Group Theory

SOS 2024: Midterm Report

Aditya Khambete (23B3315)
Mentor: Sahil Rathour

Contents

Chapter 1

Some Basic Concepts

1.1 Number Systems

- Natural Numbers: $\mathbb{N} = \{1, 2, 3, \ldots\}$, our common counting numbers
- Integers: $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, including negative numbers
- Rational Numbers: $\mathbb{Q} = \left\{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\right\}$, fractions of integers
- Real Numbers: $\mathbb{R}$, the continuous number line
- Complex Numbers: $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i^2 = -1\}$, numbers with a real and imaginary part
- $\mathbb{Z}^+$, $\mathbb{Q}^+$, $\mathbb{R}^+$: denote the non-zero positive numbers in each set

1.2 Functions

A function $f : A \to B$ is a rule that assigns each element $a \in A$ to a unique element $b \in B$. The set A is called the domain of f, and the set B is called the codomain of f. The range of f is the set of all possible outputs $f(a)$ for $a \in A$.
Functions are classified as-

- Injective (one-to-one): $f(a) = f(b) \Rightarrow a = b$
- Surjective (onto): $\forall\ b \in B$, $\exists\ a \in A$ such that $f(a) = b$
- Bijective: both injective and surjective

1.2.1 Composition of Functions

Given two functions $f : A \to B$ and $g : B \to C$, the composition of f and g is the function $g \circ f : A \to C$ defined by $(g \circ f)(a) = g(f(a))$.

1.2.2 Inverse Functions

A **bijective** function $f : A \to B$ has an inverse function $f^{-1} : B \to A$ if $f \circ f^{-1} = \mathrm{id}_B$ and $f^{-1} \circ f = \mathrm{id}_A$, where id_A is the identity function on A.

1.2.3 Extension and Restriction of a function

Let $f : A \to B$ be a function. The extension of f to $A \cup C$ is the function $f' : A \cup C \to B$ defined by $f'(x) = f(x)$ for $x \in A$ and $f'(x) =$ Any element in B for $x \in C$, where b_0 is a fixed element of B.
The restriction of f to $A \setminus C$ is the function $f'' : A \setminus C \to B$ defined by $f''(x) = f(x)$ for $x \in A \setminus C$.
Note that a Restriction from a given subset of A will always be unique, but an extension to a given superset of A may not be unique.

1.3 Relation

A relation R from set A to set B is a subset of $A \times B$. If $A = B$, then R is a relation on A.
A relation R on A is

- reflexive if $(a, a) \in R$ for all $a \in A$
- symmetric if $(a, b) \in \mathbb{R} \Rightarrow (b, a) \in R$
- transitive if $(a, b) \in R$ and $(b, c) \in R \Rightarrow (a, c) \in R$
- equivalence if it is reflexive, symmetric, and transitive

1.3.1 Equivalence Relation

An equivalence relation on a set A is a relation that is reflexive, symmetric, and transitive.

The equivalence class of an element $a \in A$ is the set of all elements in A that are related to a.
All the equivalence classes of an equivalence relation on A form a partition of A.

Note: Partition of a set A means a collection of non-empty subsets of A such that every element of A is in exactly one of these subsets. Or in other words, the subsets are pairwise disjoint and their union is A.

1.4 Properties of Integers

- GCD and LCM: For integers $a, b \in \mathbb{Z}$, the greatest common divisor (GCD) of a and b is the largest positive integer that divides both a and b. The least common multiple (LCM) of a and b is the smallest positive integer that is a multiple of both a and b.
  Mathematically, if a,b are 2 integers than GCD g is such that $g|a$ and $g|b$ and if $d|a$ and $d|b$ then $d|g$.
  Similarly, LCM l is such that $a|l$ and $b|l$ and if $a|n$ and $b|n$ then $l|n$.
- Division Algorithm: For any integers a and b with $b \neq 0$, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.
- Euclidean Algorithm: A method for finding the GCD of two integers a and b. If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$. To employ this method, we repeatedly apply the Division Algorithm until the remainder is 0.

