1

GROUPS

1.1. Introduction—equivalence relations

In this first chapter we repeat briefly some of the basic work on group theory that was done in detail in volume 1. The reader who wishes to study the elementary theory in detail should read volume 1 and omit this chapter, but the student who possesses a fair amount of mathematical maturity and who wants to study other types of algebraic structure but who needs first to know the standard theorems and definitions of group theory may substitute this chapter, which will provide him with the knowledge he requires, though not with all the detailed examples and explanations that were given in the first volume.

We assume that the reader is familiar with set notation. We use the standard notation, but the following points should be noted.

Inclusion. We denote the fact that A is contained in B by $A \subseteq B$, reserving $A \subset B$ to mean $A \subseteq B$ but $A \neq B$.

The empty and the universal sets. The empty set is denoted by $\varnothing$, and we use no special notation for the universal set.

Complement and difference. The complement of A is written as A'; the difference $(A - B)$ means the set of elements in the universal set that are in A but not in B: it does not imply that $B \subseteq A$.

Sets in terms of their elements. The set containing elements $a, b, c, \ldots, k$ is denoted by $\{a, b, c, \ldots, k\}$. The set of elements $x_1, x_2, \ldots, x_n$ may also be written $\{x_i : i = 1, \ldots, n\}$ or even $\{x_i\}$. Sets defined by a property are denoted thus: $\{x : x$ is a triangle$\}$.

Equivalence relations

An important method of dividing a set into mutually exclusive subsets is by means of an equivalence relation, the result used being given in the following fundamental theorem.

Theorem 1.1.1. *The equivalence classes theorem.*

Suppose in a set S we have a relation R defined between certain pairs of elements, xRy meaning that x and y stand in the given relation R.

Suppose further that R has the following 3 properties:

(1) *It is reflexive: i.e. xRx for all $x \in S$.*

(2) *It is symmetric: i.e. $xRy \Rightarrow yRx$.*

(3) *It is transitive: i.e. xRy and $yRz \Rightarrow xRz$.*

Then R is an equivalence relation*: i.e. it divides S into mutually exclusive subsets so that every element of S is in one and only one subset, and so that two elements are in the same subset if and only if they stand in the relation R to one another.*

The subsets are called the *equivalence classes* defined by R.

Given any element x in S consider all the elements y such that xRy. These form a subset of S: let us call it A_x. We show first that two elements are in the same subset A_x if and only if they stand in the relation R to one another. Suppose yRz and $y \in A_x$. Then xRy and so xRz since R is transitive. Hence $z \in A_x$. Conversely if y and z are both in A_x we have xRy and xRz, i.e. yRx by the symmetric property and xRz: thus yRz by transitivity.

For each element x we now have a subset A_x, but these will not all be distinct. We will show that two such are either mutually exclusive or else identical. Suppose A_x and A_y both have an element z. Then xRz and yRz, and so zRy by the symmetric property; hence xRy by the transitive property. Now take any element w of A_x. Then xRw and since xRy we have yRx, giving yRw. So w is in A_y. Hence we have shown that if A_x and A_y have one element z in common, any element w of A_x is in A_y, i.e. $A_x \subseteq A_y$. Similarly $A_y \subseteq A_x$, and so the subsets A_x and A_y are identical.

Thus we have mutually exclusive subsets $A_{x_1}, A_{x_2}, \ldots$. Finally, by the reflexive property any element t is in one of the subsets, viz. A_t.

Hence S is divided into a set of mutually exclusive subsets as required.

Note that the subset A_x may equally well be described as A_y for any element y in it—the important things are the equivalence classes and not the individual elements.

1.2. Algebraic structures

In order to use the methods of algebra in a set we must have some process, such as addition or multiplication, connecting our elements of the set. A set which has one or more operations such as these is called an *algebraic structure*.

Our processes may be addition or multiplication, or both. Considered in isolation addition and multiplication are formally very similar in that they both combine pairs of elements and satisfy similar laws, differing only in notation and terminology: it is only when they are both present that a distinction arises, in connection with the Distributive Law and, consequent on this, in the impossibility of dividing by zero.

