9. Prove that $\mathrm{Aut}(Q_8) \cong S_4$.

10. This exercise exhibits an automorphism of S_6 that is not inner (hence, together with Exercise 19 in Section 4.4 it shows that $|\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)| = 2$). Let $t_1' = (1\ 2)(3\ 4)(5\ 6)$, $t_2' = (1\ 4)(2\ 5)(3\ 6)$, $t_3' = (1\ 3)(2\ 4)(5\ 6)$, $t_4' = (1\ 2)(3\ 6)(4\ 5)$, and $t_5' = (1\ 4)(2\ 3)(5\ 6)$. Show that $t_1', \dots, t_5'$ satisfy the following relations:

$(t_i')^2 = 1$ for all i,

$(t_i't_j')^2 = 1$ for all i and j with $|i - j| \geq 2$, and

$(t_i't_{i+1}')^3 = 1$ for all $i \in \{1, 2, 3, 4\}$.

Deduce that $S_6 = \langle t_1', \dots, t_5' \rangle$ and that the map

$$(1\ 2) \mapsto t_1', \quad (2\ 3) \mapsto t_2', \quad (3\ 4) \mapsto t_3', \quad (4\ 5) \mapsto t_4', \quad (5\ 6) \mapsto t_5'$$

extends to an automorphism of S_6 (which is clearly not inner since it does not send transpositions to transpositions). [Use the presentation for S_6 described in Example 5.]

11. Let S be a set. The group with presentation (S, R), where $R = \{[s, t] \mid s, t \in S\}$ is called the *free abelian* group on S — denote it by $A(S)$. Prove that $A(S)$ has the following universal property: if G is any abelian group and $\varphi : S \to G$ is any set map, then there is a unique group homomorphism $\Phi : A(S) \to G$ such that $\Phi|_S = \varphi$. Deduce that if A is a free abelian group on a set of cardinality n then

$$A \cong \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \quad (n \text{ factors}).$$

12. Let S be a set and let c be a positive integer. Formulate the notion of a *free nilpotent group* on S of nilpotence class c and prove it has the appropriate universal property with respect to nilpotent groups of class $\leq c$.

13. Prove that there cannot be a nilpotent group N generated by two elements with the property that *every* nilpotent group which is generated by two elements is a homomorphic image of N (i.e., the specification of the class c in the preceding problem was necessary).

Part II

RING THEORY

The theory of groups is concerned with general properties of certain objects having an algebraic structure defined by a single binary operation. The study of rings is concerned with objects possessing two binary operations (called addition and multiplication) related by the distributive laws. We first study analogues for the basic points of development in the structure theory of groups. In particular, we introduce subrings, quotient rings, ideals (which are the analogues of normal subgroups) and ring homomorphisms. We then focus on questions about general rings which arise naturally from the presence of two binary operations. Questions concerning multiplicative inverses lead to the notion of fields and eventually to the construction of some specific fields such as finite fields. The study of the arithmetic (divisibility, greatest common divisors, etc.) of rings such as the familiar ring of integers, $\mathbb{Z}$, leads to the notion of primes and unique factorizations in Chapter 8. The results of Chapters 7 and 8 are then applied to rings of polynomials in Chapter 9.

The basic theory of rings developed in Part II is the cornerstone for the remaining four parts of the book. The theory of ring actions (modules) comprises Part III of the book. There we shall see how the structure of rings is reflected in the structure of the objects on which they act and this will enable us to prove some powerful classification theorems. The structure theory of rings, in particular of polynomial rings, forms the basis in Part IV for the theory of fields and polynomial equations over fields. There the rich interplay among ring theory, field theory and group theory leads to many beautiful results on the structure of fields and the theory of roots of polynomials. Part V continues the study of rings and applications of ring theory to such topics as geometry and the theory of extensions. In Part VI the study of certain specific kinds of rings (group rings) and the objects (modules) on which they act again gives deep classification theorems whose consequences are then exploited to provide new results and insights into finite groups.

CHAPTER 7

Introduction to Rings

7.1 BASIC DEFINITIONS AND EXAMPLES

Definition.

(1) A *ring* R is a set together with two binary operations $+$ and $\times$ (called addition and multiplication) satisfying the following axioms:

(i) $(R, +)$ is an *abelian* group,

(ii) $\times$ is associative : $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$,

(iii) the *distributive laws* hold in R : for all $a, b, c \in R$

$$(a+b) \times c = (a \times c) + (b \times c) \quad \text{and} \quad a \times (b+c) = (a \times b) + (a \times c).$$

(2) The ring R is *commutative* if multiplication is commutative.

