| Year | Subject Title | Sem. | Sub Code |
|---|---|---|---|
| 2018 -19 Onwards | ABSTRACT ALGEBRA | IV | |

**OBJECTIVES:**

To introduce concepts and algebraic structures of Groups and Rings with additional operations and axioms.

**UNIT: IV**

**RING THEORY:** Definition and examples of Rings – Some special classes of Rings – Homomorphism – Ideals and Quotient Rings.

(Chapter 3 – Sections: 3.1 to 3.4)

## 3.1 Definition and Examples of Rings

As we indicated in Chapter 2, there are certain algebraic systems which serve as the building blocks for the structures comprising the subject which is today called modern algebra. At this stage of the development we have learned something about one of these, namely groups. It is our purpose now to introduce and to study a second such, namely rings. The abstract concept of a group has its origins in the set of mappings, or permutations, of a set onto itself. In contrast, rings stem from another and more familiar source, the set of integers. We shall see that they are patterned after, and are generalizations of, the algebraic aspects of the ordinary integers.

In the next paragraph it will become clear that a ring is quite different from a group in that it is a two-operational system; these operations are usually called addition and multiplication. Yet, despite the differences, the analysis of rings will follow the pattern already laid out for groups. We shall require the appropriate analogs of homomorphism, normal subgroups, factor groups, etc. With the experience gained in our study of groups we shall be able to make the requisite definitions, intertwine them with meaningful theorems, and end up proving results which are both interesting and important about mathematical objects with which we have had long acquaintance. To cite merely one instance, later on in the book, using the tools developed here, we shall prove that it is impossible to trisect an angle of 60° using only a straight-edge and compass.

**DEFINITION** A nonempty set $R$ is said to be an *associative ring* if in $R$ there are defined two operations, denoted by $+$ and $\cdot$ respectively, such that for all $a, b, c$ in $R$:

1. $a + b$ is in $R$.
2. $a + b = b + a$.
3. $(a + b) + c = a + (b + c)$.
4. There is an element 0 in $R$ such that $a + 0 = a$ (for every $a$ in $R$).
5. There exists an element $-a$ in $R$ such that $a + (-a) = 0$.
6. $a \cdot b$ is in $R$.
7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
8. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ (the two distributive laws).

Axioms 1 through 5 merely state that $R$ is an abelian group under the operation $+$, which we call addition. Axioms 6 and 7 insist that $R$ be closed under an associative operation $\cdot$, which we call multiplication. Axiom 8 serves to interrelate the two operations of $R$.

Whenever we speak of ring it will be understood we mean associative ring. Nonassociative rings, that is, those in which axiom 7 may fail to hold, do occur in mathematics and are studied, but we shall have no occasion to consider them.

It may very well happen, or not happen, that there is an element 1 in $R$ such that $a \cdot 1 = 1 \cdot a = a$ for every $a$ in $R$; if there is such we shall describe $R$ as a *ring with unit element.*

If the multiplication of $R$ is such that $a \cdot b = b \cdot a$ for every $a, b$ in $R$, then we call $R$ a *commutative ring.*

Before going on to work out some properties of rings, we pause to examine some examples. Motivated by these examples we shall define various special types of rings which are of importance.

**Example 3.1.1** $R$ is the set of integers, positive, negative, and 0; $+$ is the usual addition and $\cdot$ the usual multiplication of integers. $R$ is a commutative ring with unit element.

**Example 3.1.2** $R$ is the set of even integers under the usual operations of addition and multiplication. $R$ is a commutative ring but has no unit element.

**Example 3.1.3** $R$ is the set of rational numbers under the usual addition and multiplication of rational numbers. $R$ is a commutative ring with unit element. But even more than that, note that the elements of $R$ different from 0 form an abelian group under multiplication. A ring with this latter property is called a *field.*

**Example 3.1.4** $R$ is the set of integers mod 7 under the addition and multiplication mod 7. That is, the elements of $R$ are the seven symbols $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$, where

1. $\bar{i} + \bar{j} = \bar{k}$ where $k$ is the remainder of $i + j$ on division by 7 (thus, for instance, $\bar{4} + \bar{5} = \bar{2}$ since $4 + 5 = 9$, which, when divided by 7, leaves a remainder of 2).
2. $\bar{i} \cdot \bar{j} = \bar{m}$ where $m$ is the remainder of $ij$ on division by 7 (thus, $\bar{5} \cdot \bar{3} = \bar{1}$ since $5 \cdot 3 = 15$ has 1 as a remainder on division by 7).

The student should verify that $R$ is a commutative ring with unit element. However, much more can be shown; namely, since

$$\bar{1} \cdot \bar{1} = \bar{1} = \bar{6} \cdot \bar{6},$$
$$\bar{2} \cdot \bar{4} = \bar{1} = \bar{4} \cdot \bar{2},$$
$$\bar{3} \cdot \bar{5} = \bar{1} = \bar{5} \cdot \bar{3},$$

the nonzero elements of $R$ form an abelian group under multiplication. $R$ is thus a field. Since it only has a finite number of elements it is called a *finite field.*

**Example 3.1.5** $R$ is the set of integers mod 6 under addition and multiplication mod 6. If we denote the elements in $R$ by $\bar{0}, \bar{1}, \bar{2}, \ldots, \bar{5}$, one sees that $\bar{2} \cdot \bar{3} = \bar{0}$, yet $\bar{2} \neq \bar{0}$ and $\bar{3} \neq \bar{0}$. *Thus it is possible in a ring $R$ that $a \cdot b = 0$ with neither $a = 0$ nor $b = 0$.* This cannot happen in a field (see Problem 10, end of Section 3.2), thus the ring $R$ in this example is certainly not a field.