- Prime Numbers: An integer $p > 1$ is prime if its only positive divisors are 1 and p. Every integer $n > 1$ has a unique prime factorization.
- Fundamental Theorem of Arithmetic: Every integer $n > 1$ can be written as a product of prime numbers, and this factorization is unique up to the order of the factors.
  From the Fundamental Theorem of Arithmetic, we have the GCD and LCM of any 2 integers as-

  $$\text{if } a = p_1^{a_1} p_2^{a_2} ... p_n^{a_n},\ b = p_1^{b_1} p_2^{b_2} ... p_n^{b_n}$$

  then

  $GCD(a,b) = p_1^{min(a_1,b_1)} p_2^{min(a_2,b_2)} ... p_n^{min(a_n,b_n)}$ and $LCM(a,b) = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} ... p_n^{max(a_n,b_n)}$
- The euler-totient function is defined as $\phi(n)$= number of integers less than n and relatively prime to n.

1.5 Modulo Relation and Residual Classes

Let n be a positive integer. The modulo relation modulo n is an equivalence relation on $\mathbb{Z}$ defined by $a \equiv b \pmod{n}$ if $n|(a-b)$. The equivalence class of a is the set of all integers b such that $a \equiv b \pmod{n}$.

Theorem 1. if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a+c \equiv b+d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

Here the set of equivalence classes is called the set of residual classes modulo n. These are denoted as $\bar{0}, \bar{1}, \ldots, n-\bar{1}$. This set is denoted by $\mathbb{Z}/n\mathbb{Z}$.
To understand better, lets take n=5, then the set of residual classes modulo 5 will be $\bar{0} = \{0,5,10,15,20,25,..\}$, $\bar{1} = \{1,6,11,16,21,26,..\}$, $\bar{2} = \{2,7,12,17,22,27,..\}$, $\bar{3} = \{3,8,13,18,23,28,..\}$, $\bar{4} = \{4,9,14,19,24,29,..\}$, and set of all these classes will be $\mathbb{Z}/5\mathbb{Z}$.
Operations on these classes are defined as-

- $\bar{a} + \bar{b} = \overline{a+b}$
- $\bar{a} \cdot \bar{b} = \overline{ab}$

An important subset of the set of residual classes is that of the residual classes that have a multiplicative Inverse, which is all $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ such that $\exists\ c \in \mathbb{Z}/n\mathbb{Z}$ where $\bar{a} \cdot \bar{c} = \bar{1}$.
This set is denoted by

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists\ \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \bar{a} \cdot \bar{c} = \bar{1}\}$$

The cardinality(for finite sets, it is the number of elements in that set) of this set is $\phi(n)$.

Chapter 2

Introduction to Groups

2.1 Definition and Examples

Definition 2.1 (Binary Operations)**.** A binary operation on a set G is a function $G \times G \to G$. If $*$ is a binary operation on G, then $a * b$ is the result of applying the operation $*$ to a and b.

- A binary operation is associative if $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
- A binary operation is commutative if $a * b = b * a$ for all $a, b \in G$.

Now we know what a binary operation is, we can define a group.

Definition 2.2 (Group)**.** A group is a set G equipped with a binary operation $*$ that satisfies the following properties:

- Closure: For all $a, b \in G$, $a * b \in G$.
- Associativity: For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.
- Identity: There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$.
- Inverses: For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Note: If the group operation is commutative, then the group is called an abelian group.

2.1.1 Examples of Groups

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ under addition form a group. The identity element is 0, and the inverse of a is $-a$. This group is abelian.
- $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ under multiplication form a group. The identity element is 1, and the inverse of a is $1/a$. (here A^* denotes the set $A - \{0\}$). This group is abelian.
- The set of all $n \times n$ matrices with real or complex entries under matrix addition forms a group. This group is abelian.
- The set of all $n \times n$ invertible matrices with real or complex entries under matrix multiplication forms a group called the general linear group, denoted $GL(n, \mathbb{R})$ or $GL(n, \mathbb{C})$. This group is non-abelian.

- The set of residual classes modulo n under addition forms a group called the additive group of integers modulo n, denoted $\mathbb{Z}/n\mathbb{Z}$. The identity element is $\bar{0}$, and the inverse of $\bar{a}$ is $\bar{-a}$. This group is abelian.
- The subset $(\mathbb{Z}/n\mathbb{Z})^\times$ of residual classes form a group under multiplication modulo n. This group is called the multiplicative group of integers modulo n This group is abelian. The identity element is $\bar{1}$, and the inverse of $\bar{a}$ is $\bar{a}^{-1}$(Which we could find by bruteforce).

