Department of Mathematics, Government Arts College (Autonomous), Coimbatore-18

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: II

GROUP THEORY: Definition of a Group – Some examples of Groups – Some preliminary lemmas – Subgroups.

(Chapter 2 – Sections: 2.1 to 2.4)

2.1 Definition of a Group

At this juncture it is advisable to recall a situation discussed in the first chapter. For an arbitrary nonempty set S we defined $A(S)$ to be the set of all *one-to-one* mappings of the set S *onto* itself. For any two elements σ, $\tau \in A(S)$ we introduced a product, denoted by $\sigma \circ \tau$, and on further investigation it turned out that the following facts were true for the elements of $A(S)$ subject to this product:

1. Whenever $\sigma, \tau \in A(S)$, then it follows that $\sigma \circ \tau$ is also in $A(S)$. This is described by saying that $A(S)$ is *closed* under the product (or, sometimes, as closed under multiplication).
2. For any three elements $\sigma, \tau, \mu \in A(S)$, $\sigma \circ (\tau \circ \mu) = (\sigma \circ \tau) \circ \mu$. This relation is called the *associative law*.
3. There is a very special element $\iota \in A(S)$ which satisfies $\iota \circ \sigma = \sigma \circ \iota = \sigma$ for all $\sigma \in A(S)$. Such an element is called an *identity element* for $A(S)$.
4. For every $\sigma \in A(S)$ there is an element, written as σ^{-1}, also in $A(S)$, such that $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \iota$. This is usually described by saying that every element in $A(S)$ has an *inverse* in $A(S)$.

One other fact about $A(S)$ stands out, namely, that whenever S has three or more elements we can find two elements $\alpha, \beta \in A(S)$ such that $\alpha \circ \beta \neq \beta \circ \alpha$. This possibility, which runs counter to our usual experience and intuition in mathematics so far, introduces a richness into $A(S)$ which would have not been present except for it.

With this example as a model, and with a great deal of hindsight, we abstract and make the

DEFINITION A nonempty set of elements G is said to form a *group* if in G there is defined a binary operation, called the product and denoted by $\cdot$, such that

1. $a, b \in G$ implies that $a \cdot b \in G$ (closed).
2. $a, b, c \in G$ implies that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associative law).
3. There exists an element $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$ (the existence of an identity element in G).
4. For every $a \in G$ there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$ (the existence of inverses in G).

Considering the source of this definition it is not surprising that for every nonempty set S the set $A(S)$ is a group. Thus we already have presented to us an infinite source of interesting, concrete groups. We shall see later (in a theorem due to Cayley) that these $A(S)$'s constitute, in some sense, a universal family of groups. If S has three or more elements, recall that we can find elements $\sigma, \tau \in A(S)$ such that $\sigma \circ \tau \neq \tau \circ \sigma$. This prompts us to single out a highly special, but very important, class of groups as in the next definition.

DEFINITION A group G is said to be *abelian* (or *commutative*) if for every $a, b \in G$, $a \cdot b = b \cdot a$.

A group which is not abelian is called, naturally enough, *non-abelian*; having seen a family of examples of such groups we know that non-abelian groups do indeed exist.

Another natural characteristic of a group G is the number of elements it contains. We call this the *order* of G and denote it by $o(G)$. This number is, of course, most interesting when it is finite. In that case we say that G is a *finite group*.

To see that finite groups which are not trivial do exist just note that if the set S contains n elements, then the group $A(S)$ has $n!$ elements. (Prove!) This highly important example will be denoted by S_n whenever it appears in this book, and will be called the *symmetric group* of degree n.' In the next section we shall more or less dissect S_3, which is a non-abelian group of order 6.

2.2 Some Examples of Groups

Example 2.2.1 Let G consist of the integers $0, \pm 1, \pm 2, \ldots$ where we mean by $a \cdot b$ for $a, b \in G$ the usual sum of integers, that is, $a \cdot b = a + b$. Then the reader can quickly verify that G is an infinite abelian group in which 0 plays the role of e and $-a$ that of a^{-1}.

Example 2.2.2 Let G consist of the real numbers $1, -1$ under the multiplication of real numbers. G is then an abelian group of order 2.

Example 2.2.3 Let $G = S_3$, the group of all 1–1 mappings of the set $\{x_1, x_2, x_3\}$ onto itself, under the product which we defined in Chapter 1. G is a group of order 6. We digress a little before returning to S_3.

For a neater notation, not just in S_3, but in any group G, let us define for any $a \in G$, $a^0 = e$, $a^1 = a$, $a^2 = a \cdot a$, $a^3 = a \cdot a^2, \ldots, a^k = a \cdot a^{k-1}$, and $a^{-2} = (a^{-1})^2$, $a^{-3} = (a^{-1})^3$, etc. The reader may verify that the usual rules of exponents prevail; namely, for any two integers (positive, negative, or zero) m, n,

$$a^m \cdot a^n = a^{m+n}, \tag{1}$$

$$(a^m)^n = a^{mn}. \tag{2}$$

(It is worthwhile noting that, in this notation, if G is the group of Example 2.2.1, a^n means the integer na).

