Introduction to Group Theory

MATH2201/MATH2203

Sandip Chatterjee, Department of Mathematics

Reference

1. A First Course in Abstract Algebra, J.B. Fraleigh
2. Abstract Algebra, I. N. Herstein
3. Abstract Algebra, T. W. Judson
4. Higher Algebra, S.K.Mappa

It's nice to solve a given problem, but it is more important to make an attempt to solve it.

I.N. Herstein

University of Chicago, 1986

With the development of computing in the last several decades, applications that involve abstract algebra and discrete mathematics have become increasingly important in different fields of science and engineering, specifically in computer science. Though theory still occupies a central role in the subject of abstract algebra and no student should go through such a course without a good notion of what a proof is, the importance of applications such as coding theory and cryptography has grown significantly.

The Most Fundamental Phrases

If we can prove a statement true, then that statement is called a **proposition**. A proposition of major importance is called a **theorem**. Sometimes instead of proving a theorem or proposition all at once, we break the proof down into modules; that is, we prove several supporting propositions, which are called **lemmas**, and use the results of these propositions to prove the main result. If we can prove a proposition or a theorem, we will often, with very little effort, be able to derive other related propositions called **corollaries**.

Some Cautions and Suggestions

There are several different strategies for proving propositions. In addition to using different methods of proof, students often make some common mistakes when they are first learning how to prove theorems. To aid students who are studying abstract mathematics for the first time, we list here some of the difficulties that they may encounter and some of the strategies of proof available to them. It is a good idea to keep referring back to this list as a reminder. (Other techniques of proof will become apparent throughout this chapter and the remainder of the text.)

- A theorem cannot be proved by example; however, the standard way to show that a statement is not a theorem is to provide a counterexample

- Quantifiers are important. Words and phrases such as *only*, *for all*, *for every*, and *for some* possess different meanings.

- Never assume any hypothesis that is not explicitly stated in the theorem. You cannot take things for granted.

- Suppose you wish to show that an object exists and is unique. First show that there actually is such an object. To show that it is unique, assume that there are two such objects, say r and s, and then show that r = s.

- Sometimes it is easier to prove the contra-positive of a statement. Proving the statement “If p, then q" is exactly the same as proving the statement “If not q, then not p.”

- Although, it is usually better to find a direct proof of a theorem, this task can sometimes be difficult. It may be easier to assume that the theorem that you are trying to prove is false, and to hope that in the course of your argument you are forced to make some statement that cannot possibly be true.

Remember that one of the main objectives of higher mathematics is proving theorems. Theorems are tools that make new and productive applications of mathematics possible. We use examples to give insight into existing theorems and to foster intuitions as to what new theorems might be true. Applications, examples, and proofs are tightly interconnected-much more so than they may seem at first appearance.

1. Cartesian Products

Given sets A and B, we can define a new set A×B, called the *Cartesian product* of A and B, as a set of ordered pairs. That is,

$$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$$

Example 1.1. If $A = \{x, y\}$, $B = \{1, 2, 3\}$, and $C = \varphi$, then $A \times B$ is the set $\{(x,1),(x, 2),(x,3), (y,1); (y; 2); (y; 3)\}$ and $A \times C = \varphi$

We define the Cartesian product of n sets to be

$$A_1 \times \ldots\ldots \times A_n = \{(a_1,\ldots.,a_n) : a_i \in A_i \text{ for } i = 1,2,\ldots..,n\}$$

If $A = A_1 = A_2 = \ldots\ldots\ldots\ldots = A_n$, we often write A^n for $A\times\ldots.\times A$ (where A would be written n times). For example, the set R^3 consists of all of 3-tuples of real numbers.

2. Binary Operations

Definition 2.1. A ***binary operation*** ∗ on a non-empty set S is a rule that assigns to each ordered pair of elements of elements of S a uniquely determined element of S. The element assigned to the ordered pair (a, b) with a, b ∈ S is denoted by a ∗ b.

Remark. In other words, a binary operation of a set S is a function ∗ : S×S → S from the Cartesian product S × S to the set S. The only difference is that the value of the function ∗ at an ordered pair (a, b) is denoted by a ∗ b rather than ∗((a, b)).

Let S = N = {1, 2, 3, . . .}

Example 2.1. a ⋆ b = max(a, b), e.g. 2 ⋆ 3 = 3, 3 ⋆ 2 = 3, 3 ⋆ 3 = 3.

Example 2.2. a ⋄ b = a, e.g. 2 ⋄ 3 = 2, 3 ⋄ 2 = 3, 3 ⋄ 3 = 3.

Example 2.3. a¤b = a^b, e.g. 2¤3 = 2^3= 8, 3¤2 = 3^2 = 9, 3¤3 = 3^3 = 27.

Definition 2.2. A binary operation $*$ on a set S is ***commutative***, if

$$a * b = b * a \qquad \forall a, b \in S.$$

The binary operation $\star$ is commutative, but the binary operations $\diamond$ and ¤ are not commutative.

Let $*$ be a binary operation on a set S. and let a, b, c $\in$ S. Consider the expression $a * b * c$. This expression doesn't have a meaning since $*$ gives only a meaning to ordered pairs of elements. In fact, there are two ways of making $a*b*c$ meaningful, namely $(a * b) * c$ and $a * (b * c)$.

For the operation $\star$ we have,

$(3 \star 2) \star 4 = 3 \star 4 = 4$

$3 \star (2 \star 4) = 3 \star 4 = 4.$

In fact, for all a, b, c $\in$ N we have $(a \star b) \star c = a \star (b \star c) = \max(a, b, c)$.

For the operation $\diamond$ we have,

$$(3 \diamond 2) \diamond 4 = 3 \diamond 4 = 3$$

$$3 \diamond (2 \diamond 4) = 3 \diamond 2 = 3.$$

In fact, for all a, b, c ∈ N we have $(a \diamond b) \diamond c = a \diamond (b \diamond c) = a$.

But, things are different for the operation ¤. Here we have,

$$(3 ¤ 3) ¤ 3 = (3^3\ ) ¤ 3 = (3^3)^3 = 3^9$$

$$3 ¤ (3 ¤ 3) = 3 ¤ (3^3\ ) = 3^{27}.$$

So, in general, $(a ¤ b) ¤ c \neq a ¤ (b ¤ c)$.

Definition 2.3. A binary operation $*$ on a set S is called associative, if

$$(a * b) * c = a * (b * c).\ \forall a, b, c \in S.$$

In our examples, $\star$ is both commutative and associative, $\diamond$ is not commutative, but associative, ¤ is neither commutative nor associative.

If $*$ is an associative operation on S, then we can write $a * b * c$ for the common value of $(a * b) * c$ and $a * (b * c)$:

$$a * b * c = (a * b) * c = a * (b * c).$$

NB. This works only for associative operations!

Our three examples $\star$, $\diamond$, ¤ are of course artificially made up operations. But there are many natural examples of binary operations.

(a) $* = +$. Addition of numbers is a binary operation on N, Z, Q, R, C.

(b) $* = \times$. Multiplication of numbers is a binary operation on N, Z, Q, R, C and also on $R^+ = \{r \in R : r > 0\}$ and on $\{1, -1\}$.

(c) Addition and multiplication modulo n are binary operations on the set $Z_n = \{0, 1, \ldots, n - 1\}$ of residues modulo n.

(d) Matrix addition and matrix multiplication are binary operations on the set $M_n(R)$ of all n × n matrices with entries in R, also on $M_n(Q)$, $M_n(C)$, $M_n(Z_n)$.

(e) $*$ = $\circ$ = composition of functions. This is a binary operation on the set $F(\Omega) = \{f \mid f : \Omega \to \Omega\}$ of all functions from Ω to itself. Recall: If $f : \Omega \to \Omega$ and $g : \Omega \to \Omega$ are functions from Ω to Ω, then $f \circ g \in F(\Omega)$ is the function defined by $(f \circ g)(x) = f(g(x))\ \forall x \in \Omega$.

ALL the binary operations in Examples (a) – (e) are associative, and all EXCEPT matrix multiplication and composition of functions are commutative.

Important points about binary operations:

(i) The result of the operation must be an element of S. This fails, for example, for + on the set $S = \{-1, 0, 1\}$ (as $1 + 1 = 2 \notin S$). (**Closure Property**)

(ii) The operation must be defined for ***all*** elements of S. This fails, for example for $A * B = A^{-1}BA$ on $M_n(R)$ (as the matrix A^{-1} may not exist).

