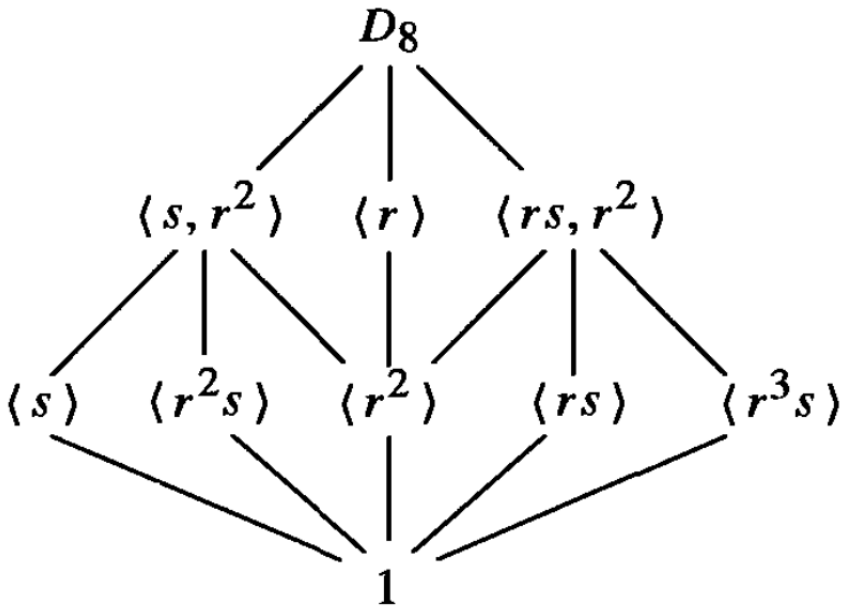
SoS Endterm Report 2022

Abstract Algebra

Mentor- Shantanu Nene

Mentee- Ameya Deshmukh (210050011)



Contents

Chapter 1

Abstract and Preliminaries

1.1 Abstract

Abstract algebra is the branch of Mathematics that deals with certain algebraic structures, eg. Groups, Rings, Fields, Vector Spaces etc.

Studying these abstract objects with well-defined properties leads to useful applications of specific examples of these structures.

Example. Consider the Fermat's Little theorem: if p is a prime, then for any $a \in \mathbb{Z}$ not divisible by p, $a^{p-1} - 1$ is divisible by p.

This result in number theory emerges on considering a non-trivial, general property for only an example of the algebraic structure, 'Group', which is $(\mathbb{Z}/p\mathbb{Z})^{\times}$.

1.2 Preliminaries

As part of reading Abstract Algebra, it was necessary to revise the following basics:

1.2.1 Set Theory, Functions

- $A \times B = \{(a, b) \mid a \in A, b \in B\}$ is the **Cartesian Product** of 2 sets
- A **function** is equivalent to a well-defined, *unambiguous* map between 2 sets, A, B.
- range(f)/image$(f) = f(A) = \{b \in B \mid b = f(a) \text{ for some } a \in A\}$
- for $C \subset B$, $f^{-1}(C) = \{a \in A \mid f(a) \in C\}$
- If $f : A \to B$ and $g : B \to C$, then their **composition** is another function $g \circ f : A \to C$, and $(g \circ f)(a) = g(f(a))$
- A function $f : A \to B$ is called:
  - **Injective** if $f(a_1) = f(a_2) \implies a_1 = a_2$
  - **Surjective** if range$(f) = B$
  - **Bijective** if f is both injective and surjective
- $f : A \to B$ has a **left-inverse**, if $\exists$ a function, $g : B \to A$ such that $g \circ f$ is the **identity** map on A

Remark. f is injective $\iff$ f has a left-inverse

- $f : A \to B$ has a **right-inverse**, if $\exists$ a function, $g : B \to A$ such that $f \circ g$ is the **identity** map on B

Remark. f is surjective $\iff$ f has a right-inverse

- A **permutation** of a set A is a bijective function, $f : A \to A$

1.2.2 Relations

- A relation R, on a set A is a subset of $A \times A$
- if $(a, b) \in R$ then $a \sim b$
- A relation R is called:
  - **Reflexive** if $a \sim a \quad \forall a \in A$
  - **Symmetric** if $a \sim b \implies b \sim a \quad \forall a, b \in A$
  - **Transitive** if $a \sim b, b \sim c \implies a \sim c \quad \forall a, b, c \in A$
  - **An equivalence relation** if R is reflexive, symmetric and transitive
- A partition of a set A is any collection of *disjoint* subsets of A, whose union is A.

$$\text{partition}(A) = \{A_i | i \in I\}, \quad A_i \cap A_j = \varnothing, \quad \cup_{i \in I} A_i = A$$

Equivalence relations on a set A are in bijective correspondence with partitions of A.