Our processes need not be of the addition and multiplication type. If we consider the set whose elements are all the subsets of a given set then we can define the intersection and union of two subsets, and such processes satisfy laws similar to our fundamental laws of algebra, but not quite the same. Again, we could form a new positive integer from two given positive integers x and y by raising x to the power y: but this is neither commutative nor associative and is not likely to be a fruitful idea as an algebraic operation.

It is possible that *three* (or more) elements need to be taken in order to define a new element. An example of this would be the formation of $\mathbf{a} \wedge (\mathbf{b} \wedge \mathbf{c})$ for the three-dimensional vectors $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{c}$. We must expect the fundamental laws of combination for these more difficult processes to be correspondingly complicated. As is to be expected, by far the most fruitful ideas are those involving two elements only, and among these it is found that those which satisfy some of the ordinary fundamental laws of algebra are most useful in practice. This is natural, since these laws are precisely those which hold when we are dealing with ordinary numbers, which always remain one of the most fruitful sets in which to work. The processes of union and intersection are used in chapter 11, and in chapter 9 when we deal

with vector spaces we introduce a rather different type of process, but on the whole we will be concerned in this and later chapters with forming sums and products.

1.3. Groups

We give at once the abstract definition of a group. For the ideas which lead us to adopt this definition, and for more discussion on its meaning and significance, see volume 1. The numbering of the laws refers to volume 1 also.

Abstract definition of a group

A set S of elements forms a group if to any two elements x and y of S taken in a particular order there is associated a unique third element of S, called their product and denoted by xy, which satisfies the following laws:

M2 *For any three elements x, y and z, $(xy)\,z = x(yz)$.*
M3 *There is an element called the* 'neutral element' *and denoted by e which has the property that $xe = ex = x$ for all elements x.*
M4 *Corresponding to each element x there is an element x^{-1} called the* 'inverse' *of x which has the property that*

$$xx^{-1} = x^{-1}x = e.$$

Thus given a set and a product we need five things to make it a group.

(*a*) The product must be unique. This is usually implicit in its definition.

(*b*) The product must be in the set. This again is usually obvious from the definition.

(*c*) The Associative Law M 2 must hold. This is nearly always obvious, possibly needing a little thought.

(*d*) There must be a neutral element. It is usually clear which element this must be and it can then easily be tested.

(*e*) There must be an inverse to *every* element. This again is not often difficult to identify.

It seems from the above that it is usually a straightforward matter to test whether a structure is a group or not, and this is generally the case.

Elementary consequences

The following elementary but important theorems are all easily proved from the definition, and the reader is referred to volume 1 (§10.6) for the detailed proofs (§11.3 for theorem 1.3.1).

Theorem 1.3.1. *The Associative Law extends to the product of more than three elements, i.e. the product* $x_1 x_2 x_3 \dots x_n$ *is independent of the order in which we perform the multiplications of pairs, provided that we keep the x's in the same relative position.*

Theorem 1.3.2. *The uniqueness of the neutral element.*
There cannot be two different elements each having the property possessed by e.

Theorem 1.3.3. *The uniqueness of the inverse.*
For any x there cannot be two different elements each with the property possessed by x^{-1}.

Theorem 1.3.4. *The inverse of e is e.*

Theorem 1.3.5. $(x^{-1})^{-1} = x$.

Theorem 1.3.6. *The Cancellation Law.*

$$xy = xz \Rightarrow y = z.$$

$$yx = zx \Rightarrow y = z.$$

Note. We need to prove both parts, since we do not assume commutativity.

Theorem 1.3.7. *The equation* $ax = b$ *has the unique solution* $x = a^{-1}b$. *The equation* $xa = b$ *has the unique solution* $x = ba^{-1}$.
The first is proved by multiplying both sides of the equation $ax = b$ *on the left* by a^{-1}, and the second by similar multiplication *on the right*. There is no question of excluding 0: in a group *every* element has an inverse.

The order of a group

If a group has a finite number of elements this number is called the *order* of the group, and the group is said to be of finite order. A group with an infinite number of elements is said to be of infinite order.

It is possible to have a group consisting of just one element e with $ee = e$. This group has order 1 and is sometimes known as the trivial group.