(iii) The result of the operation must be ***uniquely determined***. This fails, for example, if we set $a * b = c$ where $c^2 = ab$ on C (as for $a = b = 2$, c may be 2 or -2).

Composition Tables

Let S = $\{a_1, a_2, . . . , a_n\}$ be a finite set, and let $*$ be a binary operation on S. The multiplication table of $*$ is the table

*	a_1	a_2	…	a_j	…	a_n
a_1	a_1*a_1	a_1*a_2	…	a_1*a_j	…	a_1*a_n
…	…	…	…	…	…	…
a_i	a_i*a_1	a_i*a_2	…	a_i*a_j	…	a_i*a_n
…	…	…	…	…	…	…
a_n	a_n*a_1	a_n*a_2	…	a_n*a_j	…	a_n*a_n

Example 2.4. For multiplication modulo 3, the multiplication table is

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Remark. Commutativity of a binary operation is instantly recognizable from the multiplication table: $*$ is commutative if and only if its multiplication table is symmetric with respect to the main diagonal. There is no easy way of detecting associativity from the multiplication table.

Definition 2.4. Let $*$ be a binary operation on a set S. An element $e \in S$ is an ***identity element*** for $*$ if

$$e * a = a * e = a \qquad \forall a \in S.$$

Example 2.5. Recall our examples $\star$, $\diamond$ and ¤.

- $a \star b = \max(a, b)$. $e = 1$ is an identity element: $1 \star a = a \star 1 = a$ $\forall a \in N$.
- $a \diamond b = a$. There is no identity element. Indeed, suppose $e \in N$ is an identity element. Then we must have $e \diamond 1 = 1$. But $e \diamond 1 = e$. Hence $e = 1$. But we also must have $e \diamond 2 = 2$. However, for $e = 1$ we get $1 \diamond 2 = 1 \neq 2$. Hence there is no identity element.
- a¤b $= a^b$. No identity element. Indeed, if e was an identity element, we would have 2¤e = 2, that is $2^e = 2$. This gives $e = 1$. At the same time we must have e¤2 = 2, that is $e^2 = 2$. But for $e = 1$ we get 1¤2 $= 1^2 = 1 \neq 2$. Hence there is no identity element.

Example 2.6.

(a) $* = +$: $e = 0$ ($a + 0 = 0 + a = a, \forall a$)

(b) $* = \times$: $e = 1$ ($a1 = 1a = a, \forall a$)

(c) $* = +$ on Z_n : $e = 0$. $* = \times$ on Z_n: $e = 1$.

(d) The identity element for addition of $n \times n$ matrices is $e = O_n$ (the zero matrix). The identity element for matrix multiplication on $M_n(R)$ is $e = I_n$ (the identity matrix).

(e) $* = \circ$ on $F(\Omega)$: $e = id$ (the identity map defined by $id(x) = x$ for all $x \in \Omega$). Indeed, for any function $\varphi : \Omega \to \Omega$ we have $\varphi \circ id = id \circ \varphi = \varphi$

Proposition 2.1. If there is an identity element for a binary operation, then this element is unique.

Proof. Suppose e and f are identity elements for a binary operation $*$ on a set S. Then $e * f = e$, since f is an identity element. At the same time, $e * f = f$ since f is an identity element. Hence $e = f$ (since $*$ is a binary operation implying that $e*f$ is unique).

Definition 2.5. For an associative binary operation $*$ on a set S, and a natural number n we define

$$a^n = a * a * \cdots * a \qquad \text{(operated n-times)}$$

Proposition 2.2. Let $*$ be an associative binary operation $*$ on a set S. Then, for all $a \in S$ and all natural numbers m and n, we have

(i) $a^m * a^n = a^{m+n}$

(ii) $(a^m)^n = a^{mn}$

Proof. Left as exercise

3. Integer Equivalence Classes and Symmetries

Let us now investigate some mathematical structures that can be viewed as sets with single operations.

The Integers modulo n

The integers mod n have become indispensable in the theory and applications of algebra. In mathematics they are used in cryptography, coding theory, and the detection of errors in identification codes.

We have already seen that two integers a and b are equivalent *mod n* if n divides a-b. The integers *mod n* also partition Z into n different equivalence classes; we will denote the set of these equivalence classes by Z_n. Consider the integers modulo 12 and the corresponding partition of the integers:

$$[0] = \{. . ., -12, 0, 12, 24, . . . \},$$

$$[1] = \{. . ., -11, 1, 13, 25, . . .\},$$

$$...$$

$$[11] = \{. . ., -1, 11, 23, 35, . . . \}.$$

When no confusion can arise, we will use 0, 1, . . ., 11 to indicate the equivalence classes [0], [1], . . ., [11] respectively. We can do arithmetic on Z_n. For two integers a and b, define *addition modulo n* to be *(a+b) (mod n)*, that is, the remainder when a + b is divided by n. Similarly, *multiplication modulo n* is defined as *(ab) (mod n)*, the remainder when ab is divided by n.

Table 3.1. Multiplication table for Z_6

.	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	0
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Example 3.1. The following examples illustrate integer arithmetic modulo n:

$7 + 4 \equiv 1 \pmod{5}$ $\quad$ $3 + 5 \equiv 0 \pmod{8}$ $\quad$ $3 + 4 \equiv 7 \pmod{12}$
$7 \,.\, 3 \equiv 1 \pmod{5}$ $\quad$ $3 \,.\, 5 \equiv 7 \pmod{8}$ $\quad$ $3 \,.\, 4 \equiv 0 \pmod{12}$.

In particular, notice that it is possible that the product of two nonzero numbers modulo n can be equivalent to 0 modulo n.

Proposition 3.1. Let Z_n be the set of equivalence classes of the *integers mod n* and a, b, c ϵ Z_n. Then,

1. Addition and multiplication are commutative:

$$a + b \equiv b + a \pmod{n}$$

$$ab \equiv ba \pmod{n}$$

2. Addition and multiplication are associative:

$$(a + b) + c \equiv a + (b + c) \pmod{n}$$

$$(ab)c \equiv a(bc) \pmod{n}$$

3. There are both an additive and a multiplicative identity:

$$a + 0 \equiv a \pmod{n}$$

$$a.\ 1 \equiv a \pmod{n}$$

4. Multiplication distributes over addition: $a(b + c) \equiv ab + ac \pmod{n}$

5. For every integer a there is an additive inverse -a: $a + (-a) \equiv 0 \pmod{n}$

6. Let a be a nonzero integer. Then gcd(a; n) = 1 if and only if there exists a multiplicative inverse b for a (mod n); that is, a nonzero integer b such that $ab \equiv 1 \pmod{n}$.

Proof. We will prove (1) and (6) and leave the remaining properties to be left as exercise.

