, it is not part of the definition of binary operation.

Statement **(b)** says that if $a = c$ and $b = d$, we can *substitute* c for a and d for b in the expression $a * b$ and we obtain the expression $c * d$ which is equal to $a * b$. One might not think that such a natural statement is necessary. To see the need for it, see Problem 1.7 below.

Part **(c)** of the above lemma says that *we can multiply both sides of an equation on the right by the the same element.* Part **(d)**, says that *we can multiply both sides of an equation on the left by the same element.*

Binary operations are usually denoted by symbols such as

$$+, \cdot, *, \times, \circ, \star, \bullet, \diamond, \boxdot, \boxtimes, \otimes, \oplus, \odot, \vee, \wedge, \cup, \cap, \cdots$$

Just as one often uses f for a generic function, we use $*$ to indicate a generic binary operation. Moreover, if $* : S \times S \to S$ is a given binary operation on

a set S, we write $a * b$ instead of $*(a, b)$. This is called **infix** notation. In practice, we abbreviate even more; just as we use ab instead of $a \cdot b$ or $a \times b$ in high school algebra, we will often use ab instead of $a * b$ for a generic binary operation.

Notation. We denote the *natural numbers*, the *integers*, the *rational numbers*, and the *real numbers* by the symbols $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, respectively. Recall that

$$\begin{aligned} \mathbb{N} &= \{1, 2, 3, \dots\} \\ \mathbb{Z} &= \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} \\ \mathbb{Q} &= \{\frac{n}{m} : n, m \in \mathbb{Z} \text{ and } m \neq 0\} \end{aligned}$$

For now, we assume that students have a basic knowledge of all these number systems. Later in the course, we will give a list of axioms from which all properties of these number systems can be derived. See Appendix C for some basic properties of $\mathbb{N}$ *and* $\mathbb{Z}$ *that we will need from time to time.*

We now list some examples of binary operations. Some should be very familiar to you. Some may be new to you.

Example 1.1 *Ordinary addition on* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ *and* $\mathbb{R}$.

Example 1.2 *Ordinary multiplication on* $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ *and* $\mathbb{R}$.

Example 1.3 *Ordinary subtraction on* $\mathbb{Z}$, $\mathbb{Q}$ *and* $\mathbb{R}$. *Note that subtraction is not a binary operation on* $\mathbb{N}$ *since, for example,* $1 - 2 \notin \mathbb{N}$.

Example 1.4 *Ordinary division on* $\mathbb{Q} - \{0\}$ *and* $\mathbb{R} - \{0\}$. *Note that division is not a binary operation on* $\mathbb{N}$ *and* $\mathbb{Z}$ *since, for example,* $\frac{1}{2} \notin \mathbb{N}$ *and* $\frac{1}{2} \notin \mathbb{Z}$. *Also note that we must remove 0 from* $\mathbb{Q}$ *and* $\mathbb{R}$ *since division by 0 is not defined.*

Example 1.5 *For each integer* $n \geq 2$ *define the set*

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}.$$

For all $a, b \in \mathbb{Z}_n$ *let*

$a + b =$ *remainder when the ordinary sum of* a *and* b *is divided by* n, *and*

$a \cdot b =$ *remainder when the ordinary product of* a *and* b *is divided by* n.

The binary operations defined in Example 1.5 are usually referred to as **addition modulo** n and **multiplication modulo** n. The integer n in $\mathbb{Z}_n$ is called the **modulus**. The plural of modulus is **moduli**.

In Example 1.5, it would be more precise to use something like $a +_n b$ and $a \cdot_n b$ for addition and multiplication in $\mathbb{Z}_n$, but in the interest of keeping the notation simple we omit the subscript n. Of course, this means that in any given situation, we must be very clear about the value of n. Note also that this is really an infinite class of examples: $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_3 = \{0, 1, 2\}$, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, etc. Just to be clear, we give a few examples of addition and multiplication:

In $\mathbb{Z}_4$: $2 + 3 = 1$, $2 + 2 = 0$, $0 + 3 = 3$, $2 \cdot 3 = 2$, $2 \cdot 2 = 0$ and $1 \cdot 3 = 3$.

In $\mathbb{Z}_5$: $2 + 3 = 0$, $2 + 2 = 4$, $0 + 3 = 3$, $2 \cdot 3 = 1$, $2 \cdot 2 = 4$ and $1 \cdot 3 = 3$

Example 1.6 *For each integer $n \geq 1$ we let $[n] = \{1, 2, \cdots, n\}$.*
A **permutation** *on $[n]$ is a function from $[n]$ to $[n]$ which is both one-to-one and onto. We define S_n to be the set of all permutations on $[n]$. If σ and τ are elements of S_n we define their product $\sigma\tau$ to be the composition of σ and τ, that is,*

$$\sigma\tau(i) = \sigma(\tau(i)) \quad \textit{for all } i \in [n].$$

See Appendix B if any of the terms used in this example are unfamiliar.

Again, we have an infinite number of examples: S_1, S_2, S_3, S_4, etc. We discuss this example as well as the other examples in more detail later. First, we give a few more examples:

Example 1.7 *Let K denote any one of the following: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$. Let $M_2(K)$ be the set of all 2×2 matrices*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where a, b, c, d are any elements of K. Matrix addition and multiplication are defined by the following rules:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} a + a' & b + b' \\ c + c' & d + d' \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix} = \begin{bmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}$$

for all $a, b, c, d, a', b', c', d' \in K$.

Example 1.8 *The usual addition of vectors in* $\mathbb{R}^n$, $n \in \mathbb{N}$. *More precisely*

$$\mathbb{R}^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{R} \text{ for all } i\}.$$

Addition is defined by the rule:

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

where $x_i + y_i$ *denotes the usual addition of the real numbers* x_i *and* y_i.

Example 1.9 *Addition modulo 2 for binary sequences of length* n, $n \in \mathbb{N}$. *(This example is important for computer science.) In this case the set is*

$$\mathbb{Z}_2^n = \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{Z}_2 \text{ for all } i\}.$$

Recall that $\mathbb{Z}_2 = \{0, 1\}$. *Addition is defined by the rule:*

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n).$$

where $x_i + y_i$ *denotes addition modulo 2 (also called* exclusive or*) of* x_i *and* y_i. *More precisely* $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$ *and* $1 + 1 = 0$.

Example 1.10 *The cross product* $\mathbf{u} \times \mathbf{v}$ *of vectors* $\mathbf{u}$ *and* $\mathbf{v}$ *in* $\mathbb{R}^3$. *Recall that if*

$$\begin{aligned} \mathbf{u} &= (u_1, u_2, u_3) \\ \mathbf{v} &= (v_1, v_2, v_3) \end{aligned}$$

then $\mathbf{u} \times \mathbf{v}$ *is defined by the formula*

$$\mathbf{u} \times \mathbf{v} = \left(\begin{vmatrix} u_2 & u_3 \\ v_2 & v_3 \end{vmatrix}, - \begin{vmatrix} u_1 & u_3 \\ v_1 & v_3 \end{vmatrix}, \begin{vmatrix} u_1 & u_2 \\ v_1 & v_2 \end{vmatrix} \right),$$

where

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Example 1.11 *The set operations $\cup$ and $\cap$ are binary operations on the set $\mathcal{P}(X)$ of all subsets of X. Recall that the set $\mathcal{P}(X)$ is called the* power set of *X; and, if A and B are sets, then $A \cup B$ is called the* union *of A and B and $A \cap B$ is called the* intersection *of A and B.*

Definition 1.2 *Assume that $*$ is a binary operation on the set S.*

1. *We say that $*$ is* **associative** *if*

$$x * (y * z) = (x * y) * z \quad \text{for all } x, y, z \in S.$$

2. *We say that an element e in S is an* **identity** *with respect to $*$ if*

$$x * e = x \text{ and } e * x = x \quad \text{for all } x \text{ in } S.$$

3. *Let $e \in S$ be an identity with respect to $*$. Given $x \in S$ we say that an element $y \in S$ is an* **inverse** *of x if both*

$$x * y = e \text{ and } y * x = e.$$

4. *We say that $*$ is* **commutative** *if*

$$x * y = y * x \quad \text{for all } x, y \in S.$$

5. *We say that an element a of S is* **idempotent** *with respect to $*$ if*

$$a * a = a.$$

6. *We say that an element z of S is a* **zero** *with respect to $*$ if*

$$z * x = z \text{ and } x * z = z \quad \text{for all } x \in S.$$

Problem 1.1 *Assume that $*$ is a binary operation on the set S. Prove the following statements.*

(i) If e and e' are identities with respect to $*$ on S then $e = e'$. [Hint: What is $e * e'$?]

(ii) If z and z' are zeros with respect to $*$ on S then $z = z'$. [Hint: What is $z * z'$?]

Problem 1.2 *Go through all of the above examples of binary operations and determine which* are not *associative. Show non-associativity by giving three specific elements a, b, c such that $a * (b * c) \neq (a * b) * c$.*

Problem 1.3 *Go through all of the above examples of binary operations and determine which are not commutative. Show non-commutativity by giving two specific elements a, b such that $a * b \neq b * a$.*

Remark A set may have several binary operations on it. For example, consider the set $\mathbb{R}$ of real numbers. We write $(\mathbb{R}, \cdot)$, $(\mathbb{R}, +)$, and $(\mathbb{R}, -)$ to indicate the set $\mathbb{R}$ with the binary operations multiplication, addition and subtraction, respectively. Similarly, we use this notation for other sets such as the set $M_2(\mathbb{R})$, of 2×2 matrices over the real numbers $\mathbb{R}$. We use $(M_2(\mathbb{R}), \cdot)$ and $(M_2(\mathbb{R}), +)$ to denote matrix multiplication and matrix addition, respectively, on $M_2(\mathbb{R})$.

Problem 1.4 *Determine which of the examples $(\mathbb{R}, \cdot)$, $(\mathbb{R}, +)$, $(M_2(\mathbb{R}), \cdot)$, and $(\mathcal{P}(X), \cup)$ have identities. If there is an identity, determine the elements which* do not *have inverses.*

Problem 1.5 *Determine which of the examples $(\mathbb{R}, \cdot)$, $(\mathbb{R}, +)$, $(M_2(\mathbb{R}), \cdot)$, and $(\mathcal{P}(X), \cup)$ have zeros. If there is a zero, determine whether or not there are non-zero elements whose product is zero.*

Problem 1.6 *Determine which of the examples $(\mathbb{R}, \cdot)$, $(\mathbb{R}, +)$, $(M_2(\mathbb{R}), \cdot)$, and $(\mathcal{P}(X), \cup)$ have idempotents. Try to find all idempotents in each case.*

Problem 1.7 *Here we give an example of a rule that appears to define a binary operation, but does not, since substitution is not permissible. Let a, b, c, d be integers with $b \neq 0$ and $d \neq 0$. Then*

$$\frac{a}{b} \in \mathbb{Q} \quad \textit{and} \quad \frac{c}{d} \in \mathbb{Q}.$$

Define $*$ on $\mathbb{Q}$ by:

$$\frac{a}{b} * \frac{c}{d} = \frac{a+c}{b^2+d^2}.$$

Show that

$$\frac{a}{b} * \frac{c}{d} \in \mathbb{Q},$$

so $\mathbb{Q}$ is closed under $*$. Show by specific example that this rule does not permit substitution.

Chapter 2

Introduction to Groups

Definition 2.1 *A* **group** *is an ordered pair* $(G, *)$ *where* G *is a set and* $*$ *is a binary operation on* G *satisfying the following properties*

1. $x * (y * z) = (x * y) * z$ *for all* x, y, z *in* G.
2. *There is an element* $e \in G$ *satisfying* $e * x = x$ *and* $x * e = x$ *for all* x *in* G.
3. *For each element* x *in* G *there is an element* y *in* G *satisfying* $x * y = e$ *and* $y * x = e$.

Thus, to describe a group one must specify two things:

1. a set, and
2. a binary operation on the set.

Then, one must verify that the binary operation is associative, that there is an identity in the set, and that every element in the set has an inverse.

Convention If it is clear what the binary operation is, then the group $(G, *)$ may be referred to by its *underlying set* G alone.

Examples of Groups:

1. $(\mathbb{Z}, +)$ is a group with identity 0. The inverse of $x \in \mathbb{Z}$ is $-x$.
2. $(\mathbb{Q}, +)$ is a group with identity 0. The inverse of $x \in \mathbb{Q}$ is $-x$.
3. $(\mathbb{R}, +)$ is a group with identity 0. The inverse of $x \in \mathbb{R}$ is $-x$.

4. $(\mathbb{Q} - \{0\}, \cdot)$ is a group with identity 1. The inverse of $x \in \mathbb{Q} - \{0\}$ is x^{-1}.

5. $(\mathbb{R} - \{0\}, \cdot)$ is a group with identity 1. The inverse of $x \in \mathbb{R} - \{0\}$ is x^{-1}.

6. $(\mathbb{Z}_n, +)$ is a group with identity 0. The inverse of $x \in \mathbb{Z}_n$ is $n - x$ if $x \neq 0$, the inverse of 0 is 0. See Corollary C.5 in Appendix C for a proof that this binary operation is associative.

7. $(\mathbb{R}^n, +)$ where $+$ is vector addition. The identity is the zero vector $(0, 0, \ldots, 0)$ and the inverse of the vector $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ is the vector $-\mathbf{x} = (-x_1, -x_2, \ldots, -x_n)$.

8. $(\mathbb{Z}_2^n, +)$ where $+$ is vector addition modulo 2. The identity is the zero vector $(0, 0, \ldots, 0)$ and the inverse of the vector $\mathbf{x}$ is the vector itself.

9. $(M_2(K), +)$ where K is any one of $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{Z}_n$ is a group whose identity is the zero matrix
$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$
and the inverse of the matrix
$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$
is the matrix
$$-A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}.$$

Note that the binary operations in the above examples are all commutative. For historical reasons, there is a special name for such groups:

Definition 2.2 *A group $(G, *)$ is said to be* **abelian** *if $x * y = y * x$ for all x and y in G. A group is said to be* **non-abelian** *if it is not abelian.*

Examples of Non-Abelian Groups:

1. For each $n \in \mathbb{N}$, the set S_n of all permutations on $[n] = \{1, 2, \ldots, n\}$ is a group under compositions of functions. This is called the **symmetric group of degree** n. We discuss this group in detail in the next chapter. The group S_n is non-abelian if $n \geq 3$.

2. Let K be any one of $\mathbb{Q}, \mathbb{R}$ or $\mathbb{Z}_p$, where p is a prime number. Define $GL(2,K)$ to be the set of all matrices in $M_2(K)$ with non-zero determinant. Then $(GL(2,K),\cdot)$ is a group. Here $\cdot$ represents matrix multiplication. The identity of $GL(2,K)$ is the identity matrix

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and the inverse of

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is

$$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}.$$

$GL(2,K)$ is called the **general linear group of degree** 2 **over** K. These groups are non-abelian. We discuss them in more detail later.

Math Joke:
Question: What's purple and commutes? (For the answer see page 15.)

Theorem 2.1 *If $(G,*)$ is a group then:*
(a) The identity of G is unique.
(b) The inverse of each element in G is unique. ■

Problem 2.1 *Prove Theorem 2.1. Hints: To establish (a) assume that e and e' are identities of G and prove that $e = e'$. [This was done in the previous chapter, but do it again anyhow.] To establish (b) assume that x and y are both inverses of some element $a \in G$. Use the group axioms to prove that $x = y$. Show carefully how each axiom is used. Don't skip any steps.*

Now we can speak of *the* identity of a group and *the* inverse of an element of a group. Since the inverse of $a \in G$ is unique, the following definition makes sense:

Definition 2.3 *Let $(G,*)$ be a group. Let a be any element of G. We define a^{-1} to be the inverse of a in the group G.*

The above definition is used when we think of the group's operation as being a type of multiplication or product. If instead the operation is denoted by $+$, we have instead the following definition.

Definition 2.4 *Let $(G, +)$ be a group. Let a be any element of G. We define $-a$ to be the inverse of a in the group G.*

Theorem 2.2 *Let $(G, *)$ be a group with identity e. Then the following hold for all elements a, b, c, d in G:*

1. *If $a * c = a * b$, then $c = b$.* [Left cancellation law for groups.]
2. *If $c * a = b * a$, then $c = b$.* [Right cancellation law for groups.]
3. *Given a and b in G there is a* unique *element x in G such that $a * x = b$.*
4. *Given a and b in G there is a* unique *element x in G such that $x * a = b$.*
5. *If $a * b = e$ then $a = b^{-1}$ and $b = a^{-1}$.* [Characterization of the inverse of an element.]
6. *If $a * b = a$ for just one a, then $b = e$.*
7. *If $b * a = a$ for just one a, then $b = e$.*
8. *If $a * a = a$, then $a = e$.* [The only idempotent in a group is the identity.]
9. $(a^{-1})^{-1} = a$.
10. $(a * b)^{-1} = b^{-1} * a^{-1}$.

Problem 2.2 *Prove Theorem 2.2.*

Problem 2.3 *Restate Theorem 2.2 for a group $(G, +)$ with identity 0. (See Definition 2.4.)*

Problem 2.4 *Give a specific example of a group and two specific elements a and b in the group such that $(a * b)^{-1} \neq a^{-1} * b^{-1}$.*

Problem 2.5 *Let $*$ be an associative binary operation on the set S and let $a, b, c, d \in S$. Prove the following statements. [Be careful what you assume.]*

1. $(a * b) * (c * d) = ((a * b) * c) * d$.

2. $(a * b) * (c * d) = a * (b * (c * d))$.