Every example given so far has been a commutative ring. We now present a noncommutative ring.

**Example 3.1.6** $R$ will be the set of all symbols

$$\alpha_{11}e_{11} + \alpha_{12}e_{12} + \alpha_{21}e_{21} + \alpha_{22}e_{22} = \sum_{i,j=1}^{2} \alpha_{ij}e_{ij},$$

where all the $\alpha_{ij}$ are rational numbers and where we decree

$$\sum_{i,j=1}^{2} \alpha_{ij}e_{ij} = \sum_{i,j=1}^{2} \beta_{ij}e_{ij} \tag{1}$$

if and only if for all $i, j = 1, 2$, $\alpha_{ij} = \beta_{ij}$,

$$\sum_{i,j=1}^{2} \alpha_{ij}e_{ij} + \sum_{i,j=1}^{2} \beta_{ij}e_{ij} = \sum_{i,j=1}^{2} (\alpha_{ij} + \beta_{ij})e_{ij}. \tag{2}$$

$$\left(\sum_{i,j=1}^{2} \alpha_{ij}e_{ij}\right) \cdot \left(\sum_{i,j=1}^{2} \beta_{ij}e_{ij}\right) = \sum_{i,j=1}^{2} \gamma_{ij}e_{ij}, \tag{3}$$

where

$$\gamma_{ij} = \sum_{\nu=1}^{2} \alpha_{i\nu}\beta_{\nu j} = \alpha_{i1}\beta_{1j} + \alpha_{i2}\beta_{2j}.$$

This multiplication, when first seen, looks rather complicated. However, it is founded on relatively simple rules, namely, multiply $\sum\alpha_{ij}e_{ij}$ by $\sum\beta_{ij}e_{ij}$ formally, multiplying out term by term, and collecting terms, and using the relations $e_{ij} \cdot e_{kl} = 0$ for $j \neq k$, $e_{ij} \cdot e_{jl} = e_{il}$ in this term-by-term collecting. (Of course those of the readers who have already encountered some linear algebra will recognize this example as the ring of all $2 \times 2$ matrices over the field of rational numbers.)

To illustrate the multiplication, if $a = e_{11} - e_{21} + e_{22}$ and $b = e_{22} + 3e_{12}$, then

$$\begin{aligned} a \cdot b &= (e_{11} - e_{21} + e_{22}) \cdot (e_{22} + 3e_{12}) \\ &= e_{11} \cdot e_{22} + 3e_{11} \cdot e_{12} - e_{21} \cdot e_{22} - 3e_{21} \cdot e_{12} + e_{22} \cdot e_{22} + 3e_{22} \cdot e_{12} \\ &= 0 + 3e_{12} - 0 - 3e_{22} + e_{22} + 0 \\ &= 3e_{12} - 3e_{22} + e_{22} = 3e_{12} - 2e_{22}. \end{aligned}$$

Note that $e_{11} \cdot e_{12} = e_{12}$ whereas $e_{12} \cdot e_{11} = 0$. Thus the multiplication in $R$ is not commutative. Also it is possible for $u \cdot v = 0$ with $u \neq 0$ and $v \neq 0$.

The student should verify that $R$ is indeed a ring. It is called the ring of $2 \times 2$ rational matrices. It, and its relative, will occupy a good deal of our time later on in the book.

**Example 3.1.7** Let $C$ be the set of all symbols $(\alpha, \beta)$ where $\alpha, \beta$ are real numbers. We define

$$(\alpha, \beta) = (\gamma, \delta) \text{ if and only if } \alpha = \gamma \text{ and } \beta = \delta. \tag{1}$$

In $C$ we introduce an addition by defining for $x = (\alpha, \beta), y = (\gamma, \delta)$

$$x + y = (\alpha, \beta) + (\gamma, \delta) = (\alpha + \gamma, \beta + \delta). \tag{2}$$

Note that $x + y$ is again in $C$. We assert that $C$ is an abelian group under this operation with $(0, 0)$ serving as the identity element for addition, and $(-\alpha, -\beta)$ as the inverse, under addition, of $(\alpha, \beta)$.

Now that $C$ is endowed with an addition, in order to make of $C$ a ring we still need a multiplication. We achieve this by defining

$$\text{for } X = (\alpha, \beta), \qquad Y = (\gamma, \delta) \text{ in } C,$$

$$X \cdot Y = (\alpha, \beta) \cdot (\gamma, \delta) = (\alpha\gamma - \beta\delta, \alpha\delta + \beta\gamma). \tag{3}$$

Note that $X \cdot Y = Y \cdot X$. Also $X \cdot (1, 0) = (1, 0) \cdot X = X$ so that $(1, 0)$ is a unit element for $C$.

Again we notice that $X \cdot Y \in C$. Also, if $X = (\alpha, \beta) \neq (0, 0)$ then, since $\alpha$, $\beta$ are real and not both 0, $\alpha^2 + \beta^2 \neq 0$; thus

$$Y = \left( \frac{\alpha}{\alpha^2 + \beta^2}, \frac{-\beta}{\alpha^2 + \beta^2} \right)$$

is in $C$. Finally we see that

$$(\alpha, \beta) \cdot \left( \frac{\alpha}{\alpha^2 + \beta^2}, \frac{-\beta}{\alpha^2 + \beta^2} \right) = (1, 0).$$

All in all we have shown that $C$ is a field. If we write $(\alpha, \beta)$ as $\alpha + \beta i$, the reader may verify that $C$ is merely a disguised form of the familiar complex numbers.

