The Carus Mathematical Monographs

NUMBER EIGHT

RINGS AND IDEALS

By

NEAL H. McCOY
Professor of Mathematics
Smith College

Published by
THE MATHEMATICAL ASSOCIATION OF AMERICA

PREFACE

During the last twenty or thirty years abstract algebra has been developed in very rapid fashion by an increasingly large number of research workers. In fact, the general methods and most fundamental results of the theory have become of considerable interest to mathematicians generally, even though their primary interests may lie in other directions. The purpose of this monograph is to present an introduction to that branch of abstract algebra having to do with the theory of rings, with some emphasis on the role of ideals in the theory.

Except for a knowledge of certain fundamental theorems about determinants which is assumed in Chapter VIII, and at one point in Chapter VII, the book is almost entirely self-contained. Of course, the reader must have a certain amount of "mathematical maturity" in order to understand the illustrative examples, and also to grasp the significance of the abstract approach. However, in so far as formal technique is concerned, little more than the elements of algebra are presupposed.

The first four chapters treat those fundamental concepts and results which are essential in a more advanced study of any branch of ring theory. The rest of the monograph deals with somewhat more specialized results which, however, are of fairly wide interest and application. Naturally, many other topics of equal significance have had to be omitted simply because of space limitations. For the most part, material has been chosen which does not require any finiteness assumptions on the rings considered—the concept of a chain condition is not even mentioned until late in the last chapter!

Chapter V consists primarily of an exposition of Krull's results on prime ideals in a commutative ring. Since no finiteness conditions are imposed, it is necessary to use transfinite methods in establishing the existence of the prime ideals. Actually, Zorn's Maximum Principle is all that is required, and this is carefully stated and illustrated at an appropriate point in the chapter.

An exposition of the theory of subdirect sums of rings is given in Chapter VI, together with a brief introduction to the Jacobson radical of a ring. Chapter VII is concerned with Boolean rings and with a number of algebraic generalizations of these rings. In particular, Stone's theorem on the representation of any Boolean ring as a ring of subsets of some set is obtained quite easily from results of the preceding chapter.

The theory of matrices with elements in a commutative ring is the subject of Chapter VIII. Obviously, in one brief chapter it is impossible to give a comprehensive account of the theory. However, this short exposition has been included partly because of the generality of the approach, and partly because the material furnishes illustrations of a number of fundamental methods in the elementary theory of rings. This chapter is independent of the two preceding chapters. Finally, Chapter IX is an introduction to the study of primary ideals in a commutative ring. It ends with a short discussion of Noetherian rings (rings with ascending chain condition) and a brief section on algebraic manifolds.

Since a considerable part of the material of this monograph has not previously appeared in book form, it has seemed desirable to give somewhat more complete references than might otherwise be the case. Accordingly, at the end of each chapter there appears a list of references to supplement the general material of the chapter, and also occasional source references to some of the more specific results which are not adequately treated in the available treatises. The bibliography at the back of the book is by no means complete; for the most part, only those items have been included to which reference is made at some point in the text.

It would be impossible to list here all the books and articles to which I am indebted. However, it may not be out of order to mention van der Waerden's *Moderne Algebra* which has played an important role in the development of widespread interest in abstract algebra. In so far as content is concerned, much of the first four chapters of this monograph, and a small part of the last, cover material which is included in van der Waerden's treatise.

I am greatly indebted to Professors Bailey Brown, R. E. Johnson, and Saunders MacLane, who have read the entire manuscript and made many valuable suggestions. In particular, Professor Brown has taken an active interest in this project from its very inception and I have profited much by many discussions with him. Not only has he read the manuscript in all its versions in an unusually careful and critical manner, but he also has been of invaluable assistance in reading the proofs.