3. *In 1. and 2. we see three different ways to properly place parentheses in the product:* $a * b * c * d$*? Find all possible ways to properly place parentheses in the product* $a*b*c*d$ *and show that all lead to the same element in* S.

Theorem 2.3 (The Generalized Associative Law) *Let* $*$ *be an associative binary operation on a set* S*. If* $a_1, a_2, \ldots, a_n$ *is a sequence of* $n \geq 3$ *elements of* S*, then the product*

$$a_1 * a_2 * \cdots * a_n$$

is unambiguous; that is, the same element will be obtained regardless of how parentheses are inserted in the product (in a legal manner).

Proof The case $n = 3$ is just the associative law itself. The case $n = 4$ is established in Problem 2.5. The general case can be proved by induction on n. The details are quite technical, so to save time, we will omit them. One of the problems is stating precisely what is meant by "inserting the parentheses in a legal manner". The interested reader can find a proof in most introductory abstract algebra books. See for example Chapter 1.4 of the book **Basic Algebra I** [9] by Nathan Jacobson.

Remark. From now on, unless stated to the contrary, we will assume the Generalized Associative Law. That is, we will place parentheses in a product at will without a detailed justification. *Note, however, the order may still be important, so unless the binary operation is commutative we must still pay close attention to the order of the elements in a product or sum.*

Problem 2.6 *Show that if* a_1, a_2, a_3 *are elements of a group then*

$$(a_1 * a_2 * a_3)^{-1} = a_3^{-1} * a_2^{-1} * a_1^{-1}.$$

Show that in general if $n \in \mathbb{N}$ *and* $a_1, a_2, \ldots, a_n$ *are elements of a group then*

$$(a_1 * a_2 * \cdots * a_n)^{-1} = a_n^{-1} * \cdots * a_2^{-1} * a_1^{-1}.$$

Now that we have the Generalized Associative Law, we can define a^n for $n \in \mathbb{Z}$.

Definition 2.5 *Let $(G, *)$ be a group with identity e. Let a be any element of G. We define integral powers a^n, $n \in \mathbb{Z}$, as follows:*

$$\begin{aligned} a^0 &= e \\ a^1 &= a \\ a^{-1} &= \text{the inverse of } a \end{aligned}$$

and for $n \geq 2$:

$$\begin{aligned} a^n &= a^{n-1} * a \\ a^{-n} &= (a^{-1})^n \end{aligned}$$

Using this definition, it is easy to establish the following important theorem.

Theorem 2.4 (Laws of Exponents for Groups) *Let $(G, *)$ be a group with identity e. Then for all $n, m \in \mathbb{Z}$ we have*

$$a^n * a^m = a^{n+m} \quad \text{for all } a \in G,$$

$$(a^n)^m = a^{nm} \quad \text{for all } a \in G,$$

and whenever $a, b \in G$ and $a * b = b * a$ we have

$$(a * b)^n = a^n * b^n. \blacksquare$$

This theorem is easy to check for $n, m \in \mathbb{N}$. A complete proof for $n, m \in \mathbb{Z}$ involves a number of cases and is a little tedious, but the following problem gives some indication of how this could be done.

Problem 2.7 *Let $(G, *)$ be a group with identity e. Prove using Definition 2.5 the following special cases of Theorem 2.4. For $a, b \in G$:*

1. $a^2 * a^3 = a^5$.
2. $a^2 * a^{-6} = a^{-4}$.
3. $a^{-2} * a^6 = a^4$.
4. $a^{-2} * a^{-3} = a^{-5}$
5. $a^{-2} * a^2 = a^0$.
6. *Assuming $a * b = b * a$, $a^3 * b^3 = (a * b)^3$.*

7. *Assuming* $a * b = b * a$, $a^{-3} * b^{-3} = (a * b)^{-3}$.

Problem 2.8 *Restate Definition 2.5 for additive notation.* (In this case a^n is replaced by na.)

Problem 2.9 *Restate Theorem 2.4 for a group whose operation is* $+$.

Answer to question on page 11: An abelian grape.

Chapter 3

The Symmetric Groups

Recall that if n is a positive integer, $[n] = \{1, 2, \ldots, n\}$. A **permutation** of $[n]$ is a one-to-one, onto function from $[n]$ to $[n]$ and S_n is the set of all permutations of $[n]$. If these terms are not familiar, it would be a good idea to take some time to study Appendix B before proceeding.

Let us discuss the different ways to specify a function from $[n]$ to $[n]$ and how to tell when we have a permutation. It is traditional (but not compulsory) to use lower case Greek letters such as σ, τ, α, β, etc., to indicate elements of S_n. To be specific let $n = 4$. We may define a function $\sigma : [4] \to [4]$ by specifying its values at the elements $1, 2, 3$, and 4. For example, let's say:

$$\sigma(1) = 2 \qquad \sigma(2) = 3 \qquad \sigma(3) = 1 \qquad \sigma(4) = 4.$$

Another way to specify σ is by exhibiting a table which gives its value:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}.$$

We call this the *two line* or *two row* notation. The function σ just defined is one-to-one and onto, that is, it is a permutation of $[4]$.

For another example, let

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 1 & 4 \end{pmatrix}.$$

The function τ is not one-to-one since $1 \neq 3$ but $\tau(1) = \tau(3)$. This problem can always be identified by the existence of the same element more than

once in the second line of the two line notation. τ is also not onto since the element 2 does not appear in the second line.

Let

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

be the two line notation of an arbitrary function $\sigma : [n] \to [n]$. Then:

(1) σ is *one-to-one* if and only if no element of $[n]$ appears more than once in the second line.

(2) σ is *onto* if and only if every element of $[n]$ appears in the second line at least once.

Thus σ is a permutation if and only if the second row is just a rearrangement or shuffling of the numbers $1, 2, \ldots, n$.

The composition of two permutations:

If σ and τ are elements of S_n, then $\sigma\tau$ is defined to be the **composition** of the functions σ and τ. That is, $\sigma\tau$ is the function whose rule is given by:

$$\sigma\tau(x) = \sigma(\tau(x)), \quad \text{for all } x \in [n].$$

We sometimes call $\sigma\tau$ simply the *product* of σ and τ. Let's look at an example to see how this works. Let σ and τ be defined as follows:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

It follows that

$$\begin{array}{lllll} \sigma\tau(1) & = & \sigma(\tau(1)) & = & \sigma(2) = 1 \\ \sigma\tau(2) & = & \sigma(\tau(2)) & = & \sigma(3) = 3 \\ \sigma\tau(3) & = & \sigma(\tau(3)) & = & \sigma(1) = 2 \end{array}$$

Thus we have

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

One can also find products of permutations directly from the two line notation as follows:

$$\text{First Step:} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & - & - \end{pmatrix}$$

$$\text{Second Step:} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & - \end{pmatrix}$$

$$\text{Third Step:} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Problem 3.1 *Compute the following products in S_4:*

$$(1) \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$(2) \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$(3) \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$(4) \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Whenever we need to prove two functions are equal, we require the following definition:

Definition 3.1 *If $\sigma : A \to B$ and $\tau : A \to B$ are functions then $\sigma = \tau$ if and only if*

$$\sigma(x) = \tau(x), \quad \textit{for all } x \in A.$$

In particular, if σ and τ are in S_n then $\sigma = \tau$ if and only if

$$\sigma(x) = \tau(x), \quad \textit{for all } x \in [n].$$

The identity of S_n:

The identity of S_n is the so-called **identity function**

$$\iota : [n] \to [n].$$

which is defined by the rule:

$$\iota(x) = x, \quad \text{for all } x \in [n].$$

In the two line notation ι is described by

$$\iota = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

The function ι is clearly one-to-one and onto and satisfies

$$\iota\sigma = \sigma \quad \text{and} \quad \sigma\iota = \sigma, \qquad \text{for all } \sigma \in S_n.$$

So ι is the identity of S_n with respect to the binary operation of composition. [Note that we use the Greek letter ι (iota) to indicate the identity of S_n.]

The inverse of an element $\sigma \in S_n$:

If $\sigma \in S_n$, then by definition $\sigma : [n] \to [n]$ is one-to-one and onto. Hence the rule

$$\sigma^{-1}(y) = x \quad \text{if and only if} \quad \sigma(x) = y$$

defines a function $\sigma^{-1} : [n] \to [n]$. The function σ^{-1} is also one-to-one and onto (check this!) and satisfies

$$\sigma\sigma^{-1} = \iota \qquad \text{and} \qquad \sigma^{-1}\sigma = \iota,$$

so it is the inverse of σ in the group sense also.

In terms of the two line description of a permutation, if

$$\sigma = \begin{pmatrix} \cdots & x & \cdots \\ \cdots & y & \cdots \end{pmatrix}$$

then

$$\sigma^{-1} = \begin{pmatrix} \cdots & y & \cdots \\ \cdots & x & \cdots \end{pmatrix}$$

The inverse of a permutation in the two line notation may be obtained by interchanging the two lines and then reordering the columns so that the numbers on the top line are in numerical order. Here's an example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Interchanging the two lines we have:

$$\begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}.$$

Reordering the columns we obtain

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Problem 3.2 *Find the inverses of each of the following permutations in two line notation. Check in each case that* $\sigma\sigma^{-1} = \iota$ *and* $\sigma^{-1}\sigma = \iota$.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

Theorem 3.1 *For any three functions*

$$\alpha : A \to B, \quad \beta : B \to C, \quad \gamma : C \to D$$

we have

$$(\gamma\beta)\alpha = \gamma(\beta\alpha).$$

Proof Let $x \in A$. Then

$$(\gamma\beta)\alpha(x) = \gamma\beta(\alpha(x)) = \gamma(\beta(\alpha(x))).$$

and

$$\gamma(\beta\alpha)(x) = \gamma(\beta\alpha(x)) = \gamma(\beta(\alpha(x))).$$

It follows that

$$(\gamma\beta)\alpha(x) = \gamma(\beta\alpha)(x) \quad \text{for all } x \in A.$$

Hence $(\gamma\beta)\alpha = \gamma(\beta\alpha)$.

Corollary 3.2 *The binary operation of composition on S_n is associative.*

With this corollary, we complete the proof that S_n under the binary operation of composition is a group.

The Cycle Diagram of a Permutation

An important way to visualize an element σ of S_n is as follows. Arrange n dots in the plane. Number the dots 1 through n. For all $i \in [n]$, if $\sigma(i) = j$ draw an arrow from dot number i to dot number j. We call this picture the **cycle diagram** of σ. To get a nice picture, it is best to use the following technique for drawing the diagram.

1. Draw a dot and number it 1. Let $i_1 = \sigma(1)$. If $i_1 \neq 1$ draw another dot and label it i_1.

2. Draw an arrow from dot 1 to dot i_1. (Note that $i_1 = 1$ is possible.)

3. Assume that dots numbered $1, i_1, i_2, \ldots, i_k$ have been drawn. Consider two cases:

   (i) There is an arrow leaving every dot drawn so far. In this case let i_{k+1} be the smallest number in $[n]$ not yet labeling a dot. If there are no such then stop, you have completed the diagram, otherwise draw a new dot and label it i_{k+1}

   (ii) There is a dot numbered j with no arrow leaving it. In this case let $i_{k+1} = \sigma(j)$. If there is no dot labeled i_{k+1} draw a new dot and label it i_{k+1}. Draw an arrow from dot j to dot i_{k+1}.

4. Now repeat step 3 with $k + 1$ replacing k.

Example 3.1 *: The cycle diagram of the following permutation is given in Figure 3.1.*

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 11 & 7 & 6 & 5 & 4 & 3 & 10 & 2 & 12 & 14 & 1 & 15 & 9 & 8 \end{pmatrix}.$$

Notice that the diagram consists of five "cycles": one "6-cycle", one "4-cycle", two "2-cycles" and one "1-cycle". Every cycle diagram will look something like this. That's why we call it the cycle diagram.

[diagram goes here]

The cycle diagram of α from Exercise 3.1

Problem 3.3 *Draw the cycle diagrams for all 24 elements of S_4. You will need a systematic way to list the elements S_4 to make sure you have not missed any.*

We now give a more precise definition of a "cycle".

Definition 3.2 *Let $i_1, i_2, \ldots, i_k$ be a list of k distinct elements from $[n]$. Define a permuation σ in S_n as follows:*

$$\begin{array}{rcl} \sigma(i_1) & = & i_2 \\ \sigma(i_2) & = & i_3 \\ \sigma(i_3) & = & i_4 \\ \vdots & \vdots & \vdots \\ \sigma(i_{k-1}) & = & i_k \\ \sigma(i_k) & = & i_1 \end{array}$$

and if $x \notin \{i_1, i_2, \ldots, i_k\}$ then

$$\sigma(x) = x$$

Such a permutation is called a **cycle** *or a k-***cycle** *and is denoted by*

$$(i_1\ i_2\ \cdots\ i_k).$$

If $k = 1$ then the cycle $\sigma = (i_1)$ is just the identity function, i.e., $\sigma = \iota$.

For example, let σ be the 3-cycle defined by $\sigma = (3\ 2\ 1)$. σ may be considered as an element of S_3 in which case in two line notation we have

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Notice that according to the definition if $x \notin \{3, 2, 1\}$ then $\sigma(x) = x$. So we could also consider (3 2 1) as an element of S_4. In which case we would have:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

Or we could consider (3 2 1) as an element of S_5. In which case we would have:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}.$$

Similarly, (3 2 1) could be an element of S_n for any $n \geq 3$. Note also that we could specify the same permutation by any of the following

$$\sigma = (3\ 2\ 1), \quad \sigma = (2\ 1\ 3), \quad \sigma = (1\ 3\ 2).$$

In this case, there are three numbers 1, 2, 3 in the cycle, and we can begin the cycle with any one of these. In general, there are k different ways to write a k-cycle. One can start with any number in the cycle.

Problem 3.4 Below are listed 5 different cycles in S_5.
(a) Describe each of the given cycles in two line notation.
(b) Draw the cycle diagram of each cycle.

1. (4)
2. (3 4)
3. (4 1 5)
4. (1 3 5 4)
5. (1 3 5 4 2)

Definition 3.3 *Two cycles* $(i_1\ i_2\ \cdots\ i_k)$ *and* $(j_1\ j_2\ \cdots\ j_\ell)$ *are said to be* **disjoint** *if the sets* $\{i_1, i_2, \ldots, i_k\}$ *and* $\{j_1, j_2, \ldots, j_\ell\}$ *are disjoint.*

So, for example, the cycles (1 2 3) and (4 5 8) are disjoint, but the cycles (1 2 3) and (4 2 8) are not disjoint.

Theorem 3.3 *If* σ *and* τ *are disjoint cycles, then* $\sigma\tau = \tau\sigma$.

Proof Let $\sigma = (a_1 \cdots a_k)$ and $\tau = (b_1 \cdots b_\ell)$. Let $\{c_1, \cdots, c_m\}$ be the elements of $[n]$ that are in neither $\{a_1, \ldots, a_k\}$ nor $\{b_1, \cdots, b_\ell\}$. Thus

$$[n] = \{a_1, \ldots, a_k\} \cup \{b_1, \cdots, b_\ell\} \cup \{c_1, \cdots, c_m\}.$$

We want to show $\sigma\tau(x) = \tau\sigma(x)$ for all $x \in [n]$. To do this we consider first the case $x = a_i$ for some i. Then $a_i \notin \{b_1, \cdots, b_\ell\}$ so $\tau(a_i) = a_i$. Also $\sigma(a_i) = a_j$, where $j = i + 1$ or $j = 1$ if $i = k$. So also $\tau(a_j) = a_j$. Thus

$$\sigma\tau(a_i) = \sigma(a_i) = a_j = \tau(a_j) = \tau(\sigma(a_i) = \tau\sigma(a_i).$$

Thus, $\sigma\tau(a_i) = \tau\sigma(a_i)$. It is left to the reader to show that $\sigma\tau(x) = \tau\sigma(x)$ if $x = b_i$ or $x = c_i$, which will complete the proof.

Problem 3.5 *Show by example that if two cycles are not disjoint they need not commute.*

Theorem 3.4 *Every element $\sigma \in S_n$, $n \geq 2$, can be written as a product*

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_m \tag{3.1}$$

where $\sigma_1, \sigma_2, \ldots, \sigma_m$ are pairwise disjoint cycles, that is, for $i \neq j$, σ_i and σ_j are disjoint. If all 1-cycles of σ are included, the factors are unique except for the order. ■

The factorization (3.1) is called the **disjoint cycle decomposition of** σ.

To save time we omit a formal proof of this theorem. The process of finding the disjoint cycle decomposition of a permutation is quite similar to finding the cycle diagram of a permutation. Consider, for example, the permutation $\alpha \in S_{15}$

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 11 & 7 & 6 & 5 & 4 & 3 & 10 & 2 & 12 & 14 & 1 & 15 & 9 & 8 \end{pmatrix}.$$

The disjoint cycle decomposition of α is

$$\alpha = (1\ 13\ 15\ 8\ 10\ 12)(2\ 11\ 14\ 9)(3\ 7)(4\ 6)(5).$$

Compare this with the cycle diagram given for this same permutation on page **??**. To obtain this, one starts a cycle with 1, since $\alpha(1) = 13$ we

have the partial cycle (1 13. Next, we observe that $\alpha(13) = 15$. This gives the partial cycle (1 13 15. We continue in this way till we obtain the cycle (1 13 15 8 10 12). Then we pick the smallest number in [15] not used so far, namely, 2. We start a new cycle with 2: Noting that $\alpha(2) = 11$ we have the partial cycle (2 11. Continuing we obtain the cycle (2 11 14 9). And we continue in this way till all the elements of [15] are in some cycle.