The subsets of the partition corresponding to an equivalence relation R are its equivalence classes, which are the sets of all elements which are related to each other.

1.2.3 Properties of Integers

- For $a, b \in \mathbb{Z} - \{0\}$, $\exists$ a unique $d \in \mathbb{Z} - \{0\}$ such that, $d|a, d|b$ and $e|a, e|b \implies e|d$.
  d is called the greatest common divisor of a, b and denoted by (a, b).
- For $a, b \in \mathbb{Z} - \{0\}$, $\exists$ a unique $l \in \mathbb{Z} - \{0\}$ such that, $a|l, b|l$ and $a|m, b|m \implies l|m$.
  l is called the least common multiple of a, b.
- **The Division Algorithm**: for $a, b \in \mathbb{Z} - \{0\}$, $\exists$ unique $q, r \in \mathbb{Z}$ such that

$$a = q \cdot b + r, \quad 0 \leq r < |b|$$

The Euclidean Algorithm applies the Division algorithm repeatedly to get the g.c.d. of any two non-zero integers:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

Here, there will always be a 0 remainder at some point $\because$ the series $|b| > |r_0| > |r_1| \ldots$ is a strictly decreasing sequence of positive integers.

Also, from the algorithm, it is clear that $r_n | r_{n-1} \implies r_n | r_{n-2}, \quad r_n | r_{n-1}, r_{n-2} \implies r_n | r_{n-2}, r_{n-3}$ $\ldots \quad r_n | r_2, r_1 \implies r_n | r_1, r_0 \implies r_n | r_0, b \implies r_n | b, a.$

Moreover, starting from r_{n-1} in $r_n = r_{n-2} - q_n r_{n-1}$, substituting each r_i as a linear combination of r_{i-1}, r_{i-2}, we get to the following important result:

$$r_n = ax + by, \quad x, y \in \mathbb{Z}$$

From here, it follows that $e|a, e|b \implies e|d$.

Hence, $r_n = (a, b)$.

- The **Fundamental theorem of Arithmetic**: The prime factorization of $n \in \mathbb{Z}, n > 1$ is *unique*.
- The **Euler φ function**: $\varphi(n)$ for $n \in \mathbb{Z}^+$ is the number of positive integers $a \leq n$, such that $(a, n) = 1$. If the prime factors of n are $\{p_1, p_2 \dots p_{s-1}, p_s\}$ then:

$$\varphi(n) = n \prod_{i=1}^{i=s} \left(1 - \frac{1}{p_i}\right)$$

1.2.4 $\mathbb{Z}/n\mathbb{Z}$

- $\mathbb{Z}/n\mathbb{Z}$ denotes the set of the **equivalence classes** created due to the equivalence relation:

$$a \sim b \iff n|(a-b), \quad \text{this is also denoted by } a \equiv b \bmod n$$

$\bar{a}$ denotes the equivalence/congruence/residue class of a mod n.

- **Modular Arithmetic**: Under the above relation on the integers, we can construct some well defined operations on the *residue classes*.

$$\bar{a} + \bar{b} = \overline{a+b} \qquad \bar{a}\bar{b} = \overline{ab}$$

- $(\mathbb{Z}/n\mathbb{Z})^\times$: this set consists of those equivalence classes that have a *multiplicative inverse*.

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

Proposition. $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff (a, n) = 1$

Proof. Assume that $(a, n) \neq 1$, in that case $\bar{b} = \overline{\frac{n}{(a,n)}} \neq \bar{0}$. Now, $\bar{a}\bar{b} = \overline{\frac{a}{(a,n)}n} = \bar{0}$. If $\exists\ \bar{c} \in \mathbb{Z}/n\mathbb{Z}$, such that $\bar{c}\bar{a} = \bar{1}$ then, $\bar{c}\bar{a}\bar{b} = \bar{b}$ and $\bar{c}\bar{a}\bar{b} = \bar{c}\bar{0} = \bar{0}$ which is a contradiction. For the converse, we can directly use that $(a, n) = 1 \implies \exists\ x, y \in \mathbb{Z}$ such that $ax + ny = 1 \implies \bar{a}\bar{x} = \bar{1}$. □

Chapter 2

Introduction to Group Theory

2.1 Basic Axioms

In order to understand what a group is, we first need to understand what a binary operation is.

