SOS - Group Theory
Final Report

Mentored by
Arpon Basu

Anumalasetty Varshith
22b0907

27 July 2023

Contents

Chapter 1

Preliminaries

Before understanding about “group” I have revised some basic concepts in Algebra. I am stating them below

- **Well ordering principle**
  Any non-empty set of positive “integers” have a smallest integer.
- **Division algorithm**
  a,b are integers with $b > 0$. ∃ “unique” integers q,r such that
  $$a = bq + r$$
  where $0 \leq r < b$.
- **GCD as linear combination**
  For non-zero integers a,b ∃ “integers” s,t such that
  $$gcd(a, b) = sa + tb$$
  And gcd(a,b) is smallest positive member of set $\{sa + tb \mid a, b \in \mathbb{Z}^+$ and s,t $\in \mathbb{Z}\}$
- If a and b are relatively prime, then ∃ integers s and t such that $as + bt = 1$
- **Euclid’s lemma**
  If p is a prime that divides ab, then p divides a or p divides b.
- **FTA(Fundamental theorm of arithmetic)**
  Every integer greater than 1 is a prime or a product of primes and this product is unique.
- **Modular arithmetic**
  If a,b,q,r are as stated in Division algoritm, then a congruence r mod b. i.e.,
  $$a \equiv r\, (mod\, b)$$
- **Mathematical induction**

  1. **First principle**
     Let S be a set of integers containing a. Suppose S has the property that whenever some integer n $\geq$ a belongs to S, then the integer n + 1 also belongs to S. Then, S contains every integer greater than or equal to a.

2. **Second principle**
   Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.

- **Equivalence relations**
  A relation is equivalent if it is reflexive, symmetric and transitive.
  - (reflexive) : a $\in$ S, implies (a,a) $\in$ R
  - (symmetric) : (a,b) $\in$ S, implies (b,a) $\in$ R
  - (transitive) : (a,b) , (b,c) $\in$ S, implies (a,c) $\in$ R

- **Equivalence classes partition**
  The equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation on S whose equivalence classes are the elements of P.

- **Properties of functions**
  α : A $\rightarrow$ B, β : B $\rightarrow$ C, γ : C $\rightarrow$ D then,
  1. $\gamma(\alpha\beta) = (\gamma\alpha)\beta$ (associative)
  2. α, β one-one, implies $\beta\alpha$ is one-one
  3. α, β onto, implies $\beta\alpha$ is onto
  4. If α is one-one and onto, then $\exists$ α^{-1} : B $\rightarrow$ A, such that $\alpha\alpha^{-1}$(b) = b $\forall$ b $\in$ B
     and $\alpha^{-1}\alpha$(a) = a $\forall$ a $\in$ A

  (Where product implies composition here)

Chapter 2

Basics of Groups

2.1 Definitions related to Groups

- **Binary operation**
  Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G.
  This condition is called “closure”
  Division of integers is not a binary operation on integers

- **Group**
  a group is a set together with an associative opera- tion such that there is an identity, every element has an inverse, and any pair of elements can be combined without going outside the set.

  - (associative) : (ab)c = a(bc) for all a, b, c in G
  - (existence of identity) : $\exists$ e $\in$ G such that ae = ea = a for all a in G
  - (existence of inverse) : $\forall$ a $\in$ G, $\exists$ b $\in$ G, such that ab = ba = e

- **Abelian**
  $\forall$ a,b $\in$ G, if ab = ba then group is called an Abelian.
  if $\exists$ atleat one pair a,b in G, such that ab $\neq$ ba then G is called non-Abelian.

2.2 Standard examples of Groups

Given below are some standard examples of Groups on specified operation as given in 2.1. Mostly used examples are defined below.

- $\mathbb{Z}_n$ = {r | a $\equiv r\,(mod\,n)\ \forall a \in \mathbb{Z}$}
- $U(n)$ = {x | $\exists$ k such that kx $\equiv 1\,(mod\,n)$}