It might be expected that nearly all important groups were infinite, since the sets used in elementary algebra (such as the real or complex numbers or the integers are). This is not the case. While many infinite groups are extremely useful there is a large number of important finite ones, and these in fact are usually more interesting as groups. The reason is, roughly speaking, that in a finite group the structure must, after a certain stage, turn over upon itself and become intertwined: it cannot continue indefinitely along a straight course. Such intertwinings and foldings back may occur of course in infinite groups, but it is usually in the finite case that they are exhibited to the highest degree. Thus a great deal of the interest and usefulness of the subject lies in finite groups, so much so that many works deal with these almost exclusively.

Abelian groups

In our definition of a group we did not assume the truth of the Commutative Law, that $xy = yx$ for all x and y. The reason was that it is not essential to much of our algebra and we wish in fact to work with many structures within which it does not hold.

On the other hand many groups *are* commutative. Such are called *Abelian groups* (after the Norwegian mathematician N. H. Abel (1802–29) who anticipated some of the later work in group theory). They have of course properties which are not possessed by non-commutative groups, on the whole they are easier to work with, but in many ways they are not as interesting as the others.

It is usual, though not universal, to use the addition rather than the multiplication notation for Abelian groups. We then have the following four laws.

A1 *For any two elements x and y, $x+y = y+x$.*

(The Commutative Law.)

A2 *For any three elements x, y, and z,*

$$(x+y)+z = x+(y+z).$$

(The Associative Law.)

A3 *There is an element called the* 'zero', *and denoted by* 0 *which has the property that* $x+0 = 0+x = x$ *for all elements* x.

A4 *Corresponding to each element* x *there is an element* $-x$ *called the* 'negative' *of* x *which has the property that*

$$x+(-x) = (-x)+x = 0.$$

The elementary theorems 1.3.1–1.3.7 are likewise modified.

We will not often use the additive notation when dealing with groups, but in the case of other structures, such as rings and fields, which possess two basic operations, it will be in general use.

The multiplication table

For finite groups it is possible to write out all possible products of two elements in the form of a table. Suppose we have n elements. Then we take a table with n rows and n columns and place each element at the head of one row and one column, usually taking them in the same order for columns as for rows. In the space of the table which is the intersection of the row headed by x and the column headed by y we place the element xy. The table so formed has several properties and is particularly useful for groups of small order.

Abstract groups

The only thing that we need to know about a given group is the product of any pair of elements. A set of abstract symbols, representing elements and combining in a given way, is known as an *abstract group*, and it is with these that we work when investigating group properties, although we think of and use many concrete examples when dealing with groups. This is an example of our familiar mathematical idea of abstraction. We isolate certain aspects of our set (in this case the group aspect), work with a model which exhibits these aspects without the extraneous properties possessed by the original, and then apply our results to our given set.

The inverse of a product

Theorem 1.3.8. $(xy)^{-1} = y^{-1}x^{-1}$.

For
$$\begin{aligned}(y^{-1}x^{-1})\,(xy) &= y^{-1}(x^{-1}x)\,y\\ &= y^{-1}ey\\ &= y^{-1}y\\ &= e.\end{aligned}$$

Also
$$\begin{aligned}(xy)\,(y^{-1}x^{-1}) &= x(yy^{-1})\,x^{-1}\\ &= xex^{-1}\\ &= xx^{-1}\\ &= e.\end{aligned}$$

As an extension we have that $(xyz)^{-1} = z^{-1}y^{-1}x^{-1}$, proved in the same way. Similarly for any number of elements.

The above theorem is easy to prove, but the result is extremely important, being rather surprising and a common source of error. To find the inverse of a product of two or more elements we must take the product of the inverses *in the reverse order*.

Notice that for an Abelian group $y^{-1}x^{-1} = x^{-1}y^{-1}$ and the difficulty disappears.

Powers of an element

We define x^2 to mean xx, x^3 to mean xxx, and generally x^r, where r is any positive integer, to mean the product of r x's.