2.2 Properties of Groups

Theorem 2. For a group G under binary operation *-

- The identity element is unique.
- The inverse of each element is unique.
- $(a^{-1})^{-1} = a$ for all $a \in G$.
- $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.
- for any $a_1 * a_2 * \ldots * a_n$ the way in which we put the paranthesis doesn't matter, until we are not changing the order. This is called the generalised associative property.

From here on, we will denote the group G with the binary operation as $\cdot$ and with the identity element as 1 (which is the multiplicative notation of the group). From this notation, further we can define x^n as $x \cdot x \cdot x \ldots n$ times. Similarly x^{-n} as $(x^{-1})^n$ (Which is inturn the inverse of x^n).
Note- For additive groups, this notation doesn't quite make sense, so we'll continue using $+$ for those specific type of groups.

The above theorem 2.1 gives us the following useful properties-

- if $au = bu$ then $a = b$ for all $a, b, u \in G$. (Right Cancellation Law)
- if $va = vb$ then $a = b$ for all $a, b, v \in G$. (Left Cancellation Law)

Definition 2.3 (Order of an element)**.** Order of an element a $\in$ G is minimum n such that $a^n = 1$. If no such n exists, the order is said to be infinite.

Definition 2.4 (Multiplication Table)**.** For a finite group $G = \{a_1, a_2 \ldots, a_n\}$ the multiplication table is a $n \times n$ matrix whose $(i, j)^{th}$ element is $a_i \cdot a_j$.

Chapter 3

Common Families of Groups

3.1 Dihedral Groups

The dihedral group D_{2n} is the group of symmetries of a regular n-gon. It has $2n$ elements and is generated by two elements r and s such that $r^n = s^2 = 1$ and $rs = sr^{-1}$. The element r represents a rotation of $\frac{2\pi}{n}$ radians, and the element s represents a reflection across a line of symmetry.

To visualise it better, consider any regular polygon. The dihedral group represents all its rigid motions in the 3D space such that the polygon remains invariant.
Now say a polygon has n sides, so the vertex 1, could go to n possible places on motion, so after choosing the place for vertex 1 say it goes to i-th vertex, then vertex 2 can either go to i-1 or i+1, so there are total n ways for vertex 1, and then 2 choices for vertex 2, which gives us the total number of elements as $2n$.
Here the group operation is applying the rigid motion one after the other, and the identity element is the motion which doesn't change the polygon. So from this we can conclude the element r^i means rotating the polygon by $\frac{2\pi i}{n}$ radians and s means reflecting the polygon across a line of symmetry.
Henceforth, the relation $r^n = s^2 = 1$ signifies after n rotations or after 2 reflections, the polygon comes back to its original orientation, while the relation $rs = sr^{-1}$ tells us that rotating it first and then taking the reflection has the same effect as taking the reflection first and then rotating it in the opposite direction. This also tells us that this group is not abelian.

3.1.1 Generator and Relations

For any group G, the subset S of G is said to generate G if every element of G can be written as a product of elements of S and their inverses. The group G is said to be generated by S, and S is called the set of generators of G.
But clearly, only the set of generators is not enough, we also need to have some relation between the generators, which are called the relations of the group.
For the dihedral group, the set of generators is $\{r, s\}$ and the relations are $r^n = s^2 = 1$ and $rs = sr^{-1}$.
Together we denote this as a 'presentation' of group, which is denoted as $G = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$.

3.2 Symmetric Groups

The symmetric group S_n is the group of all bijections of the set $\{1, 2, \ldots, n\}$ under the group operation of function composition. It has $n!$ elements, and is denoted by S_n.
Clearly since we are talking about bijections on itself, the number of elements in the group will be $n!$.
Since the group operation is function composition, and the identity element is the identity function. The inverse of a bijection is its inverse function.