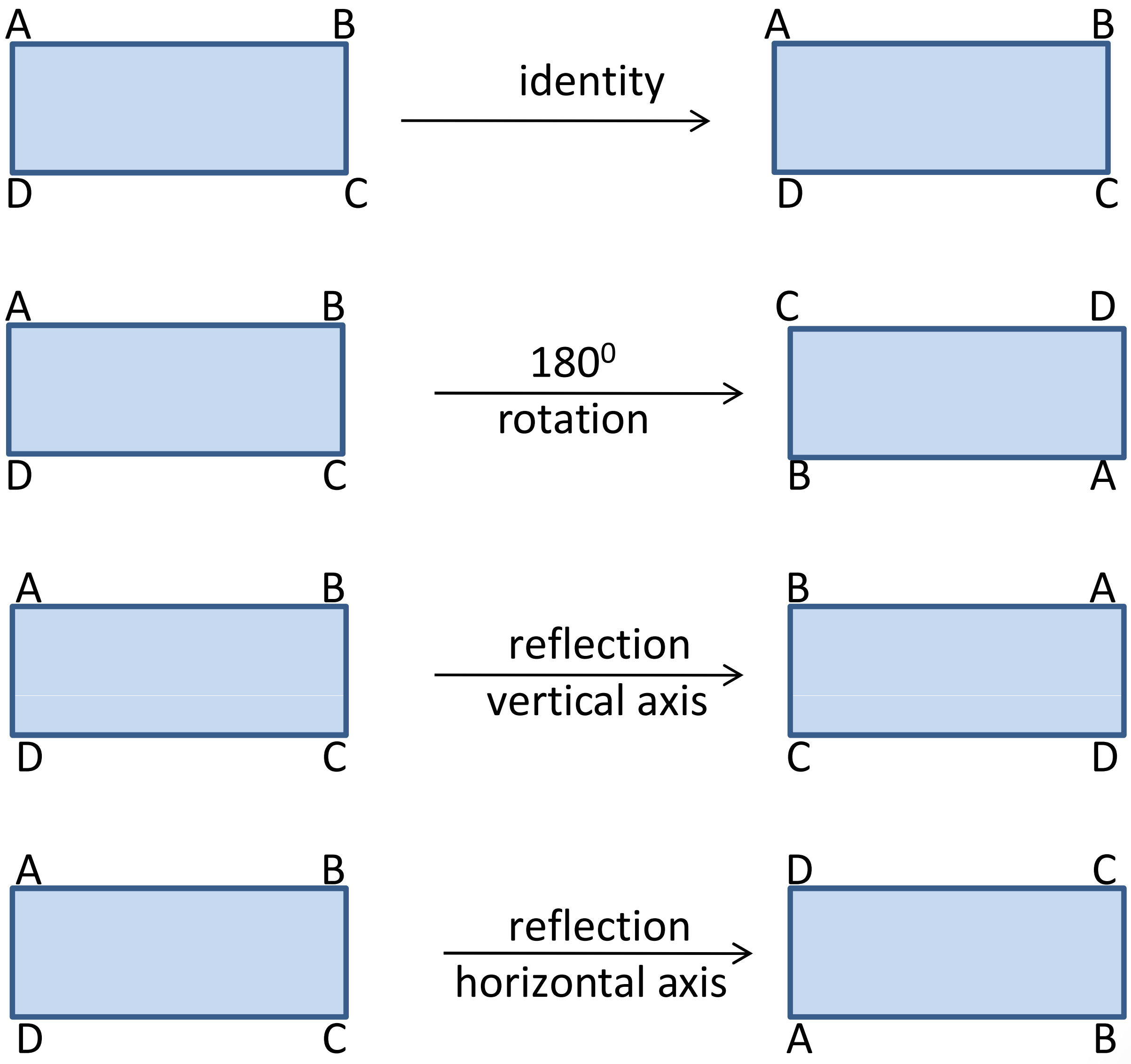
(1) Addition and multiplication are commutative modulo n since the remainder of a+b divided by n is the same as the remainder of b+a divided by n.

(6) Suppose that gcd(a; n) = 1. Then there exist integers r and s such that ar + ns = 1. Since ns = 1-ar, ra ≡ 1 (mod n). Letting b be the equivalence class of r, ab ≡ 1 (mod n).

Conversely, suppose that there exists a b such that ab ≡ 1 (mod n). Then n divides ab-1, so there is an integer k such that ab - nk = 1. Let d = gcd(a; n). Since d divides ab-nk, d must also divide 1; hence, d = 1.

Symmetries

Figure 3.1. Rigid motions of a rectangle



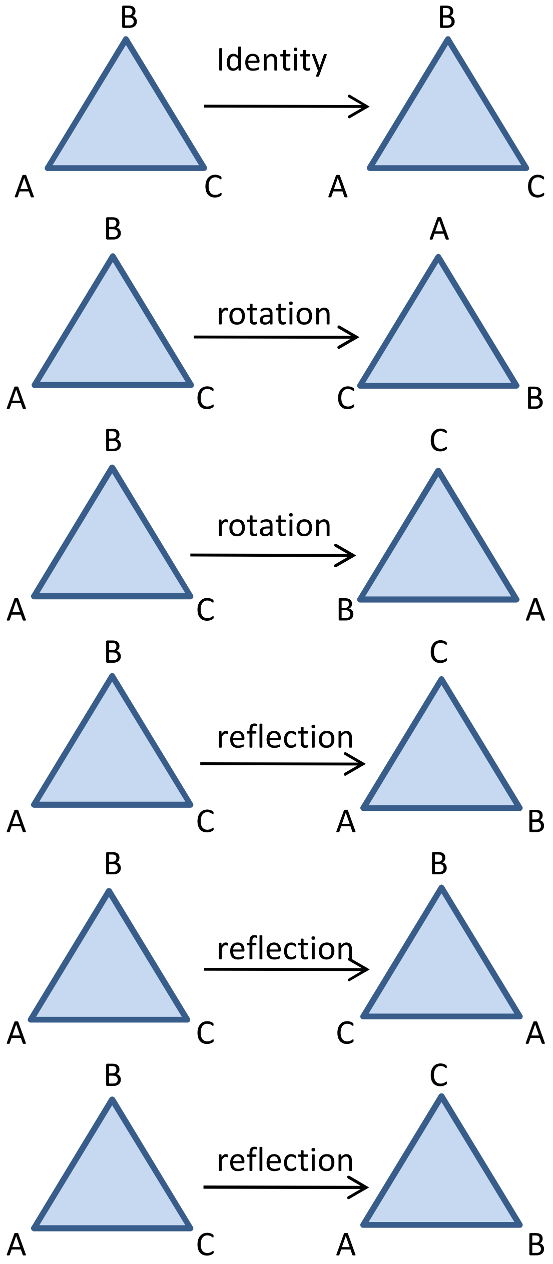
A **symmetry** of a geometric figure is a rearrangement of the figure preserving the arrangement of its sides and vertices as well as its distances and angles. A map from the plane to itself preserving the symmetry of an object is called a **rigid motion**. For example, if we look at the rectangle in Figure 3.1, it is easy to see that a rotation of 180^0 or 360^0 returns a rectangle in the plane with the same orientation as the original rectangle and the same relationship among the vertices. A reflection of the rectangle across either the vertical axis or the horizontal axis can also be seen to be a symmetry. However, a 90^0 rotation in either direction cannot be a symmetry unless the rectangle is a square.

Example 3.3. Suppose that S = {1, 2, 3}. Define a map π : S → S by π(1) = 2, π(2) = 1, π(3) = 3. This is a bijective map. An alternative way to write π is

$$\begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

For any finite set S, a one-to-one and onto mapping π: S → S is called a **permutation** of S.

Example 3.4.



$$i = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

$$\mu_3 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

4. Group

Definition 4.1. A nonempty set G is said to be a *group* if in G there is defined a **binary operation** * such that:

- (G1) Given a, b, c ∈G, then a* (b * c)= *(a * b) * c.*

(This is described by saying that the ***associative law*** holds in *G.)*

- (G2) There exists a special element e ∈ G such that

$$a * e = e * a = a, \text{ for all } a \in G$$

(e is called the ***identity* or *unit element*** of *G).*

- (G3) For every *a* ∈ G there exists an element *b* ∈ *G* such that

$$a * b = b * a = e$$

(We write this element *b* as a^{-1} and call it the ***inverse*** of *a* in *G.)*

The binary operation * in G is usually called the *product,* but keep in mind that this has nothing to do with product as we know it for the integers, rationals, reals, or complexes. In fact, as we shall see below, in many familiar examples of groups that come from numbers, what we call the product in these groups is actually the addition of numbers. *However, a general group need to have no relation whatsoever to a set of numbers.* We reiterate: A group is no more, no less, than a nonempty set with a binary operation * satisfying the three group axioms.

Before starting to look into the nature of groups, we look at some examples.

Example 4.1. Let *Z* be the set of all integers and let * be the ordinary addition, +, in *Z.* That *Z* is closed and associative under * are basic properties of the integers. What serves as the unit element, *e,* of *Z* under *? Clearly, since $a = a * e = a + e$, we have e =0, and 0 is the required identity element under addition. What about a^{-1}? Here too, since $e = 0 = a * a^{-1} = a + a^{-1}$, the a^{-1} in this instance is *-a,* and clearly a *(-a) =a + *(-a)* =0.

Example 4.2. Let Q be the set of all rational numbers and let the operation * on Q be the ordinary addition of rational numbers. As above, 0 is easily shown to be a group under *. Note that Z∈Q and both *Z* and Q are groups under the same operation *.

Example 4.3. Let Q' be the set of all *nonzero* rational numbers and let the operation * on Q' be the ordinary multiplication of rational numbers. By the familiar properties of the rational numbers we see that Q' forms a group relative to *.