With this notation at our disposal let us examine S_3 more closely. Consider the mapping ϕ defined on the set x_1, x_2, x_3 by

$$\phi: \quad \begin{aligned} x_1 &\to x_2 \\ x_2 &\to x_1 \\ x_3 &\to x_3, \end{aligned}$$

and the mapping

$$\psi: \quad \begin{aligned} x_1 &\to x_2 \\ x_2 &\to x_3 \\ x_3 &\to x_1. \end{aligned}$$

Checking, we readily see that $\phi^2 = e$, $\psi^3 = e$, and that

$$\phi \cdot \psi: \quad \begin{aligned} x_1 &\to x_3 \\ x_2 &\to x_2 \\ x_3 &\to x_1, \end{aligned}$$

whereas

$$\psi \cdot \phi: \quad \begin{aligned} x_1 &\to x_1 \\ x_2 &\to x_3 \\ x_3 &\to x_2. \end{aligned}$$

It is clear that $\phi \cdot \psi \neq \psi \cdot \phi$ for they do not take x_1 into the same image. Since $\psi^3 = e$, it follows that $\psi^{-1} = \psi^2$. Let us now compute the action of $\psi^{-1} \cdot \phi$ on x_1, x_2, x_3. Since $\psi^{-1} = \psi^2$ and

$$\psi^2: \qquad \begin{array}{l} x_1 \to x_3 \\ x_2 \to x_1 \\ x_3 \to x_2, \end{array}$$

we have that

$$\psi^{-1} \cdot \phi: \qquad \begin{array}{l} x_1 \to x_3 \\ x_2 \to x_2 \\ x_3 \to x_1. \end{array}$$

In other words, $\phi \cdot \psi = \psi^{-1} \cdot \phi$. Consider the elements $e, \phi, \psi, \psi^2, \phi \cdot \psi, \psi \cdot \phi$; these are all distinct and are in G (since G is closed), which only has six elements. Thus this list enumerates all the elements of G. One might ask, for instance, What is the entry in the list for $\psi \cdot (\phi \cdot \psi)$? Using $\phi \cdot \psi = \psi^{-1} \cdot \phi$, we see that $\psi \cdot (\phi \cdot \psi) = \psi \cdot (\psi^{-1} \cdot \phi) = (\psi \cdot \psi^{-1}) \cdot \phi = e \cdot \phi = \phi$. Of more interest is the form of $(\phi \cdot \psi) \cdot (\psi \cdot \phi) = \phi \cdot (\psi \cdot (\psi \cdot \phi)) = \phi \cdot (\psi^2 \cdot \phi) = \phi \cdot (\psi^{-1} \cdot \phi) = \phi \cdot (\phi \cdot \psi) = \phi^2 \cdot \psi = e \cdot \psi = \psi$. (The reader should not be frightened by the long, wearisome chain of equalities here. It is the last time we shall be so boringly conscientious.) Using the same techniques as we have used, the reader can compute to his heart's content others of the 25 products which do not involve e. Some of these will appear in the exercises.

Example 2.2.4 Let n be any integer. We construct a group of order n as follows: G will consist of all symbols $a^i, i = 0, 1, 2, \ldots, n - 1$ where we insist that $a^0 = a^n = e$, $a^i \cdot a^j = a^{i+j}$ if $i + j \leq n$ and $a^i \cdot a^j = a^{i+j-n}$ if $i + j > n$. The reader may verify that this is a group. It is called a *cyclic group* of order n.

A geometric realization of the group in Example 2.2.4 may be achieved as follows: Let S be the circle, in the plane, of radius 1, and let ρ_n be a rotation through an angle of $2\pi/n$. Then $\rho_n \in A(S)$ and ρ_n in $A(S)$ generates a group of order n, namely, $\{e, \rho_n, \rho_n^2, \ldots, \rho_n^{n-1}\}$.

Example 2.2.5 Let S be the set of integers and, as usual, let $A(S)$ be the set of all one-to-one mappings of S onto itself. Let G be the set of all elements in $A(S)$ which move only a *finite* number of elements of S; that is, $\sigma \in G$ if and only if the number of x in S such that $x\sigma \neq x$ is finite. If $\sigma, \tau \in G$, let $\sigma \cdot \tau$ be the product of σ and τ as elements of $A(S)$. We claim that G is a group relative to this operation. We verify this now.

To begin with, if $\sigma, \tau \in G$, then σ and τ each moves only a finite number of elements of S. In consequence, $\sigma \cdot \tau$ can possibly move only those elements in S which are moved by at least one of σ or τ. Hence $\sigma \cdot \tau$ moves only a finite number of elements in S; this puts $\sigma \cdot \tau$ in G. The identity element, ι, of $A(S)$ moves no element of S; thus ι certainly must be in G. Since the associative law holds universally in $A(S)$, it holds for elements of G. Finally, if $\sigma \in G$ and $x\sigma^{-1} \neq x$ for some $x \in S$, then $(x\sigma^{-1})\sigma \neq x\sigma$, which is to say, $x(\sigma^{-1} \cdot \sigma) \neq x\sigma$. This works out to say merely that $x \neq x\sigma$. In other words, σ^{-1} moves only those elements of S which are moved by σ. Because σ only moves a finite number of elements of S, this is also true for σ^{-1}. Therefore σ^{-1} must be in G.