Problem 3.6 *Find the disjoint cycle decomposition of the following permutations in S_6:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 6 & 5 & 1 \end{pmatrix}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 3 & 6 \end{pmatrix}$$

Problem 3.7 *Find the disjoint cycle decomposition of the following permutations in S_6: [Each permutation is given as a product of cycles. Try to do this without converting the cycle notation to the two line notation.]*

(1) (1 2 3)(2 4 5)
(2) (3 4 5 1 2)(4 5 6)(1 2 3)
(3) (1 3)(1 2)
(4) (1 4)(1 3)(1 2)

Problem 3.8 *(a) Verify that if a, b, c, d, e are distinct elements of $[n]$ then each of the following cycles can be written as a product of 2-cycles: [Hint: look at (3) and (4) in Problem 3.7.] (b) Verify that the inverse of each of these cycles is a cycle of the same size.*

(1) (a b c).
(2) (a b c d)
(3) (a b c d e).

Definition 3.4 *An element of S_n is called a* **transposition** *if and only if it is a 2-cycle.*

Note that the transposition $(i\ j)$ interchanges i and j and leaves the other elements of $[n]$ fixed. It *transposes* i and j.

Definition 3.5 *An integer n is* **even** *if $n = 2k$ for some integer k. It is* **odd** *if $n = 2k + 1$ for some integer k. The* **parity** *of an integer is the property of being even or odd. Two integers have the* **same parity** *if they are both even or if they are both odd. They have* **different parity** *if one is even and the other is odd.*

Theorem 3.5 *Every element of S_n can be written as a product of transpositions. The factors of such a product are not unique, however, if $\sigma \in S_n$ can be written as a product of k transpositions and if the same σ can also be written as a product of ℓ transpositions, then k and ℓ have the same parity.* ■

The first part of this theorem is easy. Generalizing Problem 3.8, we see that every cycle can be written as a product of transpositions as follows:

$$(i_1\ i_2\ i_3\ \cdots i_k) = (i_1\ i_k)\cdots(i_1\ i_3)(i_1\ i_2).$$

Then, since each permutation is a product of cycles, we can obtain each permutation as a product of transpositions. The second part is more difficult to prove and, in the interest of time, we omit the proof. A nice proof may be found in Fraleigh ([1], page 108.)

Problem 3.9 *Write the permutation α on page* **??** *as a product of transpositions. Do it in more than one way. How many transpositions are in each of your products?*

Problem 3.10 *Give the disjoint cycle decomposition of each of the 6 elements of S_3. Also write each element of S_3 as a product of transpositions.*

Definition 3.6 *A permutation is* ***even*** *if it is a product of an even number of transpositions and is* ***odd*** *if it is a product of an odd number of transpositions. We define the function* $\text{sign} : S_n \to \{1, -1\}$ *by*

$$\text{sign}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

If $n = 1$ then there are no transpositions. In this case to be complete we define the identity permutation ι to be ***even****.*

Problem 3.11 *Show that the function* sign *satisfies*

$$\text{sign}(\sigma\tau) = \text{sign}(\sigma)\text{sign}(\tau)$$

for all σ *and* τ *in* S_n.

Remark. Let $A = [a_{ij}]$ be an $n \times n$ matrix. The determinant of A may be defined by the sum

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

For example, if $n = 2$ we have only two permutations ι and (1 2). Since $\text{sign}(\iota) = 1$ and $\text{sign}((1\ 2)) = -1$ we obtain

$$\det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

Problem 3.12 *Find the sign of each element of* S_3 *and use this information to write out the formula for* $\det(A)$ *when* $n = 3$. *(Note that in this case the determinant is a sum of 6 terms.)*

Problem 3.13 *If* $n = 10$ *how many terms are in the above formula for the determinant?*

Definition 3.7 *If* $(G, *)$ *is a group, the number of elements in* G *is called the* ***order*** *of* G. *We use* $|G|$ *to denote the order of* G.

Note that $|G|$ may be finite or infinite. If it is finite $|G| = n$ for some positive integer n. An interesting but difficult problem is that of determining all groups of a fixed order n. For small n this can be done as we shall see, but there seems to be no hope of answering the question for all values of n in spite of the efforts of many mathematicians who specialize in the study of finite groups.

Problem 3.14 *Find* $|GL(2, \mathbb{Z}_2)|$ *and* $|M_2(\mathbb{Z}_2)|$.

Theorem 3.6 $|S_n| = n!$ *for all* $n \geq 1$.

Proof Let n be any positive integer. Elements of S_n have the form

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}$$

where $a_1, a_2, \dots, a_n$ is any rearrangement of the numbers $1, 2, \dots, n$. So the problem is how many ways can we select the $a_1, a_2, \dots, a_n$? Note that there are n ways to select a_1. Once a choice is made for a_1, there are $n-1$ remaining possibilities for a_2. Thus, there are altogether $n(n-1)$ ways to select $a_1 a_2$. Then, for each choice of $a_1 a_2$, there are $n-2$ remaining possibilities for a_3. Thus, there are $n(n-1)(n-2)$ ways to select $a_1 a_2 a_3$. Continuing in this way, we see that there are

$$n(n-1)(n-2)\cdots 2 \cdot 1 = n!$$

ways to choose $a_1, a_2, \dots, a_n$. ■

Problem 3.15 *Show that the inverse of a k-cycle is also an k-cycle. Hint: Show that if $a_1, a_2, \dots, a_k$ are distinct elements of $[n]$ then*

$$(a_1\ a_2)^{-1} = (a_2\ a_1)$$
$$(a_1\ a_2\ a_3)^{-1} = (a_3\ a_2\ a_1)$$
$$(a_1\ a_2\ a_3\ a_4)^{-1} = (a_4\ a_3\ a_2\ a_1)$$

and more generally

$$(a_1\ a_2\ \cdots\ a_k)^{-1} = (a_k\ \cdots\ a_2\ a_1)$$

Hint: Let $\sigma = (a_1\ a_2\ \cdots\ a_k)$ and $\tau = (a_k\ \cdots\ a_2\ a_1)$. Show that $\tau(\sigma(a_i)) = a_i$ for all i by considering three cases: $i \notin \{1, 2, \dots, k\}$, $i \in \{1, 2, \dots, k-1\}$ and $i = k$.

Problem 3.16 *Show that if σ is a k-cycle then* $\operatorname{sign}(\sigma) = 1$ *if k is odd and* $\operatorname{sign}(\sigma) = -1$ *if k is even.*

Problem 3.17 (Challenge Problem) *For $\sigma \in S_n$ prove that*

$$\sigma \text{ is even} \iff \prod_{i<k} \frac{\sigma(k) - \sigma(i)}{k - i} = 1$$
$$\sigma \text{ is odd} \iff \prod_{i<k} \frac{\sigma(k) - \sigma(i)}{k - i} = -1$$

Chapter 4

Subgroups

From now on, unless otherwise stated, G will denote a group whose binary operation is denoted by $a \cdot b$ or simply ab for $a, b \in G$. The identity of G will be denoted by e and the inverse of $a \in G$ will be denoted by a^{-1}. Sometimes, however, we may need to discuss groups whose operations are thought of as addition. In such cases we write $a + b$ instead of ab. Also in this case, the identity is denoted by 0 and the inverse of $a \in G$ is denoted by $-a$. Definitions and results given using multiplicative notation can always be translated to additive notation if necessary.

Definition 4.1 Let G be a group. A **subgroup** of G is a subset H of G which satisfies the following three conditions:

1. $e \in H$.
2. If $a, b \in H$, then $ab \in H$.
3. If $a \in H$, then $a^{-1} \in H$.

For convenience we sometimes write $H \leq G$ to mean that H is a subgroup of G.

Problem 4.1 *Translate the above definition into additive notation.*

Remark If H is a subgroup of G, then the binary operation on G when restricted to H is a binary operation on H. From the definition, one may easily show that a subgroup H is a group in its own right with respect to this binary operation. Many examples of groups may be obtained in this way. In fact, in a way we will make precise later, every finite group may be thought of as a subgroup of one of the groups S_n.

Problem 4.2 *Prove that if G is any group, then*

1. $\{e\} \leq G$.
2. $G \leq G$.

The subgroups $\{e\}$ and G are said to be **trivial** subgroups of G.

Problem 4.3 *(a) Determine which of the following subsets of S_4 are subgroups of S_4.*

1. $H = \{\iota, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$
2. $K = \{\iota, (1\ 2\ 3), (1\ 3\ 2)\}$
3. $J = \{\iota, (1\ 2), (1\ 2\ 3)\}$
4. $L = \{\sigma \in S_4 \mid \sigma(1) = 1\}$.

(b) Determine which of the following subsets of $\mathbb{Z}_{12}$ are subgroups of $\mathbb{Z}_{12}$. (Here the binary operation is addition modulo 12.)

1. $A = \{0, 3, 6, 9, \}$
2. $B = \{0, 6\}$
3. $C = \{0, 1, 2, 3, 4, 5\}$

(c) Determine which of the following subsets of $\mathbb{Z}$ are subgroups of $\mathbb{Z}$. (Here the binary operation is addition.)

1. $U = \{5k \mid k \in \mathbb{Z}\}$
2. $V = \{5k + 1 \mid k \in \mathbb{N}\}$
3. $W = \{5k + 1 \mid k \in \mathbb{Z}\}$

Problem 4.4 *Let*

$$SL(2, \mathbb{R}) = \{A \in GL(2, \mathbb{R}) \mid \det(A) = 1\}.$$

Prove that $SL(2, \mathbb{R}) \leq GL(2, \mathbb{R})$.

$SL(2, \mathbb{R})$ is called the *Special Linear Group of Degree 2 over* $\mathbb{R}$

Problem 4.5 *For $n \in \mathbb{N}$, let A_n be the set of all even permutations in the group S_n. Show that A_n is a subgroup of S_n.*

A_n is called the **alternating group of degree** n.

Problem 4.6 *List the elements of A_n for $n = 1, 2, 3, 4$. Based on this try to guess the order of A_n for $n > 4$.*

Definition 4.2 *Let a be an element of the group G. If there exists $n \in \mathbb{N}$ such that $a^n = e$ we say that a has **finite order**. and we define*

$$\mathrm{o}(a) = \min\{n \in \mathbb{N} \,|\, a^n = e\}$$

*If $a^n \neq e$ for all $n \in \mathbb{N}$, we say that a has **infinite order** and we define*

$$\mathrm{o}(a) = \infty.$$

*In either case we call $\mathrm{o}(a)$ the **order** of a.*

Note carefully the difference between the order of a group and the order of an element of a group. Some authors make matters worse by using the same notation for both concepts. Maybe by using different notation it will make it a little easier to distinguish the two concepts.

If $n \geq 2$, to prove that $\mathrm{o}(a) = n$ we must show that $a^i \neq e$ for $i = 1, 2, \ldots, n-1$ and $a^n = e$. Note also that $a = e$ if and only if $\mathrm{o}(a) = 1$. So every element of a group other than e has order $n \geq 2$ or ∞.

Problem 4.7 *Translate the above definition into additive notation. That is, define the order of an element of a group G with binary operation $+$ and identity denoted by 0.*

Problem 4.8 *Find the order of each element of S_3.*

Problem 4.9 *Find the order of a k-cycle when $k = 2, 3, 4, 5$. Guess the order of a k-cycle for arbitrary k.*

Problem 4.10 *Find the order of the following permutations:*

(a) (1 2)(3 4 5)

(b) (1 2)(3 4)(5 6 7 8)

(c) (1 2)(3 4)(5 6 7 8)(9 10 11)

(d) Try to find a rule for computing the order of a product disjoint cycles in terms of the sizes of the cycles.

Problem 4.11 *Find the order of each element of the group* $(\mathbb{Z}_6, +)$.

Problem 4.12 *Find the order of each element of* $GL(2, \mathbb{Z}_2)$. *[Recall that* $GL(2, \mathbb{Z}_2)$ *is the group of all* 2×2 *matrices with entries in* Z_2 *with non-zero determinant. Recall that* $\mathbb{Z}_2 = \{0, 1\}$ *and the operations are multiplication and addition modulo 2.]*

Problem 4.13 *Find the order of the element 2 in the group* $(\mathbb{R} - \{0\}, \cdot)$. *Are there any elements of finite order in this group?*

Definition 4.3 *Let* a *be an element of the group* G. *Define*

$$\langle a \rangle = \{a^i : i \in \mathbb{Z}\}.$$

We call $\langle a \rangle$ *the* ***subgroup of*** G ***generated by*** a.

Remark Note that

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots\}.$$

In particular, $a = a^1$ and $e = a^0$ are in $\langle a \rangle$.

Problem 4.14 *Translate the above definition of* $\langle a \rangle$ *and the remark into additive notation.*

Theorem 4.1 *For each* a *in the group* G, $\langle a \rangle$ *is a subgroup of* G. $\langle a \rangle$ *contains* a *and is the smallest subgroup of* G *that contains* a.

Proof As just noted $e = a^0 \in \langle a \rangle$. Let $a^n, a^m \in \langle a \rangle$. Since $n + m \in \mathbb{Z}$ it follows from Theorem 2.4 that

$$a^n a^m = a^{n+m} \in \langle a \rangle.$$

Also from Theorem 2.4, if $a^n \in \langle a \rangle$, since $n(-1) = -n$ we have

$$(a^n)^{-1} = a^{-n} \in \langle a \rangle.$$

This proves that $\langle a \rangle$ is a subgroup.

Since $a = a^1$ it is clear that $a \in \langle a \rangle$. If H is any subgroup of G that contains a, since H is closed under taking products and taking inverses, $a^n \in \langle a \rangle$ for every $n \in \mathbb{Z}$. So $\langle a \rangle \subseteq H$. That is, every subgroup of G that contains a also contains $\langle a \rangle$. This implies that $\langle a \rangle$ is the smallest subgroup of G that contains a.

Theorem 4.2 *Let G be a group and let $a \in G$. If $\mathrm{o}(a) = 1$, then $\langle a \rangle = \{e\}$. If $\mathrm{o}(a) = n$ where $n \geq 2$, then*

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

and the elements $e, a, a^2, \ldots, a^{n-1}$ are distinct, that is,

$$\mathrm{o}(a) = |\langle a \rangle|.$$

Proof Assume that $\mathrm{o}(a) = n$. The case $n = 1$ is left to the reader. Suppose $n \geq 2$. We must prove two things.

1. If $i \in \mathbb{Z}$ then $a^i \in \{e, a, a^2, \ldots, a^{n-1}\}$.
2. The elements $e, a, a^2, \ldots, a^{n-1}$ are distinct.

To establish 1 we note that if i is any integer we can write it in the form $i = nq + r$ where $r \in \{0, 1, \ldots, n-1\}$. Here q is the quotient and r is the remainder when i is divided by n. Now using Theorem 2.4 we have

$$a^i = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r.$$

This proves 1. To prove 2, assume that $a^i = a^j$ where $0 \leq i < j \leq n-1$. It follows that

$$a^{j-i} = a^{j+(-i)} = a^j a^{-i} = a^i a^{-i} = a^0 = e.$$

But $j - i$ is a positive integer less than n, so $a^{j-i} = e$ contradicts the fact that $\mathrm{o}(a) = n$. So the assumption that $a^i = a^j$ where $0 \leq i < j \leq n-1$ is false. This implies that 2 holds. It follows that $\langle a \rangle$ contains exactly n elements, that is, $\mathrm{o}(a) = |\langle a \rangle|$.

Theorem 4.3 *If G is a finite group, then every element of G has finite order.*

Proof Let a be any element of G. Consider the infinite list

$$a^1, a^2, a^3, \ldots, a^i, \ldots$$

of elements in G. Since G is finite, all the elements in the list cannot be different. So there must be positive integers $i < j$ such that $a^i = a^j$. Since $i < j$, $j - i$ is a positive integer. Then using Theorem 2.4 we have

$$a^{j-i} = a^{j+(-i)} = a^j a^{-i} = a^i a^{-i} = a^0 = e.$$

That is, $a^n = e$ for the positive integer $n = j - i$. So a has finite order, which is what we wanted to prove.

Problem 4.15 *For each choice of G and each given $a \in G$ list all the elements of the subgroup $\langle a \rangle$ of G.*

1. $G = S_3$, $a = (1\ 2)$.
2. $G = S_3$, $a = (1\ 2\ 3)$.
3. $G = S_4$, $a = (1\ 2\ 3\ 4)$.
4. $G = S_4$, $a = (1\ 2)(3\ 4)$.
5. $G = \mathbb{Z}$, $a = 5$.
6. $G = \mathbb{Z}$, $a = -1$.
7. $G = \mathbb{Z}_{15}$, $a = 5$.
8. $G = \mathbb{Z}_{15}$, $a = 1$.
9. $G = GL(2, \mathbb{Z}_2)$, $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
10. $G = GL(2, \mathbb{R})$, $a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Problem 4.16 *Suppose a is an element of a group and $o(a) = n$. Prove that $a^m = e$ if and only if $n \mid m$. [Hint: The Division Algorithm from Appendix C may be useful for the proof in one direction.]*

Chapter 5

The Group of Units of $\mathbb{Z}_n$

Definition 5.1 *Let $n \geq 2$. An element $a \in \mathbb{Z}_n$ is said to be a **unit** if there is an element $b \in \mathbb{Z}_n$ such that $ab = 1$. Here the product is multiplication modulo n. We denote the set of all units in $\mathbb{Z}_n$ by U_n.*

Note that 2 is a unit in $\mathbb{Z}_5$ since $2 \cdot 3 = 1$. Since the multiplication is commutative, 2 and 3 are both units. We say that 2 and 3 are inverses of each other. But note that if we write $2^{-1} = 3$, we must keep in mind that by 2^{-1} in this context we do not mean the rational number $1/2$. The following theorem is easy to prove if we assume that multiplication modulo n is associative and commutative.