Example 4.4. Let R^+ be the set of all *positive real* numbers and let the operation * on R^+ be the ordinary product of real numbers. Again it is easy to check that R^+ is a group under *.

Example 4.5. The integers mod n form a group under addition modulo n. Consider Z_5, consisting of the equivalence classes of the integers 0, 1, 2, 3, and 4. We define the group operation on Z_5 by modular addition. We write the binary operation on the group additively; that is, we write m + n. The element 0 is the identity of the group and each element in Z5 has an inverse. For instance, 2+3 = 3+2 = 0. Table 4.1 is a Cayley table for Z_5. By proposition 3.1., Z_n = {0, 1, . . . , n − 1} is a group under the binary operation of *addition mod n* (Verify!).

Table 4.1. Multiplication table for Z_5

.	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	0	2
3	0	3	0	3	0
4	0	4	2	0	4

Example 4.6. Not every set with a binary operation is a group. For example, if we let modular multiplication be the binary operation on Z_n, then Z_n fails to be a group. The element 1 acts as a group identity since 1·k=k·1=k for any k ∈ Z_n; however, a multiplicative inverse for 0 does not exist since 0·k = k·0 = 0 for every k in Z_n. Even if we consider the set $Z_n \setminus \{0\}$, we still may not have a group. For instance, let $2 \in Z_6$. Then 2 has no multiplicative inverse since 0·2=0 ; 1·2=2; 2·2=4; 3·2=0; 4·2=2; 5·2=4

By proposition 3.1., every nonzero k does have an inverse in Z_n if k is relatively prime to n. Denote the set of all such nonzero elements in Z_n by U(n). Then U(n) is a group called the group of units of Z_n. Table 4.2. is a Cayley table for the group U(8).

Table 4.2. Multiplication table for U(8)

.	**1**	**3**	**5**	**7**
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Definition 4.2. A group G is said to be a ***finite group*** if it has a finite number of elements. The number of elements in G is called the ***order* of G** and is denoted by IGI.

Definition 4.3. A group G is said to be ***abelian*** if $a * b = b * a$ for all $a, b \in G$.

Example 4.7. The symmetries of an equilateral triangle described in Example 3.4. form a nonabelian group. As we observed, it is not necessarily true that αβ = βα for two symmetries α and β. Using Table 4.3., which is a Cayley table for this group, we can easily check that the symmetries of an equilateral triangle are indeed a group. We will denote this group by either S_3 or D_3, for reasons that will be explained later.

Table 4.3. Symmetries of an equilateral triangle

o	**i**	**ρ_1**	**ρ_2**	**μ_1**	**μ_2**	**μ_3**
i	i	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	i	μ_3	μ_1	μ_2
ρ_2	ρ_2	i	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	i	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	i	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	i

Example 4.8. We use $M_2(R)$ to denote the set of all 2 × 2 matrices. Let $GL_2(R)$ be the subset of $M_2(R)$ consisting of invertible matrices; that is, a matrix

$$A= \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $GL_2(R)$ if there exists a matrix A^{-1} such that $AA^{-1} = A^{-1}A = I$, where I is the 2×2 identity matrix. For A to have an inverse is equivalent to requiring that the determinant of A be nonzero; that is, $\det A = ad - bc \neq 0$. The set of invertible matrices forms a group called the ***general linear group***. The identity of the group is the identity matrix. The identity of the group is the identity matrix. The inverse can be calculated easily.

The product of two invertible matrices is again invertible. Matrix multiplication is associative, satisfying the other group axiom. For matrices it is not true in general that AB = BA; hence, $GL_2(R)$ is another example of a non-abelian group.

Example 4.9. Let

$$1= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad I= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad J= \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad K= \begin{pmatrix} i & 0 \\ 0 & -I \end{pmatrix}$$

Then the relations $I^2=J^2=K^2=-1$, IJ=K, JK=I, KI=J, JI=-K, KJ=-I and IK=-J hold (verify). The set $Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$ is a group called **Quaternion Group**. It is to be noted that Q_8 is a non-commutative group.

Example 4.10. Let C^* be the set of nonzero complex numbers. Under the operation of multiplication C^* forms a group. The identity is 1. If z = a + ib is a nonzero complex number, then

$$z^{-1} = \frac{a-ib}{a^2+b^2}$$

is the inverse of z. It is easy to see that the remaining group axioms hold.

A(S) (THE SET OF 1-1 MAPPINGS OF S ONTO ITSELF)

We focus our attention in this section on particularly nice mappings of a non empty set, S, into itself. Namely, we shall consider the set, *A(S),* of all 1-1 mappings of S onto itself. Although most of the concern in this note will be in the case in which S is a finite set, we do not restrict ourselves to that situation here.

When S has a finite number of elements, say *n,* then A(S) has a special name. It is called the ***symmetric group of degree n*** and is often denoted by S_n. Its elements are called ***permutations*** of S. If we are interested in the structure of S_n, it really does not matter much what our underlying set S is. So, you can think of S as being the set {1, ... , n}. In the investigation of finite groups, S_n plays a central role.

There are many properties of the set A(S) on which we could concentrate. We have chosen to develop those aspects here which will motivate the notion of a group and which will give the reader some experience, and feeling for, working in a group-theoretic framework.

Lemma 4.1. $A(S)$ satisfies the following:

(a) $f, g \in A(S)$ implies that $fg \in A(S)$.

(b) $f, g, h \in A(S)$ implies that$(fg)h= f(gh)$.

(c) There exists an element, the identity mapping i, such that $fi = if = f$, for every $f \in A (S)$.

(d) Given $f \in A(S)$, there exists a $g \in A(S)$ ($g = f^{-1}$) such that $fg = gf= i$.

Proof: Left as an exercise.

We should now like to know how many elements there are in $A(S)$ when S is a finite set having *n* elements. To do so, we first make a slight digression.

Suppose that you can do a certain thing in *r* different ways and a second independent thing in *s* different ways. In how many distinct ways can you do both things together? The best way of finding out is to picture this in a concrete context. Suppose that there are *r* highways running from Kolkata to Mumbai and *s* highways running from Mumbai to Delhi. In how many ways can you go first to Mumbai, then to Delhi? Clearly, for every road you take from Kolkata to Mumbai you have *s* ways of continuing on to Delhi. You can start your trip from Kolkata in *r* distinct ways, hence you can complete it in *rs* different ways.

It is fairly clear that we can extend this from doing two independent things to doing m independent ones, for an integer $m > 2$. If we can do the first things in r_1 distinct ways, the second in r_2 ways, , the m-th in r_m distinct ways, then we can do all these together in $r_1\, r_2 \ldots\ldots. r_m$ different ways.

Lemma 4.2. If S has n elements, then $A(S)$ has $n!$ elements.

Proof: Let $f \in A(S)$, where $S = \{x_1, x_2, \ldots , x_n\}$. How many choices does f have as a place to send x_1? Clearly n, for we can send x_1 under f to any element of S. But now f is *not* free to send x_2 anywhere, for since f is 1-1, we must have $f(x_1) \neq f(x_2)$. So we can send x_2 anywhere except onto $f(x_1)$. Hence, f can send x_2 into $n-1$ different images. Continuing this way, we see that f can send x_i into $n - (i - 1)$ different images. Hence the number of such f's is $n(n- 1)(n- 2)\ldots..1= n!$. □

Example 4.11. The number *n*! gets very large quickly. To be able to see the picture in its entirety, we look at the special case *n* = 3, where *n*! is still quite small.

Consider $A(S) = S_3$, where S consists of the three elements x_1, x_2, x_3. We list all the elements of S_3, writing out each mapping explicitly by what it does to each of x_1, x_2, x_3.

1. i: $x_1 \rightarrow x_1$, $x_2 \rightarrow x_2$, $x_3 \rightarrow x_3$
2. f: $x_1 \rightarrow x_2$, $x_2 \rightarrow x_3$, $x_3 \rightarrow x_1$
3. g: $x_1 \rightarrow x_2$, $x_2 \rightarrow x_1$, $x_3 \rightarrow x_3$
4. gf: $x_1 \rightarrow x_1$, $x_2 \rightarrow x_3$, $x_3 \rightarrow x_2$
5. fg: $x_1 \rightarrow x_3$, $x_2 \rightarrow x_2$, $x_3 \rightarrow x_1$
6. ff/f^2: $x_1 \rightarrow x_3$, $x_2 \rightarrow x_1$, $x_3 \rightarrow x_2$

Since we have listed here six different elements of S_3, and S_3 has only six elements, we have a complete list of all the elements of S_3. What does this list tell us?