3.2.1 Cycle Notation

The cycle notation is a way of writing permutations as a product of disjoint cycles. A cycle is a permutation that moves elements in a cyclic order, and a disjoint cycle is a cycle that doesn't share any elements with another cycle.
But what is a cycle? To say simply, its a permutation containing some elements, and the first element goes to the second, the second to the third, and so on, and the last element goes to the first element. For example consider the cycle (3 12 1), say we denote bijection by σ, then we have-

$$\sigma(1) = 3, \sigma(3) = 12, \sigma(12) = 1$$

Cycle Decomposition Algorithm

To write a permutation as a product of disjoint cycles, we can use the following algorithm:

- Start with the first element i that hasn't been assigned to a cycle, usually we go with the smallest one
- Write down the cycle that starts with i and keep following the permutation until you reach i again
- Repeat the above steps until all elements have been assigned to a cycle
- Remove all the one element cycles

Note that a bijection is a product of all the cycles in its cycle Decomposition. Order of that bijection is the LCM of all the lengths of the cycles.
This tells us in a symmetric group, disjoint cycles commute, but its not the case with cycles with some common element.

3.3 Matrix Groups

Matrix groups are groups of $n \times n$ matrices under matrix multiplication. Typically, the entries we consider in the matrix are from a 'Field'.
For that we need to define Fields first.

Definition 3.1. A field is a set F equipped with two binary operations $+$ and $\cdot$ that satisfy the following properties:

- $(F, +)$ is an abelian group with identity element 0.
- $(F - \{0\}, \cdot)$ is an abelian group with identity element 1.

- Multiplication distributes over addition: $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

There are both finite fields like $\mathbb{Z}/p\mathbb{Z}$ (p is a prime) and infinite fields like $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$. Now we can define the matrix groups-

Definition 3.2. The general linear group $GL(n, F)$ is the group of all invertible $n \times n$ matrices with entries from a field F under matrix multiplication.

Definition 3.3. The special linear group $SL(n, F)$ is the subgroup of $GL(n, F)$ consisting of matrices with determinant 1.

For a finite field, the $|F|$ is of the form p^n where p is a prime and n is a positive integer. If F is a finite field, then the order of $GL(n, F)$ is $(q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1})$, where q is the number of elements in the field.

3.4 Quaternion Group

The Quaternion Group (Q_8) is a group of order 8. It is non-abelian and is generated by two elements i and j such that $i^2 = j^2 = -1$ and $ij = k = -ji$. The elements of the group are $\{1, -1, i, -i, j, -j, k, -k\}$.
Given are the main products of the group-

$$i^2 = j^2 = k^2 = -1$$
$$ij = k, jk = i, ki = j$$
$$ji = -k, kj = -i, ik = -j$$

3.5 Homomorphism and Isomorphism

These things are our formal notion when 2 groups 'look' the same. So lets start with Homomorphisms.

Definition 3.4. Homomorphism: Let (G,*) and (H,@) be 2 groups. A Homomorphism is a function from G to H such that-

$$f(a * b) = f(a)@f(b) \text{ for all } a, b \in G$$

If we are not explicitly mentioned with the group operations, we simply write-

$$f(ab) = f(a)f(b) \text{ for all } a, b \in G$$

Here the LHS is the group operation of G and RHS is the group operation of H.
Clearly, the map f should respect the domain and codomain, and only then it is a Homomorphism.

Definition 3.5. Isomorphism: A Homomorphism is said to be an Isomorphism if it is bijective.
If there exists an isomorphism between 2 groups, then we say that the 2 groups are isomorphic, and we denote it as $G \cong H$.

Theorem 3. If f is an isomorphism from G to H, then-

- The identity element of G is mapped to the identity element of H.

- The inverse of an element in G is mapped to the inverse of the image of that element in H.
- The order of an element in G is the same as the order of its image in H.
- The cardinality of G is the same as the cardinality of H.

3.6 Group Actions

Definition 3.6. A group action of a group G on a set X is a function $G \times X \to X$ that satisfies the following properties: (We are writing f(g,x) as gx)

- For all $x \in X$, $1 \cdot x = x$.
- For all $g, h \in G$ and $x \in X$, $(gh) \cdot x = g \cdot (h \cdot x)$.

We'll from now on denote the group action as a group G acting on set X.