**Example 3.1.8** This last example is often called the ring of *real quaternions.* This ring was first described by the Irish mathematician Hamilton. Initially it was extensively used in the study of mechanics; today its primary interest is that of an important example, although it still plays key roles in geometry and number theory.

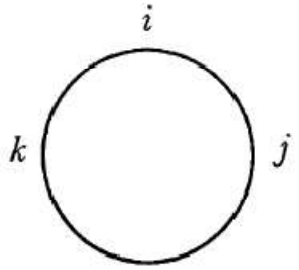
Let $Q$ be the set of all symbols $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, where all the numbers $\alpha_0$, $\alpha_1$, $\alpha_2$, and $\alpha_3$ are real numbers. We declare two such symbols, $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ and $\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$, to be equal if and only if $\alpha_t = \beta_t$ for $t = 0, 1, 2, 3$. In order to make $Q$ into a ring we must define a $+$ and a $\cdot$ for its elements. To this end we define

1. For any $X = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, $Y = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$ in $Q$, $X + Y = (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) + (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k) = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)i + (\alpha_2 + \beta_2)j + (\alpha_3 + \beta_3)k$

and

2. $X \cdot Y = (\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k) \cdot (\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k) = (\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)i + (\alpha_0\beta_2 + \alpha_2\beta_0 + \alpha_3\beta_1 - \alpha_1\beta_3)j + (\alpha_0\beta_3 + \alpha_3\beta_0 + \alpha_1\beta_2 - \alpha_2\beta_1)k.$

Admittedly this formula for the product seems rather formidable; however, it looks much more complicated than it actually is. It comes from multiplying out two such symbols formally and collecting terms using the relations $i^2 = j^2 = k^2 = ijk = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. The latter part of these relations, called the multiplication table of the quaternion units, can be remembered by the little diagram on page 125. As you go around clockwise you read off the product, e.g., $ij = k$, $jk = i$, $ki = j$; while going around counterclockwise you read off the negatives.




Notice that the elements $\pm 1, \pm i, \pm j, \pm k$ form a non-abelian group of order 8 under this product. In fact, this is the group we called the group of quaternion units in Chapter 2.

The reader may prove that $Q$ is a noncommutative ring in which $0 = 0 + 0i + 0j + 0k$ and $1 = 1 + 0i + 0j + 0k$ serve as the zero and unit elements respectively. Now if $X = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ is not 0, then not all of $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are 0; since they are real, $\beta = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \neq 0$ follows. Thus

$$Y = \frac{\alpha_0}{\beta} - \frac{\alpha_1}{\beta} i - \frac{\alpha_2}{\beta} j - \frac{\alpha_3}{\beta} k \in Q.$$

A simple computation now shows that $X \cdot Y = 1$. Thus the nonzero elements of $Q$ form a non-abelian group under multiplication. A ring in which the nonzero elements form a group is called a *division ring* or *skew-field*. Of course, a commutative division ring is a field. $Q$ affords us a division ring which is not a field. Many other examples of noncommutative division rings exist, but we would be going too far afield to present one here. The investigation of the nature of division rings and the attempts to classify them form an important part of algebra.

## 3.2 Some Special Classes of Rings

The examples just discussed in Section 3.1 point out clearly that although rings are a direct generalization of the integers, certain arithmetic facts to which we have become accustomed in the ring of integers need not hold in general rings. For instance, we have seen the possibility of $a \cdot b = 0$ with neither $a$ nor $b$ being zero. Natural examples exist where $a \cdot b \neq b \cdot a$. All these run counter to our experience heretofore.

For simplicity of notation we shall henceforth drop the dot in $a \cdot b$ and merely write this product as $ab$.

**DEFINITION** If $R$ is a commutative ring, then $a \neq 0 \in R$ is said to be a *zero-divisor* if there exists a $b \in R$, $b \neq 0$, such that $ab = 0$.

**DEFINITION** A commutative ring is an *integral domain* if it has no zero-divisors.

The ring of integers, naturally enough, is an example of an integral domain.

**DEFINITION** A ring is said to be a *division ring* if its nonzero elements form a group under multiplication.

The unit element under multiplication will be written as 1, and the inverse of an element $a$ under multiplication will be denoted by $a^{-1}$.

Finally we make the definition of the ultra-important object known as a field.

**DEFINITION** A *field* is a commutative division ring.

In our examples in Section 3.1, we exhibited the noncommutative division ring of real quaternions and the following fields: the rational numbers, complex numbers, and the integers mod 7. Chapter 5 will concern itself with fields and their properties.

We wish to be able to compute in rings in much the same manner in which we compute with real numbers, keeping in mind always that there are differences—it may happen that $ab \neq ba$, or that one cannot divide. To this end we prove the next lemma, which asserts that certain things we should like to be true in rings are indeed true.

**LEMMA 3.2.1** *If $R$ is a ring, then for all $a, b \in R$*

1. $a0 = 0a = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.

*If, in addition, $R$ has a unit element* 1, *then*

4. $(-1)a = -a$.
5. $(-1)(-1) = 1$.