To begin with, we note that *fg* ≠gf*,* so one familiar rule of the kind of arithmetic we have been used to is violated. Since gϵS_3 and gϵS_3, we must have *gg* (g^2) also in S_3. What is it? If we calculate *gg,* we easily get *gg* = *i.* Similarly, we get

$(f\text{g})\,(f\text{g}) = i = (\text{g}f)\,(\text{g}f)$

Note also that $f\ (ff) = i$, hence $f^{-1} = ff$. Finally, we leave it to the reader to show that gf = f^{-1}g.

From now on we shall start using the shorthand of exponents, to avoid expressions like *ffffffff.* We define, for $f \in A\ (S)$, $f^0 = i$, $f^2 = ff$, and so on. For negative exponents $-n$ we define f^{-n} by $f^{-n} = (f^{-1})^n$, where n is a positive integer. The usual rules of exponents prevail, namely $f^r f^s = f^{r+s}$ and $(f^r)^s = f^{rs}$. We leave these as exercises-somewhat tedious ones at that-for the reader.

Caution! Do not jump to conclusions that all familiar properties of exponents go over.For instance, in the example of the *f,* g ϵ S_3 defined above, it can be easily verified that $(fg)^2 \neq f^2g^2$.

However, some other familiar properties do go over. For instance, if *f,* g, *h* are in *A(S)* and *fg = fh,* then g = *h.* Why? Because, from *fg* = *fh* we have $f^{-1}(fg) = f^{-1}(fh)$; therefore, g = *ig* = $(f^{-1}f)g = f^{-1}(fg) = f^{-1}(fh) = (f^{-1}f)h = ih = h$. Similarly, *gf* = *hf* implies that g = *h.* So we can cancel an element in such an equation provided that we *do not change sides.* In S_3 our *f,* g satisfy $gf = f^{-1}g$, but since $f \neq f^{-1}$ we *cannot cancel* the g here.

Basic Properties of Groups

Proposition 3.2 : The identity element in a group G is unique; that is, there exists only one element e ∈ G such that eg = ge = g for all g ∈ G.

Proof. Suppose that e and e’ are both identities in G. Then eg = ge=g and e’g=ge’=g for all g∈G. We need to show that e=e’. If we think of e as the identity, then ee’ = e’; but if e’ is the identity, then ee’ = e. Combining these two equations, we have e = ee’ = e’.

Proposition 3.3: If g is any element in a group G, then the inverse of g, g^{-1}, is unique.

Proof: Inverses in a group are also unique. If g’ and g’’ are both inverses of an element g in a group G, then gg’ =g’g=e and gg’’ =g’’g=e. We want to show that g’ = g’’, but g’ = g’e = g’(gg’’) = (g ’g)g’’ = eg’’ = g’’.

Proposition 3.4: Let G be a group. If a, b $\in$ G, then $(ab)^{-1} = b^{-1} a^{-1}$.

Proof. Let a,b $\in$ G. Then $abb^{-1} a^{-1} = aea^{-1} = aa^{-1} = e$. Similarly, $b^{-1}a^{-1} ab = e$. But by the previous proposition, inverses are unique; hence, $(ab)^{-1} = b^{-1} a^{-1}$.

Proposition 3.5: Let G be a group. For any a $\in$ G, $(a^{-1})^{-1} = a$.

Proof. Observe that $a^{-1} (a^{-1})^{-1} = e$. Consequently, multiplying both sides of this equation by a, we have

$$(a^{-1})^{-1} = e(a^{-1})^{-1} = aa^{-1}(a^{-1})^{-1} = ae = a.$$

Proposition 3.6: Let G be a group and a and b be any two elements in G. Then the equations ax = b and xa = b have unique solutions in G.

Proof. Suppose that ax = b. We must show that such an x exists. Multiplying both sides of ax = b by a^{-1}, we have $x = ex = a^{-1}ax = a^{-1}b$.

To show uniqueness, suppose that x_1 and x_2 are both solutions of ax = b; then $ax_1=b=ax_2$. So $x_1=a^{-1}ax =a^{-1}ax_2 =x_2$. The proof for the existence and uniqueness of the solution of xa = b is similar.

Proposition 3.7: If G is a group and $a,b,c \in G$, then $ba = ca$ implies $b = c$ and $ab=ac$ implies $b=c$.

This proposition tells us that the ***right and left cancellation laws*** are true in groups. We leave the proof as an exercise.

We can use exponential notation for groups just as we do in ordinary algebra. If G is a group and $g \in G$, then we define $g^0 = e$. For $n \in N$, we define

$$g^n = g \cdot g \cdots g \text{ (n times) and } g^{-n} = g^{-1} \cdot g^{-1} \cdot \cdot \cdot g^{-1} \text{ (n times)}$$

Theorem 3.8: In a group, the usual laws of exponents hold; that is, for all $g, h \in G$,

1. $g^m g^n = g^{m+n}$ for all $m,n \in Z$;
2. $(g^m)^n = g^{mn}$ for all $m,n \in Z$;
3. $(gh)^n = (h^{-1} g^{-1})^{-n}$ for all $n \in Z$.

Furthermore, if G is abelian, then $(gh)^n = g^n h^n$.

Proof. We will leave the proof of this theorem as an exercise.

Notice that $(gh)^n \neq g^n h^n$ in general, since the group may not be abelian.

Subgroups

Definitions and Examples :

Sometimes we wish to investigate smaller groups sitting inside a larger group. The set of even integers 2Z = {...,−2,0,2,4,...} is a group under the operation of addition. This smaller group sits naturally inside of the group of integers under addition.

We define a **subgroup** H of a group G to be a subset H of G such that when the group operation of G is restricted to H, H is a group in its own right.

Observe that every group G with at least two elements will always have at least two subgroups, the subgroup consisting of the identity element alone and the entire group itself. The subgroup H = {e} of a group G is called the **trivial subgroup**. A subgroup that is a proper subset of G is called a **proper subgroup**. In many of the examples that we have investigated up to this point, there exist other subgroups besides the trivial and improper subgroups.

Example 10. Consider the set of nonzero real numbers, $R*$, with the group operation of multiplication. The identity of this group is 1 and the inverse of any element $a \in R*$ is just $1/a$. We will show that

$$Q* = \{p/q : p \text{ and } q \text{ are nonzero integers}\}$$

is a subgroup of $R*$. The identity of $R*$ is 1; however, $1 = 1/1$ is the quotient of two nonzero integers. Hence, the identity of $R*$ is in $Q*$. Given two elements in $Q*$, say p/q and r/s, their product pr/qs is also in $Q*$. The inverse of any element $p/q \in Q*$ is again in $Q*$ since $(p/q)-1 = q/p$. Since multiplication in $R*$ is associative, multiplication in $Q*$ is associative.

Example 11. Recall that $C*$ is the multiplicative group of nonzero complex numbers. Let $H = \{1, -1, i, -i\}$. Then H is a subgroup of $C*$. It is quite easy to verify that H is a group under multiplication and that $H \subset C*$.

Example 12. Let $SL_2(R)$ be the subset of $GL_2(R)$ consisting of matrices of determinant one; that is, a matrix

$$A= \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $SL_2(R)$ exactly when ad − bc = 1. To show that $SL_2(R)$ is a subgroup of the general linear group, we must show that it is a group under matrix multiplication. The 2×2 identity matrix is in $SL_2(R)$, as is the inverse of the matrix A:

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

It remains to show that multiplication is closed; that is, that the product of two matrices of determinant one also has determinant one. We will leave this task as an exercise. The group $SL_2(R)$ is called the ***special linear group***.

Example 13. It is important to realize that a subset H of a group G can be a group without being a subgroup of G. For H to be a subgroup of G it must inherit G’s binary operation. The set of all 2 × 2 matrices, $M_2(R)$, forms a group under the operation of addition. The 2 × 2 general linear group is a subset of $M_2(R)$ and is a group under matrix multiplication, but it is not a subgroup of $M_2(R)$. If we add two invertible matrices, we do not necessarily obtain another invertible matrix. Observe that

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

but the zero matrix is not in GL2(R).