Theorem 5.1 *U_n is a group under multiplication modulo n.* ■

We call U_n the **group of units of $\mathbb{Z}_n$**.

Problem 5.1 *List all the elements of U_n for $n \in \{2, 3, 4, \ldots, 12\}$.*

Problem 5.2 *For which $n \in \{2, 3, 4, \ldots, 12\}$ is there an element $a \in U_n$ such that $U_n = \langle a \rangle$?*

Theorem 5.2 *For $n \geq 2$, $U_n = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$.* ■

Remark. This theorem is established in number theory courses. In number theory, the order of the group U_n is important enough to have its own name and notation. The order of U_n is denoted by $\phi(n)$, is called the *Euler totient function* and is pronounced *fee of n*. In number theory it is proved that if a

and b are positive integers such that $\gcd(a,b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$ and if p is prime and $n \in \mathbb{N}$ then $\phi(p^n) = p^n - p^{n-1}$. These facts make it easy to compute $\phi(n)$ if one can write n as a product of primes. But there is no known easy way to compute $\phi(n)$ if the factorization of n is unknown.

Note that there are four different but similar symbols used in mathematics:

1. ϕ : lower case Greek letter phi (pronounced *fee*)
2. Φ : capital Greek letter Phi
3. φ : lower case script Greek letter phi
4. $\emptyset$: slashed zero (not Greek, but Danish) and symbol for the empty set

Problem 5.3 *Prove the easy part of Theorem 5.2; namely, show that if $a \in \mathbb{Z}_n$ and $\gcd(a,n) = d > 1$, then a is not a unit. [Hint: Show (1) that if $a \in \mathbb{Z}_n$ and $\gcd(a,n) = d > 1$ there is an element $b \in \mathbb{Z}_n - \{0\}$ such that $ab = 0$. (2) If $b \in \mathbb{Z}_n - \{0\}$ and $ab = 0$ then a is not a unit.]*

Theorem 5.3 *If p is a prime then there is an element $a \in U_p$ such that $U_p = \langle a \rangle$.* ■

Proof. This theorem is proved in advanced courses in number theory or abstract algebra.

Problem 5.4 *Demonstrate Theorem 5.3 for all primes $p < 12$.*

Remark It will be noted that sometimes even when n is not prime there is an $a \in U_n$ such that $U_n = \langle a \rangle$. In fact, the following theorem from advanced number theory tells us exactly when such an a exists.

Theorem 5.4 *If $n \geq 2$ then U_n contains an element a satisfying $U_n = \langle a \rangle$ if and only if a has one of the following forms: 2, 4, p^k, or $2p^k$ where p is an odd prime and $k \in \mathbb{N}$.* ■

So, for example, there is no such a in U_n if $n = 2^k$ when $k \geq 3$, nor for $n = 12$ or 15.

Chapter 6

Direct Products of Groups

Recall that the Cartesian product $X_1 \times X_2 \times \cdots \times X_n$ of n sets $X_1, X_2, \ldots, X_n$ is the set of all ordered n-tuples $(x_1, x_2, \ldots, x_n)$ where $x_i \in X_i$ for all $i \in \{1, 2, \ldots, n\}$. Equality for n-tuples is defined by

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \iff x_i = y_i \text{ for all } i \in \{1, 2, \ldots, n\}.$$

Definition 6.1 *If $G_1, G_2, \ldots, G_n$ is a list of n groups we make the Cartesian product $G_1 \times G_2 \times \cdots \times G_n$ into a group by defining the binary operation*

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_n \cdot b_n).$$

Here for each $i \in \{1, 2, \ldots, n\}$ the product $a_i \cdot b_i$ is the product of a_i and b_i in the group G_i. We call this group the ***direct product*** *of the groups $G_1, G_2, \ldots, G_n$.*

As an example, consider the direct product $\mathbb{Z}_2 \times \mathbb{Z}_3$ of the two groups $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0),\ (0,1),\ (0,2),\ (1,0),\ (1,1),\ (1,2)\}.$$

We add modulo 2 in the first coordinate and modulo 3 in the second coordinate. Since the binary operation in each factor is addition, we use $+$ for the operation in the direct product. So, for example, in this group

$$(1,1) + (1,1) = (1+1, 1+1) = (0,2).$$

The identity is clearly $(0,0)$ and, for example, the inverse of $(1,1)$ is $(1,2)$. It is clear that this is a group. More generally we have the following result.

Theorem 6.1 *If $G_1, G_2, \ldots, G_n$ is a list of n groups the direct product $G = G_1 \times G_2 \times \cdots \times G_n$ as defined above is a group. Moreover, if for each i, e_i is the identity of G_i then $(e_1, e_2, \ldots, e_n)$ is the identity of G, and if*

$$\mathbf{a} = (a_1, a_2, \ldots, a_n) \in G$$

then the inverse of $\mathbf{a}$ *is given by*

$$\mathbf{a}^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$$

where a_i^{-1} is the inverse of a_i in the group G_i. ■

Problem 6.1 *Prove the above theorem for the special case $n = 2$.*

Problem 6.2 *Find the order of each of the following groups. Also give the identity of each group and the inverse of just one element of the group other than the identity.*

1. $\mathbb{Z}_2 \times \mathbb{Z}_2$
2. $\mathbb{Z}_3 \times S_3 \times U_5$
3. $\mathbb{Z} \times \mathbb{Z}_3 \times \mathbb{Z}_2$
4. $GL(2, \mathbb{Z}_2) \times \mathbb{Z}_4 \times U_7 \times \mathbb{Z}_2$

Chapter 7

Isomorphism of Groups

Two groups may look different yet be essentially the same. This concept of *sameness* is formalized in mathematics by the concept of *isomorphism* (from the Greek: *isos* meaning the same and *morphe* meaning form). Before we give a precise definition of isomorphism, let's look at some small groups and see if we can see whether or not they meet our intuitive notion of sameness.

Problem 7.1 *Go through the examples of groups we have covered so far and make a list of all those with order* ≤ 12*. List them according to their orders. For example, the following groups have order 6:*

$$GL(2,\mathbb{Z}_2), \quad \mathbb{Z}_6, \quad S_3, \quad U_7, \quad U_9, \quad \mathbb{Z}_2 \times \mathbb{Z}_3.$$

Make a similar list for all integers from 1 to 12.

Definition 7.1 *Let* $G = \{g_1, g_2, \ldots, g_n\}$*. Let* $o(g_i) = k_i$ *for* $i = 1, 2, \ldots, n$*. We say that the sequence* $(k_1, k_2, \ldots, k_m)$ *is the* ***order sequence*** *of the group* G*. To make the sequence unique we assume that the elements are ordered so that* $k_1 \leq k_2 \leq \cdots \leq k_n$*.*

For example, the order sequence of S_3 is $(1, 2, 2, 2, 3, 3)$.

Problem 7.2 *Consider the following list of properties that may be used to distinguish groups.*

1. *The order of the group.*
2. *The order sequence of the group.*

3. *Whether the group is abelian or not.*

Look carefully at the groups in the list you made for the previous problem and see which may be distinguished by one or more of the three listed properties.

Definition 7.2 *Let $(G, *)$ and $(H, \bullet)$ be groups. A function $f : G \to H$ is said to be a* ***homomorphism*** *from G to H if*

$$f(a * b) = f(a) \bullet f(b)$$

for all $a, b \in G$. If in addition f is one-to-one and onto, f is said to be an ***isomorphism*** *from G to H.*

We say that G and H are ***isomorphic*** *if and only if there is an isomorphism from G to H. We write $G \cong H$ to indicate that G is isomorphic to H.*

Examples 7.1 *Some familiar examples of homomorphisms and isomorphisms are:*

1. $\det : GL(2, \mathbb{R}) \to \mathbb{R} - \{0\}$ *is a homomorphism since*

$$\det(AB) = \det(A) \det(B)$$

for all $A, B \in GL(2, \mathbb{R})$.

2. $sign : S_n \to \{1, -1\}$ *is a homomorphism since*

$$sign(\sigma\tau) = sign(\sigma) sign(\tau)$$

for all $\sigma, \tau \in S_n$.

3. $\log : \mathbb{R}^+ \to \mathbb{R}$, *where $\mathbb{R}^+$ denotes the positive real numbers and the operations are respectively multiplication and addition, is an isomorphism since from calculus we know that* log *is one-to-one and onto and*

$$\log(xy) = \log(x) + \log(y)$$

for all positive real numbers x and y. [Here $\log(x) = \ln(x)$.]

4. $\exp : \mathbb{R} \to \mathbb{R}^+$, *where* $\mathbb{R}^+$ *denotes the positive real numbers and the operations are respectively addition and multiplication, is an isomorphism since from calculus we know that* exp *is one-to-one and onto and*

$$\exp(x+y) = \exp(x)\exp(y)$$

for all real numbers x *and* y. *Note that* $\exp(x)$ *is an alternative notation for* e^x.

The last two examples show that the group of positive real numbers under multiplication is isomorphic to the group of all real numbers under addition.

Theorem 7.1 (Isomorphism is An Equivalence Relation) *If* G, H *and* K *are groups then*

1. $G \cong G$,
2. *If* $G \cong H$ *then* $H \cong G$, *and*
3. *If* $G \cong H$ *and* $H \cong K$, *then* $G \cong K$.

Problem 7.3 *Prove Theorem 7.1.*

Problem 7.4 *Prove that every group of order 1 is isomorphic to the group* U_2.

Problem 7.5 *Prove that every group of order 2 is isomorphic to the group* $\mathbb{Z}_2$.

Problem 7.6 *Prove that every group of order 3 is isomorphic to the group* $\mathbb{Z}_3$.

Problem 7.7 *Prove that if* G *and* H *are isomorphic groups then* $|G| = |H|$.

Problem 7.8 *Prove that if* G *and* H *are groups then* $G \times H \cong H \times G$.

Theorem 7.2 *Let* $(G, *)$ *and* $(H, \bullet)$ *be groups and let* $f : G \to H$ *be a homomorphism. Let* e_G *denote the identity of* G *and,* e_H *denote the identity of* H. *Then*

1. $f(e_G) = e_H$,

2. $f(a^{-1}) = f(a)^{-1}$, *and*

3. $f(a^n) = f(a)^n$ *for all* $n \in \mathbb{Z}$.

Problem 7.9 *Prove parts 1 and 2 of Theorem 7.2.*

Problem 7.10 *Prove part 3 of Theorem 7.2 for* $n = 2, -2, 3, -3$.

The general case of Theorem 7.2 can be proved by induction on n. We will come back to this later.

Problem 7.11 *Restate Theorem 7.2 (a) in the case that both* G *and* H *use additive notation, (b) in the case where* G *uses additive notation and* H *uses multiplicative notation, and (c) in the case where* G *uses multiplicative notation and* H *uses additive notation.*

Theorem 7.3 *Let* $(G, *)$ *and* $(H, \bullet)$ *be groups and let* $f : G \to H$ *be an isomorphism. Then* $\mathrm{o}(a) = \mathrm{o}(f(a))$ *for all* $a \in G$. *It follows that* G *and* H *have the same number of elements of each possible order.*

Problem 7.12 *Prove Theorem 7.3. Hint: Use the Theorem 7.2.*

Theorem 7.4 *If* G *and* H *are isomorphic groups, and* G *is abelian, then so is* H.

Problem 7.13 *Prove Theorem 7.4.*

Definition 7.3 *A group* G *is* ***cyclic*** *if there is an element* $a \in G$ *such that* $\langle a \rangle = G$. *If* $\langle a \rangle = G$ *then we say that* a *is a* ***generator*** *for* G.

Problem 7.14 *Find an example of a cyclic group that has more than one generator.*

Theorem 7.5 *If* G *and* H *are isomorphic groups and* G *is cyclic then* H *is cyclic.*

Problem 7.15 *Prove Theorem 7.5.*

Problem 7.16 *Determine which of the following groups are cyclic and which are not cyclic.*

1. $\mathbb{Z}$ *under ordinary addition.*
2. $\mathbb{Z}_n$ *under addition modulo* n.
3. U_n *for* $n \leq 12$.
4. S_3.
5. $\mathbb{Z}_2 \times \mathbb{Z}_3$.
6. $\mathbb{Z}_2 \times \mathbb{Z}_2$.
7. $\mathbb{Z}_3 \times \mathbb{Z}_5$.
8. A_3.
9. S_4.
10. $GL(2, \mathbb{Z}_2)$.

Problem 7.17 (Challenge Problem) *Prove that if* G *is a finite cyclic group of order* n *then* G *has* $\phi(n)$ *generators. Hint: Let* $G = \langle a \rangle$. *Show than an element* $b = a^i \in G$ *is a generator of* G *if and only if* $\gcd(i, n) = 1$.

Theorem 7.6 *Let* a *be an element of a group* G.

1. *If* $o(a) = \infty$ *then* $\langle a \rangle \cong \mathbb{Z}$.
2. *If* $o(a) = n \in \mathbb{N}$ *then* $\langle a \rangle \cong \mathbb{Z}_n$.

Proof of 1 Assume that $o(a) = \infty$. Define the function $\varphi : \mathbb{Z} \to \langle a \rangle$ by the rule $\varphi(n) = a^n$ for $n \in \mathbb{Z}$. φ is onto by definition of $\langle a \rangle$. To prove that φ is one-to-one let $\varphi(n) = \varphi(m)$ for some $n, m \in \mathbb{Z}$. Then $a^n = a^m$. If $n \neq m$ by symmetry we can assume $n < m$. Then

$$e = a^0 = a^{n-n} = a^n a^{-n} = a^m a^{-n} = a^{m-n}.$$

But $n < m$ so $m - n \in \mathbb{N}$. This contradicts the assumption that $o(a) = \infty$. So we must have $n = m$. This shows that φ is one-to-one. Since

$$\varphi(n + m) = a^{n+m} = a^n a^m = \varphi(n)\varphi(m)$$

φ is a homomorphism and it follows that φ is an isomorphism. Hence $\mathbb{Z} \cong \langle a \rangle$. By Theorem 7.1 $\langle a \rangle \cong \mathbb{Z}$.

Proof of 2 Assume that $o(a) = n \in \mathbb{N}$. For our proof we need to introduce the following notation from Appendix C.

Definition 7.4 *Let $n \in \mathbb{N}$. For each $a \in \mathbb{Z}$ by the Division Algorithm there are unique integers q and r satisfying*

$$a = nq + r \qquad \text{and} \qquad 0 \leq r < n.$$

We denote r by $a \bmod n$. That is, $a \bmod n$ is the remainder when a is divided by n.

Now using this we can define precisely addition modulo n by the rule:

$$a \oplus b = (a + b) \bmod n.$$

Note that here we write $a + b$ for addition in $\mathbb{Z}$ and $a \oplus b$ for addition in $\mathbb{Z}_n$. So to be precise, by $\mathbb{Z}_n$ we mean the group $(\mathbb{Z}_n, \oplus)$.

Recall that $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$. On the other hand by Theorem 4.2 since $o(a) = n$ we have

$$\langle a \rangle = \{a^0, a^1, \ldots, a^{n-1}\}.$$

So the mapping $\varphi : \mathbb{Z}_n \to \langle a \rangle$ defined by the rule $\varphi(i) = a^i$ for $i = 0, 1, 2, \ldots, n-1$, is clearly one-to-one and onto. It remains to show that φ is a homomorphism. To prove this note first that $i \oplus j = r$ means that $i + j = qn + r$ where $0 \leq r \leq n - 1$. Now we have

$$\begin{aligned} \varphi(i \oplus j) &= \varphi(r) = a^r = a^{i+j-qn} = a^i a^j a^{-qn} = a^i a^j (a^n)^{-q} \\ &= a^i a^j e^{-q} = a^i a^j e = a^i a^j = \varphi(i)\varphi(j). \end{aligned}$$

Hence $\varphi(i \oplus j) = \varphi(i)\varphi(j)$. That is, φ is a homomorphism. Since it is also one-to-one and onto it is an isomorphism. Hence $\mathbb{Z}_n \cong \langle a \rangle$ and by Theorem 7.1 $\langle a \rangle \cong \mathbb{Z}_n$. ■

Problem 7.18 *Prove that if G is a cyclic group then G is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$.*

The above shows that a group generated by one element is easily describable. What about groups that are not generated by one element but are "generated" by two (or more elements)? The following exercise introduces a notation to make precise such matters.

Problem 7.19 (Challenge Problem) *Let G be a group and let $S \subset G$. Define $\langle S \rangle$ to be the subset of G whose elements have the form $s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n}$ where $n \in \mathbb{N}$, $s_i \in S$ and $\epsilon_i = \pm 1$ for $i = 1, 2, \ldots, n$. Prove*

1. *$\langle S\rangle$ is a subgroup of G.*

2. *$\langle S\rangle$ is the smallest subgroup of G that contains S, that is, if K is a subgroup of G and $S \subset K$ then $\langle S\rangle \subset K$.*

3. *Show that for $n \geq 3$ the group S_n is not cyclic, but $S_n = \langle\{\tau, \sigma\}\rangle$ where $\tau = (1\ 2)$ and $\sigma = (1\,2\,\cdots\,n)$.*

Note that the above problem shows that although S_n, $n \geq 3$, is not cyclic, it is generated by two elements. However, unlike the cyclic groups one can say very little about groups generated by two elements.