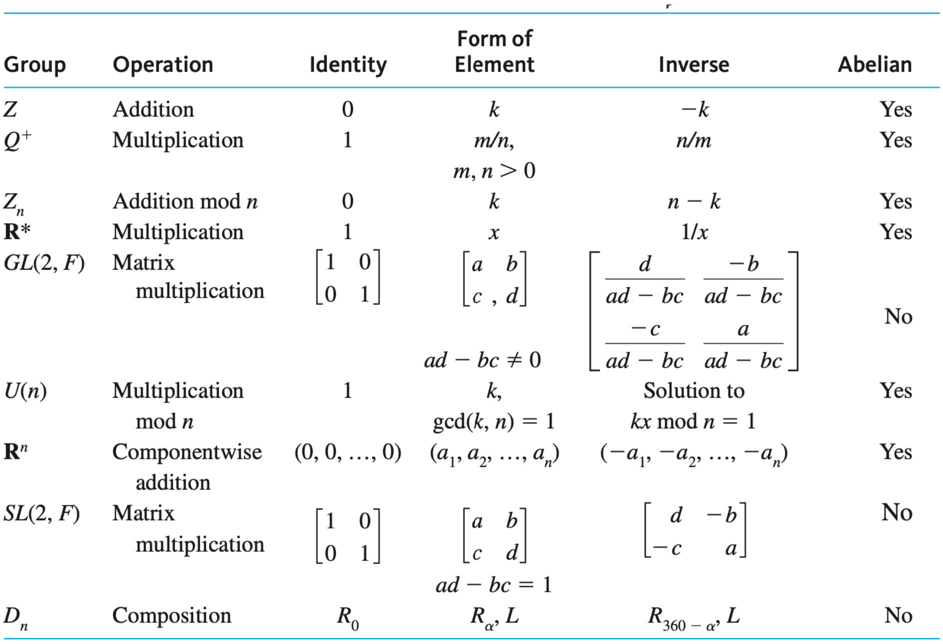
2.3 Properties of Groups

- **Uniqueness of the Identity**
  In a group G, there is only one identity element

- **Cancellation**
  In a group G, the right and left cancellation laws hold i.e.,

$$ba = ca \implies b = c, \textit{ and } ab = ac \implies b = c$$

- **Uniqueness of Inverses**
  For each element a in a group G, there is a unique element b in G such that ab = ba = e
- **Socks-Shoes Property**
  For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$



Group	Operation	Identity	Form of Element	Inverse	Abelian
Z	Addition	0	k	$-k$	Yes
Q^+	Multiplication	1	m/n, $m, n > 0$	n/m	Yes
Z_n	Addition mod n	0	k	$n - k$	Yes
$\mathbf{R}^*$	Multiplication	1	x	$1/x$	Yes
$GL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c\ , & d \end{bmatrix}$ $ad - bc \neq 0$	$\begin{bmatrix} \frac{d}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{a}{ad - bc} \end{bmatrix}$	No
$U(n)$	Multiplication mod n	1	k, $\gcd(k, n) = 1$	Solution to $kx \bmod n = 1$	Yes
$\mathbf{R}^n$	Componentwise addition	$(0, 0, \ldots, 0)$	$(a_1, a_2, \ldots, a_n)$	$(-a_1, -a_2, \ldots, -a_n)$	Yes
$SL(2, F)$	Matrix multiplication	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $ad - bc = 1$	$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	No
D_n	Composition	R_0	R_α, L	$R_{360 - \alpha}, L$	No

Figure 2.1: Some examples of groups

Chapter 3

Finite Groups & Subgroups

3.1 Important definitions

- **Order of a group**
  The number of elements of a group (finite or infinite) is called its order. |G| is used to denote the order of G.
- **Order of an element**
  The order of an element g in a group G is the smallest positive integer n such that g^n = e. (In additive notation, this would be ng = 0.) If no such integer exists, we say that g has infinite order. The order of an element g is denoted by |g|.
- **Subgroup**
  If a subset H of a group G is itself a group under the operation of G, we say that H is a subgroup of G.

3.2 Tests for Subgroups

- **One step subgroup test**
  Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a and b are in H, then H is a subgroup of G.
- **Two step subgroup test**
  Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a and b are in H, and a^{-1} is in H whenever a is in H, then H is a subgroup of G.
- **Finite subgroup test**
  Let H be a nonempty finite subset of a group G. If H is closed under the operation of G, then H is a subgroup of G.

3.3 Propositions related to subgroups

- Let G be a group, and let a be any element of G. Then, $\langle a \rangle$ is a subgroup of G.
  Where $\langle a \rangle$ denote set $\{a^n \mid \text{n} \in \mathbb{Z}\}$
- **Center of a group**
  The center Z(G) of a group G is the subset of elements in G that commute with every element of G.
  $$Z(G) = \{a \in G \mid ax = xa \ \forall x \in G\}$$

- The center of a group G is a subgroup of G.
- **Centralizer of an element**
  Let a be a fixed element of a group G. The centralizer of a in G, C(a), is the set of all elements in G that commute with a.
  $$C(a) = \{g \in G \mid ag = ga\}$$
- For each a in a group G, the centralizer of a,C(a), is a subgroup of G.