Example 14. One way of telling whether or not two groups are the same is by examining their subgroups. Other than the trivial subgroup and the group itself, the group Z_4 has a single subgroup consisting of the elements 0 and 2. From the group Z_2, we can form another group of four elements as follows. As a set this group is $Z_2 \times Z_2$. We perform the group operation coordinate-wise; that is, (a, b) + (c, d) = (a + c, b + d). Since there are three nontrivial proper subgroups of $Z_2{\times}Z_2$, $H_1=\{(0,0),(0,1)\}$, $H_2=\{(0,0),(1,0)\}$, and $H_3=\{(0,0),(1,1)\}$, Z_4 and $Z_2 \times Z_2$ must be different groups.

+	(0,0)	(0,1)	(1,0)	(0,1)
(0,0)				
(0,1)				
(1,0)				
(1,1)				

Proposition 3.9: A subset H of G is a subgroup if and only if it satisfies the following conditions.

1. The identity e of G is in H.
2. If $h_1, h_2 \in H$, then $h_1h_2 \in H$.
3. If $h \in H$, then $h^{-1} \in H$.

Proof. First suppose that H is a subgroup of G. We must show that the three conditions hold. Since H is a group, it must have an identity e_H . We must show that $e_H = e$, where e is the identity of G. We know that $e_He_H = e_H$ and that $ee_H = e_H e = e_H$; hence, $ee_H = e_He_H$. By right-hand cancellation, $e = e_H$. The second condition holds since a subgroup H is a group. To prove the third condition, let $h \in H$. Since H is a group, there is an element $h' \in H$ such that $hh' = h'h = e$. By the uniqueness of the inverse in G, $h' = h^{-1}$.

Conversely, if the three conditions hold, we must show that H is a group under the same operation as G; however, these conditions plus the associativity of the binary operation are exactly the axioms stated in the definition of a group.

Proposition 3.10: Let H be a subset of a group G. Then H is a subgroup of G if and only if H ≠ ∅, and whenever g, h∈H then gh^{-1} is in H.

Proof. Let H be a nonempty subset of G. Then H contains some element g. So gg^{-1} =e is in H. If g∈H, then eg^{-1} =g^{-1} is also in H. Finally, let g,h ∈ H. We must show that their product is also in H. However, $g(h^{-1})^{-1}$= gh ∈ H. Hence, H is indeed a subgroup of G. Conversely, if g and h are in H, we want to show that gh^{-1}∈H. Since h is in H, its inverse h^{-1} must also be in H. Because of the closure of the group operation, gh^{-1} ∈ H.

Cyclic Group

The groups Z and Z_n, which are among the most familiar and easily under- stood groups, are both examples of what are called cyclic groups. In this chapter we will study the properties of cyclic groups and cyclic subgroups, which play a fundamental part in the classification of all abelian groups.

4.1 Cyclic Subgroups

Often a subgroup will depend entirely on a single element of the group; that is, knowing that particular element will allow us to compute any other element in the subgroup.

Example 1. Suppose that we consider $3 \in Z$ and look at all multiples (both positive and negative) of 3. As a set, this is

$$3Z = \{\ldots,-3,0,3,6,\ldots\}.$$

Example 2. If H = $\{2^n : n \in Z\}$, then H is a subgroup of the multiplicative group of nonzero rational numbers, Q∗. If a = 2^m and b = 2^n are in H, then $ab^{-1} = 2^m\, 2^{-n} = 2^{m-n}$ is also in H. By Proposition 3.10, H is a subgroup of Q∗ determined by the element 2.

Theorem 4.1. Let G be a group and a be any element in G. Then the set $\langle a\rangle=\{a^k : k\in Z\}$ is a subgroup of G. Furthermore, $\langle a\rangle$ is the smallest subgroup of G that contains a.

Proof. The identity is in $\langle a\rangle$ since $a^0 = e$. If g and h are any two elements in $\langle a\rangle$, then by the definition of $\langle a\rangle$ we can write $g=a^m$ and $h=a^n$ for some integers m and n. So $gh = a^m a^n = a^{m+n}$ is again in $\langle a\rangle$. Finally, if $g=a^n$ in $\langle a\rangle$, then the inverse $g^{-1} = a^{-n}$ is also in $\langle a\rangle$. Which proves $\langle a\rangle$ is a subgroup of G. Clearly, any subgroup H of G containing a, must contain all the powers of a by closure; hence, H contains $\langle a\rangle$. Therefore, $\langle a\rangle$ is the smallest subgroup of G containing a.

Remark. If we are using the "+" notation, as in the case of the integers under addition, we write $\langle a \rangle = \{na : n \in Z\}$.

For a $\in$ G, we call $\langle a \rangle$ the **cyclic subgroup generated by a**. If G contains some element a such that $G = \langle a \rangle$, then G is a **cyclic group**. In this case a is a **generator** of G. If a is an element of a group G, we define the **order of a** to be the smallest positive integer n such that $a^n = e$, and we write $|a| = n$. If there is no such integer n, we say that the order of a is infinite and write $|a| = \infty$ to denote the order of a.

Example 3. Notice that a cyclic group can have more than a single generator. Both 1 and 5 generate Z_6; hence, Z_6 is a cyclic group. Not every element in a cyclic group is necessarily a generator of the group. The order of $2 \in Z_6$ is 3. The cyclic subgroup generated by 2 is $\langle 2 \rangle = \{0, 2, 4\}$.

The groups Z and Z_n are cyclic groups. The elements 1 and −1 are generators for Z. We can certainly generate Z_n with 1 although there may be other generators of Z_n, as in the case of Z_6.

Example 4. The group of units, U(9), in Z_9 is a cyclic group. As a set, U(9) is {1,2,4,5,7,8}. The element 2 is a generator for U(9) since

$$\begin{array}{ccc} 2^1 = 2 & 2^3 = 8 & 2^5 = 5 \\ 2^2 = 4 & 2^4 = 7 & 2^6 = 1 \end{array}$$

Example 5. Not every group is a cyclic group. Consider the symmetry group of an equilateral triangle S_3. The multiplication table for this group is Table 3.2. (Verify!)

Theorem 4.2 Every cyclic group is abelian.

Proof. Let G be a cyclic group and $a \in G$ be a generator for G. If g and h are in G, then they can be written as powers of a, say $g=a^r$ and $h=a^s$. Since $gh=a^r a^s =a^{r+s} =a^{s+r} =a^s a^r =hg$, G is abelian.

Subgroups of Cyclic Groups

We can ask some interesting questions about cyclic subgroups of a group and subgroups of a cyclic group. If G is a group, which subgroups of G are cyclic? If G is a cyclic group, what type of subgroups does G possess?

Theorem 4.3. Every subgroup of a cyclic group is cyclic.

Proof. The main tool used in this proof are the division algorithm and the Principle of Well-Ordering. Let G be a cyclic group generated by a and suppose that H is a subgroup of G. If H = {e}, then trivially H is cyclic. Suppose that H contains some other element g distinct from the identity. Then g can be written as a^n for some integer n. We can assume that n > 0.

Let m be the smallest natural number such that $a^m \in$ H. Such an m exists by the Principle of Well-Ordering. We claim that h = a^m is a generator for H. We must show that every h′ ∈H can be written as a power of h. Since h′ ∈H and H is a subgroup of G, h′ = a^k for some positive integer k. Using the division algorithm, we can find numbers q and r such that k = mq + r where 0 ≤ r < m; hence,

$$a^k = a^{mq+r} = (am)^q a^r = h^q\, a^r$$

So $a^r = a^k\, h^{-q}$. Since a^k and h^{-q} are in H, a^r must also be in H. However, m was the smallest positive number such that am was in H; consequently, r=0 and so k=mq. Therefore,

$$h' = a^k = a^{mq} = h^q$$

and H is generated by h.

Corollary 4.4. The subgroups of Z are exactly nZ for n = 0, 1, 2, ...

Proposition 4.5. Let G be a cyclic group of order n and suppose that a is a generator for G. Then $a^k = e$ if and only if n divides k.

Proof. First suppose that $a^k = e$. By the division algorithm, k = nq + r where $0 \leq r < n$; hence

$$e=a^k =a^{nq+r} =a^{nq}\, a^r =ea^r =a^r$$

Since the smallest positive integer m such that am = e is n, r = 0. Conversely, if n divides k, then k = ns for some integer s. Consequently,

$a^k =a^{ns} =(a^n)^s =e^s =e.$

Theorem 4.6. Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d, where d = gcd(k, n).

