Contents

1 Abstract

The following paper provides a brief introduction to group theory. We begin by providing a brief context of the historical evolution of group theory within different areas of mathematics. Then, we define a group, provide examples, and discuss the basic properties of groups. We conclude by discussing a few specific types of groups and their corresponding properties, including subgroups, isomorphic groups, and symmetric and alternating groups.

2 Introduction

The main objective of this report is to introduce the concepts of group theory. Groups in the abstract algebra plays important roles. Historically, group theory has three main sources: number theory, the theory of algebraic equations, and geometry. The algebraic systems with which you are familiar, such as the integers, rational numbers, real numbers, and other rings all have two operations: addition and multiplication. In this paper, we introduce a different kind of algebraic structure, called a group, that uses a single operation. Groups arise naturally in the study of symmetry, geometric transformations, algebraic coding theory, and in the analysis of the solutions of polynomial equations. In Section 3, we define a Group and look at some of the examples of Groups such as Abelian Groups and Permutation Groups. In Section 4, we look at a few basic properties of groups such as unique identity, cancellation, unique inverses, and the inverse of an inverse. We also define the order of a group and discussed the difference between finite order and infinite order. In Section 5, we first define Subgroups and look at a few specific examples, such as the intersection of two subgroups and the Cartesian product of two subgroups. We also define the center Z(G) of a group G, cyclic subgroups, and generators of a group. In Section 6, we introduce the definitions of homomorphism and isomorphism, as well as Cayley's Theorem. In section 7, we discuss the permutation notation of groups in S_n.

3 Definitions and Examples of Groups

Definition: A **group** is a nonempty set G equipped with a binary operation * that satisfies the following axioms:

1. *Closure:* If $a \in G$ and $b \in G$, then $a * b \in G$.
2. *Associativity:* $a * (b * c) = (a * b) * c$, for all $a, b, c \in G$.
3. *Identity:* There is an element $e \in G$ (called the identity element) such that $a * e = a = e * a$ for every $a \in G$.
4. *Inverse:* For each $a \in G$, there is an element $d \in G$ (called the inverse of a) such that $a * d = e$ and $d * a = e$.

A group is said to be **abelian** if it also satisfies this axiom:

- *Commutativity:* $a * b = b * a$ for all $a, b \in G$.

Example 1: Permutation Groups
Let $T = \{1, 2, 3\}$ and consider the six possible permutations of the elements of T.

$$P_3 = \{(1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1)\}$$

To each element $(i, j, k) \in P_3$ of S_3 there corresponds a map $\sigma_{ijk} : P \to P$ defined as follows: σ_{ijk} maps any $(a, b, c) \in P$ to the element of P for which a is the i^{th} component, b is the j^{th} component, and c is the k^{th} component.

$$(\sigma_{ijk}(a,b,c))_i = a$$
$$(\sigma_{ijk}(a,b,c))_j = b$$
$$(\sigma_{ijk}(a,b,c))_k = c$$

Since $i = j = k$, we easily conclude that these maps are bijective. In fact, every bijection from T to T must correspond to a σ_{ijk} for some
$(i, j, k) \in S_3$. Since the composition of any two bijective functions is itself bijective, the set of maps $S_3 = \{\sigma_{ijk} : (i, j, k) \in P_3\}$is closed under functional composition. Note that the function σ_{123} acts like an identity transformation with respect to functional composition; i.e., $(\sigma_{ijk} \circ \sigma_{123})(1, 2, 3) = \sigma_{ijk}(1, 2, 3)$and $(\sigma_{123} \circ \sigma_{ijk})(1, 2, 3) = \sigma_{123}(i, j, k) = (i, j, k) = \sigma_{ijk}(1, 2, 3)$ so $\sigma_{123} \circ \sigma_{ijk} = \sigma_{ijk} = \sigma_{ijk} \circ \sigma_{123}, \forall \sigma_{ijk} \in S_3$.

Note also that because element of S_3 is a bijection from T to T, and every bijection from T to T can be regarded as an element of T, every element of S_3 has an inverse in S_3. Finally, we note that the composition of maps is associative. We have thus verified that the set S_3 has the structure of a group when the group operation is defined as the composition of functions.
Consider the composition of $\sigma_{213} \circ \sigma_{312}$. We have
$(\sigma_{213} \circ \sigma_{312})(1, 2, 3) = \sigma_{213}(2, 3, 1) = (3, 2, 1)$. Thus $\sigma_{213} \circ \sigma_{312} = \sigma_{132}$.

This example generalizes as follows. Let n be a fixed positive integer and let T be the

set $\{1, 2, 3, ..., n\}$, and let S_n denote the set of all bijective maps from T to T . Each element $\sigma \in S$ sends a given $i \in T$ to an element $\sigma(i) \in T$.

Example 2:
Let T be a nonempty set and A(T) the set of all permutations of T. Show that A(T) is a group under the operation of composition function.
Consider T be a nonempty set say $T = \{1, 2, \ldots., n\}$ where $n \in Z$ and $A(T)$ be the set of all permutations of T. Take any two bijections f and g of $A(T)$. Then $f \circ g \in A(T)$ because composition of two bijections is again a bijection. Hence $A(T)$ is closed under the operation of composition of functions. Now, take any three bijections, $f, g, h \in A(T)$. Then it is known that under composition functions, $(f \circ g) \circ h = f \circ (g \circ h)$. Hence, associativity holds in $A(T)$. Then, take a bijection f from A(T), then identity map e from T to T is the identity of A(T). Then $f \circ e = e \circ f = f$ is always true. Hence identity function e is the identity of $A(T)$. Thus $A(T)$ is a group under the operation as composition of functions.

Theorem 3.1: Every ring is an abelian group under addition.
Proof: An examination of the first five axioms for a ring shows that they are identical to the five axioms for an abelian group, with operation $*$ being $+$, the identity element e being 0_R and the inverse of a being $-a$.

Example 3:
By Theorem 3.1, the following rings are abelian groups under addition: Z, Z_n, Q, R, C**, matrix rings, and polynomial rings**.

Theorem 3.2: The nonzero elements of a field F form an abelian group under multiplication.
Proof: Multiplication in F* satisfies the following ring axioms: closure, associativity, identity, inverse and commutativity. So F* satisfies group axioms 1-5 and therefore is an abelian group under multiplication.

Theorem 3.3: If R is a ring with identity, then the set U of all units in R is a group under multiplication.
Proof: The product of units is a unit, so U is closed under multiplication. Multiplication in R is associative, so Axiom 2 holds. Since 1_R is obviously a unit, U has an identity element (Axiom 3). Axiom 4 holds in U by the definition of unit. Therefore U is a group.

Example 4:
Some examples of Groups are Real Numbers with addition, Non-zero Real Numbers with multiplication, Integers with addition, and Set of congruence classes modulo n with addition

Theorem 3.4: Let G with operation * and H with operation # be groups. Define an operation on $G \times H$ by $(g, h)(g', h') = (g * g', h\#h')$. Then $G \times H$ is a group. If G and H are abelian, then so is $G \times H$.
Proof: Take any two elements $(g_1, h_1), (g_2, h_2) \in G \times H$. Then $(g_1, h_1)(g_2, h_2) = (g_1 *$

$g_2, h_1 \# h_2)$. But G and H are groups with respect to operations $*$ and $\#$ respectively and therefore G and H are closed under these operations. So $g_1 * g_2 \in G$ and $h_1 \# h_2 \in H$. Hence $(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \# h_2) \in G \times H$.
Secondly, take any three elements $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$. Then $[(g_1, h_1)(g_2, h_2)](g_3, h_3) = (g_1 * g_2, h_1 \# h_2)(g_3, h_3) = (g_1 * g_2 * g_3, h_1 \# h_2 \# h_3) = (g_1 * (g_2 * g_3), h_1 \# (h_2 \# h_3)) = (g_1, h_1)[(g_2, h_2)(g_3, h_3)]$. Thus, since associativity holds for * and # in G and H respectively, then associativity holds in $G \times H$. Next, note that since G and H are groups, then $e_G \in G$ and $e_H \in H$ exist. Now for any element $(g, h) \in G \times H$, we have $(e_G, e_H)(g, h) = (e_G * g, e_H \# h) = (g, h)$. Similarly, $(g, h)(e_G, e_H) = (g * e_G, h \# e_H) = (g, h)$. Therefore, $(e_G, e_H) \in G \times H$ is the identity of $G \times H$.
Lastly, we must show that each element of $G \times H$ has an inverse in $G \times H$. Now since G and H are groups, for all $g \in G$ and $h \in H$, there exists $g^{-1} \in G$ and $h^{-1} \in H$. Thus for all $(g, h) \in G \times H$, there exists $(g^{-1}, h^{-1}) \in G \times H$.
Therefore, $G \times H$ is a group. Now, suppose G and H are both abelian groups. Then $*$ and $\#$ are commutative, so $(g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \# h_2) = (g_2 * g_1, h_2 \# h_1) = (g_2, h_2)(g_1, h_1)$. Thus is commutative, so $G \times H$ is an abelian group.