Chapter 4

Cyclic Groups

4.1 Definitions and it's properties

- **Cyclic group**
  A group G is called cyclic if there is an element a in G such that G = $\{a^n \mid$ n $\in$ Z$\}$.Such an element a is called a generator of G.
  For example, 1 and -1 are generators of set of integers $\mathbb{Z}$.

- **Criteria for finite or infinite order of an element**
  Let G be a group, and let a belong to G. If a has infinite order, then $a^i = a^j$ if and only if i = j. If a has finite order, say n,then ⟨a⟩ = $\{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides i – j.

- For any group element a, |a| = |⟨a⟩|.

- Let G be a group and let a be an element of order n in G. If a^k = e, then n divides k.

- The cyclic groups Z_n and Z serve as prototypes for all finite and infinite cyclic groups respectively.

- Let a be an element of order n in a group and let k be a positive integer.
  Then $\langle a^k \rangle = \langle a^{gcd(k,n)} \rangle$ and $|a^k|$ = n/gcd(n,k).

- **Relation btn order of element and order of a cyclic group**
  In a finite cyclic group, the order of an element divides the order of the group.

- **Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$**
  Let $|a|$ = n. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if gcd(n, i) = gcd(n, j) and
  $|a^i| = |a^j|$ if and only if gcd(n, i) = gcd(n, j)

- **Multile Generators**
  Let $|a|$ = n. Then $\langle a \rangle = \langle a^j \rangle$ if and only if gcd(n,j) = 1 and $|a| = |a^j|$ if and only if gcd(n, j) = 1. So by using above result if one generator of a cyclic group has been found, all generators of the cyclic group can easily be determined.

- **Generators of Z_n**
  An integer k in Z_n is a generator of Z_n if and only if gcd(n,k) = 1.

4.2 Classification of Subgroups of Cyclic Groups

- **Fundamental theorem of cyclic groups**
  Every subgroup of a cyclic group is cyclic.

Moreover, if $|\langle a\rangle|$ = n, then the order of any subgroup of $\langle a\rangle$ is a divisor of n;
For each positive divisor k of n, the group $\langle a\rangle$ has exactly one subgroup of order k—namely, $\langle a^{n/k}\rangle$

- **Subgroups of Z_n**
  For each positive divisor k of n, the set $\langle n/k\rangle$ is the unique subgroup of Z_n of order k;
  moreover, these are the only subgroups of Z_n.

- **No of elements of each Order in a Cyclic Group**
  If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is ϕ(d).
  Where ϕ(d) is "Euler phi function" i.e., no of numbers less than d and relatively prime to d if d > 1 and $\phi(1) = 1$.
  For example, $\phi(8) = 4$.({1,3,5,7} are relatively prime to 8).

- **Number of elements of Order d in a Finite Group**
  There is no formula for the number of elements of each order for arbitrary finite groups, but below proposition gives a relation.

  In a finite group, the number of elements of order d is divisible by ϕ(d).

- Although cyclic groups constitute a very narrow class of finite groups, they play the role of building blocks for all finite Abelian groups

Chapter 5

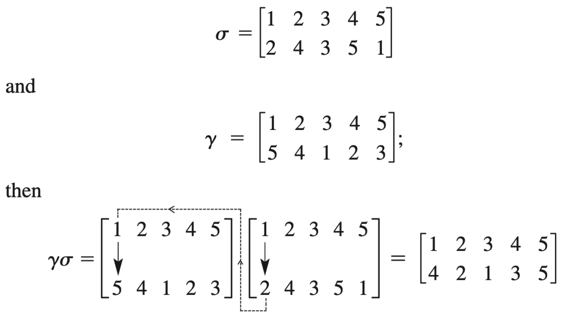
Permutation groups

5.1 Basic definitions

- **Permutation of a Group**
  A permutation of a set A is a function from A to A that is both one- to-one and onto.
- **Permutation Group of a Group**
  A permutation group of a set A is a set of permutations of A that forms a group under function composition.
- We generally learn about permutations for finite groups.
- We use notation for a permutation α, if $\alpha(1) = 2$, $\alpha(2) = 3$, $\alpha(3) = 1$, $\alpha(4) = 4$, is

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

- Composition of permutations is as shown in figure 5.1



$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$$

and

$$\gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix};$$

then

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

Figure 5.1: Composition of two permutations

5.2 Symmetric Groups

- **Symmetric Group S_n**
  Let A $= \{1, 2, \ldots, n\}$. The set of all permutations of A is called the symmetric group of degree n under the operation of function composition and is denoted by S_n. Elements of S_n have the form

$$\alpha = \begin{bmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{bmatrix}$$