NEAL HENRY McCOY

Northampton, Mass.
August 22, 1947

TABLE OF CONTENTS

CHAPTER PAGE

I. Definitions and Fundamental Properties

II. Polynomial Rings

III. Ideals and Homomorphisms

IV. Some Imbedding Theorems

V. Prime Ideals in Commutative Rings

VI. Direct and Subdirect Sums

此为试读，需要完整PDF请访问：www.ertongbook.com

Chapter I

DEFINITIONS AND FUNDAMENTAL PROPERTIES

1. **Definition of a ring.** Let us consider a set R of elements $a, b, c, \cdots$, such that for arbitrary elements a and b of R there is a uniquely defined *sum* $a + b$ and *product* ab (sometimes written as $a \cdot b$) which are also elements of R. The words *addition* and *multiplication*, as in the ordinary usage of elementary algebra, will be respectively associated with the operations of forming a sum, or a product, of elements of R. Such a set is said to be a *ring* if addition and multiplication have the five properties listed below, it being assumed that a, b, and c are arbitrary elements of R, either distinct or identical:

P_1. $a + (b + c) = (a + b) + c$ (*associative law of addition*);

P_2. $a + b = b + a$ (*commutative law of addition*);

P_3. *The equation* $a + x = b$ *has a solution* x *in* R;

P_4. $a(bc) = (ab)c$ (*associative law of multiplication*);

P_5. $a(b + c) = ab + ac$, $(b + c)a = ba + ca$ (*distributive laws*).

The importance of the concept of *ring* follows primarily from the fact that there are so many important mathematical systems of quite different types which are rings according to the above definition. Naturally, what they all have in common are the properties used in the definition of a ring, together with any properties which are logical consequences of these. Later on, we shall deduce a number of these logical consequences and thus obtain properties which all rings must have. However, before proceeding further in this direction, we pause to give a number of examples which will help to clarify the concepts involved and also to illustrate something of the variety of mathematical systems which are rings.

2. **Examples of rings.** In order to give an example of a ring, it is necessary to exhibit a set of elements and also to give definitions of addition and multiplication of these elements which satisfy the five properties listed above. In some of the illustrations to be given presently, the actual verification of these properties will be left to the reader since they follow by straightforward calculations, or are already well known.

In the first place, it is clear that many of the number systems of ordinary algebra are rings with respect to the usual definitions of addition and multiplication. Thus we have *the ring of even integers* (positive, negative and zero), *the ring of all integers*, *the ring of rational numbers*, *the ring of real numbers*, *the ring of complex numbers*. It will be noticed that each of these rings is contained in each of the ones following it, and is therefore said to be a *subring* of each following one. It is also readily verified that the set of all numbers of the form $a + b\sqrt{2}$, where a and b are rational, is a ring; as is also the set of all polynomials in a real variable, with real coefficients. Furthermore, since the sum and product of continuous functions are also continuous, it is easily seen that the class of all real functions which are continuous in an arbitrary fixed interval is a ring. It may also be shown that the set of all power series in a real variable, which converge in some interval, is a ring with respect to the usual definitions of addition and multiplication of power series.

The ring of all integers is of such fundamental importance and will be referred to so frequently that it will be convenient to have a consistent notation for this ring.

Hereafter, the letter I will be used to denote the ring of all integers.

In addition to these most familiar rings, we now give, in somewhat more detail, a few additional examples. As a matter of fact, most of the rings to be presented will be considered in later chapters and hence, at the present time, no attempt will be made to indicate the importance or significance of these examples. At this point, our primary purpose is to give some indication of the great variety of rings, and also to have a body of examples from which to obtain illustrations of the various results to be established in later sections.

Example 1. *The ring I_n of integers modulo n*, where n is any positive integer. The elements of this ring are the symbols $0', 1', 2', \cdots, (n-1)'$. If a' and b' are any of these elements, we define $a' + b'$ to be r', where r is the least nonnegative remainder when the ordinary sum of a and b is divided by n. Similarly, by $a'b'$ we mean s', where s is the least nonnegative remainder when the ordinary product of a and b is divided by n. Thus, by way of illustration, the ring I_6 of integers modulo 6 consists of the six elements $0', 1', 2', 3', 4', 5'$. If the ordinary sum of 4 and 5 is divided by 6, the remainder is 3, hence in this ring, $4' + 5' = 3'$. Similarly, $2' + 4' = 0'$, $2' \cdot 4' = 2'$, $2' \cdot 3' = 0'$, and so on.