Now for a particular element $g \in G$, we can define a permutation of X, which is denoted as σ_g such that $\sigma_g(x) = gx$ for all $x \in X$. This is called the permutation representation of the group action. The set of this permutation representation is the symmetric group S_X, and is itself a group under function composition. Interestingly, this permutation representation is a homomorphism from G to S_X (the symmetric group of X).
Lets define this homomorphism now as a function-

$$\phi : G \to S_X \text{ such that } \phi(g) = \sigma_g$$

Note that the Group action we referred in this section is more precisely a left group action, but we can also define right group actions, which are similar to left group actions, but the group elements act on the right of the set elements.

3.6.1 Properties

- The action ga=a for all $a \in X$ and $g \in G$ is called the trivial action. Here all the elements of G act as the identity permutation.
- **Faithful Action** is an action where no non-identity element of G acts as the identity permutation, or in other words the homomorphism is injective.
- **Kernel** of the action is the set of all elements of G that act as the identity permutation. For trivial action, the kernel is the whole group. While for Faithful action, the kernel is just the identity element.
- If we act a group on itself, then the action is called a **Conjugation Action** or **Regular Action**. Here the permutation representation is a homomorphism from G to S_G. This action is faithful.

Chapter 4

Subgroups

4.1 Definition and Examples

Definition 4.1. A subset H of a group G is a subgroup of G if H is itself a group under the group operation of G.
This is denoted as $H \leq G$.
Further if $H \neq G$, then H is called a proper subgroup of G, denoted as $H < G$.

Note- The operation of the subgroup is the same as the operation of the group.

4.1.1 Examples

- The group itself H=G and trivial subgroup H={1} is a subgroup of any group G. So a group has atleast 2 subgroups.
- The additive group of real numbers $\mathbb{R}$ has subgroups $\mathbb{Z}$ and $\mathbb{Q}$
- The multiplicative group of real numbers $\mathbb{R}^*$ has subgroups $\mathbb{Q}^*$ and $\mathbb{Z}^*$

Note: The relation 'is subgroup of' is transitive, so if H is a subgroup of G and G is a subgroup of K, then H is a subgroup of K.

Theorem 4. Let H be a subset of a group G. Then H is a subgroup of G if and only if-

- H is non-empty
- For all $a, b \in H$, $ab^{-1} \in H$

Furthermore if H is finite(and non empty), then it is enough to check closure under the group operation.

4.2 Family of Subgroups

4.2.1 Centralizers and Normalizers

Definition 4.2. The center of a group G, denoted by $Z(G)$, is the set of all elements of G that commute with every element of G.

$$Z(G) = \{g \in G \mid gx = xg \text{ or } x = gxg^{-1} \text{ for all } x \in G\}$$

If we add restriction that the x can only be from a certain non empty subset, say A of G, then the subgroup we get the centralizer of A in G, denoted as $C_G(A)$. So essentially we can say, the center of a group is the centralizer of the whole group.
Clearly, the center of a group is a subgroup of the group, in which all the elements commute with each other or in other words, the center of a group is an abelian subgroup of the not-necessarily abelian group G.

Definition 4.3. The **normalizer** of a subset A of a group G, denoted by $N_G(A)$, is the set of all elements of G that normalize A i.e. $gAg^{-1} = A$. Here $gAg^{-1} = \{gag^{-1} \mid a \in A\}$.

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$$

We can easily proof that the normalizer of a subset is a subgroup of the group. Furthermore $C_G(A)$ is a subgroup of $N_G(A)$

4.2.2 Stabilizers and Kernels

Definition 4.4. The stabilizer of an element $a \in X$ under a group action of G on a set X is the set of all elements of G that fix a i.e. $ga = a$.

$$\mathrm{Stab}_G(a) = \{g \in G \mid ga = a\}$$

It is a subgroup of G

Definition 4.5. The kernel of a group action of G on a set X is the set of all elements of G that act as the identity permutation.

$$\mathrm{Ker}(X) = \{g \in G \mid \phi(g) = \mathrm{id}_X \text{ or } gx = x \text{ for all } x \in X\}$$

It is a subgroup of G

Notice the difference between the stabilizer and the kernel. The stabilizer is the set of elements that fix a particular element, while the kernel is the set of elements that fix all elements.

