BOOK I

ALGEBRAIC PRELIMINARIES

CHAPTER I

RINGS AND FIELDS

THE READER is assumed to be familiar with the use of homogeneous and non-homogeneous coordinates in geometry, when the coordinates are real or complex numbers. When geometry is developed with the help of these coordinates, results are obtained by methods which belong to algebra, the differential calculus, and so on. Those results which can be obtained by purely algebraic processes (and they include many which are usually obtained by the methods of the calculus) make up the subject with which we are concerned in this work.

The operations of algebra we shall study are those of addition, subtraction, multiplication, division, and the solution of algebraic equations. While ordinary complex numbers are the most familiar elements for which these operations are defined, there are more general sets of elements for which it is possible to define them. By allowing our coordinates to belong to these sets, a more general geometry is obtained. We thus arrive at the definition of a more general space than that considered in elementary geometry, and the study of this space is the purpose of this work.

In this and succeeding chapters we consider sets of elements for which some or all of the algebraic operations cited above are defined, and step by step we arrive at a characterisation of the sets of elements from which our coordinates may be chosen. These sets are known in algebra as *fields*. In order, however, that the geometry which we derive may conform to the general pattern which appears when the field is that of the complex numbers, we shall find it desirable to impose certain restrictions on the fields considered. These restrictions are not all imposed simultaneously, but in succession; and only when we have proceeded under the limitations already adopted as far as our subject demands do we impose a new condition. The mathematical advantages of such a method are evident.

1. Groups. Consider a set S of elements, which we denote by $a, b, c, \ldots$. A law by which, given any ordered pair of elements a and b of S, possibly not distinct, we can derive a unique element c of S, is called a *law of composition* for S. A non-vacuous set S of elements with a law of composition which satisfies certain conditions, explained below, is called a *group*.

We denote the element resulting from the combination of a and b (in the given order) by ab; if the resulting element of S is c, we write

$$ab = c.$$

ab is a uniquely defined element of S, but may be different from ba.

The law of composition is said to be *associative* if, given any three elements a, b, c of S, we have the equation

$$(ab)c = a(bc).$$

We then write this element as abc.

The conditions that a set S, with a given law of composition, should form a group are that

(i) the law of composition is associative;

(ii) given any two elements a, b of S, there exist elements x, y such that

$$ax = b \quad \text{and} \quad ya = b.$$

As an example of a group, consider the possible derangements of the integers 1, 2, 3. If α, β, γ is any derangement of these integers, we denote the operation of replacing 1, 2, 3 by α, β, γ by the symbol

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

The successive application of any two of the six possible operations is equivalent to some single operation of the set, and hence a law of composition for the set of operations is defined. If we denote the six operations

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

by a, b, c, d, e, f respectively, and denote the result of performing

first the substitution x and then the substitution y by xy, the complete law of composition is given by the table of double entry:

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	e	f	d
c	c	a	b	f	d	e
d	d	f	e	a	c	b
e	e	d	f	b	a	c
f	f	e	d	c	b	a

where the entry in the row containing x and the column containing y is xy. From the table, or directly from the definition, it is at once seen that the law of composition is associative. Again, since each row contains all six elements, the equation

$$px = q$$

always has a solution; the corresponding result for the equation

$$yp = q$$

follows from the fact that each column contains all six elements. Hence the six elements, with the law of composition, form a group.

We notice in this group that $bd = e$, but $db = f$. Hence the equation $xy = yx$ does not hold for all pairs of elements in the group. Such a group is called *non-commutative*. If, in a given group, the equation $xy = yx$ is always true, we say the group is *commutative*, or *Abelian*. A very simple example of such a group is provided by the natural integers (positive, zero and negative), the law of composition being ordinary addition of integers.

It is often convenient, when dealing with commutative groups, to use the symbol of addition for the law of composition, writing $a+b$ instead of ab. We then call the group an *additive* group. It is important to remember that this notation is never used for a non-commutative group.

We now obtain certain properties common to all groups. From condition (ii) we know that, given any element a, there exist elements e and f such that

$$ae = a, \quad fa = a.$$

Let b be any element of S. Then there exist elements c, d such that

$$ac = b, \quad da = b.$$

From condition (i) we have

$$be = (da)e = d(ae) = da = b,$$
$$fb = f(ac) = (fa)c = ac = b.$$

In particular, in the first of these equations put $b = f$, and in the second put $b = e$. Then $f = fe$, and $fe = e$. Hence $e = f$. If there is another element e' with the properties of e,

$$e'e = e', \quad \text{and} \quad e'e = e,$$

and therefore e is unique. We have thus established the existence of a unique element e of the group such that

$$ae = a = ea$$

for every element of the group. This element e is called the *unity* of the group. In the case of an additive group it is usually called the *zero* of the group, and denoted by 0.