4 Basic Properties of Groups

Theorem 4.1: Let G be a group and let a, b, c ∈ G. Then,
1) G has a unique identity element.
2) Cancelation holds in G:
If ab = ac, then b = c
If ba = ca, then b = c
3) Each element of G has a unique inverse.

Proof: (1) According to the definition of a group, group G has at least one identity. Then, let e and e* be the identity elements such that ee* = e (since e* is and identity element) and ee* = e* (since e is an identity element). Hence, e = ee* = e*. Therefore, G has a unique identity element.
(2) According to the definition of a group, element a has at least one inverse x such that xa = e = ax. Suppose ab = ac, then x(ab) = x(ac) when multiplying x to both sides. Then, by the associative property, (xa)b = (xa)c and, since a and x are inverses of one another, eb = ec and b = c when dividing e from both sides. Similarly, suppose ba = ca, then (ba)x = (ca)x when multiplying x to both sides. Then, again by the associative property, b(ax) = c(ax) and, since a and x are inverses of one another, be = ce and b = c when dividing e from both sides. Therefore, cancelation holds in G for the two cases.
(3) Suppose x and x* are inverses of a ∈ G. Then, ax = e = ax*, meaning x = x*, as we saw in (2). Hence, a has one, and only one, inverse. Therefore, each element of G has a unique inverse.

Example 1:
Let G be a group with this property: If a,b,c ∈ G and ab = ca, then b = c. Prove that G is abelian.
Solution: Let x,y ∈ G. Then, xyx = xyx. Using the associative property, we can rearrange the equality as x(yx) = (xy)x. Then, using the unique inverse property of Theorem 4.1, we can simplify the equation to yx = xy. Since x,yG, yx and xy are also elements of G. The group is closed under the binary operations. Therefore, G is abelian.

Corollary 4.2: If G is a group and a,b ∈ G, then
1) $(ab)^{-1} = (b^{-1})a^{-1}$**;**
2) $(a^{-1})^{-1} = a$.
Proof : (1)We know that $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$.
Similarly, we know $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$. Theorem 4.1 tells us the inverse of ab is unique so we can assume that $b^{-1}a^{-1}$.Therefore, $(ab)^{-1} = b^{-1}a^{-1}$.(2)$a^{-1}a = e$ and $(a^{-1})(a^{-1})^{-1} = e$ by definition. Comparing the equalities and cancelling a^{-1} by Theorem 4.1, we can conclude $(a^{-1})^{-1} = a$.

Example 2:
Prove that G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ **for all a,b ∈ G.**
Solution: Using the basic properties of a group, we want to compute $(ab)^{-1}$. To do this we can find x(ab) = e for some x ∈ G. Solving for x....
$x(ab)b^{-1} = xa(bb^{-1}) = eb^{-1}$

$xae = xa = b^{-1}$
$xaa^{-1} = xe = b^{-1}a^{-1}$
$x = b^{-1}a^{-1}$
Hence, $(ab)^{-1} = b^{-1}a^{-1}$. Therefore, G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a,b $\in$ G.

Example 3:
If a,b $\in$ G, $b^6 = e$, and $ab = b^4a$, prove that $b^3 = e$ and $ab = ba$.
Solution: Taking $ab = b^4a$, we can multiply both sides of the equations from the left by a^{-1}. Then, $aa^{-1}b = b = a^{-1}b^4a$. Then, $b^2 = (a^{-1}b^4a)(a^{-1}b^4a) = a^{-1}b^4(aa^{-1})b^4a = a^{-1}b^4eb^4a = a^{-1}b^8a$. Similarly, $b^3 = (a^{-1}b^4a)(a^{-1}b^4a)(a^{-1}b^4a) = a^{-1}b^{12}a = a^{-1}(b^6)^2a = a^{-1}e^2a = a^{-1}a = e$. Therefore, $b^3 = e$. Now, based off our previous calculations, $ba = b^3(ba) = ab$. Therefore, if $a, b \in$ G, $b^6 = e$, and $ab = b^4a, b^3 = e$ and $ab = ba$.

Theorem 4.3:
Let G be a group and let a $\in$ G. Then, for all integers m,n
$a^m a^n = a^{m+n}$
$(a^m)^n = a^{mn}$.
Proof :
(1) We will use induction to prove the first case. We will induct on n with our base case of n = 0. Then, $a^m a^0 = a^m(1) = a^m = a^{m+0}$, so the hypothesis holds for the base case. Now, let n = k+1. Then, $a^m a^{k+1} = a^m(a^k a) = (a^m a^k)a = a^{(m+k)+1}a^{m+(k+1)}$, so the hypothesis holds for all cases.
(2) In order to prove the theorem, one can use induction by looking at 3 cases:
(*i*)Suppose $m > 0$ and $n > 0$. Then, as our base case, let n = 1. Then, $a^m a^1 = a^{m(1)}$ which simplifies to $a^m = a^m$. Now, suppose $(a^m)^k = a^{mk}$. Then, $(a^m)^{(k+1)} = a^{m(k+1)}$ which simplifies to $a^{m(k+1)} = a^{m(k+1)}$ by the power of a power rule and associativity.
(ii) Suppose m = 0 and n = 0. Then, it follows automatically $(a^m)^n = a^{mn}$ since 1 = 1 (assuming a $\neq$ 0).
(iii) Suppose $0 > m$ and $0 > n$. Then, let m = -x and n =-y for some $x, y > 0$. Then, $(a^m)^n = (a^{-x})^{-y} = (((a^{-1})^x)^y)^{-1} = ((a^{-1})^{xy})^{-1} = (a^{-nx})^{-1} = (a^{nx})^{-1} = a^{n(-1)x} = a^{mn}$.
Therefore, by induction, $(a^m)^n = a^{mn}$.

Example 4:
If $(ab)^3 = a^3b^3$ and $(ab)^5 = a^5b^5$ for all a,b $\in$ G, prove that G is abelian.
Solution: Suppose $(ab)^3 = a^3b^3$. Then, when we multiply a^{-1} from the left and b^{-1} from the right, we get $(ba)^2 = baba = a^2b^2$. Similarly, when we multiply a^{-1} from the left and b^{-1} from the right for $(ab)^5 = a^5b^5$, we get $(ba)^4 = babababa = a^4b^4$. Then, from Theorem 4.3, we determine $((ba)^2)^2 = (ba)^4$ so $a^2b^2a^2b^2 = (a^2b^2)^2 = ((ba)^2)^2 = (ba)^4 = a^4b^4$. Hence, $b^2a^2 = a^2b^2$ and so $b^2a^2 = a^2b^2 = (ba)^2 = baba$. When we multiply b^{-1} on the left and a^{-1} on the right, ba = ab. Therefore, G is abelian.

Definitions:
Finite Order- An element a has finite order if $a^k = e$ for some integer k.
Order of an Element- The smallest integer n such that a^n = e is said to be the order of an element.

Infinite Order- An element a has infinite order if $a^k \neq e$ for any positive integer k.