An interesting thing is the fact that the normalizers and centralizers are subgroups of the group, is just a special case of the stabilizers and kernels being subgroups of the group.

4.2.3 Cyclic Groups and Subgroups

Definition 4.6. A group G is cyclic if there exists an element $a \in G$ such that every element of G can be written as a power of a.

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$$

Using the laws of exponents, we can easily conclude that cyclic groups are abelian.

Theorem 5. If G=$\langle x \rangle$ is a cyclic group of order n, then-

- If n is finite then order of x= n, and $x^n = 1$ with only 1,x,x^2,x^3,...,x^{n-1} as distinct elements.
- If n is infinite then order of x is infinite, and x^m=x^n if and only if m=n.

Theorem 6. If in a finite cyclic group, $x^m = 1$ and $x^n = 1$, then $x^d = 1$ where d=gcd(m,n) which is precisely the order of the element x and the cardinality of the group.

Theorem 7. Any 2 cyclic groups of the same order are isomorphic. In particular-

- if $\langle x \rangle$ and $\langle y \rangle$ are cyclic groups of order n then,

$$\phi : \langle x \rangle \to \langle y \rangle \text{ such that } \phi(x^i) = y^i \text{ is an isomorphism}$$

- if G is an infinite cyclic group then G is isomorphic to $\mathbb{Z}$ where-

$$\phi : G \to \mathbb{Z} \text{ such that } \phi(x^i) = i \text{ is an isomorphism}$$

Notation: The cyclic group of order n upto isomorphism is denoted as $\mathbb{Z}_n$. This is indeed same as set of residual classes modulo n under addition(Upto Isomorphism).

Generators of a Cyclic Group

A cyclic group can be generated by more than one element. But before moving to that, lets see this theorem about the order of elements in a group, which will be vital in understanding the generators of a cyclic group.

Theorem 8. Let G be a group, x be an element of G and a be a non zero integer. Let's denote order of x as $|x|$ for now, so we have-

- $|x| = \infty$ then $|x^a| = \infty$ for all a
- $|x| = n$ then $|x^a| = \frac{n}{gcd(n,a)}$

So now lets move to the generators of a cyclic group. We will write G=$\langle x \rangle$ to show that G is generated by x.

Theorem 9. Let G=$\langle x \rangle$ be a cyclic group, then-

- if $|x| = \infty$ then G=$\langle 1 \rangle$ or G=$\langle -1 \rangle$
- if $|x| = n$ then G=$\langle x^d \rangle$ where GCD(d,n)=1, Particularly the number of generators of a cyclic group of order n is $\phi(n)$ where ϕ is the euler-totient function.

Subgroups of a Cyclic Group

Let's conclude this section with a theorem about the subgroups of a cyclic group.

Theorem 10. Let G=$\langle x \rangle$ be a cyclic group, then-

- If H is a subgroup of G, then H is cyclic. Moreover, H=$\{1\}$ or H=$\langle x^d \rangle$ where d is the smallest positive integer such that $x^d \in H$.
- If $|G| = \infty$, then $\langle x^d \rangle = \langle x^m \rangle$ if and only if absolute value of d and m are equal.
- If $|G| = n$, then for all positive integers $a|n$, there is exactly one subgroup of order a which is $\langle x^{\frac{n}{a}} \rangle$.

4.2.4 Subgroups generated by subsets of a group

For any subgroup of G containing {x}, the smallest subgroup containing {x} is the cyclic group generated by x i.e. for any subgroup of G containing {x}, it will contain $\langle x \rangle$.
This is precisely the subgroups generated by singleton subset of a group, lets move to the subgroups generated by any subset of a group. Note we are only interested in finding minimal subgroups containing the subset.
Before that we need the notion of the intersection of subgroups-

Theorem 11. The intersection of a family of subgroups of a group G is a subgroup of G.

Definition 4.7. The subgroup generated by a subset A of a group G, denoted by $\langle A \rangle$, is the intersection of all subgroups of G containing A.

$$\langle A \rangle = \bigcap_{H \leq G, A \subseteq H} H$$

The above definition is a top down approach, where we are looking for the minimal subgroup containing the subset A. But we can also define the subgroup generated by a subset A as a bottom up approach, where we will simply use the fact that the subgroup is getting 'generated' by the subset A.