(3) The ring R is said to have an *identity* (or *contain a* 1) if there is an element $1 \in R$ with

$$1 \times a = a \times 1 = a \qquad \text{for all } a \in R.$$

We shall usually write simply ab rather than $a \times b$ for $a, b \in R$. The additive identity of R will always be denoted by 0 and the additive inverse of the ring element a will be denoted by $-a$.

The condition that R be a group under addition is a fairly natural one, but it may seem artificial to require that this group be *abelian*. One motivation for this is that if the ring R has a 1, the commutativity under addition is *forced* by the distributive laws. To see this, compute the product $(1+1)(a+b)$ in two different ways, using the distributive laws (but not assuming that addition is commutative). One obtains

$$(1+1)(a+b) = 1(a+b) + 1(a+b) = 1a + 1b + 1a + 1b = a + b + a + b$$

and

$$(1+1)(a+b) = (1+1)a + (1+1)b = 1a + 1a + 1b + 1b = a + a + b + b.$$

Since R is a group under addition, this implies $b+a = a+b$, i.e., that R under addition is necessarily commutative.

Fields are one of the most important examples of rings. Note that their definition below is just another formulation of the one given in Section 1.4.

Definition. A ring R with identity 1, where $1 \neq 0$, is called a *division ring* (or *skew field*) if every nonzero element $a \in R$ has a multiplicative inverse, i.e., there exists $b \in R$ such that $ab = ba = 1$. A commutative division ring is called a *field.*

More examples of rings follow.

Examples

(1) The simplest examples of rings are the *trivial rings* obtained by taking R to be any commutative group (denoting the group operation by $+$) and defining the multiplication $\times$ on R by $a \times b = 0$ for all $a, b \in R$. It is easy to see that this multiplication defines a commutative ring. In particular, if $R = \{0\}$ is the trivial group, the resulting ring R is called the *zero ring*, denoted $R = 0$. Except for the zero ring, a trivial ring does not contain an identity ($R = 0$ is the only ring where $1 = 0$; we shall often exclude this ring by imposing the condition $1 \neq 0$). Although trivial rings have two binary operations, multiplication adds no new structure to the additive group and the theory of rings gives no information which could not already be obtained from (abelian) group theory.

(2) The ring of integers, $\mathbb{Z}$, under the usual operations of addition and multiplication is a commutative ring with identity (the integer 1). The ring axioms (as with the additive group axioms) follow from the basic axioms for the system of natural numbers. Note that under *multiplication* $\mathbb{Z}-\{0\}$ is *not* a group (in fact, there are very few multiplicative inverses to elements in this ring). We shall come back to the question of these inverses shortly.

(3) Similarly, the rational numbers, $\mathbb{Q}$, the real numbers, $\mathbb{R}$, and the complex numbers, $\mathbb{C}$, are commutative rings with identity (in fact they are fields). The ring axioms for each of these follow ultimately from the ring axioms for $\mathbb{Z}$. We shall verify this when we construct $\mathbb{Q}$ from $\mathbb{Z}$ (Section 7.5) and $\mathbb{C}$ from $\mathbb{R}$ (Example 1, Section 13.1); both of these constructions will be special cases of more general processes. The construction of $\mathbb{R}$ from $\mathbb{Q}$ (and subsequent verification of the ring axioms) is carried out in basic analysis texts.

(4) The quotient group $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with identity (the element $\bar{1}$) under the operations of addition and multiplication of residue classes (frequently referred to as "modular arithmetic"). We saw that the additive abelian group axioms followed from the general principles of the theory of quotient groups (indeed this was the prototypical quotient group). We shall shortly prove that the remaining ring axioms (in particular, the fact that multiplication of residue classes is well defined) follow analogously from the general theory of quotient rings.

In all of the examples so far the rings have been commutative. Historically, one of the first noncommutative rings was discovered in 1843 by Sir William Rowan Hamilton (1805–1865). This ring, which is a division ring, was extremely influential in the subsequent development of mathematics and it continues to play an important role in certain areas of mathematics and physics.

(5) (The *(real) Hamilton Quaternions*) Let $\mathbb{H}$ be the collection of elements of the form $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ are real numbers (loosely, "polynomials in $1, i, j, k$ with real coefficients") where addition is defined "componentwise" by

$$(a+bi+cj+dk) + (a'+b'i+c'j+d'k) = (a+a') + (b+b')i + (c+c')j + (d+d')k$$

and multiplication is defined by expanding $(a + bi + cj + dk)(a' + b'i + c'j + d'k)$ using the distributive law (being careful about the order of terms) and simplifying