We have verified that G satisfies the requisite four axioms which define a group, relative to the operation we specified. Thus G is a group. The reader should verify that G is an infinite, non-abelian group.

#Example 2.2.6 Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are real numbers, such that $ad - bc \neq 0$. For the operation in G we use the multiplication of matrices; that is,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{pmatrix}.$$

The entries of this 2×2 matrix are clearly real. To see that this matrix is in G we merely must show that

$$(aw + by)(cx + dz) - (ax + bz)(cw + dy) \neq 0$$

(this is the required relation on the entries of a matrix which puts it in G). A short computation reveals that

$$(aw + by)(cx + dz) - (ax + bz)(cw + dy) = (ad - bc)(wz - xy) \neq 0$$

since both

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} w & x \\ y & z \end{pmatrix}$$

are in G. The associative law of multiplication holds in matrices; therefore it holds in G. The element

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is in G, since $1 \cdot 1 - 0 \cdot 0 = 1 \neq 0$; moreover, as the reader knows, or can verify, I acts as an identity element relative to the operation of G. Finally, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ then, since $ad - bc \neq 0$, the matrix

$$\begin{pmatrix} \dfrac{d}{ad - bc} & \dfrac{-b}{ad - bc} \\ \dfrac{-c}{ad - bc} & \dfrac{a}{ad - bc} \end{pmatrix}$$

makes sense. Moreover,

$$\left(\frac{d}{ad-bc}\right)\left(\frac{a}{ad-bc}\right)-\left(\frac{-b}{ad-bc}\right)\left(\frac{-c}{ad-bc}\right)=\frac{ad-bc}{(ad-bc)^2}=\frac{1}{ad-bc}\neq 0,$$

hence the matrix

$$\begin{pmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{pmatrix}$$

is in G. An easy computation shows that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} \dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc} \\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc} \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix};$$

thus this element of G acts as the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. In short, G is a group. It is easy to see that G is an infinite, non-abelian group.

#**Example 2.2.7** Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where a, b, c, d are real numbers such that $ad - bc = 1$. Define the operation $\cdot$ in G, as we did in Example 2.2.6, via the multiplication of matrices. We leave it to the reader to verify that G is a group. It is, in fact, an infinite, non-abelian group.

One should make a comment about the relationship of the group in Example 2.2.7 to that in Example 2.2.6. Clearly, the group of Example 2.2.7 is a subset of that in Example 2.2.6. However, more is true. Relative to the same operation, as an entity in its own right, it forms a group. One could describe the situation by declaring it to be a *subgroup* of the group of Example 2.2.6. We shall see much more about the concept of subgroup in a few pages.

#**Example 2.2.8** Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, where a and b are real numbers, not both 0. (We can state this more succinctly by saying that $a^2 + b^2 \neq 0$.) Using the same operation as in the preceding two examples, we can easily show that G becomes a group. In fact, G is an infinite, abelian group.

Does the multiplication in G remind you of anything? Write $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ as $aI + bJ$ where $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and compute the product in these terms. Perhaps that will ring a bell with you.

#Example 2.2.9 Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo p, p a prime number, such that $ad - bc \neq 0$. Define the multiplication in G as we did in Example 2.2.6, understanding the multiplication and addition of the entries to be those modulo p. We leave it to the reader to verify that G is a non-abelian *finite* group.

In fact, how many elements does G have? Perhaps it might be instructive for the reader to try the early cases $p = 2$ and $p = 3$. Here one can write down all the elements of G explicitly. (A word of warning! For $p = 3$, G already has 48 elements.) To get the case of a general prime, p will require an idea rather than a direct hacking-out of the answer. Try it!

2.3 Some Preliminary Lemmas

We have now been exposed to the theory of groups for several pages and as yet not a single, solitary fact has been proved about groups. It is high time to remedy this situation. Although the first few results we demonstrate are, admittedly, not very exciting (in fact, they are rather dull) they will be extremely useful. Learning the alphabet was probably not the most interesting part of our childhood education, yet, once this hurdle was cleared, fascinating vistas were opened before us.

We begin with

LEMMA 2.3.1 *If G is a group, then*

a. The identity element of G is unique.
b. Every $a \in G$ has a unique inverse in G.
c. For every $a \in G$, $(a^{-1})^{-1} = a$.
d. For all $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Proof. Before we proceed with the proof itself it might be advisable to see what it is that we are going to prove. In part (a) we want to show that if two elements e and f in G enjoy the property that for every $a \in G$, $a = a \cdot e = e \cdot a = a \cdot f = f \cdot a$, then $e = f$. In part (b) our aim is to show that if $x \cdot a = a \cdot x = e$ and $y \cdot a = a \cdot y = e$, where all of a, x, y are in G, then $x = y$.