*Proof.*

1. If $a \in R$, then $a0 = a(0 + 0) = a0 + a0$ (using the right distributive law), and since $R$ is a group under addition, this equation implies that $a0 = 0$.

   Similarly, $0a = (0 + 0)a = 0a + 0a$, using the left distributive law, and so here too, $0a = 0$ follows.
2. In order to show that $a(-b) = -(ab)$ we must demonstrate that $ab + a(-b) = 0$. But $ab + a(-b) = a(b + (-b)) = a0 = 0$ by use of

the distributive law and the result of part 1 of this lemma. Similarly $(-a)b = -(ab)$.

3. That $(-a)(-b) = ab$ is really a special case of part 2; we single it out since its analog in the case of real numbers has been so stressed in our early education. So on with it:

$$\begin{aligned}(-a)(-b) &= -(a(-b)) \quad \text{(by part 2)}\\ &= -(-(ab)) \quad \text{(by part 2)}\\ &= ab\end{aligned}$$

since $-(-x) = x$ is a consequence of the fact that in any group $(u^{-1})^{-1} = u$.

4. Suppose that $R$ has a unit element 1; then $a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0$, whence $(-1)a = -a$. In particular, if $a = -1$, $(-1)(-1) = -(-1) = 1$, which establishes part 5.

With this lemma out of the way we shall, from now on, feel free to compute with negatives and 0 as we always have in the past. The result of Lemma 3.2.1 is our permit to do so. For convenience, $a + (-b)$ will be written $a - b$.

The lemma just proved, while it is very useful and important, is not very exciting. So let us proceed to results of greater interest. Before we do so, we enunciate a principle which, though completely trivial, provides a mighty weapon when wielded properly. This principle says no more or less than the following: if a postman distributes 101 letters to 100 mailboxes then some mailbox must receive at least two letters. It does not sound very promising as a tool, does it? Yet it will surprise us! Mathematical ideas can often be very difficult and obscure, but no such argument can be made against this very simple-minded principle given above. We formalize it and even give it a name.

**THE PIGEONHOLE PRINCIPLE** *If $n$ objects are distributed over $m$ places, and if $n > m$, then some place receives at least two objects.*

An equivalent formulation, and one which we shall often use is: If $n$ objects are distributed over $n$ places in such a way that no place receives more than one object, then each place receives *exactly* one object.

We immediately make use of this idea in proving

**LEMMA 3.2.2** *A finite integral domain is a field.*

***Proof.*** As we may recall, an integral domain is a commutative ring such that $ab = 0$ if and only if at least one of $a$ or $b$ is itself 0. A field, on the other hand, is a commutative ring with unit element in which every non-zero element has a multiplicative inverse in the ring.

Let $D$ be a finite integral domain. In order to prove that $D$ is a field we must

1. Produce an element $1 \in D$ such that $a1 = a$ for every $a \in D$.
2. For every element $a \neq 0 \in D$ produce an element $b \in D$ such that $ab = 1$.

Let $x_1, x_2, \ldots, x_n$ be all the elements of $D$, and suppose that $a \neq 0 \in D$. Consider the elements $x_1a, x_2a, \ldots, x_na$; they are all in $D$. We claim that they are all distinct! For suppose that $x_ia = x_ja$ for $i \neq j$; then $(x_i - x_j)a = 0$. Since $D$ is an integral domain and $a \neq 0$, this forces $x_i - x_j = 0$, and so $x_i = x_j$, contradicting $i \neq j$. Thus $x_1a, x_2a, \ldots, x_na$ are $n$ distinct elements lying in $D$, which has exactly $n$ elements. By the pigeonhole principle these must account for all the elements of $D$; stated otherwise, every element $y \in D$ can be written as $x_ia$ for some $x_i$. In particular, since $a \in D$, $a = x_{i_0}a$ for some $x_{i_0} \in D$. Since $D$ is commutative, $a = x_{i_0}a = ax_{i_0}$. We propose to show that $x_{i_0}$ acts as a unit element for every element of $D$. For, if $y \in D$, as we have seen, $y = x_ia$ for some $x_i \in D$, and so $yx_{i_0} = (x_ia)x_{i_0} = x_i(ax_{i_0}) = x_ia = y$. Thus $x_{i_0}$ is a unit element for $D$ and we write it as 1. Now $1 \in D$, so by our previous argument, it too is realizable as a multiple of $a$; that is, there exists a $b \in D$ such that $1 = ba$. The lemma is now completely proved.

COROLLARY *If $p$ is a prime number then $J_p$, the ring of integers* mod $p$, *is a field.*

*Proof.* By the lemma it is enough to prove that $J_p$ is an integral domain, since it only has a finite number of elements. If $a, b \in J_p$ and $ab \equiv 0$, then $p$ must divide the ordinary integer $ab$, and so $p$, being a prime, must divide $a$ or $b$. But then either $a \equiv 0 \bmod p$ or $b \equiv 0 \bmod p$, hence in $J_p$ one of these is 0.

The corollary above assures us that we can find an infinity of fields having a finite number of elements. Such fields are called *finite fields*. The fields $J_p$ do not give all the examples of finite fields; there are others. In fact, in Section 7.1 we give a complete description of all finite fields.

We point out a striking difference between finite fields and fields such as the rational numbers, real numbers, or complex numbers, with which we are more familiar.