Example 5:
If |G| is even, prove that G contains an element of order 2.
We know that any element and its inverse have the same order. Then, each element of G with order larger than 2 can be paired off with a distinct inverse. Let K be the set of these pairs such that for any $x \in G$ where $x \neq x^{-1}$, then $x, x^{-1} \in K$. Therefore, since all elements come in pairs, |K| is even. However, |G| is also even so G has an odd number of non-identity elements. Therefore, G must have an element with its own inverse. Arbitrarily let's call this element a. Then, $a = a^{-1}$ so $a^2 = 1_R$. Therefore, G contains an element of order 2.

Theorem 4.4: Let G be a group and let $a \in G$.
If a has and infinite order, then the elements a^k, with $k \in Z$, are all distinct.
If $a^i = a^j$ with $i \neq j$, then a has finite order.
Given that each statement is the contrapositive of the other, statement 1 is true if and only if statement 2 is true.
Proof: (2) Suppose $a^i = a^j$ with i > j. Then, $a^i a^{-j} = a^j a^{-j} = a^{i-j} = a^0 = e$. Therefore, since i > j, a has finite order.
(1) This is already proven given that statement 1 is the contrapositive of statement 2.

Theorem 4.5: Let G be a group and $a \in G$ an element of finite order n. Then....
1) $a^k = e$ if and only if n | k.
2) $a^i = a^j$ if and only if $i \equiv j$ (modn).
3) If n = td, with $d \geq 1$, then a^t has order d.
Proof: (1) Suppose n | k. Then, k = nx for some integer x. Then, $a^k = a^{nx} = (a^n)^x = e^x = e$ (since a has finite order). Hence, $a^k = e$ if n | k. Conversely, suppose $a^k = e$. Then, using the Division Algorithm, let k = nq + r for some $n > r \geq 0$. Then, $e = a^k = a^{nq+r} = (a^n)^q a^r = e^q a^r = ea^r = a^r$. Then, n is the smallest positive integer with $e = a^n$. $e = a^r$ is only possible when r = 0, since n > r. Hence, k = nq and n | k by definition.
(2) We know from our proof of Theorem 4.4 that $a = a^j$ if and only if $a^{i-j} = e$. If we let k = i-j, then from statement 1, we can say $a^{i-j} = e$ if and only if n | (i-j). Then, by definition, $i \equiv j$ (modn). Therefore, $a^i = a^j$ if and only if $i \equiv j$ (modn).
(3) Let |a| = n = td. Then, $(a^t)^d = a^{td} = a^n = e$. To show that d is the smallest positive integer in which the property holds, let k be any positive integer such that $(a^t)^k = e$. Then, $a^{tk} = e$ and n | tk (from statement 1). Then, tk = nr = (td)r. Hence, k = dr. $k \geq r$, since the 2 integers are positive and d | k. Therefore, if n = td, with $d \geq 1$, then a^t has order d.

Corollary 4.6: Let G be an abelian group in which every element has finite order. If $c \in G$ is an element of largest order in G (that is, $|a| \leq |c|$ for all $a \in G$), then the order of every element of G divides |c|.
Proof: Suppose $a \in G$ but |a| does not divide |c|. Then, a prime integer p in the prime factorization of |a| appears to a higher power than that of the prime factorization of |c|. Then, by prime factorization, there are integers m,n,r,s such that $|a| = p^r m$ and $|c| = p^s n$ with (p,m) = 1 and (p,n) = 1 and $r \geq s$. Then, from statement 3 in Theorem 4.5, we can say

the element a^m has order p^r and c^{p^s} has order n. Then, $a^m c^{p^s}$ has order $p^r n$. Hence, $|a^m c^p| = p^r n > p^s n = |c|$. This is a contradiction since c is an element of largest order. Hence, |a| divides |c|. Therefore, if $c \in G$ is an element of largest order in G, then the order of every element of G divides |c|.

5 Subgroups

Now that we have defined groups, given some examples, and explored a few basic properties of groups, we will now explain what it means to be a subgroup.

Definition 5.1: H is a subgroup of G if $H \subseteq G$ and H is a group under the operation of G.

There are three types of subgroups:

1. A group G is always a subgroup of itself.
2. The group $\{e_G\}$, which contains only the identity element of G, is called the trivial subgroup.
3. All other subgroups of G are called proper subgroups.

Example 1
Let G_1 be a subgroup of a group G and H_1 be a subgroup of a group H. Prove that $G_1 \times H_1$ is a subgroup of $G \times H$.
Solution: Clearly $G_1 \times H_1 \subseteq G \times H$, and G $\times$ H is a group by Theorem 3.4, so in order to check that $G_1 \times H_1$ is a subgroup of $G \times H$, we must check that $G_1 \times H_1$ is a group.

1. *Closure:* Consider $(a_g, a_h), (b_g, b_h) \in G_1 \times H_1$. Then $(a_g, a_h)(b_g, b_h) = (a_g b_g, a_h b_h)$. Since G_1 and H_1 are subgroups of G and H respectively, they are both also groups. Thus $a_g b_g \in G_1$ and $a_h b_h \in H_1$, so $(a_g b_g, a_h b_h) \in G_1 \times H_1$.
2. *Associativity:* Consider $(a_g, a_h), (b_g, b_h), (c_g, c_h) \in G_1 \times H_1$. Since the operations in G and H are both associative (because G and H are both groups), then $[(a_g, a_h)(b_g, b_h)](c_g, c_h) = (a_g b_g, a_h b_h)(c_g, c_h) = (a_g b_g c_g, a_h b_h c_h) = (a_g, a_h)(b_g c_g, b_h c_h) = (a_g, a_h)[(b_g, b_h)(c_g, c_h)]$. Therefore associativity holds in $G_1 \times H_1$.
3. *Identity*: Since G_1 and H_1 are subgroups of G and H, respectively, they each contain an identity element. Call these e_g and e_h. The identity element of $G_1 \times H_1$ is (e_g, e_h).
4. *Inverse*: Since G_1 and H_1 are subgroups of G and H, respectively, each element in G_1 or H_1 has an inverse. Therefore if $(a_g, a_h) \in G_1 \times H_1$, we can find $(a_g, a_h)^{-1} = (a_g^{-1}, a_h^{-1})$.

Therefore $G_1 \times H_1$ is a subgroup of $G \times H$.

Example 2:
Suppose that H is a subgroup of a group G and that $a \in G$ has order n. If $ak \in H$ and (k,n) = 1, prove that $a \in H$.
Solution: Since $(k, n) = 1$ we can write $ku + nv = 1$ for some $u, v \in Z$. Also, since a has order n, then we know $a^n = e$. Then using Theorem 4.3, we can write $a = a^1 = a^{ku+nv} = a^{ck} a^{bn} = (a^k)^c (a^n)^b = (a^k)^c$. Since H is a subgroup, it is closed under the operation in G. Therefore since $a^k \in H$, Then $(a^k)^c = a \in H$.

Theorem 5.2: A nonempty subset H of a group G is a subgroup of G if the following conditions hold:

1. ***Closure:*** **If** $a, b \in H$**, then** $ab \in H$**.**
2. ***Inverse:*** **If** $a \in H$**, then** $a^{-1} \in H$**.**

Proof: The closure and inverse properties of (1) and (2) satisfy the first two axioms for a group. Since G is a group, associativity holds for all elements of G. It follows that since $H \subseteq G$, associativity must hold for all elements of H. Finally, since H is a nonempty subset, there exists some element $h \in H$. By property (2), $a^{-1} \in H$ exists. By property (1), $aa^{-1} = e \in H$. Therefore H has identity. Hence all axioms have been checked, so H is a subgroup of G.