First let us consider part (a). Since $e \cdot a = a$ for every $a \in G$, then, in particular, $e \cdot f = f$. But, on the other hand, since $b \cdot f = b$ for every $b \in G$, we must have that $e \cdot f = e$. Piecing these two bits of information together we obtain $f = e \cdot f = e$, and so $e = f$.

Rather than proving part (b), we shall prove something stronger which immediately will imply part (b) as a consequence. Suppose that for a in G, $a \cdot x = e$ and $a \cdot y = e$; then, obviously, $a \cdot x = a \cdot y$. Let us make this our starting point, that is, assume that $a \cdot x = a \cdot y$ for a, x, y in G. There is an element $b \in G$ such that $b \cdot a = e$ (as far as we know yet there may be several such b's). Thus $b \cdot (a \cdot x) = b \cdot (a \cdot y)$; using the associative law this leads to

$$x = e \cdot x = (b \cdot a) \cdot x = b \cdot (a \cdot x) = b \cdot (a \cdot y) = (b \cdot a) \cdot y = e \cdot y = y.$$

We have, in fact, proved that $a \cdot x = a \cdot y$ in a group G forces $x = y$. Similarly we can prove that $x \cdot a = y \cdot a$ implies that $x = y$. This says that we can cancel, from the same side, in equations in groups. A note of caution, however, for we cannot conclude that $a \cdot x = y \cdot a$ implies $x = y$ for we have no way of knowing whether $a \cdot x = x \cdot a$. This is illustrated in S_3 with $a = \phi$, $x = \psi$, $y = \psi^{-1}$.

Part (c) follows from this by noting that $a^{-1} \cdot (a^{-1})^{-1} = e = a^{-1} \cdot a$; canceling off the a^{-1} on the left leaves us with $(a^{-1})^{-1} = a$. This is the analog in general groups of the familiar result $-(-5) = 5$, say, in the group of real numbers under addition.

Part (d) is the most trivial of these, for

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot ((b \cdot b^{-1}) \cdot a^{-1}) = a \cdot (e \cdot a^{-1}) = a \cdot a^{-1} = e,$$

and so by the very definition of the inverse, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Certain results obtained in the proof just given are important enough to single out and we do so now in

LEMMA 2.3.2 *Given a, b in the group G, then the equations $a \cdot x = b$ and $y \cdot a = b$ have unique solutions for x and y in G. In particular, the two cancellation laws,*

$$a \cdot u = a \cdot w \textit{ implies } u = w$$

and

$$u \cdot a = w \cdot a \textit{ implies } u = w$$

hold in G.

The few details needed for the proof of this lemma are left to the reader.

Problems

1. In the following determine whether the systems described are groups. If they are not, point out which of the group axioms fail to hold.
   (a) G = set of all integers, $a \cdot b \equiv a - b$.
   (b) G = set of all positive integers, $a \cdot b = ab$, the usual product of integers.
   (c) $G = a_0, a_1, \ldots, a_6$ where

$$a_i \cdot a_j = a_{i+j} \quad \text{if} \quad i + j < 7,$$
$$a_i \cdot a_j = a_{i+j-7} \quad \text{if} \quad i + j \geq 7$$

   (for instance, $a_5 \cdot a_4 = a_{5+4-7} = a_2$ since $5 + 4 = 9 > 7$).
   (d) G = set of all rational numbers with odd denominators, $a \cdot b \equiv a + b$, the usual addition of rational numbers.

2. Prove that if G is an abelian group, then for all $a, b \in G$ and all integers n, $(a \cdot b)^n = a^n \cdot b^n$.

3. If G is a group such that $(a \cdot b)^2 = a^2 \cdot b^2$ for all $a, b \in G$, show that G must be abelian.

*4. If G is a group in which $(a \cdot b)^i = a^i \cdot b^i$ for three consecutive integers i for all $a, b \in G$, show that G is abelian.

5. Show that the conclusion of Problem 4 does not follow if we assume the relation $(a \cdot b)^i = a^i \cdot b^i$ for just two consecutive integers.

6. In S_3 give an example of two elements x, y such that $(x \cdot y)^2 \neq x^2 \cdot y^2$.

7. In S_3 show that there are four elements satisfying $x^2 = e$ and three elements satisfying $y^3 = e$.

8. If G is a finite group, show that there exists a positive integer N such that $a^N = e$ for all $a \in G$.

9. (a) If the group G has three elements, show it must be abelian.
   (b) Do part (a) if G has four elements.
   (c) Do part (a) if G has five elements.

10. Show that if every element of the group G is its own inverse, then G is abelian.

11. If G is a group of even order, prove it has an element $a \neq e$ satisfying $a^2 = e$.

12. Let G be a nonempty set closed under an associative product, which in addition satisfies:
    (a) There exists an $e \in G$ such that $a \cdot e = a$ for all $a \in G$.
    (b) Give $a \in G$, there exists an element $y(a) \in G$ such that $a \cdot y(a) = e$.
    Prove that G must be a group under this product.