You may be interested in the curious fact (first discovered by Philip Hall) that $(A_5)^{19}$ (*i.e.*, the direct product of 19 copies of the alternating group of degree 5) can be generated by two elements, but $(A_5)^{20}$ cannot. On the other hand, the group $(\mathbb{Z}_2)^n$, that is, the direct product of n copies of $\mathbb{Z}_2$, requires a minimum of n generators for each positive integer n.

We state without proof the following theorem. A proof may be found, in any of the references [1, 2, 3, 4].

Theorem 7.7 (Cayley's Theorem) *If G is a finite group of order n, then there is a subgroup H of S_n such that $G \cong H$.* ■

This makes precise the idea that every finite group is "contained" in S_n for some positive integer n. For example, the group $U_8 = \{1, 3, 5, 7\}$ is isomorphic to the subgroup

$$H = \{\iota, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

of S_4. Note that a group of order k may well be isomorphic to a subgroup of S_n where $n < k$.

Problem 7.20 *Find a group of order 120 which is ismorphic to a subgroup of S_n where $n < 120$.*

Chapter 8

Cosets and Lagrange's Theorem

Definition 8.1 *Let G be a group and let H be a subgroup of G. For each element a of G we define*

$$aH = \{ah \mid h \in H\}.$$

We call aH the ***coset of H in G generated by*** *a.*

Remark In the case of additive notation the coset of H in G generated by a is written in the form

$$a + H = \{a + h \mid h \in H\}$$

Sometimes aH is called a *left coset* and the set $Ha = \{ha \mid h \in H\}$ is called a *right coset*. Since we will only use left cosets, we will leave off the modifier *left*.

Problem 8.1 *Here we consider all the cosets of a particular subgroup of the group U_{13}. Recall that*

$$U_{13} = \{1, 2, \ldots, 11, 12\}$$

and that the element $2 \in U_{13}$ has order 12, so

$$U_{13} = \{1, 2, 2^2, 2^3, \ldots, 2^{11}\}.$$

Since 2 has order 12, $2^{12} = 1$, but $2^i \neq 1$ for $1 \leq i \leq 11$. It follows that $(2^4)^2 = 2^8 \neq 1$, but $(2^4)^3 = 2^{12} = 1$. Hence 2^4 has order 3 so

$$H = \langle 2^4 \rangle = \{1, 2^4, 2^8\}$$

is a subgroup of U_{13}.

Show that the subgroup H *just defined has exactly four different cosets in* U_{13}. *Note that if we list all the cosets*

$$2H,\ 2^2H,\ 2^3H,\ \ldots,\ 2^{11}H,\ 2^{12}H,$$

it appears that there are 12 cosets. Show however that there are only four different cosets.

Note that none of the cosets overlap, that is, if two cosets are different, then their intersection is the empty set. Also note that every element of U_{13} *is in one and only one of the four different cosets and each coset of* H *has the same number of elements as* H.

Problem 8.2 *Find all cosets of the subgroup* $H = \langle (1\ 2) \rangle$ *of the group* S_3.

Problem 8.3 *Let* G *be a finite group and let* H *be a subgroup of* G. *Let* $a, b \in G$. *Prove the following statements.*

1. $a \in aH$.
2. $|aH| = |H|$.
3. *If* $aH \cap bH \neq \emptyset$, *then* $aH = bH$.

Remark Suppose $G = \{g_1, g_2, \ldots, g_n\}$ is a group with n elements and $H \leq G$. Then if we form the list of *all* cosets of H in G we have

$$g_1H, g_2H, \ldots, g_nH.$$

But as noted in the above examples some of the cosets in this list are repeated several times. If we remove all repetitions from the list we are left with what we shall call the *distinct* cosets of H in G. If there are s distinct cosets we may denote them by $a_1H, a_2H, \ldots, a_sH$.

Theorem 8.1 (Lagrange's Theorem) *If* G *is a finite group and* $H \leq G$ *then* $|H|$ *divides* $|G|$.

Proof Let n be the order of G, and let k be the order of H. We want to show that $k \mid n$. Let $a_1H, a_2H, \ldots, a_sH$ be the distinct cosets of H in G.

Note that s is the number of distinct cosets. By Problem 8.3, these cosets are pairwise disjoint and their union is the whole group. That is,

$$G = a_1H \cup a_2H \cup \cdots \cup a_sH \quad \text{and } a_iH \cap a_jH = \emptyset \text{ when } i \neq j.$$

Since also each coset has the same number of elements as H, we have

$$\begin{aligned} |G| &= |a_1H| + |a_2H| + \cdots + |a_sH| \\ &= |H| + |H| + \cdots + |H| \\ &= k + k + \cdots + k \\ &= ks. \end{aligned}$$

It follows that $n = ks$. This shows that $k \mid n$, and proves the theorem.

The following problems give some important corollaries of Lagrange's Theorem.

Problem 8.4 *Prove that if G is a finite group and $a \in G$ then $o(a)$ divides $|G|$.*

Problem 8.5 *Prove that if G is a finite group and $a \in G$ then $a^{|G|} = e$.*

Problem 8.6 *Prove that if p is a prime and a is a non-zero element of $\mathbb{Z}_p$ then $a^{p-1} = 1$.* [Here the product is multiplication modulo p.] *In number theory this is called* Fermat's Little Theorem

Problem 8.7 *Prove that if $n \in \mathbb{N}$ and $a \in U_n$ then $a^{\phi(n)} = 1$.* [Here the product is multiplication modulo n.] *In number theory this is called* Euler's Theorem.

Problem 8.8 *Prove that if $|G| = p$ where p is a prime then G is a cyclic group.*

Problem 8.9 *Prove that if G and H are groups of order p where p is prime then $G \cong H$.*

Problem 8.10 *Let G be a group. Prove the following statements.*

1. *If $|G| = 2$ then $G \cong \mathbb{Z}_2$.*

2. *If* $|G| = 3$ *then* $G \cong \mathbb{Z}_3$.

3. *If* $|G| = 5$ *then* $G \cong \mathbb{Z}_5$.

Note that we have seen the first two items previously. But now we may give easier proofs.

Problem 8.11 *Find two groups of order 4 that are not isomorphic.*

Problem 8.12 *Find two groups of order 6 that are not isomorphic.*

Definition 8.2 *We say that there are* k ***isomorphism classes of groups of order*** n *if there are* k *groups* $G_1, G_2, \ldots, G_k$ *such that (1) if* $i \neq j$ *then* G_i *and* G_j *are not isomorphic, and (2) every group of order* n *is isomorphic to* G_i *for some* $i \in \{1, 2, \ldots, k\}$.

This is sometimes expressed by saying that *there are* k *groups of order* n *up to isomorphism* or that *there are* k *non-isomorphic groups of order* n.

In more advanced courses in algebra, it is shown that the number of isomorphism classes of groups of order n for $n \leq 17$ is given by the following table:

Order :	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Number :	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1

This table means, for example, that one may find 14 groups of order 16 such that every group of order 16 is isomorphic to one and only one of these 14 groups.

Gordon Royle has such a list for groups of order up to 1000 (with the exception of orders 512 and 768). It is interesting to note that the largest number of groups seems to appear when the order is a power of 2, that is for 2, 4, 8, 16 32, etc. There are, for example, 56092 non-isomorphic groups of order 256. For the entire list go to Gordon Royle's homepage at

http://www.cs.uwa.edu.au/~gordon/

and follow the link to **Combinatorial Data**. In a recent paper *The groups of order at most 2000* by H. U. Besche, B. Eick, and E. A. O'Brien it is announced that they have been able to extend known results so that the number of groups of each order up to 2000 is now known. The research announcement may be found at

http://www.ams.org/jourcgi.

In Table 8.1, we list the ten most challenging orders as taken from the paper by Besche, *et al* and the number of groups of each order. It is interesting to note that according to this paper there are 49, 487,365,422 groups of order 2^{10} and only 423,164,062 remaining groups of order ≤ 2000. Thus in excess of 99 % of the groups of order ≤ 2000 are of order 2^{10}.

Table 8.1: The ten most difficult orders

Order	Number
2^{10}	49 487 365 422
$2^9 \cdot 3$	408 641 062
2^9	10 494 213
$2^8 \cdot 5$	1 116 461
$2^8 \cdot 3$	1 090 235
$2^8 \cdot 7$	1 083 553
$2^7 \cdot 3 \cdot 5$	241 004
$2^7 \cdot 3^2$	157 877
2^8	56 092
$2^6 \cdot 3^3$	47 937

At the opposite extreme there are some orders for which there is only one isomorphism class of groups. For example, there is only one isomorphism class of groups of order n if n is prime. But there are some non-primes that have this property, for example, 15.

No formula is known for the number of isomorphism classes of groups of order n. Although the number isomorphism classes of groups of order n is not known in general, it is possible to calculate easily the number of isomorphism classes of *abelian* groups of order n using the following famous theorem which we state without proof.

The Fundamental Theorem of Finite Abelian Groups *If G is a finite abelian group of order at least two then*

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_s^{n_s}}$$

where for each i, p_i is a prime and n_i is a positive integer. Moreover, the prime powers $p_i^{n_i}$ are unique except for the order of the factors. ■

If the group G in the above theorem has order n then

$$n = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}.$$

So the p_i may be obtained from the prime factorization of the order of the group G. These primes are not necessarily distinct, so we cannot say what the n_i are. However, we can find all possible choices for the n_i. For example, if G is an abelian group of order $72 = 3^2 \cdot 2^3$ then G is isomorphic to one and only one of the following groups. Note that each corresponds to a way of factoring 72 as a product of prime powers.

$\mathbb{Z}_9 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$72 = 9 \cdot 2 \cdot 2 \cdot 2$
$\mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	$72 = 9 \cdot 4 \cdot 2$
$\mathbb{Z}_9 \times \mathbb{Z}_8$	$72 = 9 \cdot 8$
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$72 = 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2$
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2$	$72 = 3 \cdot 3 \cdot 4 \cdot 2$
$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_8$	$72 = 3 \cdot 3 \cdot 8$

Thus there are exactly 6 non-isomorphic abelian groups of order 72.

Corollary *For $n \geq 2$, the number of isomorphism classes of abelian groups of order n is equal to the number of ways to factor n as a product of prime powers (where the order of the factors does not count).* ■

Problem 8.13 *Determine the number of non-isomorphic abelian groups of order n where $n \in \{4, 6, 8, 16, 1800\}$*

Problem 8.14 *Prove that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.*

Remark: In number theory it is proven that if $n = ab$ and $\gcd(a, b) = 1$ then $\mathbb{Z}_n \cong \mathbb{Z}_a \times \mathbb{Z}_b$. This is called the *Chinese Remainder Theorem*.

Chapter 9

Introduction to Ring Theory

Definition 9.1 *A **ring** is an ordered triple $(R, +, \cdot)$ where R is a set and $+$ and $\cdot$ are binary operations on R satisfying the following properties:*

A1 $a + (b + c) = (a + b) + c$ *for all* a, b, c *in* R.

A2 $a + b = b + a$ *for all* a, b *in* R.

A3 *There is an element* $0 \in R$ *satisfying* $a + 0 = a$ *for all* a *in* R.

A4 *For every* $a \in R$ *there is an element* $b \in R$ *such that* $a + b = 0$.

M1 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ *for all* a, b, c *in* R.

D1 $a \cdot (b + c) = a \cdot b + a \cdot c$ *for all* a, b, c *in* R.

D2 $(b + c) \cdot a = b \cdot a + c \cdot a$ *for all* a, b, c *in* R.

Terminology If $(R, +, \cdot)$ is a ring, the binary operation $+$ is called *addition* and the binary operation $\cdot$ is called *multiplication. In the future we will usually write* ab *instead of* $a \cdot b$. The element 0 mentioned in A3 is called the **zero** of the ring. Note that we have not assumed that 0 behaves like a *zero*, that is, we have not assumed that $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$. What A3 says is that 0 is an identity with respect to addition. Note that *negative* (as the opposite of *positive*) has no meaning for most rings. We do not assume that multiplication is commutative and we have not assumed that there is an identity for multiplication, much less that elements have inverses with respect to multiplication.

Definition 9.2 *The element b mentioned in A4 is written $-a$ and we call it* minus a *or the* additive inverse *of a. Subtraction in a ring is defined by the rule $a - b = a + (-b)$ for all a, b in R.*

Unless otherwise stated, from now on we will refer to the ring R rather than the ring $(R, +, \cdot)$. Of course, if we define a ring, we must say what the binary operations of addition and multiplication are.

Problem 9.1 *How could one state properties A1–A4 in a more compact manner using previous definitions?*

Definition 9.3 *Let R be a ring. If there is an identity with respect to multiplication, it is called the* ***identity*** *of the ring and is usually denoted by* 1. *If such an element exists, we say that R is a* ***ring with identity****.*

In some cases, the identity of a ring may be denoted by some symbol other than 1 such as e or I.

Definition 9.4 *We say that a ring R is* ***commutative*** *if the multiplication is commutative. Otherwise, the ring is said to be* ***non-commutative****.*

Note that the addition in a ring is always commutative, but the multiplication may not be commutative.

Definition 9.5 *A ring R is said to be an* ***integral domain*** *if the following conditions hold:*

1. *R is commutative.*
2. *R contains an identity $1 \neq 0$.*
3. *If $a, b \in R$ and $ab = 0$ then either $a = 0$ or $b = 0$.*

Definition 9.6 *A ring R is said to be a* ***field*** *if it satisfies the following properties.*

1. *R is commutative.*
2. *R contains an identity $1 \neq 0$.*
3. *For each $x \in R$ such that $x \neq 0$, there is a $y \in R$ such that $xy = 1$.*

Problem 9.2 *Which of the following are rings? If so which have identities, which are commutative, which are integral domains and which are fields?*

1. $(\mathbb{N}, +, \cdot)$.
2. $(2\mathbb{Z}, +, \cdot)$ *where* $2\mathbb{Z}$ *is the set of even integers.*
3. $(\mathbb{R}, +, \cdot)$.
4. $(\mathbb{Q}, +, \cdot)$.
5. $(\mathbb{Z}, +, \cdot)$.
6. $(\mathbb{Z}_2, +, \cdot)$.
7. $(\mathbb{Z}_3, +, \cdot)$.
8. $(\mathbb{Z}_4, +, \cdot)$.
9. $(M_2(\mathbb{R}), +, \cdot)$.
10. $(M_2(\mathbb{Z}_n), +, \cdot)$.

Definition 9.7 *Let R be a ring with an identity 1. An element $a \in R$ is said to be a* ***unit*** *of R if there is an element $b \in R$ such that $ab = ba = 1$. We let $U(R)$ denote the set of all units of R. If such a b exists we write $b = a^{-1}$. We sometimes call a^{-1} the* multiplicative inverse *of a.*

It is easy to see that if R is a ring with identity 1, then $U(R)$ is a group under multiplication. It is called the **group of units** of R.

Example 9.1 (The ring $F[x]$ of polynomials in x over the field F.) Let F be a field. A **polynomial** in the indeterminate (or variable) x over F is an expression of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where the coefficients a_i are elements of the field F and n may be any non-negative integer. The rules for multiplication and addition of polynomials are exactly as in high school algebra. The only exception is that we permit the coefficients to be from any field F, and when coefficients are added or multiplied, we use the binary operations in F. This ring is usually denoted by $F[x]$. For each field F the ring $F[x]$ is an integral domain. But $F[x]$ is not a field since the only units of $F[x]$ are the non-zero constants, that is polynomials of the form a_0 where a_0 is a non-zero element of F.

Problem 9.3 *Find the group of units of each of the following rings:* $\mathbb{Z}$, $\mathbb{R}$, $M_2(\mathbb{R})$, $\mathbb{Z}_n$.

Definition 9.8 *If R is a ring, $a \in R$ and $n \in \mathbb{N}$ we define a^n by the following rules:*

$a^1 = a$,

$a^n = aa \cdots a$ *(n copies of a) if $n \geq 2$.*

If R has an identity 1 and a is a unit then we can also define:

$a^0 = 1$,

a^{-1} = *multiplicative inverse of a,*

$a^{-n} = (a^{-1})^n$ *for $n \geq 2$.*

Note that since generally an element a of a ring is not a unit, we cannot expect a^n to be defined for negative integers.

Problem 9.4 *What is the smallest ring? What is the smallest field?*

Theorem 9.1 *Let R be a ring and let a, b, $c \in R$. Then the following hold.*

1. *If $a + b = a + c$ then $b = c$.*
2. *If $a + b = 0$ then $b = -a$.*
3. $-(-a) = a$.
4. $-(a + b) = (-a) + (-b)$.
5. $a0 = 0$ *and* $0a = 0$.
6. $a(-b) = (-a)b = -(ab)$.
7. $(-a)(-b) = ab$.
8. $a(b - c) = ab - ac$.
9. $(b - c)a = ba - ca$.

Problem 9.5 *Prove Theorem 9.1.*

Problem 9.6 *Show that condition 3 in the definition of integral domain can be replaced by the following cancellation law:*

If a, b, $c \in R$, $a \neq 0$ and $ab = ac$ then $b = c$.

Problem 9.7 *Prove that every field is an integral domain. Show by example that the converse of this statement is not true.*

Problem 9.8 *Prove that $\mathbb{Z}_n$ is a field if and only if it is an integral domain.*

Problem 9.9 *Prove that $\mathbb{Z}_n$ is a field if and only if n is a prime.*

Definition 9.9 *Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be two rings. A function*

$$f : R \to S$$

is a ***homomorphism*** *if for all $a, b \in R$ we have*

$$\begin{aligned} f(a \cdot b) &= f(a) \odot f(b) \\ f(a + b) &= f(a) \oplus f(b). \end{aligned}$$

If also f is one-to-one and onto we call f an ***isomorphism****. In this case we say R and S are* ***isomorphic*** *and write $R \cong S$.*

Although it will usually be clear from the context, now that we have homomorphisms for both groups and rings, sometimes we will say *ring homomorphism* or *group homomorphism* to be specific. Similarly, for isomorphisms.