To prove that I_n is actually a ring, it is necessary to use the well-known fact that in the division of any integer by n, the least nonnegative remainder is unique. In fact, it will be clear that this property is essential for the definitions of addition and multiplication given above. We shall prove the associative law of addition as an illustration of the method which may be used.

Let a', b', c' be any elements of I_n. If

$$a + b = q_1 n + r_1, \tag{1}$$

where $0 \leq r_1 < n$, then, by definition of addition in I_n,

$$a' + b' = r_1'.$$

Hence $(a' + b') + c' = r_1' + c'$. To compute this, we write

$$r_1 + c = q_2n + r_2, \tag{2}$$

where $0 \leq r_2 < n$, and thus

$$(a' + b') + c' = r_2'.$$

However, if we substitute the value of r_1 from (2) into equation (1), we see that

$$a + b + c = (q_1 + q_2)n + r_2,$$

and thus r_2 is the least nonnegative remainder in the division of $a + b + c$ by n. A similar calculation will show that

$$a' + (b' + c') = r_2',$$

and thus

$$(a' + b') + c' = a' + (b' + c'),$$

as desired.

Properties P_4 and P_5 follow by this same type of calculation, while P_2 is obvious. To prove P_3, we observe that if a' and b' are any elements of I_n, the equation $a' + x = b'$ has the solution $x = (b - a)'$ if $b \geq a$, and the solution $x = (n + b - a)'$ if $b < a$.

We may remark that the method by which the ring I_n is constructed from the ring of integers is a special case of an important procedure to be explained fully in Chapter III.

Example 2. *The ring B of all subsets of $\mathscr{I}$*, where $\mathscr{I}$ denotes the unit interval on the x-axis, that is, $\mathscr{I}$ is the set of all points with abscissa x such that $0 \leq x \leq 1$. A set of points of $\mathscr{I}$ is naturally called a *subset* of $\mathscr{I}$. For example, any single point of $\mathscr{I}$ is a subset of $\mathscr{I}$, as is also the set of all points with abscissa x such that $0 \leq x \leq \frac{1}{2}$. These are simple illustrations, but it is clear that there is a great variety of subsets. According to our definition, it will be seen that the set of *all* points of $\mathcal{S}$ is itself a subset of $\mathcal{S}$. It will also be convenient to consider that the *void set*, that is, the set which contains no points, is a subset of $\mathcal{S}$. This will serve to simplify various statements which otherwise would not always be true without exception.

If now B is the set of *all* subsets of $\mathcal{S}$, including the void set, we shall presently make B into a ring by suitable definitions of addition and multiplication. It may be emphasized that an *element* of B is a *subset* of $\mathcal{S}$.

Let a and b be any two elements of B. With reference to a and b, the points of $\mathcal{S}$ may be distributed into the following mutually exclusive classes, certain ones of which may happen to contain no points: (1) points in neither a nor b, (2) points in a but not in b, (3) points in b but not in a, (4) points in both a and b. This fact may be exhibited in a convenient but purely symbolic way as indicated in Fig. 1. Here a is represented by the points inside circle a, and b by the points inside circle b. The classes (1), (2), (3), and (4) are respectively represented by the regions marked 1, 2, 3, and 4 in the figure.

We are now ready to define addition and multiplication in B. By ab we mean the *intersection* of a and b, that is, the set of all points in both a and b. In Fig. 1, ab is thus exhibited as the set of points in region 4. We define $a + b$ to be the set of all points in a or in b *but not in both*. Thus, in Fig. 1, regions 2 and 3 together represent $a + b$.

It is obvious that if a and b have no points in common, ab is the void set. Hence the product of two subsets of $\mathcal{S}$ would not always be a subset of $\mathcal{S}$ if it were not for our agreement that the void set is to be so considered.

Properties P_2 and P_4 are almost obvious, but we shall

此为试读,需要完整PDF请访问: www.ertongbook.

indicate a method of proof of P_1. Let a, b, c be three elements of B. With reference to these elements, the points of $\mathcal{I}$ may be separated into eight mutually exclusive classes, as indicated in Fig. 2. Here a, b, c are represented symbolically by the points inside the circles marked a, b, and c respectively. We shall not enumerate the eight classes but may point out, by way of illustration, that region 2 represents the set of all points which are in a but in neither b nor c.