Example 3:
Let H and K be subgroups of G. Prove that $H \cap K$ **is also a subgroup of G.**
Solution:
Since H and K are subgroups of G, then H and K are both subsets of G, so clearly $H \cap K \subseteq G$. Note that H and K are both groups by definition of a subgroup.
First, we want to show that $H \cap K$ is closed. Let $a, b \in H \cap K$. Then $a, b \in H$ by definition of intersection, so $ab \in H$ because H is a group. Similarly, $a, b \in K$ by definition of intersection, so $ab \in K$ because K is a group. Therefore, $ab \in H \cap K$, so $H \cap K$ is closed.
Next, we want to show that every element $a \in H \cap K$ has an inverse. By definition of intersection, $a \in H$ and $a \in K$. Since H and K are groups, $a^{-1} \in H$ and $a^{-1} \in K$ exists. Note that there can only be one a^{-1} because inverses are unique. Therefore $a^{-1} \in H \cap K$. Hence by Theorem 5.2, $H \cap K$ is a subgroup of G.

Theorem 5.3: Let H be a nonempty finite subset of a group G. If H is closed under the operation in G, then H is a subgroup of G.
Proof: By Theorem 5.2, H is a subgroup of G if H is closed and each element of H has an inverse. By assumption, H is closed under the operation in G. Therefore we must only check whether each element of H has an inverse. Let $a \in H$. Then since H is closed under the operation in G, $a^k \in H$ for every $k \in N$. H is a finite group, so by Theorem 4.4, a must have a finite order n, where $a^n = e$. Now $(n-1) \equiv -1(modn)$, so by Theorem 4.5, $a^{n-1} = a^{-1}$. If n = 1, then $a^{n-1} = a^0 = a^{-1} = e$, so $a^{-1} \in H$. If $n > 1$, then $n - 1 > 0$, so $a^{n-1} = a^{-1} \in H$. Therefore all elements of H have an inverse. Hence H is a subgroup of G.

Definition 5.4: The **center** of a group G, denoted by Z(G), is the set $Z(G) = \{a \in G; ag = ga \text{ for all } g \in G\}$. In other words, an element is in the **center** of G if multiplying by this element on the left gives the same result as multiplying by this element on the right. If a group G is abelian, then every element of G is in Z(G) because G is commutative.

Theorem 5.5: The center Z(G) of a group G is a subgroup of G.
Proof: We will use Theorem 5.2 to prove that Z(G) is a group. Therefore, we need to show

that Z(G) is a nonempty, closed subset of G and that each element of Z(G) has an inverse under the operation in G. First, by definition of identity, we have for every $g \in G$ that $eg = g = ge$. Therefore $e \in Z(G)$, so Z(G) is nonempty. Next, consider $a, b \in Z(G)$. Then for all elements $g \in G$, we know that $ag = ga$ and $bg = gb$ by definition of Z(G). Now, consider ab. Since $a, b \in Z(G)$ and since G is a group and its operation is therefore associative, we have $(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$.
Therefore $ab \in Z(G)$, so the closure axiom is satisfied. Finally, if $a \in Z(G)$, then $a \in G$, so $a^{-1} \in G$ exists. Now since $a \in Z(G)$, we know that $ag = ga$. Multiply this equation both on the left and on the right by a^{-1} (since it is unknown whether G is abelian), we get $a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1}$, which simplifies to $ga^{-1} = a^{-1}g$. Therefore, $a^{-1} \in Z(G)$.
Hence Z(G) is a nonempty closed subset and each element of Z(G) has an inverse under the operation in G, so by Theorem 5.2, Z(G) is a subgroup of G.

Example 4:
If G is a group and $ab \in Z(G)$, prove that $ab = ba$.
Solution:
Since $ab \in Z(G)$, $(ab)c = c(ab)$ for all elements $c \in G$. Now consider c = a. Then $(ab)a = a(ab)$. Since G is a group, its operation is associative, so this equation can be written as $aba = aab$. Now by cancellation, we have that $ba = ab$.

Example 5:
If a is the only element of order 2 in a group G, prove that $a \in Z(G)$.
Since $a \in G$ has order 2, we know that $a^2 = e$. Consider some $b \in G$. We want to show that $ab = ba$. Now consider $p = b^{-1}ab$. Then $p^2 = (b^{-1}ab)^2 = (b^{-1}ab)(b^{-1}ab) = b^{-1}a(bb^{-1})ab = b^{-1}aab = b^{-1}a^2b = b^{-1}b = e$. Now since $p^2 = a^2$ and a is the only element of order 2, it must be the case that $p = a$. Then we can write $b^{-1}ab = a$. Multiplying on the left by b to both sides, we get $bb^{-1}ab = ba$, which simplifies to $ab = ba$. Therefore, $a \in Z(G)$.

Definition 5.6: The **cyclic subgroup generated by a**, denoted $\langle a \rangle$, is defined as the set $\langle a \rangle = \{ \ldots , a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots \} = \{a^n; n \in Z\}$. If $\langle a \rangle = G$, then G is called a **cyclic group**. All cyclic groups are abelian due to Theorem 7.7, because if $a^i, a^j \in \langle a \rangle$, then $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$.

Theorem 5.7: If G is a group and $a \in G$, then the cyclic subgroup generated by a, denoted by $\langle a \rangle$, is a subgroup of G.
Proof: The set $\langle a \rangle$ is clearly nonempty. Consider $a^i, a^j \in \langle a \rangle$. Then $a^i a^j = a^{i+j}$, where $i + j \in Z$. Therefore $a^i a^j \in \langle a \rangle$, so $\langle a \rangle$ is closed. Also for every $a^i \in \langle a \rangle$, there exists $a^{-i} \in \langle a \rangle$ such that $a^i a^{-i} = a^{i-i} = e$. Therefore, all elements in $\langle a \rangle$ have an inverse. Thus by Theorem 5.2, $\langle a \rangle$ is a subgroup of G.

Example 6:
Let G be a group and let $a \in G$. Prove that $\langle a \rangle = \langle a^{-1} \rangle$.
Solution: Now by definition of a cyclic group generated by a, we have
$\langle a \rangle = \{..., a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \ldots \}$ and

$\langle a^{-1}\rangle = \{..., (a^{-1})^{-3}, (a^{-1})^{-2}, (a^{-1})^{-1}, (a^{-1})^0, (a^{-1})^1, (a^{-1})^2, (a^{-1})^3, \dots\}$.
Simplifying $\langle a^{-1}\rangle$, we get $\langle a^{-1}\rangle = \{..., a^3, a^2, a^1, a^0, a^{-1}, a^{-2}, a^{-3}, ...\}$. Since the order of elements in a set does not matter, we can thus see that$\langle a^{-1}\rangle = \langle a\rangle$.

Now that we have a definition of the cyclic subgroup generated by an element a, we can use it to provide an alternate way of looking at "order", a term first defined in Section 4.

Theorem 5.8: Let G be a group and let $a \in G$.

1. **If a has infinite order, then $\langle a\rangle$ is an infinite subgroup consisting of the distinct elements a^k, for all integers k.**

2. **If a has finite order n, then $\langle a\rangle$ is also a subgroup of order n, and $\langle a\rangle = \{a^0, a^1, a^2, ..., a^{n-1}\}$, where $a^0 = e$.**

Proof: Recall from Theorem 4.4 that if a has infinite order, then a^k with $k \in Z$ are all distinct. Therefore statement (1) is an immediate result from Theorem 4.4.
Now, suppose a has finite order n, and let a^i be an arbitrary element of $\langle a\rangle$. Then i is congruent modulo n to one of 0, 1, 2, ..., n-1. Let j be the integer, $0 \leq j < n$, such that $i \equiv j(modn)$. Then by the second statement in Theorem 4.5, $a^i = a^j$. Additionally, none of the integers between 0 and n-1 are congruent modulo n, so again by the second statement in Theorem 4.5, none of $a^0, a^1, a^2, \dots, a^{n-1}$ are equal. Therefore, the order of the group $\langle a\rangle = \{a^0, a^1, a^2, ..., a^{n-1}\}$ is n.

Example 7: List or describe the elements of the given cyclic subgroup. $\langle 2\rangle$ in the multiplicative group of nonzero elements of Z_{11}.
Solution:
Call the group of nonzero elements in Z_{11} G. Then $G = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Now in Z_{11}, 2 has the order 10 because $2^{10} = 1$. Therefore by Theorem 5.8 statement (2), $\langle 2\rangle = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\} =$
$\{1, 2, 4, 8, 16, 32, 64, 128, 256, 512\} = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}$
$= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} = G$.