As in the case of groups, if two rings are isomorphic, then they share almost all properties of interest. For example, if R and S are isomorphic rings, then R is a field if and only if S is a field. We will give a non-trivial example below of two isomorphic rings.

Definition 9.10 *A subset S of a ring R is said to be a* ***subring*** *of R if the following conditions hold:*

1. $0 \in S$.

2. *If $a \in S$, then $-a \in S$.*

3. *If $a, b \in S$, then $a + b \in S$ and $ab \in S$.*

If R is a field and the following conditions also hold:

4. $1 \in S$.

5. *If $a \neq 0$ and $a \in S$, then $a^{-1} \in S$.*

we say that S is a ***subfield*** *of R.*

If S is a subring (subfield) of the ring (field) R, then it is easy to verify that S is itself a ring (field) with respect to the addition and multiplication on R. Some obvious examples are the following.

1. $\mathbb{Z}$ is a subring of $\mathbb{Q}$ and of $\mathbb{R}$.
2. $\mathbb{Q}$ is a subfield of $\mathbb{R}$.
3. $2\mathbb{Z}$ is a subring of $\mathbb{Z}$.

Problem 9.10 *Prove that there is no element $x \in \mathbb{Q}$ such that $x^2 = 2$.*

Problem 9.11 *Assume there is a positive element $\sqrt{2} \in \mathbb{R}$ such that*

$$(\sqrt{2})^2 = 2.$$

Define the following subset of $\mathbb{R}$:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Prove that $\mathbb{Q}(\sqrt{2})$ is a subfield of $\mathbb{R}$. (The tricky part is showing that all non-zero elements are units.)

Problem 9.12 *Let*

$$S = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}.$$

1. *Show that S is a subring of the ring $M_2(\mathbb{Q})$.*
2. *Show that $S \cong \mathbb{Q}(\sqrt{2})$.*

Chapter 10

Axiomatic Treatment of $\mathbb{R}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{C}$

There are several ways to axiomatize the standard number systems $\mathbb{R}$, $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$. One way is to start by laying down axioms for $\mathbb{N}$ and then using $\mathbb{N}$ and set theory to build successively the number systems $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$. A quicker way is to start with axioms for $\mathbb{R}$ and using these axioms find $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ inside of $\mathbb{R}$. We follow the latter approach here. We begin by defining an *ordered ring*.

Definition 10.1 *An **ordered ring** is a quadruple*

$$(R, +, \cdot, <)$$

where $(R, +, \cdot)$ is a commutative ring and $<$ is a binary relation on R which satisfies the following properties for all $a, b, c \in R$.

1. *$a < b$ and $b < c \Longrightarrow a < c$.*

2. *$a < b \Longrightarrow a + c < b + c$.*

3. *$a < b$ and $0 < c \Longrightarrow ac < bc$.*

4. *Given $a, b \in R$* one and only one *of the following holds:*

$$a = b, \quad a < b, \quad b < a.$$

Note that we could develop some of the theory of ordered rings without the assumption of commutativity; however, this assumption will make things a little easier. All of the ordered rings we are interested in are commutative anyhow.

Terminology The binary relation $<$ is as usual called *less than*. Condition 1 above is called *transitivity* and condition 4 is called the *Law of Trichotomy*. We also refer to $<$ as an *ordering* or *order relation* on the ring R. We use the following abbreviations:

$$\begin{aligned} b > a &\iff a < b \\ a \leq b &\iff a < b \text{ or } a = b \\ b \geq a &\iff a \leq b \\ a < b < c &\iff a < b \text{ and } b < c \\ a \leq b \leq c &\iff a \leq b \text{ and } b \leq c \end{aligned}$$

An element a is said to be **positive** if $a > 0$ and, **negative** if $a < 0$. Note that $-a$ may be positive or negative, depending on whether or not a is positive or negative. Hence it is best to read $-a$ as *minus* a rather that *negative* a.

Problem 10.1 *Let R be an ordered ring with identity $1 \neq 0$. Prove that for all $a, b, c \in R$ the following statements hold:*

1. $0 < a$ *and* $0 < b \Longrightarrow 0 < ab$.
2. $a < 0 \Longrightarrow 0 < -a$.
3. $0 < 1$.
4. $a \neq 0 \Longrightarrow 0 < a^2$.
5. *If* $a < b$ *and* $c < d$ *then* $a + c < b + d$.
6. $a < b \Longrightarrow -b < -a$.
7. $a < b$ *and* $c < 0 \Longrightarrow bc < ac$.
8. *If a is a unit and* $0 < a$ *then* $0 < a^{-1}$.
9. *If a is a unit and* $0 < a < 1$ *then* $1 < a^{-1}$.
10. *R is infinite.*

Note that some rings cannot be ordered. For example, the last statement of the above problem shows that there is no way to make the rings $\mathbb{Z}_n$ into ordered rings. As we shall see the field of complex numbers is an infinite ring that cannot be made into an ordered ring. We will give a rigorous definition of the complex numbers later. The main examples of ordered rings are $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$.

Problem 10.2 *Show that if a ring R has an identity $1 \neq 0$ and contains an element i such that $i^2 = -1$, then R cannot be an ordered ring.*

If an ordered ring R is a integral domain (or field), we call R an **ordered domain** (or **ordered field**). Now we can distinguish $\mathbb{Z}$ from $\mathbb{Q}$ and $\mathbb{R}$ by the fact that $\mathbb{Z}$ is an ordered domain and not an ordered field, whereas both $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields. The problem is how to distinguish $\mathbb{Q}$ from $\mathbb{R}$. This was historically a difficult thing to accomplish. The first clue was the fact that $\sqrt{2}$ is not a rational number. To describe the difference, we need a few more definitions.

Definition 10.2 *Let R be an ordered ring. Let S be a subset of R. An element b of R is called an **upper bound** for S if $x \leq b$ for all $x \in S$. If S has an upper bound we say that S is **bounded from above**.*

Problem 10.3 *Give examples of subsets S of $\mathbb{R}$ satisfying the following conditions:*

1. *S has no upper bound.*

2. *S has an upper bound $b \in S$.*

3. *S is bounded from above but has no upper bound $b \in S$.*

Definition 10.3 *Let S be a subset of an ordered ring R which is bounded from above. An element $\ell \in R$ is a **least upper bound (l.u.b)** for S if ℓ is an upper bound for S and $\ell \leq b$ for all upper bounds b of S.*

Problem 10.4 *Give least upper bounds for the following subsets of $\mathbb{R}$.*

1. $[0, 1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$.
2. $[0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$.

Definition 10.4 *An ordered field R is said to be* ***complete*** *if it satisfies the following:*

Least Upper Bound Axiom *Every non-empty subset of R which is bounded from above has a least upper bound.*

Theorem 10.1 *There exists a complete ordered field. Any two such fields are isomorphic.*

The proof of this is beyond the scope of this course. Many books on analysis begin by just assuming that there exists such a field. Actually we began this course by assuming familiarity with $\mathbb{R}$ as well as $\mathbb{N}$, $\mathbb{Q}$ and $\mathbb{Z}$.

Definition 10.5 *The* unique *complete ordered field whose existence is asserted by Theorem 10.1 is called the* ***field of real numbers*** *and denote by* $\mathbb{R}$.

All properties of the real numbers follow from the defining properties of a complete ordered field. For example, one can prove that if $a \in \mathbb{R}$ and $a > 0$, then there is a unique element $x \in \mathbb{R}$ such that $x^2 = a$ and $x > 0$.

It can be shown that $\mathbb{Q}$ is not complete. For example, the set

$$S = \{x \in \mathbb{Q} \,|\, x^2 < 2\}$$

is bounded from above but has no least upper bound in $\mathbb{Q}$. Since we assume $\mathbb{R}$ is complete, the set S does have a least upper bound ℓ in $\mathbb{R}$ which one can prove is positive and satisfies $\ell^2 = 2$.

We also observe that just as we defined subtraction in a ring by the rule

$$a - b = a + (-b),$$

we define division in a field as follows:

Definition 10.6 *Let a and b be elements of a field. If $b \neq 0$ we define*

$$a/b = \frac{a}{b} = a \div b = a \cdot b^{-1}$$

where b^{-1} is the inverse of b with respect to multiplication.

Under the assumption of the existence of a complete ordered field $\mathbb{R}$, we can define $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ as follows. First we define $\mathbb{N}$.

Definition 10.7 *Say that a subset S of $\mathbb{R}$ is* ***inductive*** *if it satisfies both of the following conditions:*

1. $1 \in S$.
2. *If* $n \in S$, *then* $n + 1 \in S$.

Definition 10.8 *Then we define the* ***natural numbers*** $\mathbb{N}$ *to be the intersection of the collection of all inductive subsets of* $\mathbb{R}$.

Definition 10.9 *Let* 1 *denote the identity of* $\mathbb{R}$. *Define* $2 = 1+1$, $3 = 2+1$, $4 = 3 + 1$, $5 = 4 + 1$, $6 = 5 + 1$, $7 = 6 + 1$, $8 = 7 + 1$, $9 = 8 + 1$.

If we start with only the axioms for a complete ordered field, we have initially only the numbers 0 and 1. From the above definition we obtain in addition the numbers 2,3,4,5,6,7,8,9. Using the fact that for each $a \in \mathbb{R}$ we have $-a \in \mathbb{R}$ we get also $-1, -2, -3, -4, -5, \ldots$, as well as numbers such as

$$\frac{1}{2} = 2^{-1}, \quad \frac{1}{3} = 3^{-1}, \quad \frac{1}{4} = 4^{-1}, \quad \frac{2}{3} = 2 \cdot 3^{-1}, \ldots$$

Example 10.1 *Show that each of the following is an inductive subset of* $\mathbb{R}$.

1. $\mathbb{R}$.
2. $\{x \in \mathbb{R} \,|\, x \geq 1\}$.
3. $\{1, 2\} \cup \{x \in \mathbb{R} \,|\, x \geq 3\}$.
4. $\{1, 2, 3\} \cup \{x \in \mathbb{R} \,|\, x \geq 4\}$.

From Definitions 10.7 and 10.8 one may prove the following two theorems:

Theorem 10.2 $\mathbb{N}$ *is an inductive subset of* $\mathbb{R}$. ■

Theorem 10.3 (The Principle of Mathematical Induction) *If* $S \subseteq \mathbb{N}$ *and* S *is inductive then* $S = \mathbb{N}$. ■

Problem 10.5 *(a) Prove that* $2, 3, 4,$ *and* 5 *are elements of* $\mathbb{N}$. *(b) Prove that* $2 + 2 = 4$, $2 \cdot 2 = 4$. *(c) Prove that* $1 < 2 < 5$.

Here are a few examples of things that can be proved by using *induction* (this is short for *The Principle of Mathematical Induction*).

Problem 10.6 *Prove that* $n \geq 1$ *for all* $n \in \mathbb{N}$. *Hint: Let*

$$S = \{n \in \mathbb{N} \mid n \geq 1\}.$$

Prove that $S \subseteq \mathbb{N}$ *and* S *is inductive. Conclude from the Principle of Mathematical Induction that* $S = \mathbb{N}$. *This is equivalent to the statement* $n \geq 1$ *for all* $n \in \mathbb{N}$ *and completes the proof.*

Problem 10.7 *Prove that* $2^n > n$ *for all* $n \in \mathbb{N}$.

Problem 10.8 *Prove Part 3 of Theorem 7.2. Hint: divide the problem into two parts. First prove* $f(a^n) = f(a)^n$ *for all* $n \in \mathbb{N}$ *using induction. Use Theorem 7.2, Part 1 to handle the case* $n = 0$ *and use Theorem 7.2, Part 2 and the laws of exponents to handle the case where* n *is negative.*

Problem 10.9 *Prove that* $0 < \frac{1}{2} < 1$.

Problem 10.10 *As noted above it may be proved that if* $a \in \mathbb{R}$ *and* $a > 0$ *there exists a unique number* $x \in \mathbb{R}$ *satisfying* $x^2 = a$ *and* $x > 0$. *The number* x *is denoted* $\sqrt{a}$. *Prove that*

$$1 < \sqrt{2} < \sqrt{3} < 2$$

and

$$\frac{5}{2} < \sqrt{8} < 3.$$

Definition 10.10 *Define* $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N}$ *where* $-\mathbb{N} = \{-n \mid n \in \mathbb{N}\}$.

The set $\mathbb{Z}$ is a subring of the ring $\mathbb{R}$ which we call the **ring of integers**. All of the properties of $\mathbb{Z}$ that we are accustomed to follow from the axioms for $\mathbb{R}$ and the above definitions. This includes things such as there is no integer x such that $1 < x < 2$. In this course we will not take the time to develop all the known results of this nature.

Definition 10.11 $\mathbb{Q} = \{n/m \mid n, m \in \mathbb{Z} \text{ and } m \neq 0\}$.

The set $\mathbb{Q}$ is a subfield of $\mathbb{R}$ called the **field of rational numbers**.

Definition 10.12 *The* ***field of complex numbers*** *is the triple* $(\mathbb{C}, +, \cdot)$ *where*

$$\mathbb{C} = \{(a, b) \mid a, b \in \mathbb{R}\},$$

and addition and multiplication are defined as follows for (a, b),$(c, d) \in \mathbb{C}$*:*

$$\begin{aligned} (a, b) + (c, d) &= (a + c, b + d) \\ (a, b) \cdot (c, d) &= (ac - bd, ad + bc) \end{aligned}$$

Theorem 10.4 $\mathbb{C}$ *is a field with zero given by* $(0, 0)$*, identity given by* $(1, 0)$*, the additive inverse of* (a, b) *is given by* $(-a, -b)$ *and if* $(a, b) \neq (0, 0)$ *then the multiplicative inverse of* (a, b) *is given by*

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right).$$

This theorem is straightforward to prove. To save time we prove only the following:

Problem 10.11 *Prove that* $(0, 0)$ *is the zero of* $\mathbb{C}$ *and the additive inverse* $-(a, b)$ *of* $(a, b) \in \mathbb{C}$ *is given by* $(-a, -b)$.

Problem 10.12 *Prove that* $(1, 0)$ *is an identity for* $\mathbb{C}$*, that* $(0, 1)^2 = -(1, 0)$ *and that if* $(a, b) \neq (0, 0)$ *then the multiplicative inverse of* (a, b) *is given as stated in the theorem.*

Remark: If we write for $a, b \in \mathbb{R}$

$$a + bi = (a, b), \quad a = (a, 0), \quad bi = (0, b), \quad i = (0, 1)$$

then

$$i^2 = -1$$

and we can consider $\mathbb{R}$ as a subset of $\mathbb{C}$ and the addition and multiplication on $\mathbb{R}$ agrees with that on $\mathbb{C}$ for elements of $\mathbb{R}$. That is, in this notation $\mathbb{R}$ is a subfield of $\mathbb{C}$.

We lack the time in this course to discuss any of the many applications of complex numbers in mathematics, engineering and physics.

Problem 10.13 *Using the notation above for elements of $\mathbb{C}$, let $z = 2+3i$, $w = -2+4i$ and $\theta = (-1/2) + (\sqrt{3}/2)i$. Write the following in the form $a+bi$ where a and b are real numbers:*

1. $z + w$.
2. zw.
3. z^{-1}.
4. θ^3.

Definition 10.13 *Let $a, b \in \mathbb{R}$ and let $z = a + bi \in \mathbb{C}$. The complex number $\overline{z} = a - bi$ is called the **conjugate** of z. $\overline{z}$ is read* "z conjugate".

Problem 10.14 *Prove the the mapping $\varphi : \mathbb{C} \to \mathbb{C}$ defined by $\varphi(z) = \overline{z}$ is a ring isomorphism from $\mathbb{C}$ to itself which is its own inverse. That is, for all $z, w \in \mathbb{C}$ prove:*

1. $\overline{zw} = \overline{z}\,\overline{w}$,
2. $\overline{z+w} = \overline{z} + \overline{w}$, *and*
3. $\overline{\overline{z}} = z$

Another way to define $\mathbb{C}$ is given in the next problem.

Problem 10.15 *Let*

$$R = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

This is a subring of the ring of all 2×2 matrices $M_2(\mathbb{R})$. In fact, R is a field. Prove that R is isomorphic (as a ring) to $\mathbb{C}$.

Problem 10.16 *Compare the formula in Theorem 10.4 for the inverse of a complex number to the formula for the inverse of a matrix of the form*

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Remarks We mention here a few interesting theorems about $\mathbb{R}$ that we will not have time to cover in this course. Proofs may be found in introductory analysis courses and advanced algebra courses.

A set S is said to be *countable* if it is finite or if there is a one-to-one correspondence between S and $\mathbb{N}$. A set which is not countable is said to be *uncountable*.

Theorem 10.5 $\mathbb{Q}$ *is countable.* ■

Theorem 10.6 $\mathbb{R}$ *is uncountable.* ■

A real number which is not in $\mathbb{Q}$, that is, is not rational, is said to be an *irrational* number.

Theorem 10.7 *The set of irrational numbers is uncountable.* ■

A real number is said to be *algebraic* if it is a root of some non-zero polynomial $a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$ where the coefficients a_i are rational numbers. For example, $\sqrt{2}$ is algebraic since it is a root of $x^2 - 2$ and $\sqrt[3]{(1+\sqrt{5})}$ is algebraic since it is a root of $x^6 - 2x^3 - 4$. A rational number q is algebraic since it is a root of $x - q$.