- S_n has n! no of elements. Also every S_n with $n > 3$ is non-Abelian.
- **Symmetric Group S_3**
  The elements of S_3 is given by
  $$S_3 = \{\epsilon,\, \alpha,\, \alpha^2,\, \beta,\, \alpha\beta,\, \alpha^2\beta\}$$
  where $\epsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}$ $\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$ $\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}$
- The symmetric groups are rich in subgroups. The group S_4 has 30 subgroups, and S_5 has well over 100 subgroups.
- **Cyclic notation**
  If α is $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$, Then cyclic notation is as shown in figure 5.2

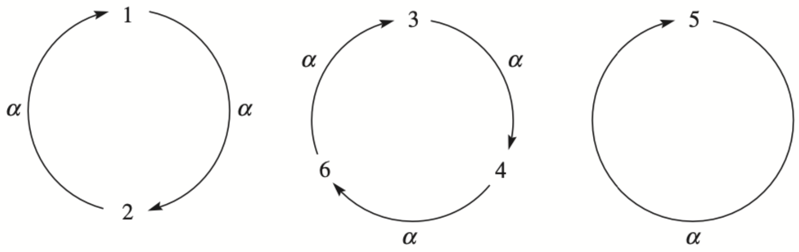


Figure 5.2: cyclic notation of a permutation

- It can also be written as $\alpha = (1,\, 2)(3,\, 4,\, 6)(5)$
- $\epsilon = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{bmatrix}$ can be denoted as $\epsilon = (5)$ or $\epsilon = (1)$.
- **Product of cycles**
  For example $\alpha = (12)(3)(45)$ and $beta = (153)(24)$,
  then $\alpha\beta = (12)(3)(45)(153)(24) = (14)(253)$.
  This comes by checking each element simultaneously passing through each disjoint cycle of (12)(3)(45)(153)(24).
  For example (24) fixes 1; (153) sends 1 to 5; (45) sends 5 to 4; and (3) and (12) both fix 4.

5.3 Properties of Permutations

- **Products of disjoint cycles**
  Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.
- **Disjoint cycles commute**
  If the pair of cycles a $\alpha = (a_1,\, a_2,\, \ldots,\, a_m)$ and $\beta = (b_1,b_2,\, \ldots,\, b_n\ )$ have no entries in common, then $\alpha\beta = \beta\alpha$
- **Order of a Permutation**
  The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

- A cycle of length 2 i.e., a permutation of the form (ab) is called as "transposition".
- **Product of 2-Cycles theorem**
  Every permutation in S_n, $n > 1$, is a product of 2-cycles.
- If $\epsilon = b_1 b_2 \ldots b_r$, where the b's are 2-cycles, then r is even.
- **Always Even or Always Odd decomposition**
  For a permutation, the number of 2-cycles may vary from one decomposition to another, but one aspect of a decomposition that never varies.

  If a permutation a can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of a into a product of 2-cycles must have an even (odd) number of 2-cycles

  In symbols, if
  $$\alpha = \beta_1 \beta_2 \ldots \beta_r \, and \, \alpha = \gamma_1 \gamma_2 \ldots \gamma_s$$
  where the β's and the γ's are 2-cycles, then r and s are both even or both odd.
- **Definition of Even and Odd permutation**
  A permutation that can be expressed as a product of an even number of 2-cycles is called an even permutation.
  A permutation that can be expressed as a product of an odd number of 2-cycles is called an odd permutation.
- **Definition of Alternating Group of Degree n**
  The set of even permutations in S_n forms a subgroup of S_n.
  This group of even permutations of n symbols is denoted by A_n and is called the "alternating group of degree n".
- **No of elements of A_n**
  For $n > 1$, A_n has order n!/2.
  That is no of even permutations and no of odd permutations are equal for S_n $\forall$ n $\in$ Z^+

Chapter 6

Isomorphisms

- **Definition of Group Isomorphism**
  An isomorphism ϕ from a group G to a group $\overline{G}$ is a one-to-one map- ping (or function) from G onto $\overline{G}$ that preserves the group operation.

- Symbolically,
  $$\phi(ab) = \phi(a)\phi(b) \;\; \forall\, a, b \, in \, G$$
  If there is an isomorphism from G onto $\overline{G}$, we say that G and $\overline{G}$ are isomorphic and write G $\approx$ $\overline{G}$.