Now if a group's operation is addition, we use additive notation to decrease confusion. Therefore, we can rewrite Theorem 5.8 in additive notation as follows:

Theorem 5.8 (Additive Notation): Let G be an additive group and let $a \in G$.

1. **If a has infinite order, then $\langle a\rangle$ is an infinite subgroup consisting of the distinct elements ka, for all integers k.**

2. **If a has finite order n, then $\langle a\rangle$ is a subgroup of order n and $\langle a\rangle = \{0, 1a, 2a, \dots (n-1)a\}$.**

Remark: The proof of the additive notation form of Theorem 5.8 follows similarly from the original proof of Theorem 5.8, with only a few minor changes of notation.

Example 8:
List or describe the elements of the given cyclic subgroup, $\langle 2 \rangle$ in the additive group Z_{12}.
Solution:
Using additive notation, $\langle 2 \rangle$ is made up of all multiples of 2 in Z_{12}. So $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$. Notice that $\langle 2 \rangle$ is a subgroup of Z_{12}, so this example supports Theorem 7.14.

Theorem 5.9: Let F be a field. Let F* be the multiplicative group of nonzero elements of F. If G is a finite subgroup of F*, then G is a cyclic group.
Proof: Since G is a finite subgroup, we can let $c \in G$ be an element of largest order. Call this order m. Thus the order of G is m. Our goal is to prove that $G = \langle c \rangle$, which proves G is a cyclic group. Now since G is finite, it is nonempty, so we can consider $a \in G$. By Corollary 4.6, the order of a divides m. Then by Theorem 4.5 statement (1), we have that $a^m = 1$. Consider the equation $x^m - 1 = 0$. Since $a^m = 1$ for all elements in $a \in G$, every element in G is a solution to the equation $x^m - 1 = 0$ and is therefore a root of the polynomial $f(x) = x^m - 1$. Now the degree of $f(x)$ equals m, so $f(x)$ has at most m roots. Therefore the order of G must be at most m. But by construction, $\langle c \rangle$ is a subgroup of G. Thus $G = \langle c \rangle$, so G is a cyclic group.

Now that we have defined subgroups and cyclic groups, we will look more closely at the subgroups of cyclic groups.

Theorem 5.10: Every subgroup of a cyclic group is itself cyclic.
Proof: Consider the cyclic group $G = \langle a \rangle$, and let H be a subgroup of G. If $H = \{e\}$, the trivial subgroup of G, then H is clearly cyclic. If $H \neq \langle e \rangle$, then H contains some element, a^i, $i \neq 0$, such that $a^i \neq e$. Since H is a subgroup, the inverse of a^i, or a^{-i}, must also be in H. Since both a^i and a^{-i} are in H, we know that H must contain positive powers of a. Therefore, we can let k equal the smallest positive integer where $a^k \in H$. To finish this proof, we want to show that $H = \langle a^k \rangle$. This means we need to prove that all elements in H are powers of a^k. Take $h \in H$. Since H is a subgroup of G, then $h \in G$ also. So $h = a^m$ for some $m \in Z$. Using the Division Algorithm, $m = kq + r$ for some unique $q, r \in Z$ where $0 \leq r < k$. Rearranging this equation, we get $r = m - kq$. Then by Theorem 4.3, we can write $a^r = a^{m-kq} = a^m a^{-kq} = a^m (a^k)^{-q}$. Since $a^m, a^k \in H$ and H is a group, then by closure, a^r is also in H. Recall that k is the smallest positive power of a in H. Then since $r < k$, $r = 0$. Therefore, $0 = m - kq$, so $m = kq$. Then by Theorem 4.3, $h = a^m = a^{kq} = (a^k)^q$. So h is a power of a^k. Therefore, $H = \langle a^k \rangle$, and is thus cyclic. Hence we can conclude that every subgroup of a cyclic group is also cyclic.

Example 9:
Let $G = \langle a \rangle$ be a cyclic group of order n. If H is a subgroup of G, show that the order of H is a divisor of n.
Solution:
If H contains one element, then the order of H equals 1, which clearly divides n. Now, suppose H has more than one element. Since H is a subgroup of G and G is cyclic, then H is also cyclic by Theorem 5.10. Then $H = \langle a^k \rangle$, where k is the order of H and is thus

the smallest positive power of a in H. By the Division Algorithm, we know that $n = kq + r$ for unique $q, r \in Z$ such that $0 \leq r < k$. Equivalently, we can write $a^n = a^{kq+r} = a^{kq}a^r$. Multiplying both sides by $a - kq$, we get $a^{-kq}a^n = a^{-kq}a^{kq}a^r$, or simply $a^{-kq}a^n = a^r$. But since the order of a is n, then $a^n = e$. So the above equation simplifies to $a^{-kq} = a^r$. By Theorem 7.7, we can rewrite this as $(a^k)^{-q} = a^r$. Therefore since $(a^k)^{-q} \in H$, $a^r \in H$ also. But we stated previously that k is the smallest positive power of a in H, and $0 \leq r < k$, so this means $r = 0$. Therefore returning to the Division Algorithm and substituting in our known r value, we have $n = kq + 0 = kq$. Thus k, which is the order of H, is a divisor of n.

Now, just as we saw that $\langle a \rangle$ is the cyclic subgroup generated by $a \in G$, we can also consider groups generated by more than one element in G. To do this, we can think of $\langle a \rangle$ as being generated by the set $S = \{a\}$, where we generate $\langle a \rangle$ by multiplying a and a^{-1} in every order possible. Now we can generalize this definition to sets with more than one element.

Definition 5.11: The group $\langle S \rangle$ is called the **subgroup generated by S**. If $\langle S \rangle = G$, then **S generates G**. In this case, we call the elements of S as the **generators** of the group.

Example 11:
Show that $(3, 1)$**,** $(-2, -1)$**, and** $(4, 3)$ **generate the additive group of** $Z \times Z$**.**
Solution:
Now to start, we note that the additive group $Z \times Z$ can be generated by the two elements $(0, 1)$ and $(1, 0)$. Thus if the set generated by $(3, 1)$, $(-2, -1)$, and $(4, 3)$ include $(0, 1)$ and $(1, 0)$, then we know these elements generate the additive group $Z \times Z$. The set generated by these three elements will include all possible linear combinations of the three elements. So since $(1, 0) = (3, 1) + (-2, -1)$, then $(1, 0)$ is in the generated set. Similarly, since $(4, 3) + 2(-2, -1) = (4, 3) + (-4, -2) = (0, 1)$, then $(0, 1)$ is also in the generated set. Therefore $(3, 1)$, $(-2, -1)$, and $(4, 3)$ generate the additive group $Z \times Z$.

Example 12:
If G is an infinite additive cyclic group with generator a. Prove that the equation $x + x = a$ **has no solution in G.**
Solution:
Since G is a cyclic group with generator a, $G = \langle a \rangle$. Now $a \neq 0$, because then G would be finite, but in the problem it states that G is an infinite cyclic group. By way of contradiction, assume that $x + x = a$ has some solution in G, say b. Then since G is an additive cyclic group, there exists some positive integer n such that $b = na$. Then since $b + b = a$, we have $na + na = 2na = a$. But if $2na = a$, then a must have a finite order and thus G is not an infinite cyclic group. Thus we have a contradiction, so $x+x = a$ has no solution in G.

Now that we have defined generators, we will finish this section with a theorem about the subgroups generated by a set.