Definition 4.8. The subgroup generated by a subset A of a group G, denoted by $\langle A \rangle$, is the set of all elements of G that can be written as a product of elements of A and their inverses.

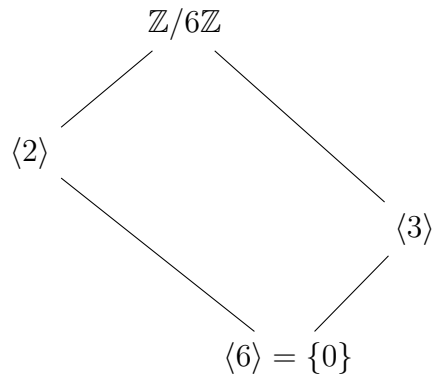
$$\langle A \rangle = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} \mid a_i \in A, \epsilon_i \in \{-1, 1\}, n \in \mathbb{N}\}$$

If the group G here is abelian, take A=$\{a_1, a_2 \dots, a_k\}$ we can easily write any member of $\langle A \rangle$ as $a_1^{n_1} a_2^{n_2} \dots a_k^{n_k}$ where $n_i \in \mathbb{Z}$. But the same is not true for non-abelian groups. It is often very hard, and maybe impossible to simplify structures like $aba^{-1}b^{-1}$ etc. All in all this shows that the subgroup generated by A when $|A| \geq 2$ is quite complicated for non-abelian groups.

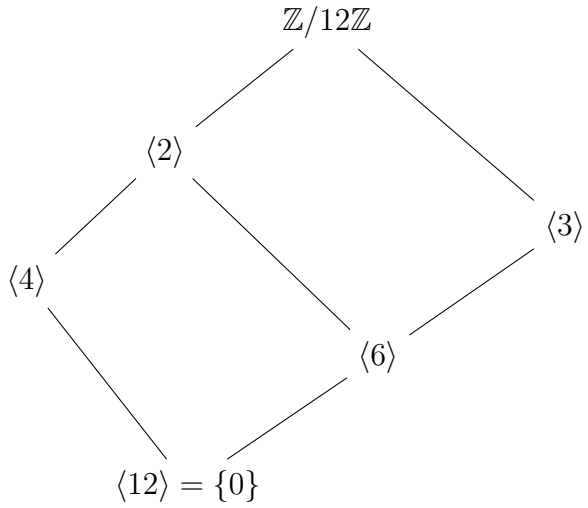
4.3 Lattice of Subgroups of a Group

The lattice of subgroups of a group is roughly a diagram showing the subgroups of a group and the relations between them
To construct a lattice at home, follow these steps-

- Start with the trivial subgroup and the whole group, with structure such that less order subgroups are below the higher order subgroups.
- For each pair of subgroups, find their intersection and their union, to get all the subgroups.
- Draw lines between the subgroups if one is contained in the other.



(a) Lattice of $\mathbb{Z}/6\mathbb{Z}$



(b) Lattice of $\mathbb{Z}/12\mathbb{Z}$

Figure 4.1: Lattices of $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$.

Appendix A

Future POA

So till now I was able to cover part upto week 3 of my original PoA, instead of the ideal week 4 scenario, so to cover it up and complete the project, here is the revised PoA-

- **upto July 1st**: Quotient Groups and Homomorphism: Definition and Examples, Cosets, Lagrange Theorem, Isomorphism Theorems, Composition Series and Holder Programs, Transpositions, Alternating Groups
- **upto July 8th**: Permutations, Cayley's Theorem, Class Equation, Automorphisms, Sylow Theorems
- **upto July 15th**: Direct and Semidirect Products and Abelian Groups
- **upto July 22nd**: p-Groups, Nilpotent and Solvable Groups, Groups of Medium Order: Applications, Free Groups
- **Onwards**: End Term Report, Review and Revision

Appendix B

References

- **Book**: Abstract Algebra by David S. Dummit and Richard M. Foote, chapters 0-3
- **Book**: Abstract Algebra by Khanna and Bhambri, chapters 1-4
- Wikipedia for some definitions and examples