Theorem 10.8 *The set of algebraic numbers forms a countable subfield of* $\mathbb{R}$.■

A real number which is not algebraic is said to be *transcendental*.

Theorem 10.9 *The set of transcendental numbers is uncountable.* ■

However it is very difficult to prove that a particular real number is transcendental. Important examples of transcendental numbers are π and e.

Theorem 10.10 (Hermite 1873) e *is transcendental.* ■

Theorem 10.11 (Lindemann 1882) π *is transcendental.* ■

Chapter 11

The Quaternions

The *quaternions* were invented by Sir William Rowan Hamilton about 1850. Hamilton was perhaps the first to note that complex numbers could be thought of as a way to multiply points in the plane. He then had the idea of trying to find a way to multiply points in $\mathbb{R}^3$ so that the field axioms would be satisfied. He was unable to do this, but he finally found a way to define multiplication on $\mathbb{R}^4$ so that the multiplication together with ordinary vector addition of elements of $\mathbb{R}^4$ would satisfy all the field axioms except for commutativity of multiplication. He called these new objects *quaternions*. They turned out, like complex numbers, to have many applications in engineering and physics. This "number system" is denoted by $\mathbb{H}$ for Hamilton since $\mathbb{Q}$ is already taken to denote the rational numbers.

Definition 11.1 *The* ***ring of quaternions*** *is the ring* $(\mathbb{H}, +, \cdot)$ *where*

$$\mathbb{H} = \mathbb{R}^4 = \{(a, b, c, d) \mid a, b, c, d \in \mathbb{R}\}$$

and where $+$ *and* $\cdot$ *are defined by the rules:*

$$\begin{aligned}(x, y, z, w) + (a, b, c, d) &= (x + a, y + b, z + c, w + d)\\ (x, y, z, w) \cdot (a, b, c, d) &= (xa - yb - zc - wd,\\ &\quad\ xb + ya + zd - wc,\\ &\quad\ xc - yd + za + wb,\\ &\quad\ xd + yc - zb + wa)\end{aligned}$$

where $x, y, z, w, a, b, c, d \in \mathbb{R}$. *The addition and multiplication inside the 4-tuples on the right represent addition and multiplication in* $\mathbb{R}$.

Stated this way the rules for multiplication are hard to remember. There is a simpler way to describe them: Let

$$\begin{aligned} 1 &= (1,0,0,0) \\ i &= (0,1,0,0) \\ j &= (0,0,1,0) \\ k &= (0,0,0,1) \end{aligned}$$

Note that here we are being a little lazy in letting 1 stand for both the vector $(1,0,0,0)$ and the real number 1. The set $\{1,i,j,k\}$ is what is called in linear algebra a *basis* for $\mathbb{R}^4$. This means that if we define for $a \in \mathbb{R}$ and $(x,y,z,w) \in \mathbb{R}^4$ the scalar by vector product

$$a(x,y,z,w) = (ax,ay,az,aw),$$

the quaternion $q = (x,y,z,w)$ may be written uniquely in the form

$$q = x1 + yi + zj + wk.$$

Now if we abbreviate $x = x1$, the quaternion takes the form

$$q = x + yi + zj + wk.$$

Addition now becomes

$$(x+yi+zj+wk)+(a+bi+cj+dk) = (x+a)+(y+b)i+(z+c)j+(w+d)k.$$

Products of the basis elements $1,i,j,k$ are defined as follows:

$$\begin{aligned} 1q = q1 = q \text{ for all } q \in \mathbb{H}, \\ i^2 = j^2 = k^2 = -1, \\ ij = -ji = k, \\ jk = -kj = i, \\ ki = -ik = j. \end{aligned}$$

Using these rules, the distributive law, and the fact that if q_1 and q_2 are any quaternions and $a \in \mathbb{R}$ then

$$a(q_1q_2) = (aq_1)q_2 = q_1(aq_2),$$

one easily calculates the product of two quaternions $q_1 = x + yi + zj + wk$ and $q_2 = a + bi + cj + dk$.

Problem 11.1 *Use the above rules to calculate the product $q_1 q_2$ of the quaternions $q_1 = 1 + i + 2j + 3k$ and $q_2 = 1 - i - 2j - 3k$. Write the product in standard form $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{R}$.*

Problem 11.2 *Show that $(1, 0, 0, 0)$ acts as an identity for $\mathbb{H}$ and that $\mathbb{H}$ is not a commutative ring.*

Problem 11.3 *Show that the quaternion $q = x+yi+zj+wk$ has an inverse given by $q^* = c(x - yi - zj - wk)$ where $c = 1/(x^2 + y^2 + z^2 + w^2)$ provided that $q \neq 0$. Here $0 = (0, 0, 0, 0)$.*

Problem 11.4 *Show that there are infinitely many quaternions q satisfying $q^2 = -1$. Hint: consider quaternions of the form $q = xi + yj + zk$.*

Problem 11.5 *Show that the 8 element set*

$$Q = \{1, -1, i, -i, j, -j, k, -k\}$$

under quaternion multiplication is a group. This is one of the five non-isomorphic groups of order 8. It is called, naturally enough, the ***quaternion group****.*

Definition 11.2 *A ring which satisfies all the field axioms except possibly for commutativity of multiplication is called a* ***division ring****.*

Note that a division ring may be defined as a ring whose non-zero elements form a group under multiplication. All fields are division rings. A commutative ring which is a division ring is a field.

Theorem 11.1 *$\mathbb{H}$ is a division ring.*

Proof. From linear algebra we already know that vector addition on $\mathbb{R}^4$ is an abelian group. From the above problems we know that $\mathbb{H}$ has an identity and every non-zero element has an inverse. It remains only to prove associativity for multiplication and the two distributive laws. The proofs of these properties are straightforward and we leave them for the interested reader.

The ring of quaternions is one of the rare examples of a non-commutative division ring. The following theorem shows why Hamilton had difficulty finding a division ring whose underlying set is $\mathbb{R}^3$.

Theorem 11.2 (Frobenius) *Let D be a division ring which is algebraic over $\mathbb{R}$. Then D is isomorphic to $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.* ■

See Chapter 7 of [4] to see what it means to be *algebraic over* $\mathbb{R}$ and how to prove this theorem. This result implies that there is no "nice" way of defining multiplication on $\mathbb{R}^n$ so that it becomes a division ring unless $n \in \{1, 2, 4\}$. There are many interesting and useful ways to make $\mathbb{R}^n$ into a ring which is not a division ring for other values of n. However, we do not have time to go into these matters.

Problem 11.6 *Define*

$$\mathcal{H} = \left\{ \begin{pmatrix} z & -\overline{w} \\ w & \overline{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\}.$$

1. *Prove that $\mathcal{H}$ is a subring of the ring $M_2(\mathbb{C})$.*

2. *Prove that $\mathcal{H}$ is a division ring. Hint: it suffices to show that the each non-zero matrix in $\mathcal{H}$ has an inverse that is also in $\mathcal{H}$.*

3. *Define the matrices*

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

   (a) *Show that every element of $\mathcal{H}$ can be written in the form:*

$$a\mathbf{1} + bI + cJ + dK$$

   where $a, b, c, d \in \mathbb{R}$.

   (b) *Show that*

$$I^2 = J^2 = K^2 = -\mathbf{1},$$
$$IJ = K, JI = -K,$$
$$JK = I, KJ = -I,$$
$$KI = J, IK = -J$$

Remark: You need not verify it, but it follows from this that $\mathcal{H} \cong \mathbb{H}$.

Chapter 12

The Circle Group

Before defining the circle group we first discuss some geometric aspects of the field of complex numbers. A typical element z of $\mathbb{C}$ will be written $z = x + yi$ where $s, y \in \mathbb{R}$. We identify $z = x + yi$ with the point (x, y) in the plane. Thus the **absolute value** $|z|$ of z is defined by

$$|z| = \sqrt{x^2 + y^2}.$$

Note that since $z\overline{z} = x^2 + y^2$ we also have:

$$|z| = \sqrt{z\overline{z}}.$$

Problem 12.1 *Prove that for* $z, w \in \mathbb{C}$

1. $|zw| = |z||w|$,
2. $|z| \geq 0$, *and*
3. $|z| = 0 \Longleftrightarrow z = 0$.

We know from analytic geometry that $|z|$ represents the distance from z to the origin 0 in the plane. The directed angle θ that the segment from 0 to z makes with the positive side of the x-axis is called the *argument* or *polar angle* of z. As in polar coordinates we write $r = |z|$. Then we have

$$x = r\cos\theta,$$

$$y = r\sin\theta,$$

and

$$z = r(\cos\theta + i\sin\theta) \tag{12.1}$$

From trigonometry we know that every non-zero complex number z may be written uniquely in the form (12.1) for real numbers r and θ satisfying $r > 0$ and $0 \leq \theta < 2\pi$.

We assume that students are familiar with the exponential function $x \mapsto e^x$ where $x \in \mathbb{R}$. We extend the definition of this function from $\mathbb{R}$ to $\mathbb{C}$.

Definition 12.1 *For $z \in \mathbb{C}$ let $z = x + yi$ where $x, y \in \mathbb{R}$, We define the* ***exponential function*** *$z \mapsto e^z$ by*

$$e^z = e^{x+yi} = e^x(\cos y + i\sin y.)$$

in particular, if $\theta \in \mathbb{R}$ we have

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

From the above we have immediately the following:

Theorem 12.1 *Every non-zero complex number z may be written uniquely in the form*

$$z = re^{i\theta} \tag{12.2}$$

where $r = |z| > 0$ and $0 \leq \theta < 2\pi$. ■

Note that the expression $e^{i\theta}$ is well-defined for all $\theta \in \mathbb{R}$.

Theorem 12.2 *Let $z_1 = r_1 e^{i\theta_1}$ and $z_2 = r_2 e^{i\theta_2}$ where $r_i \geq 0$ and θ_i are real numbers. Then*

$$z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}.$$■

Problem 12.2 *Use the addition identities for the sine and cosine to prove Theorem 12.2.*

Note that, in words, Theorem 12.2 says: *The argument of the product is the sum of the arguments of the factors and the absolute value of the product is the product of the absolute values of the factors.*. This easily generalizes via induction to the following: *If $z_j = r_j e^{i\theta_j}$, $j = 1, \ldots, n$ are complex numbers then*

$$z_1 z_2 \cdots z_n = r_1 r_2 \cdots r_n e^{(i\theta_1+\theta_2+\cdots+\theta_n)}.$$

Taking $r_j = 1$ for all j we obtain the following famous theorem:

Theorem 12.3 (De Moivre's Theorem) *For all $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$, we have*

$$(\cos(\theta) + i\sin(\theta))^n = \cos(n\theta) + i\sin(n\theta),$$

equivalently,

$$(e^{i\theta})^n = e^{in\theta}.\blacksquare$$

Definition 12.2 *We define*

$$\mathbb{T} = \{z \in \mathbb{C} \,|\, |z| = 1\};$$

$\mathbb{T}$ is a group with respect to multiplication in $\mathbb{C}$ and is called the ***circle group****.*

Note that geometrically $\mathbb{T}$ is the set of complex numbers which are at a distance 1 from the origin, that is, it's points are exactly the points on the unit circle $x^2 + y^2 = 1$.

Problem 12.3 *Show that every element $z \in \mathbb{T}$ may be uniquely written in the form $z = e^{i\theta}$ where $0 \leq \theta < 2\pi$.*

Problem 12.4 *Prove that $\mathbb{T}$ is a subgroup of $U(\mathbb{C})$.*

Problem 12.5 *(a) Prove that the mapping $\varphi : \mathbb{T} \to \mathbb{C}$ defined by $\varphi(\theta) = e^{i\theta}$ is a homomorphism from $(\mathbb{R}, +)$ onto the circle group $\mathbb{T}$. (b) Show that for every point $z \in \mathbb{T}$ there are infinitly many $\theta \in \mathbb{R}$ such that $\varphi(\theta) = z$.*

Recall that in Problem 10.15 we showed that complex numbers can be represented as certain 2×2 matrices over the real numbers. So it should come as no surprise that the circle groups can also be represented by certain 2×2 matrices over the real numbers. It turns out that this set of matrices also has another name which we give in the following definition.

Definition 12.3 *Define*

$$SO(2) = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \mid \theta \in \mathbb{R} \right\}.$$

$SO(2)$is a subgroup of $SL(2, \mathbb{R})$ and is called the ***special orthogonal group of degree 2****.*

Definition 12.4 *For $\theta \in \mathbb{R}$, define*

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

With this definition we have $SO(2,\mathbb{R}) = \{R(\theta) \mid \theta \in \mathbb{R}\}$.

Problem 12.6 *Prove (a) that $R(\theta_1)R(\theta_2) = R(\theta_1 + \theta_2)$, (b) $R(0)$ is the 2×2 identity matrix, and (c) $R(\theta)^{-1} = R(-\theta)$. Conclude that $SO(2,\mathbb{R})$ is a subgroup of $GL(2,\mathbb{R})$.*

Problem 12.7 *Prove that $SO(2,\mathbb{R}) \cong \mathbb{T}$.*

Problem 12.8 *Prove that if we represent a point $p = (x, y)$ in the plane by a 2×1 matrix $\begin{bmatrix} x \\ y \end{bmatrix}$ then the point $R(\theta)p$ given by the matrix product*

$$R(\theta)p = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

is obtained by rotating p through θ radians counter-clockwise about the origin. [Hint use the polar coordinate representation $(x, y) = (r\cos\theta, r\sin\theta)$ of the point p.]

Remark The above problem also justifies referring to the circle group as the **group of rotations of the plane**.

We now determine the order of an element $e^{i\theta} \in \mathbb{T}$.

Theorem 12.4 *An element $z = e^{i\theta} \in \mathbb{T}$ has finite order if and only if $\theta = \frac{k}{n}\pi$ for some $n \in N$ and $k \in \mathbb{Z}$, that is, if and only if θ is a rational multiple of π.*

Proof First we recall from trignometry that $(\cos\alpha, \sin\alpha) = (1, 0)$ if and only if $\alpha = 2\pi k$ for some integer k. Using exponentional notation, this says that $e^{i\alpha} = 1$ if and only if $\alpha = 2\pi k$ for some integer k.

Assume that $e^{i\theta}$ has finite order. Then by De Moivre's Theorem we have $e^{in\theta} = 1$ and by the previous remark, $n\theta = 2\pi k$ for some integer k. Solving for θ we see that $\theta = \frac{2k}{n}\pi = \frac{k'}{n}\pi$ where $k' = 2k$. That is, θ is a rational multiple of π. Conversely, suppose that $\theta = \frac{k}{n}\pi$ for some $n \in N$ and $k \in \mathbb{Z}$. Then

$$(e^{i\theta})^{2n} = e^{i(\theta 2n)} = e^{i\frac{k}{n}2n\pi} = e^{ik2\pi} = 1.$$

This shows that the order of $e^{i\theta}$ is finite and at most $2n$. ■

Problem 12.9 *Show that the order of the element $e^{i\sqrt{2}\pi}$ in $\mathbb{T}$ is infinite. What about the element $e^{i\sqrt{2}}$? (For the latter you may assume that π is transcendental.)*

Definition 12.5 *Let $n \in \mathbb{N}$. An element $z \in \mathbb{C}$ is said to be an **n-th root of unity** if $z^n = 1$.*

Problem 12.10 *Prove that for $n \in \mathbb{N}$ the set*

$$\{z \in \mathbb{C} \,|\, z^n = 1\} \tag{12.3}$$

is a subgroup of $U(\mathbb{C})$.

Definition 12.6 *The set (12.3) of all n-th roots of unity is a subgroup of $U(\mathbb{C})$ called the **group of n-th roots of unity**.*

Figure 12.1: The 12th roots of unity (= the vertices of the regular 12-gon).

Problem 12.11 *Prove that $z \in \mathbb{C}$ is an n-th root of unity if and only if z is an element in $\mathbb{T}$ of finite order k where $k \,|\, n$.*

Definition 12.7 *For $n \in \mathbb{N}$ define*

$$\zeta_n = e^{i\frac{2\pi}{n}}.$$

Theorem 12.5 *The group of n-th roots of unity is cyclic of order n. One generator of the group is ζ_n*

Proof From De Moivre's Theorem it is clear that $(\zeta_n)^n = 1$. Note that the powers

$$(\zeta_n)^k = e^{ik\frac{2\pi}{n}}, \quad k = 0, 1, \ldots, n-1$$

are the vertices of the regular n-gon centered at the origin. Hence $(\zeta_n)^k \neq 1$ for $0 < k < n$. This proves that $o(\zeta_n) = n$.