Proof. We wish to find the smallest integer m such that $e = b^m = a^{km}$. By Proposition 4.5, this is the smallest integer m such that n divides km or, equivalently, n/d divides m(k/d). Since d is the greatest common divisor of n and k, n/d and k/d are relatively prime. Hence, for n/d to divide m(k/d) it must divide m. The smallest such m is n/d.

Corollary 4.7. The generators of Z_n are the integers r such that $1 \leq r < n$ and gcd(r, n) = 1.

Permutation Group

In general, the permutations of a set X form a group S_X. If X is a finite set, we can assume X = {1,2,...,n}. In this case we write S_n instead of S_X . The following theorem says that S_n is a group. We call this group the **symmetric group** on n letters.

Theorem 5.1. The symmetric group on n letters, S_n, is a group with n! elements, where the binary operation is the composition of maps.

Proof. The identity of Sn is just the identity map that sends 1 to 1, 2 to 2, ..., n to n. If $f : S_n \rightarrow S_n$ is a permutation, then f^{-1} exists, since f is one-to-one and onto; hence, every permutation has an inverse. Composition of maps is associative, which makes the group operation associative. We leave the proof that $|S_n| = n!$ as an exercise.

A subgroup of S_n is called a **permutation group**.

A permutation $\sigma \in S_X$ is a **cycle of length k** if there exist elements $a_1, a_2, \ldots, a_k \in X$ such that

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3, \ldots\ldots\ldots, \sigma(a_k) = a_1$$

and $\sigma(x) = x$ for all other elements $x \in X$. We will write $(a_1, a_2, \ldots, a_k)$ to denote the cycle σ. Cycles are the building blocks of all permutations.

Theorem 5.3. Every permutation in S_n can be written as the product of disjoint cycles.

Proof. We can assume that $X = \{1,2,\ldots,n\}$. Let $\sigma \in S_n$, and define X_1 to be $\{\sigma(1), \sigma^2(1), . . .\}$. The set X_1 is finite since X is finite. Now let i be the first integer in X that is not in X_1 and define X_2 by $\{\sigma(i), \sigma^2(i), . . .\}$.

Again, X_2 is a finite set. Continuing in this manner, we can define finite disjoint sets $X_3, X_4, ...$ Since X is a finite set, we are guaranteed that this process will end and there will be only a finite number of these sets, say r. If σ_i is the cycle defined by

$$\sigma_i(x)=\sigma(x), \text{ when } x \in Xi \text{ and } \sigma_i (x) = x, \text{ else}$$

then $\sigma = \sigma_1\sigma_2\cdots\sigma_r$. Since the sets $X_1, X_2, \ldots, X_r$ are disjoint, the cycles $\sigma_1, \sigma_2, \ldots, \sigma_r$ must also be disjoint.

The simplest permutation is a cycle of length 2. Such cycles are called **transpositions**. Since

$(a_1, a_2, . . . , a_n) = (a_1a_n)(a_1a_{n-1}) \cdot\cdot\cdot (a_1a_3)(a_1a_2)$

any cycle can be written as the product of transpositions, leading to the following proposition.

Proposition 5.4 Any permutation of a finite set containing at least two elements can be written as the product of transpositions.

Lemma 5.5. If the identity is written as the product of r transpositions, id = $\tau_1 \tau_2 \cdots \tau_r$, then r is an even number.

Proof. We will employ induction on r. A transposition cannot be the identity; hence, r > 1. If r = 2, then we are done. Suppose that r > 2. In this case the product of the last two transpositions, $\tau_{r-1}\tau_r$, must be one of the following cases:

$$(ab)(ab) = id$$
$$(bc)(ab) = (ac)(bc)$$
$$(cd)(ab) = (ab)(cd)$$
$$(ac)(ab) = (ab)(bc),$$

where a, b, c, and d are distinct.

The first equation simply says that a transposition is its own inverse. If this case occurs, delete τ_{r-1} τ_r from the product to obtain id = $\tau_1 \tau_2 \cdot\cdot\cdot \tau_{r-3} \tau_{r-2}$. By induction r − 2 is even; hence, r must be even.

In each of the other three cases, we can replace $\tau_{r-1}\tau_r$ with the right-hand side of the corresponding equation to obtain a new product of r transpositions for the identity. In this new product the last occurrence of a will be in the next-to-the-last transposition. We can continue this process with $\tau_{r-2}\tau_{r-1}$ to obtain either a product of r−2 transpositions or a new product of r transpositions where the last occurrence of a is in τ_{r-2}. If the identity is the product of r−2 transpositions, then again we are done, by our induction hypothesis; otherwise, we will repeat the procedure with $\tau_{r-3}\ \tau_{r-2}$.

At some point either we will have two adjacent, identical transpositions canceling each other out or a will be shuffled so that it will appear only in the first transposition. However, the latter case cannot occur, because the identity would not fix a in this instance. Therefore, the identity permutation must be the product of r−2 transpositions and, again by our induction hypothesis, we are done.

Theorem 5.6. If a permutation σ can be expressed as the product of an even number of transpositions, then any other product of transpositions equaling σ must also contain an even number of transpositions. Similarly, if σ can be expressed as the product of an odd number of transpositions, then any other product of transpositions equaling σ must also contain an odd number of transpositions.

Proof. Suppose that $\sigma = \sigma_1\sigma_2 \cdots\sigma_m = \tau_1 \tau_2\cdots\tau_n$,
where m is even. We must show that n is also an even number. The inverse of σ^{-1} is $\sigma_m \cdots\sigma_1$. Since

$$\mathrm{id} = \sigma\sigma_m \cdots\sigma_1 = \tau_1 \cdots\tau_n\, \sigma_m \cdots\sigma_1,$$

n must be even by Lemma 5.5. The proof for the case in which σ can be expressed as an odd number of transpositions is left as an exercise.

In light of Theorem 5.6, we define a permutation to be **even** if it can be expressed as an even number of transpositions and **odd** if it can be expressed as an odd number of transpositions.

Cosets

Let G be a group and H a subgroup of G. Define a **left coset** of H with representative g $\in$ G to be the set

$$gH = \{gh : h \in H\}.$$

Right cosets can be defined similarly by

$$Hg = \{hg : h \in H\}.$$

If left and right cosets coincide or if it is clear from the context to which type of coset that we are referring, we will use the word coset without specifying left or right.

Example 1. Let H be the subgroup of Z_6 consisting of the elements 0 and 3. The cosets are

$$0 + H = 3 + H = \{0, 3\}$$

$$1 + H = 4 + H = \{1, 4\}$$

$$2 + H = 5 + H = \{2, 5\}.$$

Example 2. Let H be the subgroup of S_3 defined by the permutations {(1), (123), (132)}. The left cosets of H are

$$(1)H = (123)H = (132)H = \{(1), (123), (132)\}$$

$$(12)H = (13)H = (23)H = \{(12), (13), (23)\}.$$

The right cosets of H are exactly the same as the left cosets:

$$H(1) = H(123) = H(132) = \{(1),(123),(132)\}$$

$$H(12) = H(13) = H(23) = \{(12),(13),(23)\}.$$

It is not always the case that a left coset is the same as a right coset. Let K be the subgroup of S_3 defined by the permutations {(1), (12)}. Then the left cosets of K are

$$(1)K = (12)K = \{(1), (12)\}$$

$$(13)K = (123)K = \{(13), (123)\}$$

$$(23)K = (132)K = \{(23), (132)\};$$

however, the right cosets of K are

$$K(1) = K(12) = \{(1), (12)\}$$

$$K(13) = K(132) = \{(13), (132)\}$$

$$K(23) = K(123) = \{(23), (123)\}.$$

Lemma 6.1 Let H be a subgroup of a group G and suppose that g_1, g_2 $\in$ G. The following conditions are equivalent.

1. $g_1H = g_2H$;
2. $Hg_1^{-1} = Hg_2^{-1}$;
3. $g_1H \subseteq g_2H$;
4. $g_2 \in g_1H$;
5. $g_1^{-1}\, g2 \in H$.

In all of our examples the cosets of a subgroup H partition the larger group G. The following theorem proclaims that this will always be the case.