Theorem 5.12: Let S be a nonempty subset of a group G. Let $\langle S \rangle$ **be the set of all possible products, in every order, of elements of S and their inverses. Then**

1. **$\langle S \rangle$ is a subgroup of G that contains set S.**

2. **If H is a subgroup of G that contains S, then H contains the entire subgroup $\langle S \rangle$.**

Proof:

1. We will show $\langle S \rangle$ is a subgroup using Theorem 5.2, so we must show that $\langle S \rangle$ is nonempty, closed, and that every element of $\langle S \rangle$ has an inverse. First, since S is a nonempty subset, it follows directly that $\langle S \rangle$ is nonempty because every element of S is also in $\langle S \rangle$. Next, consider $a, b \in \langle S \rangle$. Then a is of the form $a = a_1 a_2 \dots a_k$ where $k \geq 1$ and all a_i are either elements in S or inverses of elements in S. Similarly, b is of the form $b = b_1 b_2 \dots b_t$ where $t \geq 1$ and all b_j are either elements of S or inverses of elements of S. Combining these two equations, we get that the product of a and b is $ab = (a_1 \dots a_k)(b_1 \dots b_t) \in \langle S \rangle$. Therefore $\langle S \rangle$ is closed. Finally, consider the same $a \in \langle S \rangle$ from above. Then the inverse of a is simply $a^{-1} = a_1^{-1} a_2^{-1} \dots a_k^{-1}$. Since all a_i are either elements in S or inverses of S, then it directly follows that all a_i^{-1}. Therefore $a^{-1} \in \langle S \rangle$, so each element of $\langle S \rangle$ has an inverse in S.

2. Suppose H is a subgroup of G that contains S. Then by Theorem 5.2, the inverse of every element in H is also in H. Therefore H contains all elements of S and all inverses of elements of S. Since H is a subgroup, it must be closed under the operation in G. Therefore H must also include all possible products in all possible orders of elements of S and their inverses. Hence H must contain the entirety of $\langle S \rangle$.

6 Isomorphisms and Homomorphisms

The best way to describe the relationship between two things in mathematics is to use the function. However, not all functions between these two things are important. For example, we only care about the group structure between the two groups, so we are only interested in some special functions. This function is called the group homomorphism. The Greek roots "homo" and "morph" together mean "same form/shape".

Definition 6.1: Let G, G' be groups. A function $\phi : G \to G'$ is said to be a **homomorphism** if $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G$.

Noted that since $a, b \in G$, so the $a \cdot b$ is the multiplication in G, while the $\phi(a), \phi(b) \in G'$ which means $\phi(a) \cdot \phi(b)$ is the multiplication in G'. In other words, a group homomorphism from G to G' is a function to keep the operation of elements between G and G'.

Definition 6.2: Suppose $\phi : G \to G'$ is a group homomorphism. The **image** of ϕ is defined to be

$$\text{im}(\phi) = \{\phi(a) \in G' | a \in G\} \tag{1}$$

and the **kernel** of ϕ is defined to be

$$\ker(\phi) = \{a \in G | \phi(a) = e'\} \tag{2}$$

called the kernel of ϕ, where e' is the identity of G'.

From the definition, we know that $\text{im}(\phi)$ is a subset of G', while $\ker(\phi)$ is a subset of G. Noted that ϕ can be considered as a surjective map from G to $\text{im}(\phi)$.

Example 1: Show that the function $f : R \to R$ defined by $f(x) = x^2$ is not a homorphism.
Proof: This is because $f(x + y) = (x + y)^2 \neq x^2 + y^2 = f(x) + f(y)$.

An isomorphism is a special type of homomorphism. In general, isomorphic groups are groups that have the same structure, in the sense that the operation table for one is the operation table of the other with the elements suitably relabeled. We introduce the formal definition here.

Definition 6.3: Let G, G' be groups. G is **isomorphic** to G' (in symbols, G $\cong G'$ if there is a function $\phi : G \to G'$ such that
(1) ϕ is injective.
(2) ϕ is surjective.
(3) $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$.
In this case, the function ϕ is called an **isomorphism**.

Example 2: Show that the function $g : R^{**} \to R^{**}$ given by $g(x) = \sqrt{x}$ is an isomorphism.

Proof: $g(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = g(x)g(y)$, therefore, g is a homomorphism.
If $g(x) = g(y)$, then $\sqrt{x} = \sqrt{y}$. That means $x = y$. So g is injective.
For $r \in R^{**}$, we always have $g(r^2) = \sqrt{r^2} = r$. So g is surjective.
Therefore, g is an isomorphism.

Example 3: Prove that the function $f : R^{**} \to R^{**}$ defined by $f(x) = |x|$ is a surjective homomorphism that is not injective.
Proof: For $x \in R^{**}$, we have $x > 0$ so that $x = |x| = f(x)$. So f is surjective. Since $f(xy) = |xy| = |x| \cdot |y| = f(x)f(y)$, f is a homomorphism. But f is not injective because $f(1) = f(-1) = 1$, but 1 is not equal to 1.

Theorem 6.4: Let G and G' be groups with identity elements e and e', respectively. If $\phi : G \to G'$ is a homomorphism, then
(1) $\phi(e) = e'$**.**
(2) $\phi(a^{-1}) = \phi(a)^{-1}$ **for any** $a \in G$**.**
(3) $\text{im}(\phi)$ **is a subgroup of** G'**.**
(4) **If ϕ is injective, then G $\cong$ $\text{im}(\phi)$.**
Proof: (1) To show that $\phi(e)$ is the identity of G', we only need to find an element b in G' such that $b \cdot \phi(e) = b$. In fact, we only need to find $b = \phi(e) \in G'$. In this way

$$b \cdot \phi(e) = \phi(e) \cdot \phi(e) = \phi(e \cdot e) = \phi(e) = b.$$

Therefore, $\phi(e)$ is the identity of G'.
(2) Similarly, to show that $\phi(a^{-1})$ is the inverse of $\phi(a)$, we only need to show that $\phi(a^{-1}) \cdot \phi(a) = e'$. However,

$$\phi(a^{-1}) \cdot \phi(a) = \phi(a^{-1} \cdot a) = \phi(e) = e'.$$

Therefore, $\phi(a^{-1}) = \phi(a)^{-1}$.
(3) We can use definition directly to show $\text{im}(\phi)$ is a subgroup of G'. First noted that e' is in $\text{im}(\phi)$ by (1). Therefore, $\text{im}(\phi)$ is nonempty. Let $\phi(a), \phi(b) \in \text{im}(\phi)$ where $a, b \in G$. Then by (2), $\phi(b)^{-1} = \phi(b^{-1})$. Then

$$\phi(a) \cdot \phi(b)^{-1} = \phi(a) \cdot \phi(b^{-1}) = \phi(a \cdot b^{-1}).$$

Since $a \cdot b^{-1}$ is in G, so $\phi(a) \cdot \phi(b)^{-1} \in \text{im}(\phi)$. Therefore, $\text{im}(\phi)$ is a subgroup of H by Theorem 5.2.
(4) As noted before the theorem, ϕ can be considered as a surjective function from G to $\text{im}(\phi)$. If ϕ is also an injective homomorphism, then ϕ is an isomorphism.

Example 4: If $f : G \to H$ is an isomorphism of groups and if T is a subgroup of G, prove that T is isomorphic to the subgroup $f(T) = \{f(a) | a \in T\}$ of H.
Proof: Since T is a subgroup of G, the map $f_1 : T \to H$, which is also injective and a homomorphism. By Theorem 6.4, $f(T) = f_1(T) = Imf_1$ is a subgroup of H. Therefore, f_1 induces an isomorphism such that $T \cong f(T)$.

Example 5: Let $G, H,$ and K be groups. If $G \cong H$ and $H \cong K$, then prove that $G \cong K$.
Proof: The problem is equivalent to show that if $f : G \to H$ and $g : H \to K$ are isomorphisms, prove that the composite function $g \circ f : G \to K$ is also an isomorphism.
If $(g \circ f)(x) = (g \circ f)(y)$, then $g(f(x)) = g(f(y)$. So $g \circ f$ is injective. But g is injective so that $f(x) = f(y)$. Since f is also injective, we get $x = y$. Thus $g \circ f$ is injective. To prove the surjectivity, let $k \in K$. Since g is also surjective, there exists some $h \in H$ such that $g(h) = k$. Moreover, since f is surjective, there is some $x \in G$ with $f(x) = h$. Then we have $(g \circ f)(x) = g(f(x)) = g(h) = k$, therefore, $g \circ f$ is surjective. To show the homomorphism, we have

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y).$$

Recall: In the last section, we learned that a group G is called cyclic group if we can find an element a in G such that the cyclic group $\langle a \rangle = \{a^i | i \in Z\}$ that a generates is G. In other words, all the elements in G are in the form of a^i.