Now consider the equation

$$ax = e,$$

where a is any element of the group, e being the unity. By (ii) this has a solution x. Then

$$xax = xe = x,$$

and therefore the element $f = xa$ has the property $fx = x$, for the x considered. But, by an argument used above, $fb = b$ for any b in the group. In fact, let c be an element satisfying the equation $xc = b$. Then

$$fb = fxc = xc = b.$$

It follows, taking $b = e$, that $f = e$. Therefore $xa = e$. If y is any element such that

$$ay = e = ya,$$

then

$$y = ye = yax = ex = x.$$

Hence x is uniquely defined by the equations

$$ax = e = xa.$$

This element is called the *inverse* of a, and is denoted by a^{-1}. (In the case of an additive group it is called the *negative* of a, and denoted by $-a$. We then write $b-a$ for $b+(-a)$.)

We now show that the equations

$$ax = b, \quad ya = b,$$

where a, b are any elements of the group, serve to define x and y uniquely. For

$$x = ex = a^{-1}ax = a^{-1}b,$$

and

$$y = ye = yaa^{-1} = ba^{-1}.$$

Hence x and y are determined explicitly. In particular the equation

$$a^{-1}x = e$$

has a unique solution. But

$$a^{-1}a = e.$$

The solution is therefore $x = a$. Therefore

$$(a^{-1})^{-1} = a.$$

In the case of an additive group this becomes

$$-(-a) = a.$$

A non-vacuous subset s of S may, with the law of composition assumed for the elements of S, also form a group. This is called a *subgroup* of the given group. The following conditions are evidently necessary and sufficient for the elements of s to form a subgroup:

(i) if s contains elements a, b, it contains ab;

(ii) if s contains an element a, it also contains a^{-1}.

We conclude this section with a brief reference to an evident generalisation of the example of a group described above, namely, the *symmetric* group whose elements are the permutations of the numbers $1, 2, 3, \ldots, n$. The law of composition is defined as in the example. An important subgroup of this group is the *alternating group*. To define the alternating group we assume the definition of polynomials in the n indeterminates $x_1, \ldots, x_n$ which will be given in § 5. Consider the polynomial

$$\Delta = \prod_{i<k} (x_i - x_k) \quad (i, k = 1, 2, \ldots, n).$$

If the suffixes $1, 2, \ldots, n$ are permuted, it is easily seen that the polynomial Δ is either unchanged (except for the order of the factors) or becomes $-\Delta$. Permutations which leave Δ invariant are called *even* permutations, the others are called *odd* permutations.

A *transposition*, that is, a permutation which interchanges two suffixes only, is seen to be an *odd* permutation. Any permutation can be regarded as the product of transpositions. Such a decomposition of a permutation into transpositions is not unique, but the parity of the number of transpositions for a given permutation is independent of the method of decomposition. The product of two even or two odd permutations is even; the product of an even and an odd permutation is an odd permutation. Hence the set of *even* permutations of the symmetric group forms a subgroup, which is called the *alternating group*, and the number of even permutations in the symmetric group is equal to the number of odd permutations.

2. Rings. A set of elements may have more than one law of composition. We shall be particularly concerned with sets having two laws of composition, under one of which the set forms a commutative group. We write this group as an additive group, and refer to the corresponding law as the *addition law* of the set. The zero of the group is called the zero of the set.

The second law of composition is called the *multiplication law*, and the result of combining elements a, b of the set by this law is denoted by the product ab. Multiplication need not be commutative, but we shall require it to be associative. It is said to be *distributive over addition* if

$$a(b+c) = ab+ac, \quad \text{and} \quad (b+c)a = ba+ca,$$

for all a, b, c in the set.

A *ring*, then, is a set of elements with two laws of composition, addition and multiplication, with the properties:

(i) the set is an additive group with respect to addition;

(ii) multiplication is associative, and distributive over addition.

The following examples will illustrate the various possibilities which may arise in the study of rings. In the first four cases the laws of composition for the elements involved are addition and multiplication as usually defined:

I. The set of all complex numbers.
II. The set of all integers, positive, zero, and negative.
III. The set of all even integers.
IV. The set of all integers, reduced *modulo* the integer m.