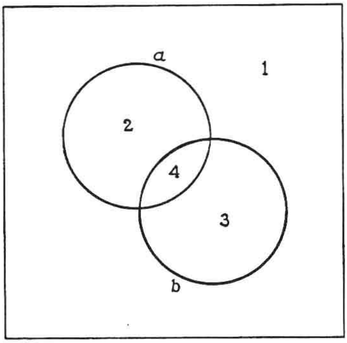

FIG. 1

Now $a + b$ is represented by regions 2, 3, 5, and 6. Since c is made up of regions 4, 5, 6, and 8, it is clear that $(a + b) + c$ is represented by regions 2, 3, 4, and 8. This graphical representation then suggests that we may characterize $(a + b) + c$ as the subset of $\mathcal{I}$ which consists of all points in exactly one of the sets a, b, c, together with those in all three. This can clearly be proved in a purely logical way without reference to the diagam, but the diagram does give a visual indication of the logical steps involved. The reader may now verify that $a + (b + c)$ can be characterized in exactly the same way, and this will establish the associative law of addition. Property P_5 can be proved by the same general method and we therefore omit the proof.

For the equation, $a + x = b$, we obtain a solution by taking x to be $a + b$ as defined above, hence P_3 is true.

It will be noted that the ring B has some remarkable properties which have not been true for the rings previously mentioned. Thus, for example, in this ring $a \cdot a = a$ for *every* element a. Rings with this property will be discussed in detail in Chapter VII. It is obvious that, in this example, any set $\mathfrak{M}$ of points may be used in place of the interval $\mathcal{I}$, and thus one may obtain *the ring of all subsets of the arbitrary set* $\mathfrak{M}$.

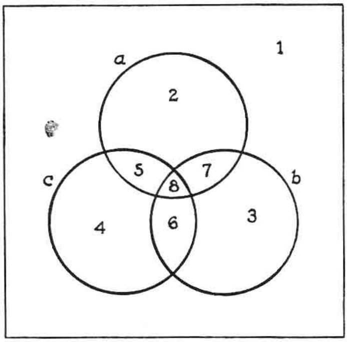

FIG. 2

Example 3. *The ring of all finite subsets of an arbitrary set* $\mathfrak{M}$. For concreteness, let $\mathfrak{M}$ be the interval $\mathcal{I}$ of the preceding example. It was shown above that the set of *all* subsets of $\mathcal{I}$ is a ring under suitable definitions of addition and multiplication. With these same definitions, it is clear that if a and b contain only a finite number of points the same is true of both $a + b$ and ab. It follows readily that the set of all finite subsets of $\mathcal{I}$ is also a ring, naturally a *subring* of the ring of all subsets of $\mathcal{I}$.

Example 4. *The ring of all real matrices of order* 2. This ring consists of all symbols of the form

$$\begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix},$$

where e_{11}, e_{12}, e_{21}, e_{22} are real numbers, with addition and multiplication defined respectively as follows:

$$\begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix} + \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix} = \begin{bmatrix} e_{11} + f_{11} & e_{12} + f_{12} \\ e_{21} + f_{21} & e_{22} + f_{22} \end{bmatrix},$$

$$\begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix} \begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix} = \begin{bmatrix} e_{11}f_{11} + e_{12}f_{21} & e_{11}f_{12} + e_{12}f_{22} \\ e_{21}f_{11} + e_{22}f_{21} & e_{21}f_{12} + e_{22}f_{22} \end{bmatrix}.$$

The proof that this is a ring may be left to the reader.

In a similar manner, one may define the ring of real matrices of order n (n rows and columns) and also one may replace the real numbers by elements of other number systems—in fact, by elements of any ring. Rings of matrices will be discussed more fully in Chapter VIII.