We now write x^{-r} for $(x^{-1})^r$, and we notice that this is the inverse of x^r, for

$$(x^r)^{-1} = (xx \ldots x)^{-1} = x^{-1}x^{-1} \ldots x^{-1} = (x^{-1})^r.$$

As in elementary algebra we define x^0 to be e, and we then have the index laws, for a proof of which see volume 1, p. 210.

Theorem 1.3.9. *The Index Laws*

If m, n are integers, positive negative or zero, we have

(i) $x^m x^n = x^{m+n}$; (ii) $(x^m)^n = x^{mn}$.

It is important to notice that powers of the same element always commute, since $x^m x^n = x^n x^m = x^{m+n}$.

Now let us consider the set of elements $e(= x^0), x, x^2, x^3, \ldots$, where x is some element of our group. In an infinite group it is possible for all these to be different but in a group of finite order we must sooner or later have two which are the same element. Suppose $x^m = x^n$ where $m < n$. Then $x^{n-m} = x^n x^{-m} = e$.

Hence in a finite group some positive power of any element must equal the neutral element. If n is the least positive integer such that $x^n = e$ we say that n is the *order* of the element x. It easily follows that the n elements $e, x, x^2, \ldots, x^{n-1}$ are distinct.

It is obvious that $x^{rn+s} = x^s$ and that $x^m = e \Leftrightarrow m$ is a multiple of n, possibly the zero multiple. We see also that

$$x^{-1} = x^n x^{-1} = x^{n-1}, \quad x^{-2} = x^{n-2}, \text{ etc.},$$

and that $x^{-n} = e$, so that the order of x is the same as the order of x^{-1}.

The order of e is 1, and e is the only element of order 1.

The order of any element is not greater than the order of the group, since the n elements $e, x, \ldots, x^{n-1}$ are all distinct.

In an infinite group there may be no n such that $x^n = e$, in which case all elements $e, x^{\pm 1}, x^{\pm 2}, \ldots$ are distinct. In this case we say that x has infinite order. There may, however, be elements of finite order even in an infinite group.

1.4. Standard examples of groups

We now give a selection of groups which occur in practice or in other branches of mathematics. They include many which are important from the theoretical point of view and we draw upon these examples later in the book, where many of them appear again as other structures. The verification that a certain set is a group will usually be left to the reader: it is not usually difficult.

Examples from sets of numbers

The real numbers form a group under addition and also, if we except 0, under multiplication.

The complex numbers form a group under addition and, except 0, under multiplication.

The rationals form groups likewise, since the sum and product of two rationals are themselves rational.

The set of integers, positive, negative, or zero, clearly form a group under addition. This is an extremely important example, known as the *group of integers* or the *infinite cyclic group*, because of its similarity to the finite cyclic groups to be discussed later.

The set of all integers, positive, negative or zero, which are multiples of a fixed integer r form a group under addition, all such being isomorphic to the infinite cyclic group (for a discussion of *isomorphism* see chapter 2, §2.4).

The positive real numbers and the positive rationals both form groups under multiplication.

Residue classes: the cyclic groups

If n is a fixed positive integer, the set of all integers, positive, negative or zero, may be decomposed into equivalence classes such that any two integers are in the same class if and only if they are congruent modulo n, that is if and only if they leave the same remainder when divided by n. These classes are called *residue classes* modulo n. We can easily see that there are just n residue classes modulo n, a typical one consisting of all those integers that leave remainder r when divided by n, where r ranges over the values $0, 1, \ldots, (n-1)$. The class of the integers congruent to any of these r's is often denoted merely by r itself, when it is understood that we are working with residues. (The term 'residue class' is often shortened to 'residue'.)

Example. If $n = 4$ we obtain 4 residue classes modulo 4, namely 0, 1, 2, 3, where 0 consists of all integers divisible by 4, 1 all those that leave remainder 1 when divided by 4, and so on.

It is easily proved that we can add, subtract and multiply residues, in the following sense. If we add any member of the class r (working modulo some fixed n) to any member of the class s then we obtain a member of the class containing $r+s$, and the sum of the classes r and s is defined to be the class containing $r+s$ (note that this may not be the *class* $r+s$, since this may be greater than n, and we denote a class by its smallest positive member—the important thing is that all the sums are