V. The set of all matrices of q rows and columns whose elements are complex numbers. A matrix of this type is the array

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & . & \alpha_{1q} \\ \alpha_{21} & \alpha_{22} & . & \alpha_{2q} \\ . & . & . & . \\ \alpha_{q1} & \alpha_{q2} & . & \alpha_{qq} \end{pmatrix},$$

where each α_{ij} is a complex number. Addition is defined by the rule

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & . & \alpha_{1q} \\ \alpha_{21} & \alpha_{22} & . & \alpha_{2q} \\ . & . & . & . \\ \alpha_{q1} & \alpha_{q2} & . & \alpha_{qq} \end{pmatrix} + \begin{pmatrix} \beta_{11} & \beta_{12} & . & \beta_{1q} \\ \beta_{21} & \beta_{22} & . & \beta_{2q} \\ . & . & . & . \\ \beta_{q1} & \beta_{q2} & . & \beta_{qq} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_{11}+\beta_{11} & \alpha_{12}+\beta_{12} & . & \alpha_{1q}+\beta_{1q} \\ \alpha_{21}+\beta_{21} & \alpha_{22}+\beta_{22} & . & \alpha_{2q}+\beta_{2q} \\ . & . & . & . \\ \alpha_{q1}+\beta_{q1} & \alpha_{q2}+\beta_{q2} & . & \alpha_{qq}+\beta_{qq} \end{pmatrix},$$

and multiplication by the rule

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & . & \alpha_{1q} \\ \alpha_{21} & \alpha_{22} & . & \alpha_{2q} \\ . & . & . & . \\ \alpha_{q1} & \alpha_{q2} & . & \alpha_{qq} \end{pmatrix} \begin{pmatrix} \beta_{11} & \beta_{12} & . & \beta_{1q} \\ \beta_{21} & \beta_{22} & . & \beta_{2q} \\ . & . & . & . \\ \beta_{q1} & \beta_{q2} & . & \beta_{qq} \end{pmatrix} = \begin{pmatrix} \gamma_{11} & \gamma_{12} & . & \gamma_{1q} \\ \gamma_{21} & \gamma_{22} & . & \gamma_{2q} \\ . & . & . & . \\ \gamma_{q1} & \gamma_{q2} & . & \gamma_{qq} \end{pmatrix},$$

where

$$\gamma_{ij} = \sum_{k=1}^{q} \alpha_{ik}\beta_{kj}.$$

The reader may easily verify that these sets, with the prescribed laws of addition and multiplication, form rings. Further study reveals certain features common to some of the rings, but not necessarily to all.

(i) In the cases I, II, III and IV the zero of the ring is the number 0. In case V the zero is the zero matrix

$$0 = \begin{pmatrix} 0 & 0 & . & 0 \\ 0 & 0 & . & 0 \\ . & . & . & . \\ 0 & 0 & . & 0 \end{pmatrix}.$$

In all five cases

$$a.0 = 0 = 0.a$$

for all elements a of the ring.

(ii) In cases I, II and IV let e be the integer 1, and in case V let

$$e = \begin{pmatrix} 1 & 0 & . & 0 \\ 0 & 1 & . & 0 \\ . & . & . & . \\ 0 & 0 & . & 1 \end{pmatrix};$$

in each of these cases e has the property given by the equations

$$ae = a = ea$$

for every element a of the ring. When such an element e exists, it will be shown to be unique. It is called the *unity* of the ring. In case III there is no element of the ring with this property.

(iii) In all but the last case multiplication is commutative. In case V it is non-commutative, since, if $q > 1$,

$$\begin{pmatrix} 1 & 0 & . & 0 \\ 0 & 0 & . & 0 \\ . & . & . & . \\ 0 & 0 & . & 0 \end{pmatrix} \begin{pmatrix} \alpha_{11} & \alpha_{12} & . & \alpha_{1q} \\ \alpha_{21} & \alpha_{22} & . & \alpha_{2q} \\ . & . & . & . \\ \alpha_{q1} & \alpha_{q2} & . & \alpha_{qq} \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & . & \alpha_{1q} \\ 0 & 0 & . & 0 \\ . & . & . & . \\ 0 & 0 & . & 0 \end{pmatrix},$$

and

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & . & \alpha_{1q} \\ \alpha_{21} & \alpha_{22} & . & \alpha_{2q} \\ . & . & . & . \\ \alpha_{q1} & \alpha_{q2} & . & \alpha_{qq} \end{pmatrix} \begin{pmatrix} 1 & 0 & . & 0 \\ 0 & 0 & . & 0 \\ . & . & . & . \\ 0 & 0 & . & 0 \end{pmatrix} = \begin{pmatrix} \alpha_{11} & 0 & . & 0 \\ \alpha_{21} & 0 & . & 0 \\ . & . & . & . \\ \alpha_{q1} & 0 & . & 0 \end{pmatrix}.$$

(iv) In cases I, II and III, if a and b are two elements of the ring such that

$$ab = 0,$$

then either $a = 0$ or $b = 0$.