13. Prove, by an example, that the conclusion of Problem 12 is false if we assume instead:

    (a′) There exists an $e \in G$ such that $a \cdot e = a$ for all $a \in G$.

    (b′) Given $a \in G$, there exists $y(a) \in G$ such that $y(a) \cdot a = e$.

14. Suppose a *finite* set G is closed under an associative product and that both cancellation laws hold in G. Prove that G must be a group.

15. (a) Using the result of Problem 14, prove that the nonzero integers modulo p, p a prime number, form a group under multiplication mod p.

    (b) Do part (a) for the nonzero integers relatively prime to n under multiplication mod n.

16. In Problem 14 show by an example that if one just assumed one of the cancellation laws, then the conclusion need not follow.

17. Prove that in Problem 14 infinite examples exist, satisfying the conditions, which are not groups.

18. For any $n > 2$ construct a non-abelian group of order $2n$. (*Hint:* imitate the relations in S_3.)

19. If S is a set closed under an associative operation, prove that no matter how you bracket $a_1a_2 \cdots a_n$, retaining the order of the elements, you get the same element in S (e.g., $(a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = a_1 \cdot (a_2 \cdot (a_3 \cdot a_4))$; use induction on n).

#20. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $ad - bc \neq 0$ is a rational number. Prove that G forms a group under matrix multiplication.

#21. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ where $ad \neq 0$. Prove that G forms a group under matrix multiplication. Is G abelian?

#22. Let G be the set of all real 2×2 matrices $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ where $a \neq 0$. Prove that G is an abelian group under matrix multiplication.

#23. Construct in the G of Problem 21 a subgroup of order 4.

#24. Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo 2, such that $ad - bc \neq 0$. Using matrix multiplication as the operation in G, prove that G is a group of order 6.

#25. (a) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $ad - bc \neq 0$ and a, b, c, d are integers modulo 3, relative to matrix multiplication. Show that $o(G) = 48$.

(b) If we modify the example of G in part (a) by insisting that $ad - bc = 1$, then what is $o(G)$?

#*26. (a) Let G be the group of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where a, b, c, d are integers modulo p, p a prime number, such that $ad - bc \neq 0$. G forms a group relative to matrix multiplication. What is $o(G)$?

(b) Let H be the subgroup of the G of part (a) defined by

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \mid ad - bc = 1 \right\}.$$

What is $o(H)$?

2.4 Subgroups

Before turning to the study of groups we should like to change our notation slightly. It is cumbersome to keep using the $\cdot$ for the group operation; henceforth we shall drop it and instead of writing $a \cdot b$ for $a, b \in G$ we shall simply denote this product as ab.

In general we shall not be interested in arbitrary subsets of a group G for they do not reflect the fact that G has an algebraic structure imposed on it. Whatever subsets we do consider will be those endowed with algebraic properties derived from those of G. The most natural such subsets are introduced in the

DEFINITION A nonempty subset H of a group G is said to be a *subgroup* of G if, under the product in G, H itself forms a group.

The following remark is clear: if H is a subgroup of G and K is a subgroup of H, then K is a subgroup of G.

It would be useful to have some criterion for deciding whether a given subset of a group is a subgroup. This is the purpose of the next two lemmas.

LEMMA 2.4.1 *A nonempty subset H of the group G is a subgroup of G if and only if*

1. *$a, b \in H$ implies that $ab \in H$.*
2. *$a \in H$ implies that $a^{-1} \in H$.*

Proof. If H is a subgroup of G, then it is obvious that (1) and (2) must hold.

Suppose conversely that H is a subset of G for which (1) and (2) hold. In order to establish that H is a subgroup, all that is needed is to verify that $e \in H$ and that the associative law holds for elements of H. Since the associative law does hold for G, it holds all the more so for H, which is a subset of G. If $a \in H$, by part 2, $a^{-1} \in H$ and so by part 1, $e = aa^{-1} \in H$. This completes the proof.

In the special case of a finite group the situation becomes even nicer for there we can dispense with part 2.

LEMMA 2.4.2 *If H is a nonempty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.*

Proof. In light of Lemma 2.4.1 we need but show that whenever $a \in H$, then $a^{-1} \in H$. Suppose that $a \in H$; thus $a^2 = aa \in H$, $a^3 = a^2a \in H$, $\ldots, a^m \in H, \ldots$ since H is closed. Thus the infinite collection of elements $a, a^2, \ldots, a^m, \ldots$ must all fit into H, which is a finite subset of G. Thus there must be repetitions in this collection of elements; that is, for some integers r, s with $r > s > 0$, $a^r = a^s$. By the cancellation in G, $a^{r-s} = e$ (whence e is in H); since $r - s - 1 \geq 0$, $a^{r-s-1} \in H$ and $a^{-1} = a^{r-s-1}$ since $aa^{r-s-1} = a^{r-s} = e$. Thus $a^{-1} \in H$, completing the proof of the lemma.

The lemma tells us that to check whether a subset of a finite group is a subgroup we just see whether or not it is closed under multiplication.