Before proceeding, we point out that in all examples preceding this last one, the order of the factors in a product is immaterial. However, this is not always the case in the ring of real matrices of order 2. Thus, for example,

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

while

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

Example 5. *The ring of real quaternions.* As elements of this ring we use all symbols

$$(e_1\,,\ e_2\,,\ e_3\,,\ e_4),$$

where e_1, e_2, e_3, e_4 are real numbers. Addition and multiplication are defined respectively as follows:

$$(e_1\,, e_2\,, e_3\,, e_4) + (f_1\,, f_2\,, f_3\,, f_4) = (e_1 + f_1\,,\ e_2 + f_2\,, e_3 + f_3\,, e_4 + f_4),$$

$$(e_1\,, e_2\,, e_3\,, e_4)(f_1\,, f_2\,, f_3\,, f_4) = (e_1f_1 - e_2f_2 - e_3f_3 - e_4f_4\,,\ e_1f_2 + e_2f_1 + e_3f_4 - e_4f_3\,, e_1f_3 - e_2f_4 + e_3f_1 + e_4f_2,\ e_1f_4 + e_2f_3 - e_3f_2 + e_4f_1).$$

We may remark that a different, but logically equivalent, definition of this ring is to be found in many texts on algebra. However, for the purpose of illustration, the present definition is simpler and entirely satisfactory.

It is fairly obvious that the properties of addition are satisfied, and P_4 and P_5 may be verified by straightforward but detailed calculations.

The ring of real quaternions also has the property that the order of the factors in a product is important. For example, we have

$$(0,\ 1,\ 0,\ 0)(0,\ 0,\ 1,\ 0) = (0,\ 0,\ 0,\ 1),$$

$$(0,\ 0,\ 1,\ 0)(0,\ 1,\ 0,\ 0) = (0,\ 0,\ 0,\ -1).$$

In any ring R, if a and b are elements such that $ab = ba$, it may be said that either of these elements is *commutative with* the other. If R has the property that a is commutative with b for *every* choice of a and b, R is said to be a *commutative ring*; otherwise it is a *noncommutative ring*. Thus all the examples of rings given above, with the exception of the last two, are commutative rings; while the last two are noncommutative rings. It is clear that for *commutative* rings either of the distributive laws P_5 is a consequence of the other.

3. Properties of addition. We now return to a further consideration of the defining properties of a ring. The properties P_1, P_2, and P_3 are precisely the properties which define an *Abelian* (commutative) *group*, and the fundamental properties of addition in a ring are simply properties of such groups. However, we do not assume a familiarity with these concepts but shall derive the required properties in some detail.

Let a and b be elements, distinct or identical, of the arbitrary ring R. By P_3, there exist elements n and n' of R such that

$$a + n = a,$$

and

$$b + n' = b.$$

Likewise there exist elements x and y such that

$$a + x = n',$$

and

$$b + y = n.$$

It follows, therefore, by using P_1 and P_2, that

$$\begin{aligned} n = b + y = y + b = y + (b + n') &= (y + b) + n' \\ &= (b + y) + n' = n + n', \end{aligned}$$

and

$$\begin{aligned} n' = a + x = x + a = x + (a + n) &= (x + a) + n \\ &= (a + x) + n = n' + n = n + n'. \end{aligned}$$

This shows that $n = n'$, and hence that there exists a *unique* element n of R with the property that

$$a + n = n + a = a$$

for *every* element a of R. Henceforth, this element n will be denoted by the familiar symbol 0 and called the *zero* *element*, or simply the *zero*, of R. Any other element is naturally said to be a *nonzero* element. Thus every ring has a zero, and clearly a ring also has nonzero elements unless it happens that the ring has only one element.

The reader will have no difficulty in identifying the zeros of the rings previously mentioned. As illustrations, we may note that in the ring of all subsets of $\mathscr{I}$, the void set is the zero; while the zero of the ring of real matrices of order 2 is the matrix

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

In the ring of real functions continuous in some interval, the zero is the function which vanishes identically.

One of the defining properties of a ring states that there exists an element x such that

$$a + x = b.$$

It is now easy to show that this equation has a *unique* solution. Suppose that also

$$a + y = b,$$

and that t is an element such that

$$a + t = 0.$$

It follows that

$$\begin{aligned} x = x + 0 = x + (a + t) &= (x + a) + t = b + t \\ &= (a + y) + t = (a + t) + y = 0 + y = y, \end{aligned}$$

and the solution is therefore unique.

The unique solution of

$$a + x = 0$$

此为试读,需要完整PDF请访问: www.ertongbook.com