Now, suppose that z is any n-th root of unity. Note that $|z|^n = |z^n| = 1$. That is, $|z|$ is a positive real number whose n-th power is 1. It follows that $|z|$ must be equal to 1. Hence $z = e^{i\theta}$. By the argument in the proof of Theorem 12.4 since $z^n = 1$, we have $\theta = k\frac{2\pi}{n}$. This shows that $z = e^{ik\frac{2\pi}{n}} = (\zeta_n)^k$, and therefore lies in the subgroup $\langle\, \zeta_n \,\rangle$ generated by ζ_n. ■

Problem 12.12 *Show that $z \in \mathbb{T}$ if and only if $z^{-1} = \overline{z}$.*

Problem 12.13 *Show that if $z = e^{i\theta}$ then $\overline{z} = e^{-i\theta}$.*

Problem 12.14 *Use the formula for $R(\theta)$ to find the coordinates of the point $(1, 1) \in \mathbb{R}^2$ after it has been rotated 30^o counter-clockwise about the origin. Do the same for 60^o. Express the coordinates of the answer as rational numbers and/or radicals, not trig functions.*

Problem 12.15 *Prove that the group $\langle\, \zeta_n \,\rangle$ is isomorphic to the group $\mathbb{Z}_n$ under addition modulo n.*

Problem 12.16 *For each $n \in \{1, 2, 3, 4, 6, 8\}$ find all the n-th roots of unity $(\zeta_n)^k$ for $k \in \{0, 1, \cdots, n-1\}$. Express them in the form $a + bi$ where a and b are real numbers not involving trig functions. Also sketch the location in the plane of the n-roots of unity for each n.*

Problem 12.17 *Prove that $\langle\, e^{i\pi\sqrt{2}} \,\rangle \cong \mathbb{Z}$.*

Appendix A

Some Rules of Logic

Constructing mathematical proofs is an art that is best learned by seeing many examples of proofs and by trying to imitate these examples when constructing one's own proofs. Nevertheless, there are a few rules of logic and language that it is useful to be aware of. Most of these are very natural and will be used without comment. Their full understanding only comes with experience. We begin with some basic assumptions concerning *equality*.

1. $x = x$ holds for all x. [Reflexivity.]

2. If $x = y$ then $y = x$. [Symmetry.]

3. If $x = y$ and $y = z$ then $x = z$. [Transitivity.]

For example, if we are able to prove $x = y$, $y = z$, $z = w$ and $w = r$, then we may conclude *by transitivity of equality* that $x = r$. Reflexivity and symmetry of equality are also very useful. It is not necessary to quote these rules everytime they are used, but it is good to be aware of them (in case someone asks).

Implications are crucial to the development of mathematics. An implication is a statement of the form

$$\text{If } P \text{ then } Q \tag{A.1}$$

where P and Q are statements. Instead of (A.1) we will sometimes write

$$P \Longrightarrow Q. \tag{A.2}$$

The statement (A.2) is read,"P implies Q". We call P the **hypothesis** and, Q the **conclusion** of the implication (A.2). Students should be careful when using this notation. For example, *do not* write

$$\text{If } P \Longrightarrow Q$$

when you mean

$$P \Longrightarrow Q \tag{A.3}$$

To prove the implication $P \Longrightarrow Q$, start by assuming that P is true and use this assumption to establish the validity of Q. It is sometimes easier to prove the equivalent statement

$$Q \text{ is false} \Longrightarrow P \text{ is false} \tag{A.4}$$

This is called the **contrapositive** of the implication (A.3).

We write

$$P \Longleftrightarrow Q \tag{A.5}$$

as an abbreviation for the two statements

$$P \Longrightarrow Q \quad \text{and} \quad Q \Longrightarrow P$$

So, for example, if you need to prove $P \Longleftrightarrow Q$ you really have two things to prove: both $P \Longrightarrow Q$ and $Q \Longrightarrow P$. The statement (A.5) is read

"P is equivalent to Q",

or

"P holds if and only if Q holds."

And sometimes we use the abbreviation "iff" for "if and only if". So an acceptable alternative to (A.5) is

$$P \text{ iff } Q$$

.

We assume that implication satisfies the following rules:

1. $P \Longrightarrow P$ holds for all P. [Reflexivity.]
2. If $P \Longrightarrow Q$ and $Q \Longrightarrow R$ then $P \Longrightarrow R$. [Transitivity.]

We assume that equivalence satisfies the following rules.

1. $P \iff P$ holds for all P. [Reflexivity.]
2. If $P \iff Q$ then $Q \iff P$. [Symmetry.]
3. If $P \iff Q$ and $Q \iff R$ then $P \iff R$. [Transitivity.]

We will often use these rules for implication and equivalence without comment.

Convention In definitions the word *if* means *if and only if*. Compare, for example, Definition 2.2.

Important Phrases In addition to looking for implications and equivalences, students should pay close attention to the following words and phrases:

1. there exists
2. there is
3. there are
4. for all
5. for each
6. for every
7. for some
8. unique
9. one and only one
10. at most one
11. at least one
12. the
13. a, an
14. such that

15. implies
16. hence
17. therefore

The use of these phrases and words will be clarified if necessary as the course progresses. Some techniques of proof such as *proof by contradiction* and *proof by induction* are best understood by examples of which we shall see many as the course progresses.

Appendix B

Functions

Here we collect a few basic facts about functions. Note that the words *function*, *map*, *mapping* and *transformation* may be used interchangeably. Here we just use the term *function*. We leave the proofs of all the results in this appendix to the interested reader.

Definition B.1 *A **function** f from the set A to the set B is a rule which assigns to each element $a \in A$ an element $f(a) \in B$ in such a way that the following condition holds for all $x, y \in A$:*

$$x = y \Longrightarrow f(x) = f(y). \tag{B.1}$$

*To indicate that f is a function from A to B we write $f : A \to B$. The set A is called the **domain** of f and the set B is called the **codomain** of f.*

If the conditions of Definition B.1 hold, it is customary to say that **the function is well-defined**. Often we speak of "the function f", but strictly speaking the domain and the codomain are integral parts of the definition, so this is short for "the function $f : A \to B$."

To describe a function one must specify the domain (a set) and the codomain (another set) and specify its effect on a typical element (variable) in its domain.

When a function is defined it is often given a name such as f or σ. So we speak of *the function f* or *the function σ*. If x is in the domain of f then $f(x)$ is the element in the codomain of f that f assigns to x. We sometimes write $x \mapsto f(x)$ to indicate that *f sends x to $f(x)$*.

We can also use the *barred arrow* to define a function without giving it a name. For example, we may speak of the function $x \mapsto x^2 + 2x + 4$ from $\mathbb{R}$ to $\mathbb{R}$. Alternatively one could define the same function as follows: Let $h : \mathbb{R} \to \mathbb{R}$ be defined by the rule $h(x) = x^2 + 2x + 4$ for all $x \in \mathbb{R}$.

Note that it is correct to say *the function* sin or *the function* $x \mapsto \sin(x)$. But it is not correct to say *the function* $\sin(x)$.

Arrows: We consistently distinguish the following types of arrows:

$\to$ As in $f : A \to B$.
$\mapsto$ As in $x \mapsto x^2 + 3x + 4$
$\Longrightarrow$ Means *implies*
$\Longleftrightarrow$ Means *is equivalent to*

Some people use $\rightsquigarrow$ in place of $\mapsto$

It is often important to know when two functions are *equal*. Then, the following definition is required.

Definition B.2 *Let $f : A \to B$ and $g : C \to D$. We write $f = g$ if and only if*

$$A = C,\ B = D \text{ and } f(a) = g(a) \text{ for all } a \in A. \tag{B.2}$$

Definition B.3 *A function $f : A \to B$ is said to be **one-to-one** if the following condition holds for all $x, y \in A$:*

$$f(x) = f(y) \Longrightarrow x = y. \tag{B.3}$$

Note carefully the difference and similiarity between (B.1) and (B.3).

Definition B.4 *A function $f : A \to B$ is said to be **onto** if the following condition holds:*

$$\text{For every } b \in B \text{ there is an element } a \in A \text{ such that } f(a) = b. \tag{B.4}$$

Some mathematicians use *injective* instead of one-to-one, *surjective* instead of onto, and *bijective* for one-to-one and onto. If $f : A \to B$ is bijective f is sometimes said to be a *bijection* or a *one-to-one correspondence* between A and B.

Definition B.5 *For any set A, we define the function $\iota_A : A \to A$ by the rule*

$$\iota_A(x) = x \text{ for all } x \in A. \tag{B.5}$$

We call ι_A the ***identity function on*** *A. If A is understood, we write simply ι instead of ι_A.*

Some people write 1_A instead of ι_A to indicate the identity function on A.

Problem B.1 *Prove that $\iota_A : A \to A$ is one-to-one and onto.*

Theorem B.1 *If $f : A \to B$ and $g : B \to C$ then the rule*

$$gf(a) = g(f(a)) \text{ for all } a \in A \tag{B.6}$$

defines a function $gf : A \to C$. This function is called the ***composition of g and f.***

Some people write $g \circ f$ instead of gf, but we will not do this.

Theorem B.2 *If $f : A \to B$ is one-to-one and onto then the rule*

$$\text{for every } b \in B \text{ define } f^{-1}(b) = a \text{ if and only if } f(a) = b, \tag{B.7}$$

defines a function $f^{-1} : B \to A$. The function f^{-1} is itself one-to-one and onto and satisfies

$$ff^{-1} = \iota_B \text{ and } f^{-1}f = \iota_A. \tag{B.8}$$

The function f^{-1} defined in the above theorem is called the **inverse of** f.

Theorem B.3 *Let $f : A \to B$ and $g : B \to C$.*

1. *If f and g are one-to-one then $gf : A \to C$ is one-to-one.*
2. *If f and g are onto then $gf : A \to C$ is onto.*
3. *If f and g are one-to-one and onto then $gf : A \to C$ is also one-to-one and onto.*

Appendix C

Elementary Number Theory

Here we review some basic number theoretic definitions and results. For the most part, we will just state the results. For a more detailed treatment, the student is referred references [1],[2], or [3] given in the bibliography. Unless otherwise stated in this appendix, all lower case letters, a, b, c, *etc.* will be integers. Recall that we use $\mathbb{N}$ to denote the set of natural numbers (also known as the positive integers) and we use $\mathbb{Z}$ to denote the set of all integers, *i.e.,*

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

and

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

Definition C.1 *Let $a, b \in \mathbb{Z}$. We say b **divides** a and we write $b \mid a$ if there is an element $c \in \mathbb{Z}$ such that $a = bc$. We write $b \nmid a$ if b does not divide a.*

If $b \mid a$ we also sometimes say that b is a **factor** of a or that a is a **multiple** of b. To tell if b divides a where $b \neq 0$, we simply divide a by b and see if the remainder is 0 or not. More generally, we have the following fundamental result.

Lemma C.1 (The Division Algorithm) *For any integers a and b with $b \neq 0$ there exists unique integers q and r such that*

$$a = bq + r, \qquad 0 \leq r < |b|.$$

Definition C.2 *The number r in the above Lemma is denoted by $a \bmod b$.*

For example we have

$$17 \bmod 5 = 2 \qquad \text{since} \quad 17 = 3 \cdot 5 + 2 \ \text{ and } \ 0 \leq 2 < 5$$

and

$$(-17) \bmod 5 = 3 \qquad \text{since} \quad -17 = (-4) \cdot 5 + 3 \ \text{ and } \ 0 \leq 3 < 5$$

.

Definition C.3 *An integer p is said to be **prime** if $p \geq 2$ and the only positive factors of p are p and 1.*

Definition C.4 *Let a and b be integers, at least one of which is non-zero. The **greatest common divisor** of a and b is the greatest positive integer, $\gcd(a, b)$, that divides both a and b. We define $\gcd(0, 0) = 0$.*

Definition C.5 *If a and b are non-zero integers, the **least common multiple** of a and b is the smallest positive integer, $\operatorname{lcm}(a, b)$, that is a multiple of both a and b. If $a = 0$ or $b = 0$, we define $\operatorname{lcm}(a, b) = 0$.*

An important property of primes is given by the following lemma.

Lemma C.2 *If p is prime and $p|ab$ then $p|a$ or $p|b$.*

Perhaps the most fundamental result concerning integers is the following theorem, which is sometimes called *The Fundamental Theorem of Arithmetic.*

Theorem C.3 (Unique Factorization for $\mathbb{N}$) *If $n \geq 2$ is an integer, then there exists a unique list of primes $p_1, p_2, \ldots, p_k$ such that the following two conditions hold:*

1. $p_1 \leq p_2 \leq \cdots \leq p_k$,
2. $n = p_1 p_2 \cdots p_k$

For example, if $n = 72$ the unique list of primes is 2, 2, 2, 3, 3.

Now fix a positive integer n. Recall that $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ and that multiplication and addition in $\mathbb{Z}_n$ are defined by

$a + b$ = remainder when the ordinary sum of a and b is divided by n, and

$a \cdot b$ = remainder when the ordinary product of a and b is divided by n.

To facilitate the proof that these two binary operations are associative, we temporarily denote addition in $\mathbb{Z}_n$ by $\oplus$ and multiplication in $\mathbb{Z}_n$ by $\odot$. This way we can use $+$ and $\cdot$ for ordinary addition and multiplication in $\mathbb{Z}$. Thus we have

$$\begin{aligned} a \oplus b &= (a + b) \bmod n \\ a \odot b &= (ab) \bmod n \end{aligned}$$

Theorem C.4 *Let n be a positive integer. Define $f : \mathbb{Z} \to \mathbb{Z}_n$ by the rule $f(a) = a \bmod n$. Then*

$$f(a + b) = f(a) \oplus f(b) \tag{C.1}$$

and

$$f(a \cdot b) = f(a) \odot f(b). \tag{C.2}$$

Proof Let $r_1 = f(a)$ and $r_2 = f(b)$. This implies that

$$a = nq_1 + r_1, \quad 0 \leq r_1 < n$$

and

$$b = nq_2 + r_2, \quad 0 \leq r_2 < n$$

Hence

$$a + b = nq_1 + r_1 + nq_2 + r_2 = n(q_1 + q_2) + r_1 + r_2$$

Now

$$f(a) \oplus f(b) = r_1 \oplus r_2 = r$$

where

$$r_1 + r_2 = qn + r, \quad 0 \leq r < n$$

Hence

$$a + b = n(q_1 + q_2 + q) + r, \quad 0 \leq r < n$$

and it follows that

$$f(a+b) = (a+b) \bmod n = r,$$

and we conclude that

$$f(a+b) = r = f(a) \oplus f(b).$$

This proves (C.1). The proof of (C.2) is similar and left to the interested reader.

Corollary C.5 *The binary operations $\oplus$ and $\odot$ on $\mathbb{Z}_n$ are associative.*

Proof Using the notation in the theorem, we have for $a, b, c \in \mathbb{Z}_n$: $f(a) = a$, $f(b) = b$ and $f(c) = c$. Hence

$$\begin{aligned}
(a \oplus b) \oplus b &= (f(a) \oplus f(b)) \oplus f(c) \\
&= f(a+b) \oplus f(b) \\
&= f((a+b)+c) \\
&= f(a+(b+c)) \\
&= f(a) \oplus f(b+c) \\
&= f(a) \oplus (f(b) \oplus f(c)) \\
&= a \oplus (b \oplus c)
\end{aligned}$$

This proves that $\oplus$ is associative on $\mathbb{Z}_n$. The proof for $\odot$ is similar and left to the interested reader.

Appendix D

Partitions and Equivalence Relations

Definition D.1 *A* ***partition*** *of a set X is a collection $\mathcal{P}$ of pairwise disjoint, non-empty subsets of X whose union is X. The elements of $\mathcal{P}$ are called the* ***blocks*** *of the partition.*

For example, if $X = [9] = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ then

$$\mathcal{P} = \{\{1, 2\}, \{3\}, \{5, 8, 9\}, \{4, 6, 7\}\}$$

is a partition of X. Note that this partition has four blocks $\{1, 2\}$, $\{3\}$, $\{5, 8, 9\}$, and $\{4, 6, 7\}$.

Remark: In the definition of partition we used the term *collection*. This is just another name for *set*. It is just more natural to say *collection of sets* than to say *set of sets*. So in fact, a partition of X is a set whose elements are themselves sets which we choose to call *blocks*– satisfying three properties:

1. Each block is a non-empty subset of X.
2. No two different blocks have an element in common.
3. Every element of X lies in at least one block.

Problem D.1 *Find all partitions of the set* $[4]$. *List them according to the numbers of blocks in each partition. The number of blocks may be any integer from 1 to 4.*

Problem D.2 *Find a partition $\mathcal{P}_k$ of the set $\mathbb{Z}$ that has exactly k blocks for each of the following values of k: 1,2,3,4,5,10.*

Definition D.2 *A **(binary) relation** on a set X is a subset ρ of the Cartesian product $X \times X$. If $(a, b) \in R$ we write $a\rho b$ and we say that a* is related to b with respect to the relation R.

Since we will only be concerned with binary relations, we will leave off the modifier *binary*. Examples of relations are $<$ and $\leq$ on the set $\mathbb{R}$, $=$ on any set, and $\cong$ on the class of all groups. Rather than use ρ for a generic relation, we use the symbol $\sim$.

Definition D.3 *A relation $\sim$ on a set X is an **equivalence relation** on X if the following properties hold for all $x, y, z \in X$.*

1. *$x \sim x$.*
2. *If $x \sim y$ then $y \sim x$.*
3. *If $x \sim y$ and $y \sim z$ then $x \sim z$.*

The properties in the above definition are called **reflexivity, symmetry, transitivity**, respectively.

The most common equivalence relation is equality. Equality is an equivalence relation on any set.

Definition D.4 *If $\sim$ is an equivalence relation on the set X, and $a \in X$ we define the set*

$$[a] = \{x \in X \mid x \sim a\}.$$

*$[a]$ is called the **equivalence class of** a relative to the equivalence relation $\sim$.*

Theorem D.1 *If $\sim$ is any equivalence relation on the set X then the collection of all equivalence classes is a partition of X. Conversely, given any partition $\mathcal{P}$ of the set X, one may define an equivalence relation $\sim$ on X by the rule*

$$a \sim b \iff a, b \in B \text{ for some block } B \in \mathcal{P}$$

in which case the equivalence classes of $\sim$ are precisely the blocks of the partition $\mathcal{P}$.

Index