- There are four separate steps involved in proving that a group G is isomorphic to a group $\overline{G}$.

  – **Step 1**
  "Mapping."Define a candidate for the isomorphism; that is, define a function f from G to $\overline{G}$.

  – **Step 2**
  "1–1."Prove that f is one-to-one; that is, assume that ϕ(a) = ϕ(b) and prove that a = b.

  – **Step 3**
  "Onto."Prove that f is onto; that is, for any element g in G, find an element $\overline{G}$ in G such that f(g) = $\overline{g}$.

  – **Step 4**
  "O.P."Prove that ϕ is operation-preserving; that is, show that ϕ(ab) = ϕ(a)ϕ(b) for all a and b in G.

- **An example**
  Let G = SL(2, $\mathbb{R}$), the group of 2x2 real matrices with determinant 1. Let M be any 2x2 real matrix with determinant 1. Then we can define a mapping from G to G itself by ϕ_M(A) = MAM^{-1} for all A in G. To verify that ϕ_M is an isomorphism, we carry out the four steps.

- **Cayley's Theorem** (1854)
  Every group is isomorphic to a group of permutations.

- **left regular representation of G**
  For any g in G, define a function T_g from G to G by
  $$T_g(x) = gx \quad \forall x \; in \; G$$
  Then $\overline{G}$ is called left regular representation of G, where $\overline{G}$ is defined as
  $$\overline{G} = \{T_g \mid \forall g \in G\}$$

- Cayley's Theorem is important for two contrasting reasons.

1. It allows us to represent an abstract group in a concrete way.
2. It shows that the present-day set of axioms we have adopted for a group is the correct abstraction of its much earlier predecessor - a group of permutations.

- It is not easy to prove that the group of nonzero complex numbers under multiplication is isomorphic to the group of complex numbers with absolute value of 1 under multiplication.
  In geometric terms, this says that, as groups, the punctured plane and the unit circle are isomorphic.

6.1 Properties of Isomorphisms

- **Properties of Isomorphisms Acting on Elements**
  Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

  1. ϕ carries the identity of G to the identity of $\overline{G}$. i.e., ϕ(e) is identity in $\overline{G}$
  2. $\forall$ n $\in \mathbb{Z}$ and $\forall$ a $\in$ G, $\phi(a^n) = [\phi$(a)$]^n$
  3. $\forall$ a,b $\in$ G, if a,b commute then ϕ(a),ϕ(b) commutes
  4. G = $\langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$.
  5. $|a| = |\phi(a)|$ $\forall$ a $\in$ G (isomorphisms preserve orders).
  6. For a fixed integer k and a fixed group element b in G, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\overline{G}$.
  7. If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

- Property 6 is quite useful for showing that two groups are not isomorphic.
  For example, equation $x^4 = 1$ has four solutions in C^* but only two in R^*. So however one tries to define isomorphism from C^* to R^*, (6) fails.

Chapter 7

Lagrange's Theorem

7.1 Cosets

- **Definition of Coset**
  When H is a subgroup of G, the set aH is called the "left coset of H in G containing a", whereas Ha is called the "right coset of H in G containing a",
  where ∀ a ∈ G, aH = { ah | h ∈ H } and Ha = { ha | h ∈ H }

- $|aH|$ denote the number of elements in the set aH, and $|Ha|$ denote the number of elements in Ha.

- Some miscellaneous concepts

  1. cosets are usually not subgroups.
  2. aH may be the same as bH, even though a is not the same as b.
  3. aH need not be the same as Ha.

- **Properties of Cosets**
  Let H be a subgroup of G, and let a,b ∈ G. Then,

  1. a ∈ aH,
     (left coset of H containing a does contain a)
  2. aH = H $\iff$ a ∈ H,
     (H "absorbs" an element if and only if the element belongs to H)
  3. aH = bH $\iff$ a ∈ bH
     (left coset of H is uniquely determined by any one of its elements.)
  4. aH = bH or aH ∩ bH = ϕ,
     (two left cosets of H are either identical or disjoint.)
  5. aH = bH $\iff$ a^{-1}b ∈ H,
     (question about equality of left cosets of H to a question about H itself and vice versa)
  6. $|aH| = |bH|$,
     (all left cosets of H have the same size)
  7. aH = Ha $\iff$ H = aHa^{-1},
     (question about the equality of the left and right cosets of H containing a is equivalent to a question about the equality of two subgroups of G)
  8. aH is a subgroup of G $\iff$ a ∈ H.
     (H itself is the only coset of H that is a subgroup of G)