Let $F$ be a finite field having $q$ elements (if you wish, think of $J_p$ with its $p$ elements). Viewing $F$ merely as a group under addition, since $F$ has $q$ elements, by Corollary 2 to Theorem 2.4.1,

$$\underbrace{a + a + \cdots + a}_{q\text{-times}} = qa = 0$$

for any $a \in F$. Thus, in $F$, we have $qa = 0$ for some positive integer $q$, even if $a \neq 0$. This certainly cannot happen in the field of rational numbers, for instance. We formalize this distinction in the definitions we give below. In these definitions, instead of talking just about fields, we choose to widen the scope a little and talk about integral domains.

**DEFINITION** An integral domain $D$ is said to be of *characteristic* 0 if the relation $ma = 0$, where $a \neq 0$ is in $D$, and where $m$ is an integer, can hold only if $m = 0$.

The ring of integers is thus of characteristic 0, as are other familiar rings such as the even integers or the rationals.

**DEFINITION** An integral domain $D$ is said to be of *finite characteristic* if there exists a *positive* integer $m$ such that $ma = 0$ for all $a \in D$.

If $D$ is of finite characteristic, then we define the *characteristic* of $D$ to be the smallest positive integer $p$ such that $pa = 0$ for all $a \in D$. It is not too hard to prove that if $D$ *is of finite characteristic, then its characteristic is a prime number* (see Problem 6 below).

As we pointed out, any finite field is of finite characteristic. However, an integral domain may very well be infinite yet be of finite characteristic (see Problem 7).

One final remark on this question of characteristic: Why define it for integral domains, why not for arbitrary rings? The question is perfectly reasonable. Perhaps the example we give now points out what can happen if we drop the assumption "integral domain."

Let $R$ be the set of all triples $(a, b, c)$, where $a \in J_2$, the integers mod 2, $b \in J_3$, the integers mod 3, and $c$ is any integer. We introduce a $+$ and a $\cdot$ to make of $R$ a ring. We do so by defining $(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$ and $(a_1, b_1, c_1) \cdot (a_2, b_2, c_2) = (a_1a_2, b_1b_2, c_1c_2)$. It is easy to verify that $R$ is a commutative ring. It is not an integral domain since $(1, 2, 0) \cdot (0, 0, 7) = (0, 0, 0)$, the zero-element of $R$. Note that in $R$, $2(1, 0, 0) = (1, 0, 0) + (1, 0, 0) = (2, 0, 0) = (0, 0, 0)$ since addition in the first component is in $J_2$. Similarly $3(0, 1, 0) = (0, 0, 0)$. Finally, for *no* positive integer $m$ is $m(0, 0, 1) = (0, 0, 0)$.

Thus, from the point of view of the definition we gave above for characteristic, the ring $R$, which we just looked at, is neither fish nor fowl. The definition just doesn't have any meaning for $R$. We could generalize the notion of characteristic to arbitrary rings by doing it locally, defining it relative to given elements, rather than globally for the ring itself. We say that $R$ has $n$-torsion, $n > 0$, if there is an element $a \neq 0$ in $R$ such that $na = 0$, and $ma \neq 0$ for $0 < m < n$. For an integral domain $D$, it turns

out that if $D$ has $n$-torsion, even for one $n > 0$, then it must be of finite characteristic (see Problem 8).

## Problems

$R$ is a ring in all the problems.

1. If $a, b, c, d \in R$, evaluate $(a + b)(c + d)$.
2. Prove that if $a, b \in R$, then $(a + b)^2 = a^2 + ab + ba + b^2$, where by $x^2$ we mean $xx$.
3. Find the form of the binomial theorem in a general ring; in other words, find an expression for $(a + b)^n$, where $n$ is a positive integer.
4. If every $x \in R$ satisfies $x^2 = x$, prove that $R$ must be commutative. (A ring in which $x^2 = x$ for all elements is called a *Boolean* ring.)
5. If $R$ is a ring, merely considering it as an abelian group under its addition, we have defined, in Chapter 2, what is meant by $na$, where $a \in R$ and $n$ is an integer. Prove that if $a, b \in R$ and $n, m$ are integers, then $(na)(mb) = (nm)(ab)$.
6. If $D$ is an integeral domain and $D$ is of finite characteristic, prove that the characteristic of $D$ is a prime number.
7. Give an example of an integral domain which has an infinite number of elements, yet is of finite characteristic.
8. If $D$ is an integral domain and if $na = 0$ for some $a \neq 0$ in $D$ and some integer $n \neq 0$, prove that $D$ is of finite characteristic.
9. If $R$ is a system satisfying all the conditions for a ring with unit element with the possible exception of $a + b = b + a$, prove that the axiom $a + b = b + a$ must hold in $R$ and that $R$ is thus a ring. (*Hint:* Expand $(a + b)(1 + 1)$ in two ways.)
10. Show that the commutative ring $D$ is an integral domain if and only if for $a, b, c \in D$ with $a \neq 0$ the relation $ab = ac$ implies that $b = c$.
11. Prove that Lemma 3.2.2 is false if we drop the assumption that the integral domain is finite.
12. Prove that any field is an integral domain.
13. Useing the pigeonhole principle, prove that if $m$ and $n$ are relatively prime integers and $a$ and $b$ are any integers, there exists an integer $x$ such that $x \equiv a \bmod m$ and $x \equiv b \bmod n$. (*Hint:* Consider the remainders of $a, a + m, a + 2m, \ldots, a + (n - 1)m$ on division by $n$.)
14. Using the pigeonhole principle, prove that the decimal expansion of a rational number must, after some point, become repeating.