Definition 2.1 (Binary Operation)**.** A **Binary Operation** $*$ is a *function*, $* : G \times G \to G$, where G is a set. $*(a, b)$ is often denoted as $a * b$.

An operation is said to be:

- **Associative**, if $\forall a, b, c \in G$, $(a * b) * c = a * (b * c)$.
- $a, b \in G$ commute under $*$ if $a * b = b * a$.
- If all pairs of elements in G commute, then $*$ is said to be **commutative**.

Some **examples** of operations are:

- The earlier defined addition and multiplication on residue classes mod n are commutative and associative operations on the set $\mathbb{Z}/n\mathbb{Z}$.
- The usual cross product $\times$ on $\mathbb{R}^3$ is a non-commutative and non-associative operation. But an arbitrary $\vec{v}$ and $\lambda\vec{v}$ commute under $\times$.
- An operation $*$ defined on $\mathbb{Z}$ as $a * b = 5(a + b)$ is commutative but not associative ∴ $(a * b) * c = 5(5(a + b) + c) = 25a + 25b + 5c$ and $a * (b * c) = 5(a + 5(b + c)) = 5a + 25b + 25c$.
- Matrix multiplication defined in the usual sense on the set of all $n \times n$ matrices is an associative but non-commutative operation.

Now, we can define the algebraic structure which will be the focus of our study. It only needs to satisfy the following few conditions, but they give rise to the many interesting properties of groups.

Definition 2.2 (Group)**.** A **Group** is an ordered pair of a set and a binary operation on the set, $(G, *)$, where the following axioms hold:

- $*$ is associative.
- $\exists$ an element $e \in G$ such that $a * e = e * a = a$ $\forall a \in G$. e is called the *identity*.
- $\forall\, a \in G \,\exists$ an element denoted as $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$. a^{-1} is called the *inverse* of a.

Remark. If the operation of a group is commutative over the group's set, we call it an *abelian* group.

Note that we take the associativity of the usual '+' and '×' operations on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ as a given here. Some **examples** of groups are

- $(\mathbb{Z}/n\mathbb{Z}, +)$. In this group $e = \bar{0}$ and $\bar{a}^{-1} = \overline{-a}$
- $(\mathbb{Q} - 0, \times)$, $(\mathbb{R} - 0, \times)$, $(\mathbb{C} - 0, \times)$, for all $e = 1$ and $a^{-1} = \frac{1}{a}$
- $((\mathbb{Z}/n\mathbb{Z})^{\times}, \times))$. In this group $e = \bar{1}$ and the existence of the inverse is guaranteed by the definition of the set.

2.1.1 Direct Product

Like the Cartesian product of 2 sets produced another set, the *direct product* allows us to create a new group from 2 groups.

Given $(A, \star)$ and $(B, \diamond)$, $(A \times B, *)$ is called their direct product where:

$$(a_1, b_1) * (a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2) \quad \forall\, (a_1, b_1), (a_2, b_2) \in A \times B$$

The closure and associative properties of this new component-wise operation follow due to the same properties of $\star$ and $\diamond$.

For the direct product, $e = (e_1, e_2)$ where e_1, e_2 are the identities of $(A, \star), (B, \diamond)$ respectively.

Also, $(a, b)^{-1} = (a^{-1}, b^{-1})$.

2.1.2 Basic Results

Consider the following for a group $(G, *)$

Proposition. The identity of a group is unique.

Proof. If there are 2 identities in a group e_1, e_2 then by the identity axiom. $e_1 * e_2 = e_2$
$\because$ an identity satifies $e * a = a * e = a \, \forall a \in G$. But $e_1 * e_2 = e_1$ by the same axiom.
Hence $e_1 = e_2$. □

Proposition. The inverse of $a \in G$ is unique.

Proof. If 2 elements b_1, b_2 of G satisfy the inverse axiom for a, then

$$\begin{aligned} a * b_1 &= e \\ b_2 * (a * b_1) &= b_2 * e \\ (b_2 * a) * b_1 &= b_2 \\ e * b_1 &= b_2 \\ \text{Hence } b_1 &= b_2. \end{aligned}$$

□

Proposition. $(a^{-1})^{-1} = a$ and $(a * b)^{-1} = b^{-1} * a^{-1}$

Proof. Follows from the definition of an inverse. □

Proposition. *The Generalized Associative Law*: for $a_1, a_2, \ldots, a_n \in G$, the value of $a_1 * a_2 * \ldots * a_n$ is independent of how it is *bracketed*.