- We may view the cosets of H as a partitioning of G into equivalence classes under the equivalence relation defined by a ∼ b if aH = bH

7.2 Lagrange's theorem and its Collaries

- **Statement : $|H|$ Divides $|G|$**
  If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.
  Moreover, the number of distinct left (right) cosets of H in G is $|G|$ / $|H|$.
- The converse of Lagrange's Theorem is false. For example, group of order 12 may have subgroups of order 12, 6, 4, 3, 2, 1, but no others. But having subgroup of order 6 is not necessery.
- **index of a subgroup**
  The index of a subgroup H in G is the number of distinct left cosets of H in G. Denoted by $|G : H|$.
- If G is a finite group and H is a subgroup of G, then $|G : H|$ = $|G|$ / $|H|$.
- In a finite group, the order of each element of the group divides the order of the group ie., $|a|$ divides $|G|$
  (The order of an element is the order of the subgroup generated by that element)
- A group of prime order is cyclic.
- Let G be a finite group, and let a $\in$ G.Then, $a^{|G|}$ = e.
- **Fermat's Little Theorem**
  For every integer a and every prime p, a^p mod p = a mod p.

7.3 Some applications of Lagrange's theorem

- **Classification of Groups of Order 2p**
  Let G be a group of order 2p, where p is a prime greater than 2. Then G is isomorphic to Z_{2p} or D_p
  (More generally, all cyclic groups are isomorphic to each other and Z_2p is one such group. Similarly, all cyclic groups are isomorphic to each other and D_p is one such group.)
- **Stabilizer of a Point**
  Let G be a group of permutations of a set S. For each i in S, let $stab_G$(i) = {ϕ $\in$ G | ϕ(i) = i}. We call $stab_G$(i) the stabilizer of i in G.
- **Orbit of a Point**
  Let G be a group of permutations of a set S. For each s in S, let orb_G(s) = {ϕ(s) | phi $\in$ G}. The set orb_G(s) is a subset of S called the orbit of s under G.
  We use $|orb_G(s)|$ to denote the number of elements in orb_G(s).
- **Orbit-Stabilizer Theorem**
  Let G be a finite group of permutations of a set S. Then, for any i from S, $|G| = |orb_G(i)|\,|stab_G(i)|$.
- $|G|/|stab_G(i)|$ is the number of distinct left cosets of $stab_G(i)$ in G.
- The group of rotations of a cube is isomorphic to S_4.

Chapter 8

External Direct Product

8.1 Defintion and its properties

- **Definition**
  Let G1, G2, . . . , Gn be a finite collection of groups. The external direct product of G_1, G_2, . . . , G_n, written as $G_1 \oplus G_2 \oplus \ldots \oplus G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is componentwise.
  In symbols,

  $$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, ..., g_n) \mid g_i \in G_i\}$$

- Well known examples, $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$ and $\mathbb{R}^3 = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$

- The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,

  $$|(g_1, g_2, \ldots, g_n)| = lcm(|g_1|, |g_2|, \ldots, |g_n|)$$

- For each divisor r of m and s of n the group $Z_m \oplus Z_n$ has a subgroup isomorphic to $Z_r \oplus Z_s$

- **Criterion for G $\oplus$ H to be Cyclic**
  Let G and H be finite cyclic groups. Then G $\oplus$ H is cyclic $\iff$ $|G|$ and $|H|$ are relatively prime.

- **Criterion for $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ to be Cyclic**
  An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of a finite number of finite cyclic groups is cyclic $\iff$ $|G_i|$ and $|G_j|$ are relatively prime when i $\neq$ j.

- **Criterion for $Z_{n_1 n_2 \ldots n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$**
  Let m = $n_1 n_2 \ldots n_k$. Then Z_m is isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$ $\iff$ n_i and n_j are relatively prime when i $\neq$ j.

- **Group of Units Modulo n i.e., U(n) as an External Direct Product**
  Suppose s and t are relatively prime. Then U(st) is isomorphic to the external direct product of U(s) and U(t). In short,

  $$U(st) \approx U(s) \oplus U(t)$$

- Moreover, U_s(st) is isomorphic to U(t) and U_t(st) is isomorphic to U(s).

- Let m = $n_1 n_2 \ldots n_k$, where gcd(n_i, n_j) = 1 for i $\neq$ j. Then, U(m) $\approx$ U(n_1)$\oplus$U(n_2)$\oplus \ldots \oplus$U(n_k).