## 3.3 Homomorphisms

In studying groups we have seen that the concept of a homomorphism turned out to be a fruitful one. This suggests that the appropriate analog for rings could also lead to important ideas. To recall, for groups a homomorphism was defined as a mapping such that $\phi(ab) = \phi(a)\phi(b)$. Since a ring has two operations, what could be a more natural extension of this type of formula than the

**DEFINITION** A mapping $\phi$ from the ring $R$ into the ring $R'$ is said to be a *homomorphism* if

1. $\phi(a + b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$,

for all $a, b \in R$.

As in the case of groups, let us again stress here that the $+$ and $\cdot$ occurring on the left-hand sides of the relations in 1 and 2 are those of $R$, whereas the $+$ and $\cdot$ occurring on the right-hand sides are those of $R'$.

A useful observation to make is that a homomorphism of one ring, $R$, into another, $R'$, is, if we totally ignore the multiplications in both these rings, at least a homomorphism of $R$ into $R'$ when we consider them as abelian groups under their respective additions. Therefore, as far as addition is concerned, all the properties about homomorphisms of groups proved in Chapter 2 carry over. In particular, merely restating Lemma 2.7.2 for the case of the additive group of a ring yields for us

**LEMMA 3.3.1** *If $\phi$ is a homomorphism of $R$ into $R'$, then*

1. $\phi(0) = 0$.
2. $\phi(-a) = -\phi(a)$ *for every* $a \in R$.

A word of caution: if both $R$ and $R'$ have the respective unit elements 1 and 1′ for their multiplications it need not follow that $\phi(1) = 1'$. However, if $R'$ is an integral domain, or if $R'$ is arbitrary but $\phi$ is onto, then $\phi(1) = 1'$ is indeed true.

In the case of groups, given a homomorphism we associated with this homomorphism a certain subset of the group which we called the kernel of the homomorphism. What should the appropriate definition of the kernel of a homomorphism be for rings? After all, the ring has two operations, addition and multiplication, and it might be natural to ask which of these should be singled out as the basis for the definition. However, the choice is clear. Built into the definition of an arbitrary ring is the condition that the ring forms an abelian group under addition. The ring multiplication

was left much more unrestricted, and so, in a sense, much less under our control than is the addition. For this reason the emphasis is given to the operation of addition in the ring, and we make the

**DEFINITION** If $\phi$ is a homomorphism of $R$ into $R'$ then the *kernel of* $\phi$, $I(\phi)$, is the set of all elements $a \in R$ such that $\phi(a) = 0$, the zero-element of $R'$.

**LEMMA 3.3.2** *If $\phi$ is a homomorphism of $R$ into $R'$ with kernel $I(\phi)$, then*

1. *$I(\phi)$ is a subgroup of $R$ under addition.*
2. *If $a \in I(\phi)$ and $r \in R$ then both $ar$ and $ra$ are in $I(\phi)$.*

*Proof.* Since $\phi$ is, in particular, a homomorphism of $R$, as an additive group, into $R'$, as an additive group, (1) follows directly from our results in group theory.

To see (2), suppose that $a \in I(\phi)$, $r \in R$. Then $\phi(a) = 0$ so that $\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$ by Lemma 3.2.1. Similarly $\phi(ra) = 0$. Thus by defining property of $I(\phi)$ both $ar$ and $ra$ are in $I(\phi)$.

Before proceeding we examine these concepts for certain examples.

**Example 3.3.1** Let $R$ and $R'$ be two arbitrary rings and define $\phi(a) = 0$ for all $a \in R$. Trivially $\phi$ is a homomorphism and $I(\phi) = R$. $\phi$ is called the zero-homomorphism.

**Example 3.3.2** Let $R$ be a ring, $R' = R$ and define $\phi(x) = x$ for every $x \in R$. Clearly $\phi$ is a homomorphism and $I(\phi)$ consists only of 0.

**Example 3.3.3** Let $J(\sqrt{2})$ be all real numbers of the form $m + n\sqrt{2}$ where $m$, $n$ are integers; $J(\sqrt{2})$ forms a ring under the usual addition and multiplication of real numbers. (Verify!) Define $\phi: J(\sqrt{2}) \to J(\sqrt{2})$ by $\phi(m + n\sqrt{2}) = m - n\sqrt{2}$. $\phi$ is a homomorphism of $J(\sqrt{2})$ onto $J(\sqrt{2})$ and its kernel $I(\phi)$, consists only of 0. (Verify!)

**Example 3.3.4** Let $J$ be the ring of integers, $J_n$, the ring of integers modulo $n$. Define $\phi: J \to J_n$ by $\phi(a) =$ remainder of $a$ on division by $n$. The student should verify that $\phi$ is a homomorphism of $J$ onto $J_n$ and that the kernel, $I(\phi)$, of $\phi$ consists of all multiples of $n$.

**Example 3.3.5** Let $R$ be the set of all continuous, real-valued functions on the closed unit interval. $R$ is made into a ring by the usual addition and multiplication of functions; that it is a ring is a consequence of the fact that the sum and product of two continuous functions are continuous

functions. Let $F$ be the ring of real numbers and define $\phi: R \to F$ by $\phi(f(x)) = f(\frac{1}{2})$. $\phi$ is then a homomorphism of $R$ onto $F$ and its kernel consists of all functions in $R$ vanishing at $x = \frac{1}{2}$.