We should, perhaps, now see some groups and some of their subgroups. G is always a subgroup of itself; likewise the set consisting of e is a subgroup of G. Neither is particularly interesting in the role of a subgroup, so we describe them as trivial subgroups. The subgroups between these two extremes we call nontrivial subgroups and it is in these we shall exhibit the most interest.

Example 2.4.1 Let G be the group of integers under addition, H the subset consisting of all the multiples of 5. The student should check that H is a subgroup.

In this example there is nothing extraordinary about 5; we could similarly define the subgroup H_n as the subset of G consisting of all the multiples of n. H_n is then a subgroup for every n. What can one say about $H_n \cap H_m$? It might be wise to try it for $H_6 \cap H_9$.

Example 2.4.2 Let S be any set, $A(S)$ the set of one-to-one mappings of S onto itself, made into a group under the composition of mappings. If $x_0 \in S$, let $H(x_0) = \{\phi \in A(S) \mid x_0\phi = x_0\}$. $H(x_0)$ is a subgroup of $A(S)$. If for $x_1 \neq x_0 \in S$ we similarly define $H(x_1)$, what is $H(x_0) \cap H(x_1)$?

Example 2.4.3 Let G be any group, $a \in G$. Let $(a) = \{a^i \mid i = 0, \pm 1, \pm 2, \ldots\}$. (a) is a subgroup of G (verify!); it is called the *cyclic subgroup generated by a*. This provides us with a ready means of producing subgroups of G. If for some choice of a, $G = (a)$, then G is said to be a *cyclic group*. Such groups are very special but they play a very important role in the theory of groups, especially in that part which deals with abelian groups. Of course, cyclic groups are abelian, but the converse is false.

Example 2.4.4 Let G be a group, W a subset of G. Let (W) be the set of all elements of G representable as a product of elements of W raised to positive, zero, or negative integer exponents. (W) is the *subgroup of G generated by W* and is the smallest subgroup of G containing W. In fact, (W) is the intersection of all the subgroups of G which contain W (this intersection is not vacuous since G is a subgroup of G which contains W).

Example 2.4.5 Let G be the group of nonzero real numbers under multiplication, and let H be the subset of positive rational numbers. Then H is a subgroup of G.

Example 2.4.6 Let G be the group of all real numbers under addition, and let H be the set of all integers. Then H is a subgroup of G.

#Example 2.4.7 Let G be the group of all real 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc \neq 0$ under matrix multiplication. Let

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G \mid ad \neq 0 \right\}.$$

Then, as is easily verified, H is a subgroup of G.

#Example 2.4.8 Let H be the group of Example 2.4.7, and let $K = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right\}$. Then K is a subgroup of H.

Example 2.4.9 Let G be the group of all nonzero complex numbers $a + bi$ (a, b real, not both 0) under multiplication, and let

$$H = \{a + bi \in G \mid a^2 + b^2 = 1\}.$$

Verify that H is a subgroup of G.

DEFINITION Let G be a group, H a subgroup of G; for $a, b \in G$ we say *a is congruent to b mod H*, written as $a \equiv b \bmod H$ if $ab^{-1} \in H$.

LEMMA 2.4.3 *The relation $a \equiv b \bmod H$ is an equivalence relation.*

Proof. If we look back in Chapter 1, we see that to prove Lemma 2.4.3 we must verify the following three conditions: For all $a, b, c \in G$,

1. $a \equiv a \bmod H$.
2. $a \equiv b \bmod H$ implies $b \equiv a \bmod H$.
3. $a \equiv b \bmod H$, $b \equiv c \bmod H$ implies $a \equiv c \bmod H$.

Let's go through each of these in turn.

1. To show that $a \equiv a \bmod H$ we must prove, using the very definition of congruence mod H, that $aa^{-1} \in H$. Since H is a subgroup of G, $e \in H$, and since $aa^{-1} = e$, $aa^{-1} \in H$, which is what we were required to demonstrate.

2. Suppose that $a \equiv b \bmod H$, that is, suppose $ab^{-1} \in H$; we want to get from this $b \equiv a \bmod H$, or, equivalently, $ba^{-1} \in H$. Since $ab^{-1} \in H$, which is a subgroup of G, $(ab^{-1})^{-1} \in H$; but, by Lemma 2.3.1, $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$, and so $ba^{-1} \in H$ and $b \equiv a \bmod H$.

3. Finally we require that $a \equiv b \bmod H$ and $b \equiv c \bmod H$ forces $a \equiv c \bmod H$. The first congruence translates into $ab^{-1} \in H$, the second into $bc^{-1} \in H$; using that H is a subgroup of G, $(ab^{-1})(bc^{-1}) \in H$. However, $ac^{-1} = aec^{-1} = a(b^{-1}b)c^{-1} = (ab^{-1})(bc^{-1})$; hence $ac^{-1} \in H$, from which it follows that $a \equiv c \bmod H$.

This establishes that congruence mod H is a bona fide equivalence relation as defined in Chapter 1, and all results about equivalence relations have become available to us to be used in examining this particular relation.