- Using above results we can obtain

  1. U(2) $\approx \{0\}$,
  2. U(4) $\approx Z_2$,
  3. U(2n) $\approx Z_2 \oplus Z_{2^{n-2}}$ for n > 3,
  4. U(p^n) $\approx Z_{p^n - p^{n-1}}$ for p an odd prime,

  For example, U(105) $\approx Z_2 \oplus Z_4 \oplus Z_6$ and U(720) $\approx Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_4$

- There are many advantages and applications to represent a finite Abelian group as a direct product of cyclic groups in Data Security, Genetics etc.

Chapter 9

Normal Subgroups and Factor Groups

9.1 Normal Subgroups

- **Definition**
  A subgroup H of a group G is called a normal subgroup of G if aH = Ha for all a in G.
  We denote this by H $\lhd$ G.

- H is normal to G,
  means if a $\in$ G and h $\in$ H, then $\exists$ elements h' and h'' in H such that ah = h'a and ha = ah''.
  doesn't mean ah = ha for a $\in$ G and h $\in$ H.

- **Normal Subgroup Test**
  A subgroup H of G is normal in G $\iff$ $xHx^{-1} \subset$ H , $\forall$ x $\in$ G.
  (It allows us to substitute a condition about two subgroups of G for a condition about two cosets of G.)

- Some familair examples of normal subgroups are

  1. Every subgroup of an Abelian group is normal.
  2. The center Z(G) of a group is always normal.
  3. The alternating group A_n of even permutations is a normal subgroup of S_n.
  4. The subgroup of rotations in D_n is normal in D_n.
  5. The group SL(2,$\mathbb{R}$) of 2x2 matrices with determinant 1 is a normal subgroup of GL(2, $\mathbb{R}$)

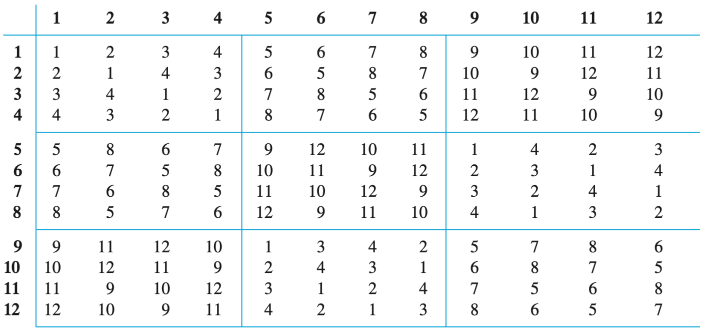
9.2 Factor Groups

- **Theorem : Definition of Factor Group of H by G**
  Let G be a group and let H be a normal subgroup of G. The set G/H = {aH | a $\in$ G} (set of left cosets of H in G) is a group under the operation (aH)(bH) = abH.

- Converse of above theorem is also true i.e.,
  if the correspondence aHbH = abH defines a group operation on the set of left cosets of H in G, then H is normal in G.

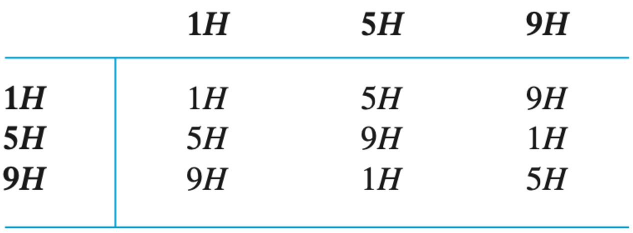
- If for any n > 0 we let nZ = {0, ±n, ±2n, ±3n, . . .}, then Z/nZ is isomorphic to Z_n.

- When H is a normal subgroup of G, the expression $|aH|$ has two possible interpretations.
  1. Thinking of aH as a set of elements and $|aH|$ as the size of the set.
  2. Thinking of aH as a group element of the factor group G/H and $|aH|$ as the order of the element aH in G/H.
- Information about a group by studying one of its factor groups. These is because a factor group G/H causes a systematic collapse of the elements of G.
- For example, Consider the group A_4 as represented by figure 9.1. (Here i denotes the permutation α_i). Let H = {1, 2, 3, 4}, We obtain the Cayley table for G/H given in figure 9.2.