All the examples given here have used commutative rings. Many beautiful examples exist where the rings are noncommutative but it would be premature to discuss such an example now.

**DEFINITION** A homomorphism of $R$ into $R'$ is said to be an *isomorphism* if it is a one-to-one mapping.

**DEFINITION** Two rings are said to be *isomorphic* if there is an isomorphism of one *onto* the other.

The remarks made in Chapter 2 about the meaning of an isomorphism and of the statement that two groups are isomorphic carry over verbatim to rings. Likewise, the criterion given in Lemma 2.7.4 that a homomorphism be an isomorphism translates directly from groups to rings in the form

**LEMMA 3.3.3** *The homomorphism $\phi$ of $R$ into $R'$ is an isomorphism if and only if $I(\phi) = (0)$.*

## 3.4 Ideals and Quotient Rings

Once the idea of a homomorphism and its kernel have been set up for rings, based on our experience with groups, it should be fruitful to carry over some analog to rings of the concept of normal subgroup. Once this is achieved, one would hope that this analog would lead to a construction in rings like that of the quotient group of a group by a normal subgroup. Finally, if one were an optimist, one would hope that the homomorphism theorems for groups would come over in their entirety to rings.

Fortunately all this can be done, thereby providing us with an incisive technique for analyzing rings.

The first business at hand, then, seems to be to define a suitable "normal subgroup" concept for rings. With a little hindsight this is not difficult. If you recall, normal subgroups eventually turned out to be nothing else than kernels of homomorphisms, even though their primary defining conditions did not involve homomorphisms. Why not use this observation as the keystone to our definition for rings? Lemma 3.3.2 has already provided us with some conditions that a subset of a ring be the kernel of a homomorphism. We now take the point of view that, since no other information is at present available to us, we shall make the conclusions of Lemma 3.3.2 as the starting point of our endeavor, and so we define

DEFINITION A nonempty subset $U$ of $R$ is said to be a (two-sided) *ideal* of $R$ if

1. $U$ is a subgroup of $R$ under addition.
2. For every $u \in U$ and $r \in R$, both $ur$ and $ru$ are in $U$.

Condition 2 asserts that $U$ "swallows up" multiplication from the right and left by arbitrary ring elements. For this reason $U$ is usually called a two-sided ideal. Since we shall have no occasion, other than in some of the problems, to use any other derivative concept of ideal, we shall merely use the word ideal, rather than two-sided ideal, in all that follows.

Given an ideal $U$ of a ring $R$, let $R/U$ be the set of all the distinct cosets of $U$ in $R$ which we obtain by considering $U$ as a subgroup of $R$ under addition. We note that we merely say coset, rather than right coset or left coset; this is justified since $R$ is an abelian group under addition. To restate what we have just said, $R/U$ consists of all the cosets, $a + U$, where $a \in R$. By the results of Chapter 2, $R/U$ is automatically a group under addition; this is achieved by the composition law $(a + U) + (b + U) = (a + b) + U$. In order to impose a ring structure on $R/U$ we must define, in it, a multiplication. What is more natural than to define $(a + U)(b + U) = ab + U$? However, we must make sure that this is meaningful. Otherwise put, we are obliged to show that if $a + U = a' + U$ and $b + U = b' + U$, then under our definition of the multiplication, $(a + U)(b + U) = (a' + U)(b' + U)$. Equivalently, it must be established that $ab + U = a'b' + U$. To this end we first note that since $a + U = a' + U$, $a = a' + u_1$, where $u_1 \in U$; similarly $b = b' + u_2$ where $u_2 \in U$. Thus $ab = (a' + u_1)(b + u_2) = a'b' + u_1b' + a'u_2 + u_1u_2$; *since $U$ is an ideal of* $R$, $u_1b' \in U$, $a'u_2 \in U$, and $u_1u_2 \in U$. Consequently $u_1b' + a'u_2 + u_1u_2 = u_3 \in U$. But then $ab = a'b' + u_3$, from which we deduce that $ab + U = a'b' + u_3 + U$, and since $u_3 \in U$, $u_3 + U = U$. The net consequence of all this is that $ab + U = a'b' + U$. We at least have achieved the principal step on the road to our goal, namely of introducing a well-defined multiplication. The rest now becomes routine. To establish that $R/U$ is a ring we merely have to go through the various axioms which define a ring and check whether they hold in $R/U$. All these verifications have a certain sameness to them, so we pick one axiom, the right distributive law, and prove it holds in $R/U$. The rest we leave to the student as informal exercises. If $X = a + U$, $Y = b + U$, $Z = c + U$ are three elements of $R/U$, where $a, b, c \in R$, then $(X + Y)Z = ((a + U) + (b + U))(c + U) = ((a + b) + U)(c + U) = (a + b)c + U = ac + bc + U = (ac + U) + (bc + U) = (a + U)(c + U) + (b + U)(c + U) = XZ + YZ$.

$R/U$ has now been made into a ring. Clearly, if $R$ is commutative then so is $R/U$, for $(a + U)(b + U) = ab + U = ba + U = (b + U)(a + U)$. (The converse to this is false.) If $R$ has a unit element 1, then $R/U$ has a

unit element $1 + U$. We might ask: In what relation is $R/U$ to $R$? With the experience we now have in hand this is easy to answer. There is a homomorphism $\phi$ of $R$ *onto* $R/U$ given by $\phi(a) = a + U$ for every $a \in R$, whose kernel is exactly $U$. (The reader should verify that $\phi$ so defined is a homomorphism of $R$ onto $R/U$ with kernel $U$.)