This property holds for the ring IV if and only if m is a prime number. If $m = pq$, where neither p nor q is 1, then p and q are two non-zero elements of the ring such that $pq = 0$. On the other hand, if m is prime and $ab = 0$, so that

$$ab = cm,$$

it follows, by the unique factorisation properties of ordinary integers, that either a or b is divisible by m.

The property we are discussing does not hold in case V if $q > 1$. For

$$\begin{pmatrix} 1 & 0 & . & 0 \\ 0 & 0 & . & 0 \\ . & . & . & . \\ 0 & 0 & . & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & . & 0 \\ 0 & 1 & . & 0 \\ . & . & . & . \\ 0 & 0 & . & 0 \end{pmatrix} = 0,$$

and neither factor is the zero of the ring.

(v) In case I there is associated with every element a of the ring, other than the zero, a unique inverse a^{-1} such that

$$aa^{-1} = a^{-1}a = e.$$

The rings II and V do not have this property, and it can be shown quite simply that the ring IV has the property only when m is a prime number. The property is meaningless in case III since the ring has not unity.

(vi) If we write

$$a+a = 2a, \quad a+2a = 3a, \quad \text{etc.},$$

the elements $a, 2a, 3a, \ldots$ $(a \neq 0)$ are all distinct, except in case IV, when

$$ma = 0$$

for all elements a in the ring.

It will be observed that only in (i) did we have a property common to the five rings, namely, the zero has the property $a0 = 0 = 0a$. We now show that this property holds for all rings, and deduce other elementary results true for any ring.

Let a, b be any two elements of a ring R, and let 0 be the zero of R. Then

$$a+0 = a,$$

and therefore $$ba = b(a+0) = ba+b0,$$

and also $$ab = (a+0)b = ab+0b.$$

From the uniqueness of the zero of a ring it follows that

$$b0 = 0 = 0b,$$

these equations holding for any element b in R.

Again, we know that any equation

$$a+x = b$$

has a unique solution

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

in R. Now

$$\begin{aligned} a(b-c)+ac &= a(b-c+c) \\ &= ab. \end{aligned}$$

Hence $$a(b-c) = ab-ac,$$

and similarly $$(b-c)a = ba-ca.$$

Therefore, taking $b = 0$, we obtain the equations

$$a(-c) = -ac, \quad (-c)a = -ca$$

for all a, c in R. Again,

$$\begin{aligned}(-a)(-b)-ab &= (-a)(-b)+(-a)b \\ &= (-a)(-b+b) \\ &= (-a)0 = 0,\end{aligned}$$

and therefore $$(-a)(-b) = ab.$$

We have thus shown that the usual multiplicative properties of the minus sign hold in any ring.

We now define the relationship between two rings known as *isomorphism*. Let R and R^* be two rings such that to each element a of R there corresponds a unique element a^* of R^*, and such that any element a^* of R^* arises from exactly one element a of R. Such a correspondence is said to be *one-to-one*. Now suppose, in addition, that the correspondence is such that if a, b correspond respectively to a^*, b^*, then $a+b$ and ab correspond respectively to a^*+b^* and to a^*b^*. The correspondence is then called an *isomorphism*.

Isomorphism between rings is a relation of the class known as *equivalence relations*. Consider any set S of elements $\alpha, \beta, \gamma, \ldots$, and let there be a relation, which we denote by $\sim$, between the elements of S, so that, given any two elements α, β, we know whether $\alpha \sim \beta$ is true or false. If the relation $\sim$ is:

(i) reflexive, that is, $\alpha \sim \alpha$ for all α in S;
(ii) symmetric, that is, $\alpha \sim \beta$ implies $\beta \sim \alpha$;
(iii) transitive, that is, if $\alpha \sim \beta$ and $\beta \sim \gamma$, then $\alpha \sim \gamma$;

we say it is an *equivalence relation*.

An equivalence relation between the elements of a set S divides S into subsets, no two of which have any elements in common. If α, β are in the same subset, $\alpha \sim \beta$. Every element of S lies in one of these subsets.

It is clear that if S is the set of all rings, and if $\alpha \sim \beta$ means that the ring α is isomorphic with the ring β, the relation is an equivalence relation. We shall often speak of two isomorphic rings as being equivalent, implying that if in our discussion we replace one ring by the other (making any necessary consequential substitutions) nothing in our conclusions is altered.