	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	6	5	8	7	10	9	12	11
3	3	4	1	2	7	8	5	6	11	12	9	10
4	4	3	2	1	8	7	6	5	12	11	10	9
5	5	8	6	7	9	12	10	11	1	4	2	3
6	6	7	5	8	10	11	9	12	2	3	1	4
7	7	6	8	5	11	10	12	9	3	2	4	1
8	8	5	7	6	12	9	11	10	4	1	3	2
9	9	11	12	10	1	3	4	2	5	7	8	6
10	10	12	11	9	2	4	3	1	6	8	7	5
11	11	9	10	12	3	1	2	4	7	5	6	8
12	12	10	9	11	4	2	1	3	8	6	5	7

Figure 9.1: Table - 1



	1*H*	**5*H***	**9*H***
1*H*	1*H*	5*H*	9*H*
5*H*	5*H*	9*H*	1*H*
9*H*	9*H*	1*H*	5*H*

Figure 9.2: Table - 2

In this way, it is easier to study G using G/H .

- We are factoring out G by a normal subgroup H i.e., we are essentially doing is defining every element in H to be the identity. (since ∀ h ∈ H, hH = H)
- If subgroup H that is not normal in G, it is impossible to represent an entire box by a single element.

9.3 Applications of Factor groups

- **The G/Z Theorem**
  Let G be a group and let Z(G) be the center of G. If G/Z(G) is cyclic, then G is Abelian.
- In practice, it is the contrapositive of the theorem that is most often used i.e.,
  If G is non-Abelian, then G/Z(G) is not cyclic.
- If G/H is cyclic, where H is a subgroup of Z(G), then G is Abelian.

- For any group G, G/Z(G) ≈ Inn(G).
- **Cauchy's Theorem for Abelian Groups**
  Let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p.
- Suppose that H is a normal subgroup of a finite group G. If G/H has an element of order n, show that G has an element of order n.

9.4 Internal Direct Products

- External direct product provides a way of putting groups together into a larger group. So it is useful if we are able to start with a large group and break it down into a product of smaller groups. For this we define the set HK = {hk | h ∈ H, k ∈ K}.
- **Definition : Internal Direct Product of H and K**
  We say that G is the internal direct product of H and K and write G = H × K if H and K are normal subgroups of G and
  $$G = HK \ \ and \ \ H \cap K = \{e\}$$
- Such a G is isomorphic to the external direct product of H and K. (The definition ensures that this is the case)
- The figures 9.3 and 9.4 best illustrates the essence of internal and external direct product respectively.

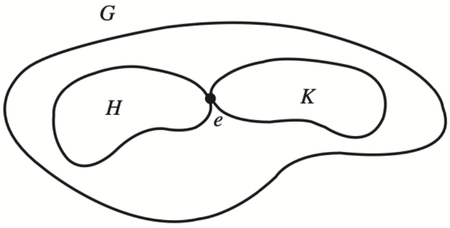


Figure 9.3: For the internal direct product, H and K must be subgroups of the same group

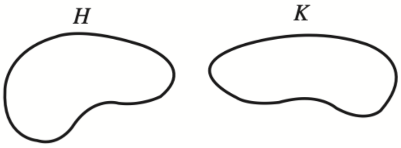


Figure 9.4: For the external direct product, H and K can be any groups

- **Internal Direct Product** $H_1 \times H_2 \times \cdots \times H_n$
  Let H_1, H_2, . . . , H_n be a finite collection of normal subgroups of G. We say that G is the internal direct product of H_1, H_2, . . . , H_n and write G = $H_1 \times H_2 \times \cdots \times H_n$,if

  1. G = $H_1 H_2 \ldots H_n = \{h_1 h_2 \ldots h_n \mid h_i \in H_i\}$
  2. $(H_1 H_2 \ldots H_n) \cap H_{i+1}$ = e for i = 1, 2, . . . , n - 1.

- $H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n$
  If a group G is the internal direct product of a finite number of subgroups H_1, H_2, . . . , H_n, then G is isomorphic to the external direct product of H_1, H_2, . . . , H_n.

- **Classification of Groups of Order** p^2
  Every group of order p^2, where p is a prime, is isomorphic to Z_{p^2} or $Z_p \oplus Z_p$.

- If G is a group of order p^2, where p is a prime, then G is Abelian.

- if G = $H_1 \oplus H_2$, then G = $\bar{H_1} \times \bar{H_2}$, where $\bar{H_1}$ = H_1 ⊕ {e} and $\bar{H_2}$ = {e} ⊕ H_2.

- if m = $n_1 n_2 \ldots n_k$, where gcd(n_i, n_j) = 1 for i ≠ j,then

$$U(m) = U_{m/n_1}(m) \times U_{m/n_2}(m) \times \cdots \times U_{m/n_k}(m)$$

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k).$$

Chapter 10

Revised Plan Of Action (POA)

10.1 Reference Book

“Contemporary Abstract Algebra” by Joseph A. Gallian