We summarize these remarks in

**LEMMA 3.4.1** *If $U$ is an ideal of the ring $R$, then $R/U$ is a ring and is a homomorphic image of $R$.*

With this construction of the *quotient ring* of a ring by an ideal satisfactorily accomplished, we are ready to bring over to rings the homomorphism theorems of groups. Since the proof is an exact verbatim translation of that for groups into the language of rings we merely state the theorem without proof, referring the reader to Chapter 2 for the proof.

**THEOREM 3.4.1** *Let $R$, $R'$ be rings and $\phi$ a homomorphism of $R$ onto $R'$ with kernel $U$. Then $R'$ is isomorphic to $R/U$. Moreover there is a one-to-one correspondence between the set of ideals of $R'$ and the set of ideals of $R$ which contain $U$. This correspondence can be achieved by associating with an ideal $W'$ in $R'$ the ideal $W$ in $R$ defined by $W = \{x \in R \mid \phi(x) \in W'\}$. With $W$ so defined, $R/W$ is isomorphic to $R'/W'$.*

## Problems

1. If $U$ is an ideal of $R$ and $1 \in U$, prove that $U = R$.
2. If $F$ is a field, prove its only ideals are (0) and $F$ itself.
3. Prove that any homomorphism of a field is either an isomorphism or takes each element into 0.
4. If $R$ is a commutative ring and $a \in R$,
   (a) Show that $aR = \{ar \mid r \in R\}$ is a two-sided ideal of $R$.
   (b) Show by an example that this may be false if $R$ is not commutative.
5. If $U$, $V$ are ideals of $R$, let $U + V = \{u + v \mid u \in U, v \in V\}$. Prove that $U + V$ is also an ideal.
6. If $U$, $V$ are ideals of $R$ let $UV$ be the set of all elements that can be written as finite sums of elements of the form $uv$ where $u \in U$ and $v \in V$. Prove that $UV$ is an ideal of $R$.
7. In Problem 6 prove that $UV \subset U \cap V$.
8. If $R$ is the ring of integers, let $U$ be the ideal consisting of all multiples of 17. Prove that if $V$ is an ideal of $R$ and $R \supset V \supset U$ then either $V = R$ or $V = U$. Generalize!

9. If $U$ is an ideal of $R$, let $r(U) = \{x \in R \mid xu = 0 \text{ for all } u \in U\}$. Prove that $r(U)$ is an ideal of $R$.

10. If $U$ is an ideal of $R$ let $[R:U] = \{x \in R \mid rx \in U \text{ for every } r \in R\}$. Prove that $[R:U]$ is an ideal of $R$ and that it contains $U$.

11. Let $R$ be a ring with unit element. Using its elements we define a ring $\tilde{R}$ by defining $a \oplus b = a + b + 1$, and $a \cdot b = ab + a + b$, where $a, b \in R$ and where the addition and multiplication on the right-hand side of these relations are those of $R$.
    (a) Prove that $\tilde{R}$ is a ring under the operations $\oplus$ and $\cdot$.
    (b) What acts as the zero-element of $\tilde{R}$?
    (c) What acts as the unit-element of $\tilde{R}$?
    (d) Prove that $R$ is isomorphic to $\tilde{R}$.

*12. In Example 3.1.6 we discussed the ring of rational $2 \times 2$ matrices. Prove that this ring has no ideals other than (0) and the ring itself.

*13. In Example 3.1.8 we discussed the real quaternions. Using this as a model we define the quaternions over the integers mod $p$, $p$ an odd prime number, in exactly the same way; however, now considering all symbols of the form $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, where $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ are integers mod $p$.
    (a) Prove that this is a ring with $p^4$ elements whose only ideals are (0) and the ring itself.
    **(b) Prove that this ring is *not* a division ring.

If $R$ is any ring a subset $L$ of $R$ is called a *left-ideal* of $R$ if
1. $L$ is a subgroup of $R$ under addition.
2 $r \in R$, $a \in L$ implies $ra \in L$.

(One can similarly define a *right-ideal.*) An ideal is thus simultaneously a left- and right-ideal of $R$.

14. For $a \in R$ let $Ra = \{xa \mid x \in R\}$. Prove that $Ra$ is a left-ideal of $R$.

15. Prove that the intersection of two left-ideals of $R$ is a left-ideal of $R$.

16. What can you say about the intersection of a left-ideal and right-ideal of $R$?

17. If $R$ is a ring and $a \in R$ let $r(a) = \{x \in R \mid ax = 0\}$. Prove that $r(a)$ is a right-ideal of $R$.

18. If $R$ is a ring and $L$ is a left-ideal of $R$ let $\lambda(L) = \{x \in R \mid xa = 0 \text{ for all } a \in L\}$. Prove that $\lambda(L)$ is a two-sided ideal of $R$.

*19. Let $R$ be a ring in which $x^3 = x$ for every $x \in R$. Prove that $R$ is a commutative ring.

20. If $R$ is a ring with unit element 1 and $\phi$ is a homomorphism of $R$ *onto* $R'$ prove that $\phi(1)$ is the unit element of $R'$.