A word about the notation we used. If G were the group of integers under addition, and $H = H_n$ were the subgroup consisting of all multiples of n, then in G, the relation $a \equiv b \bmod H$, that is, $ab^{-1} \in H$, under the additive notation, reads "$a - b$ is a multiple of n." This is the usual number theoretic congruence mod n. In other words, the relation we defined using an arbitrary group and subgroup is the natural generalization of a familiar relation in a familiar group.

DEFINITION If H is a subgroup of G, $a \in G$, then $Ha = \{ha \mid h \in H\}$. Ha is called a *right coset* of H in G.

LEMMA 2.4.4 *For all $a \in G$,*

$$Ha = \{x \in G \mid a \equiv x \bmod H\}.$$

Proof. Let $[a] = \{x \in G \mid a \equiv x \bmod H\}$. We first show that $Ha \subset [a]$. For, if $h \in H$, then $a(ha)^{-1} = a(a^{-1}h^{-1}) = h^{-1} \in H$ since H is a subgroup of G. By the definition of congruence mod H this implies that $ha \in [a]$ for every $h \in H$, and so $Ha \subset [a]$.

Suppose, now, that $x \in [a]$. Thus $ax^{-1} \in H$, so $(ax^{-1})^{-1} = xa^{-1}$ is also in H. That is, $xa^{-1} = h$ for some $h \in H$. Multiplying both sides by a from the right we come up with $x = ha$, and so $x \in Ha$. Thus $[a] \subset Ha$. Having proved the two inclusions $[a] \subset Ha$ and $Ha \subset [a]$, we can conclude that $[a] = Ha$, which is the assertion of the lemma.

In the terminology of Chapter 1, $[a]$, and thus Ha, is the equivalence class of a in G. By Theorem 1.1.1 these equivalence classes yield a decomposition of G into disjoint subsets. *Thus any two right cosets of H in G either are identical or have no element in common.*

We now claim that between any two right cosets Ha and Hb of H in G there exists a one-to-one correspondence, namely, with any element $ha \in Ha$, where $h \in H$, associate the element $hb \in Hb$. Clearly this mapping is onto Hb. We aver that it is a one-to-one correspondence, for if $h_1b = h_2b$, with $h_1, h_2 \in H$, then by the cancellation law in G, $h_1 = h_2$ and so $h_1a = h_2a$. This proves

LEMMA 2.4.5 *There is a one-to-one correspondence between any two right cosets of H in G.*

Lemma 2.4.5 is of most interest when H is a finite group, for then it merely states that any two right cosets of H have the same number of elements. How many elements does a right coset of H have? Well, note that $H = He$ is itself a right coset of H, so any right coset of H in G has $o(H)$ elements. Suppose now that G is a finite group, and let k be the number of distinct right cosets of H in G. By Lemmas 2.4.4 and 2.4.5 any two distinct right cosets of H in G have no element in common, and each has $o(H)$ elements. Since any $a \in G$ is in the unique right coset Ha, the right cosets fill out G. Thus if k represents the number of distinct right cosets of H in G we must have that $ko(H) = o(G)$. We have proved the famous theorem due to Lagrange, namely,

THEOREM 2.4.1 *If G is a finite group and H is a subgroup of G, then $o(H)$ is a divisor of $o(G)$.*

DEFINITION If H is a subgroup of G, the *index of H in G* is the number of distinct right cosets of H in G.

We shall denote it by $i_G(H)$. In case G is a finite group, $i_G(H) = o(G)/o(H)$, as became clear in the proof of Lagrange's theorem. It is quite possible for an infinite group G to have a subgroup $H \neq G$ which is of finite index in G.

It might be difficult, at this point, for the student to see the extreme importance of this result. As the subject is penetrated more deeply one will become more and more aware of its basic character. Because the theorem is of such stature it merits a little closer scrutiny, a little more analysis, and so we give, below, a slightly different way of looking at its proof. In truth, the procedure outlined below is no different from the one already given. The introduction of the congruence mod H smooths out the listing of elements used below, and obviates the need for checking that the new elements introduced at each stage did not appear before.

So suppose again that G is a finite group and that H is a subgroup of G. Let $h_1, h_2, \ldots, h_r$ be a complete list of the elements of H, $r = o(H)$. If $H = G$, there is nothing to prove. Suppose, then, that $H \neq G$; thus there is an $a \in G$, $a \notin H$. List all the elements so far in two rows as

$$\begin{gathered} h_1, h_2, \ldots, h_r, \\ h_1a,\ h_2a,\ \ldots,\ h_ra. \end{gathered}$$

We claim that all the entries in the second line are different from each other and are different from the entries in the first line. If any two in the second line were equal, then $h_ia = h_ja$ with $i \neq j$, but by the cancellation law this would lead to $h_i = h_j$, a contradiction. If an entry in the second line were equal to one in the first line, then $h_ia = h_j$, resulting in $a = h_i^{-1}h_j \in H$ since H is a subgroup of G; this violates $a \notin H$.