Theorem 6.5: Let G be a cyclic group.
(1) **If G is infinite, then $G \cong Z$.**
(2) **If G is finite of order n, then $G \cong Z_n$.**
Proof:(1) Suppose G is an infinite cyclic group and G can be produced from a. Consider $\phi : G \to Z$ such that $\phi(a^i) = i$ Then

$$\phi(a^{i+j}) = i + j = \phi(a^i \cdot a^j) = \phi(a^i) \cdot \phi(a^j).$$

Therefore ϕ is an homomorphism. Now we want to show that ϕ is well-defined. Since a has infinity order so that all a^i are distinct. Therefore, the power of a associated with any element of G is unique. For $n \in Z$, $n = \phi(a^n)$, therefore ϕ is an epimorphism. If $n = \phi(a^i)$ + $n = \phi(a^j)$, then i = $n = \phi(a^i) = n = \phi(a^j)$ = j. Therefore, i = j. Therefore, ϕ is a monomorphism.
(2) Suppose G is a cyclic group of order n. Since $G = \langle a \rangle$ so order$(a) = n$. By Theorem 5.8, $G = \{b^0, b^1, b^2, \ldots, b^{n-1}\}$, and by Corollary 2.5, $Z_n = \{[0], [1], [2], \ldots [n-1]\}$. Define $g : G \to Z$ by $g(b') = [i]$. Clearly g is a bijection. Finally,

$$g(bb') = g(b^{i+j}) = [i + j] = [i] + [j] = g(b') + g(b).$$

Hence, g is an isomorphism and $G \cong Z_n$.

Theorem 6.5 tells us that cyclic groups can be categorized by their number. That means given a positive integer n, from the perspective of isomorphism, there is only one kind of cyclic group which order is n.

Given a set S, we define $A(S)$ as all permutations of the set S, which consists of all bijective functions from S to S with compositions as the group operations. If f, g in $A(S)$, then their compositions are still bijective, therefore we know that $f \circ g$ in $A(S)$. Therefore, we consider the composition as the operations in $A(S)$. We know that the $A(S)$ with composition operation has the property of closure and associativity. As for the identity of $A(S)$

under this operation, it's the identity function I_S which is a function from S to S such that $I_S\ (x)$=x, $\forall x \in S$.

For all f in $A(S)$, by the property of bijection, we know that there exists g in $A(S)$ such that $f \circ g$ = g $\circ f = I_S$(that is, g is the inverse function of f). Therefore, any element in $A(S)$ has its inverse. We have shown that $A(S)$ is a group. The following theorem tells us why $A(S)$ such a group is important.

Theorem 6.6 Cayley's Theorem: Every group G is isomorphic to a group of permutations.

Proof: Here we only take G in $A(G)$ as a set, therefore, $A(G)$ consists of all bijective functions from G to G and need not be homomorphisms.
Now we want to define $\phi : G \to A(G)$ that is a homomorphism from G to $A(G)$. For any a in G, we define $\phi(a) \in A(S)$ as $T_a : G \to G$ defined by $T_a(x) = a \cdot x$ for any x in G.
First, we check if ϕ is well-defined function. The only thing we need to check here is if $\phi(a) = T_a \in A(S)$? From the definition we know that T_a is a function from G to G, so we just need to check if T_a is 1-1 and onto. If b in G, then $T_a\,(a^{-1}b) = a\,(a^{-1}b) = b$; hence, T_a is surjective. If $T_a(b)$ =$T_a(c)$, then $ab = ac$. Canceling a by Theorem 7.5, we can conclude that $b = c$. Therefore, T_a is bijective in $A(G)$.
We next show $\phi : a \mapsto T_a$ is a homomorphism from G to $A(G)$, which is to show for all $a, b \in G, \phi(a \cdot b) = \phi(a) \circ \phi(b)$. To check if $\phi(a \cdot b)$ and$\phi(a) \circ \phi(b)$ are the same, it suffices to show if these two functions mapped every element in the domain to the same value.

Since $\phi(a \cdot b) = T_{a \cdot b}$ for all x in G we have

$$T_a \circ T_b(x) = T_a\,(T_b(x)) = T_a(b \cdot x) = a \cdot (b \cdot x)$$

By the associativity of G, we know that for all x in G, $T_{a \cdot b}(x) = T_a \circ T_b(x)$. That means, $\phi(a \cdot b)$ =$\phi(a) \circ \phi(b)$. We finally want to show ϕ is 1-1. Suppose $\phi(a) = \phi(c)$, so that $T_a(x)$ = $T_c(x)$ for all x in G. Then

$$a = ae = T_{\mathrm{a}}(e) = T_{\mathrm{c}}(e) = ce = c.$$

Hence, ϕ is injective. Therefore, G is isomorphic to $im(\phi)$ by Theorem 6.4.

Cayley's Theorem makes the group not abstract anymore. You may concern that what does $A(G)$ can tell us? I thought of the same questions. But think about the structure of $A(G)$, it is not related to the group property of G and it is related to the number of G. In other words, when we want to know how many groups with order n, we only need to arbitrarily choose a set S with n element, and then discuss how many subgroups with order n in $A(S)$ (because Cayley's Theorem tells us all the group with order n must be in it).

If S has n element, consider S=1,2,...,n. Now we notate $A(S)$ which is the set with all bijective functions from 1,2,...,n to 1,2,...,n as S_n and call it as the symmetric group of degree n. Here's the Corollary from Cayley's Theorem.

Corollary 6.7: Every finite group G of order n is isomorphic to a subgroup of the symmetric group S_n.
Proof: The group G is isomorphic to a subgroup H of $A(G)$ by the proof of Theorem 6.6. Since G is a set of n elements, $A(G)$ is isomorphic to S_n. Consequently, H is isomorphic to a subgroup K of S_n by Example 4. Finally, $G \cong H$ and $H \cong K$ imply that $G \cong K$ by Example 5.

7 The Symmetric and Alternating Groups

The Symmetric Group is an act of collect all n objects. i.e, $\mathbf{S}_n$ = Group of permutation on a set with n elements and to rearrange of the set. In this notation, S=symmetric; N=the size of being permuted.
(Noticed that the cycle of length n is called n-cycles) Then, $(a_1 a_2 a_3 \dots a_k)$ be the permutation in $\mathbf{S}_n$ which can maps $\mathbf{a_1}$ to $\mathbf{a_2}$, $\mathbf{a_2}$ to $\mathbf{a_3}$, ... $\mathbf{a_{k-1}}$ to $\mathbf{a_k}$ to $\mathbf{a_1}$

Example 1: $\mathbf{S}_n$=(143) is the 3 cycle that maps 1 to 4, 4 to 3, 3 to 1, 2 to 2 can be written as

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

Example 2: Products in the cycle notation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

solution: (The action is from right to left)

1) R:1 to 2 L:2 to 4, therefore 1 to 4
2) R: 2 to 4 L:4 to 3, therefore 2 to 4
3) R: 3 to 1 L:1 to 1, therefore 3 to 1
4) R: 4 to 3 L:3 to 2, therefore 4 to 2

Definition 7.1 (Disjoint cycle): The two cycles are nothing in common. For example (14)and (1235) are disjoint in $\mathbf{S}_6$.

The inverse order of a cycle is the inverse of a cycle. For example:
$(\langle 2, 4, 5^{-1} \rangle = \langle 5, 4, 2 \rangle$

Theorem 7.2: If D = $(a_1 a_2 \dots a_k)$ and L = $(b_1 a_2 \dots b_r)$ are disjoint cycles in $\mathbf{S}_n$, then DL=LD.