Theorem 6.2 Let H be a subgroup of a group G. Then the left cosets of H in G partition G. That is, the group G is the disjoint union of the left cosets of H in G.

Proof. Let g_1H and g_2H be two cosets of H in G. We must show that either $g_1H \cap g_2H = \varnothing$ or $g_1H = g_2H$. Suppose that $g_1H \cap g_2H \neq \varnothing$ and a $\in g_1H \cap g_2H$. Then by the definition of a left coset, $a = g_1h_1 = g_2h_2$ for some elements h_1 and h_2 in H. Hence, $g_1 = g_2\, h_2\, h^{-1}$ or $g_1 \in g_2$ H. By Lemma 6.1 $g_1H=g_2H$.

Remark. There is nothing special in this theorem about left cosets. Right cosets also partition G; the proof of this fact is exactly the same as the proof for left cosets except that all group multiplications are done on the opposite side of H.

Let G be a group and H be a subgroup of G. Define the **index** of H in G to be the number of left cosets of H in G. We will denote the index by [G : H].

Example 3. Let G = Z_6 and H = {0,3}. Then [G : H] = 3.

Example 4. Suppose that G = S_3, H = {(1),(123),(132)}, and K = {(1),(12)}. Then[G:H]=2 and [G:K]=3.

Theorem 6.3 Let H be a subgroup of a group G. The number of left cosets Of H in G is the same as the number of right cosets of H in G.

Proof. Let L_H and R_H denote the set of left and right cosets of H in G, respectively. If we can define a bijective map $\phi : L_H \rightarrow R_H$, then the theorem will be proved. If $gH \in L_H$, let $\phi(gH) = Hg^{-1}$. By Lemma 6.1, the map ϕ is well-defined; that is, if $g_1H = g_2H$, then $Hg_1^{-1} = Hg_2^{-1}$. To show that ϕ is one-to-one, suppose that

$$Hg_1^{-1} = \phi(g_1H) = \phi(g_2H) = Hg_2^{-1}.$$

Again by Lemma 6.1, $g_1H = g_2H$. The map ϕ is onto since $\phi(g^{-1}H) = Hg$.

6.2 Lagrange's Theorem

Proposition 6.4 Let H be a subgroup of G with $g \in G$ and define a map $\phi : H \to gH$ by $\phi(h) = gh$. The map ϕ is bijective; hence, the number of elements in H is the same as the number of elements in gH.

Proof. We first show that the map ϕ is one-to-one. Suppose that $\phi(h_1) = \phi(h_2)$ for elements $h_1, h_2 \in H$. We must show that $h_1 = h_2$, but $\phi(h_1) = gh_1$ and $\phi(h_2) = gh_2$. So $gh_1 = gh_2$, and by left cancellation $h_1 = h_2$. To show that ϕ is onto is easy. By definition every element of gH is of the form gh for some $h \in H$ and $\phi(h)=gh$.

Theorem 6.5 (Lagrange) Let G be a finite group and let H be a subgroup of G. Then $|G|/|H| = [G : H]$ is the number of distinct left cosets of H in G. In particular, the number of elements in H must divide the number of elements in G.

Proof. The group G is partitioned into $[G : H]$ distinct left cosets. Each left coset has $|H|$ elements; therefore, $|G| = [G : H]|H|$.

Corollary 6.6 Suppose that G is a finite group and $g \in G$. Then the order of g must divide the number of elements in G.

Corollary 6.7 Let $|G| = p$ with p a prime number. Then G is cyclic and any $g \in G$ such that $g \neq e$ is a generator.

Proof. Let g be in G such that $g \neq e$. Then by Corollary 6.6, the order of g must divide the order of the group. Since $|\langle g\rangle| > 1$, it must be p. Hence, g generates G.

Normal Subgroups

A subgroup H of a group G is **normal** in G if gH = Hg for all g ∈ G. That is, a normal subgroup of a group G is one in which the right and left cosets are precisely the same.

Example 1. Let G be an abelian group. Every subgroup H of G is a normal subgroup. Since gh=hg for all g∈G and h∈H, it will always be the case that gH = Hg.

Example 2. Let H be the subgroup of S_3 consisting of elements (1) and (12). Since

$$(123)H = \{(123), (13)\} \text{ and } H\,(123) = \{(123), (23)\},$$

H cannot be a normal subgroup of S_3. However, the subgroup N, consisting of the permutations (1), (123), and (132), is normal since the cosets of N are

$$N = \{(1), (123), (132)\}$$

$$(12)N = N\,(12) = \{(12), (13), (23)\}$$

The following theorem is fundamental to our understanding of normal subgroups.

Theorem 10.1 Let G be a group and N be a subgroup of G. Then the following statements are equivalent.

1. The subgroup N is normal in G.
2. For all g $\in$ G, $gNg^{-1} \subset N$.
3. For all g $\in$ G, $gNg^{-1} = N$.

Proof. (1) ⇒ (2). Since N is normal in G, gN = Ng for all g $\in$ G. Hence, for a given $g \in G$ and $n \in N$, there exists an n′ in N such that gn=n′g. Therefore, $gng^{-1} = n' \in N$ or $gNg^{-1} \subset N$.

(2)⇒(3). Let $g \in G$. Since $gNg^{-1} \subset N$, we need only to show $N \subset gNg^{-1}$. For n $\in$ N, $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$. Hence, $g^{-1}ng = n'$ for some $n' \in N$. Therefore, $n = gn'g^{-1}$ is in gNg^{-1}.

(3)⇒(1). Suppose that $gNg^{-1} = N$ for all $g \in G$. Then for any $n \in N$ there exists an $n' \in N$ such that $gng^{-1} = n'$. Consequently, gn = n′g or $gN \subset Ng$. Similarly, $Ng \subset gN$.

Factor Groups

If N is a normal subgroup of a group G, then the cosets of N in G form a group G/N under the operation (aN)(bN) = abN. This group is called the factor or quotient group of G and N. Our first task is to prove that G/N is indeed a group.

Theorem 10.2 Let N be a normal subgroup of a group G. The cosets of N in G form a group G/N of order [G:N].

Proof. The group operation on G/N is (aN)(bN) = abN. This operation must be shown to be well-defined; that is, group multiplication must be independent of the choice of coset representative. Let aN = bN and cN = dN . We must show that

(aN)(cN) = acN = bdN = (bN)(dN).

Then $a=bn_1$ and $c=dn_2$ for some n_1 and n_2 in N. Hence,

$$\begin{aligned} acN &= bn_1dn_2N \\ &= bn_1dN \\ &= bn_1Nd \\ &= bNd \\ &= bdN. \end{aligned}$$

The remainder of the theorem is easy: eN = N is the identity and $g^{-1}N$ is the inverse of gN. The order of G/N is, of course, the number of cosets of N in G.

It is very important to remember that the elements in a factor group are sets of elements in the original group.

Example 3. Consider the normal subgroup of S_3, N = {(1), (123), (132)}. The cosets of N in S_3 are N and (12)N. The factor group S_3/ N has the following multiplication table.

	N	(12)N
N	N	(12)N
(12)	N	(12)N N

This group is isomorphic to Z_2. At first, multiplying cosets seems both complicated and strange; however, notice that S_3/N is a smaller group. The factor group displays a certain amount of information about S_3. Actually, N = A_3, the group of even permutations, and (12)N = {(12), (13), (23)} is the set of odd permutations. The information captured in G/N is parity; that is, multiplying two even or two odd permutations results in an even permutation, whereas multiplying an odd permutation by an even permutation yields an odd permutation.

Consider the normal subgroup 3Z of Z. The cosets of 3Z in Z are

$0 + 3Z = \{. . . , -3, 0, 3, 6, . . .\}$

$1 + 3Z = \{. . . , -2, 1, 4, 7, . . .\}$

$2 + 3Z = \{. . . , -1, 2, 5, 8, . . .\}$.

The group Z/3Z is given by the multiplication table below.

+	0+3Z	1+3Z	2+3Z
0+3Z	0+3Z	1+3Z	2+3Z
1+3Z	1+3Z	2+3Z	0+3Z
2+3Z	2+3Z	0+3Z	1+3Z

In general, the subgroup nZ of Z is normal. The cosets of Z/nZ are

nZ

1+nZ

2+nZ

..

(n−1)+nZ.

The sum of the cosets k+Z and l+Z is k+l+Z. Notice that we have written our cosets additively, because the group operation is integer addition.