Thus we have, so far, listed $2o(H)$ elements; if these elements account for all the elements of G, we are done. If not, there is a $b \in G$ which did not occur in these two lines. Consider the new list

$$\begin{gathered} h_1, h_2, \ldots, h_r, \\ h_1a,\ h_2a, \ldots, h_ra, \\ h_1b,\ h_2b, \ldots, h_rb. \end{gathered}$$

As before (we are now waving our hands) we could show that no two entries in the third line are equal to each other, and that no entry in the third line occurs in the first or second line. Thus we have listed $3o(H)$ elements. Continuing in this way, every new element introduced, in fact, produces $o(H)$ new elements. Since G is a finite group, we must eventually exhaust all the elements of G. But if we ended up using k lines to list all the elements of the group, we would have written down $ko(H)$ distinct elements, and so $ko(H) = o(G)$.

It is essential to point out that the converse to Lagrange's theorem is false—a group G need not have a subgroup of order m if m is a divisor of $o(G)$. For instance, a group of order 12 exists which has no subgroup of order 6. The reader might try to find an example of this phenomenon; the place to look is in S_4, the symmetric group of degree 4 which has a subgroup of order 12, which will fulfill our requirement.

Lagrange's theorem has some very important corollaries. Before we present these we make one definition.

DEFINITION If G is a group and $a \in G$, the *order* (or *period*) of a is the least positive integer m such that $a^m = e$.

If no such integer exists we say that a is of infinite order. We use the notation $o(a)$ for the order of a. Recall our other notation: for two integers $u, v, u \mid v$ reads "u is a divisor of v."

COROLLARY 1 *If G is a finite group and $a \in G$, then $o(a) \mid o(G)$.*

Proof. With Lagrange's theorem already in hand, it seems most natural to prove the corollary by exhibiting a subgroup of G whose order is $o(a)$. The element a itself furnishes us with this subgroup by considering the cyclic subgroup, (a), of G generated by a; (a) consists of $e, a, a^2, \ldots$. How many elements are there in (a)? We assert that this number is the order of a. Clearly, since $a^{o(a)} = e$, this subgroup has at most $o(a)$ elements. If it should actually have fewer than this number of elements, then $a^i = a^j$ for some integers $0 \leq i < j < o(a)$. Then $a^{j-i} = e$, yet $0 < j - i < o(a)$ which would contradict the very meaning of $o(a)$. Thus the cyclic subgroup generated by a has $o(a)$ elements, whence, by Lagrange's theorem, $o(a) \mid o(G)$.

COROLLARY 2 *If G is a finite group and $a \in G$, then $a^{o(G)} = e$.*

Proof. By Corollary 1, $o(a) \mid o(G)$; thus $o(G) = mo(a)$. Therefore, $a^{o(G)} = a^{mo(a)} = (a^{o(a)})^m = e^m = e$.

A particular case of Corollary 2 is of great interest in number theory. The Euler ϕ-function, $\phi(n)$, is defined for all integers n by the following: $\phi(1) = 1$; for $n > 1$, $\phi(n) =$ number of positive integers less than n and relatively prime to n. Thus, for instance, $\phi(8) = 4$ since only 1, 3, 5, 7 are the numbers less than 8 which are relatively prime to 8. In Problem 15(b) at the end of Section 2.3 the reader was asked to prove that the numbers less than n and relatively prime to n formed a group under multiplication mod n. This group has order $\phi(n)$. If we apply Corollary 2 to this group we obtain

COROLLARY 3 (EULER) *If n is a positive integer and a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \bmod n$.*

In order to apply Corollary 2 one should replace a by its remainder on division by n. If n should be a prime number p, then $\phi(p) = p - 1$. If a is an integer relatively prime to p, then by Corollary 3, $a^{p-1} \equiv 1 \bmod p$, whence $a^p \equiv a \bmod p$. If, on the other hand, a is not relatively prime to p, since p is a prime number, we must have that $p \mid a$, so that $a \equiv 0 \bmod p$; hence $0 \equiv a^p \equiv a \bmod p$ here also. Thus

COROLLARY 4 (Fermat) *If p is a prime number and a is any integer, then $a^p \equiv a \bmod p$.*

COROLLARY 5 *If G is a finite group whose order is a prime number p, then G is a cyclic group.*

Proof. First we claim that G has no nontrivial subgroups H; for $o(H)$ must divide $o(G) = p$ leaving only two possibilities, namely, $o(H) = 1$ or $o(H) = p$. The first of these implies $H = (e)$, whereas the second implies that $H = G$. Suppose now that $a \neq e \in G$, and let $H = (a)$. H is a subgroup of G, $H \neq (e)$ since $a \neq e \in H$. Thus $H = G$. This says that G is cyclic and that every element in G is a power of a.

This section is of great importance in all that comes later, not only for its results but also because the spirit of the proofs occurring here are genuinely group-theoretic. The student can expect to encounter other arguments having a similar flavor. It would be wise to assimilate the material and approach thoroughly, now, rather than a few theorems later when it will be too late.