Proof: Consider that the disjoint cycle D = $(a_1 a_2 \dots a_k)$ and L = $(b_1 a_2 \dots b_r)$.
We are using AL(x)=LA(x) to showing that AL=LA, where every x in A which we can write, A = $(a_1, a_2 \dots, a_k, b_1, b_2, b_r, c_1, c_2, c_3, \dots, c_m)$. Since D leaves a's untouched, then c's are the elements of left untouched.
Now, for a's $1i \leq k$ also because L leaves a's untouched, then we can get

$$DL(a_i) = D(L(a_i)) = a_i + 1$$

If i=k,then $a_{t+1} = a_1$.
Now, since L leaves the a's untouched,then we can get

$$LA(a_i) = L(A(a_i)) = L(a_{i+1}) = a_{i+1}$$

Next, we need to look at the c's with similar ideas.
Since c's left untouched by both D and L, we can get following that

$$DL(C_1) = D(L(C_1)) = D(c_i) = C_i$$

Finally, we can conclude DL=LD.

Theorem 7.3: Every permutation in $\mathbf{S}_n$ is the product of disjoint cycles.

Proof: Let a be a permutation on A=(1,2,...n). Say compute $a_2 = a(a_1)$, $a_3 = a_1(a^2)$ or $a_3 = a_2(a_1)$ ..... Then we can get that sequence $\{a_1, a(a_1), a^2(a_1), a^2(a_1)$. Since A is finite, k also finite.There exist $i < j$ for $a_i(a-1) = a_j(a_1)$.There are also some element of a may not be exhausted,then we can get that $\mathrm{E} = (\mathrm{a}_1, a_2, \ldots, a_{\mathrm{tn}})$.Then we can let $r_1$be the elements do not showed in E and apply the same progress to get a cycle $G = (b_1, b_2, \ldots .b_n)$ Noticed that cycle E and G are disjoint. However, if there are some elements in common,then some i and j would shows that $a^i(a_1) = a^j(b_1)$, then $b_1 = a^{i-j}(a_1)$ which also indicate that would be the element of E which shows that it is the contradiction of b_1 has chosen. Therefore, there are not have the element that exhausted, which implies that every permutation in s_n is the product of disjoint cycles.

Theorem 7.4: The order of a permutation τ is the least common multiple of the lengths of the disjoint cycles whose product is τ^*

Proof: Let k be the order of and suppose that $\mathrm{T} = \mathrm{c}_1\mathrm{c}_2\mathrm{c}_3 \ldots \mathrm{c}_\mathrm{r}$ where c_i are the disjoint cycles into $k_1, k_2 \ldots\ldots k_r$. There exist an integer q, since $c_1c_2 \ldots\ldots c_i$ are disjoint then $C_q = C_1^h C_2^h \ldots C_t^h$. Now, c_q is equal to the identity, if and only if $C_i^h = (i)$ for each individual term. By Theorem 7.9, $T_i^k = e$ where k_i/k. Thus, the last common multiple m of $k_1, k_2 \ldots k_i$ divides K. However,$C^m = C_1^m C_2^m C_i^m = e$ Therefore, m divides k and also $k = m$.

Definition 7.5: (The Alternating Group) The cycle of length 2 is called 2-cycle and also called a transposition which has some special properties.
Example 3a:
$\sigma = (1,2)(3,5,4) = (1,2) \circ (3,5,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}$
*action is from Right to Left.

1) Every transposition is its own inverse
2) $\mathrm{D} = \mathrm{D}_1, D_2, D_3, \ldots D_{n-1}$ and D_n are transpositions, then $(D_1D_2D_3D_{n-1})^{-1} = D_nD_{n-1} \ldots D_2D_1$

Example 3b:$(3,1,2)^{-1} = (2,1,3)$ since $(2,1,3)(3,1,2) = (1)(2)(3) = I$

Theorem 7.6: Every permutation in $\mathbf{S}_n$is a product of (not necessarily disjoint) transitions.

Proof: By Theorem 7.24 already shows that $\mathbf{S}_n$ is a product of cycles. Then,since $(a_1 a_2 \ldots a_k) = (a_1 a_2)(a_2(a_3)\ldots(a_{k-1}a_k)$ Also, noticed that in $\mathbf{S}_n$ a permutation given its even if it can be expressed as product of an even number of transition, which as same as odd.

Theorem 7.7: No permutation in $\mathbf{S_n}$ is both even and odd.

Proof: Let A in $\mathbf{S_n}$ and can be written as $a_1 a_2 \ldots\ldots a_m$ and $b_1 b_2 \ldots\ldots b_r$
Suppose that A is both even and odd where m is even and r is odd. By definition that every transition is its own inverse, and also Corollary 7.6 shows that
$AA^{-1} = (a_1 \ldots a_m)(b_1 \cdots b)^{-1} = a_1 \cdots a_m b_1^{-1} = a_1 \ldots a_m br \cdots b_1$.

We can easily concluded that m+r is odd, which also is a contradicts the lemma.

Noted that the set off all even permutation in S_n is denoted A_n which is alternating group of degree n.

Theorem 7.8 A_n is a subgroup of $\mathbf{S}_n$ of order $n!/2$.

Proof: Let P and Q are in S_n,and with very a_i, b_j transposition of m,r are even.Suppose that $P = a_1 a_2, \ldots..a_m$ and $Q = b_1 b_2, \ldots..b_r \dot{T}hen, PQ = a_1 a_2 \ldots\ldots a_m b_1 b_2 \ldots\ldots..b_r$.
We know that $m + r$ is even, and PQ is in A_n Which show that A_n is under multiplication. Since $P_{-1} = a_m a_{m-1} \ldots a_2 a_1$ and we know that m is even, and $P^{-1}i$ is in A^n, A^n is a subgroup by Theorem 7.11. Now need to show that $|A_n| = n!/2$. Let A_n and B_n be the set of even and odd permutation. Then, $C_n = A_n \cup B_n$ and the intersection of even and odd permutation is empty.Thus, $|A_n| = |B_n|$, so $|S_n| = |A_n| + |B_n| = 2|A_n|$. Since the element of symmetric group is n!, $|A_n| = n!/2$.

Example 4: Write each permutation in cycle notation: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 1 & 4 & 5 & 6 & 3 & 8 \end{pmatrix} = (137)$

Solution:
1 to 7 , 7 to 3, then 1 to 3
2 to 2 (fixed)
3 to 1 , 1 to 7, then 3 to 7
4 to 4 (fixed) 5 to 5 (fixed) 6 to 6 (fixed)
7 to 3 , 3 to 1, then 7 to 1
8 to 8 (fixed) 9 to 9 (fixed)

Example 5: Express as a product of disjoint cycles:
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 3 & 5 & 4 & 7 & 9 & 8 & 6 \end{pmatrix} = (12)(45)(679)$

Solution:
1 to 2, 2 to 1, therefore (12)

4 to 5, 5 to 4, therefore (45)
6 to 7, 7 to 9, 9 to 6 therefore (679)

Example 6: Prove that S_n is isomorphic to a subgroup of S_{n+2}.
Proof: $\phi : S_n \to A_{n+2}$ (Note that S_n is subgroup of A_{n+2}.

$$\phi(\sigma) = \begin{cases} \sigma & \text{if } \sigma \text{ is even} \\ \sigma(n+1n+2) & \text{if } \sigma \text{ is odd} \end{cases}$$

since it clearly injective, and $\phi(\beta\alpha) = \phi(\beta)\phi(\alpha)$ for all $\beta, \alpha, \epsilon s_n$. square to to the identity by using that (n+1 n+2) commute with everything in S_n.

$$\phi(\sigma)\phi(\tau) = \begin{cases} \sigma\tau & \text{if } \sigma \text{ and } \tau \text{ are both even or both odd} \\ \sigma\tau(n+1n+2) & \text{if one is even and the other is odd} \end{cases}$$

Hence, if σ and β are both even and old, then $\beta\sigma$ is even, then $\phi(\beta\sigma)$=$\beta\sigma$ Now, if only one of α, *alpha* is even and other is odd, then $\phi(\beta\sigma) = \beta\sigma(n+1n+2)$.
Therefore,in the either cases, $\phi(\beta\sigma) = \phi(\beta)\phi(\sigma)$.