Proof. For ease of notation consider the following recursive definition of some functions:

$$*^1 : G \to G, \quad *^1(a) = a \quad \forall a \in G$$
$$*^{n+1} : G^{n+1} \to G, \quad *^{n+1}(a_1, a_2, \ldots, a_n, a_{n+1}) = *^n(a_1, a_2, \ldots, a_n) * a_{n+1} \quad \forall n \geq 1$$

Remark. The $*^n$ defined here is the same as $(((\ldots((a_1) * a_2)\ldots) * a_{n-1}) * a_n)$

We need to prove the following claim:

$$\forall m, n \in \mathbb{N}$$
$$*^{m+n}(a_1, a_2, \ldots, a_{m+n}) = (*^m(a_1, a_2, \ldots, a_m)) * (*^n(a_{m+1}, \ldots, a_{m+n}))$$

$\because$ any valid *bracketing* is the same as breaking the arguments of the function at some point recursively. We proceed by induction on n. The base case for $n = 1$ is true trivially by the definition of $*^m$.

Assume that the result is true for some $n - 1$ and all $m \in \mathbb{N}$

$$\begin{aligned}
&\therefore \forall m \in \mathbb{N} \\
^{m+n}(a_1, a_2, \ldots, a_{m+n}) &= (^{m+n-1}(a_1, a_2, \ldots, a_{m+n-1})) * a_{m+n} \\
&= \big((*^m(a_1, a_2, \ldots, a_m)) * (*^{n-1}(a_{m+1}, \ldots, a_{m+n-1}))\big) * a_{m+n} \\
&= *^m(a_1, a_2, \ldots, a_m) * (*^{n-1}(a_{m+1}, \ldots, a_{m+n-1}) * a_{m+n}) \qquad \because * \text{ is associative} \\
&= (*^m(a_1, a_2, \ldots, a_m)) * (*^n(a_{m+1}, \ldots, a_{m+n}))
\end{aligned}$$

□

Notation:

- From here on, instead of using a symbol for the group operation, the function will be represented only as the arguments written in order

  $$a * b \longrightarrow ab$$

  Moreover, the identity will be written as '1'.

- For $x \in G$ and $n \in \mathbb{Z}$, $xxx\ldots x$ (n times) will be denoted by x^n, with $x^0 = 1 =$ the identity of the group.

Proposition. Let G be a group, then for $a, u, v \in G$:

$$\begin{aligned}
au = av \text{ or } ua = va &\implies u = v \\
ua = 1 \text{ or } au = 1 &\implies u = a^{-1} \\
ua = a \text{ or } au = a &\implies u = 1
\end{aligned}$$

Proof. The first statement follows from the uniqueness of the inverse while the other 2 are special cases of the same. □

Definition 2.3. For a group G and $x \in G$, the **order** of x is the smallest positive integer n such that $x^n = 1 =$ the identity of G. n is denoted by $|x|$. If no such n exists, then x is said to be of *infinite* order.

Some examples are:

- in $\mathbb{Z}/10\mathbb{Z}$ under addition, the order of the element $\bar{4}$ is 5. Since, $\bar{4}^1 = \bar{4}$, $\bar{4}^2 = \bar{4}+\bar{4} = \bar{8}$, $\bar{4}^3 = \overline{12} = \bar{2}$, $\bar{4}^4 = \bar{6}$, $\bar{4}^5 = \overline{10} = \bar{0} = e$.
- In the group $\mathbb{C} - \{0\}$ under multiplication, the order of -1 is 2, $\because (-1)^2 = -1 \times -1 = 1 = e$. The order of 1 is 1, while the order of i is 4. For z in $\mathbb{C}$ if the magnitude of $z \neq 1$, then it will be of infinite order.

Exercise 1. For a group G, $a, b \in G$, prove that $|ab| = |ba|$

Solution.
We first show that for $x, g \in G$, $|x| = |g^{-1}xg|$.
$(g^{-1}xg)^k = g^{-1}x^kg \quad \equiv \quad x^k = g((g^{-1}xg)^k)g^{-1}$
Thus, $x^k = 1 \iff (g^{-1}xg)^k = 1 \implies |x| = |g^{-1}xg|$
But, we have that $ba = a^{-1}(ab)a \implies |ab| = |ba|$.

Exercise 2. For $x \in$ a group G, show that if x has a finite order, then $|x| \leq |G|$

Solution.
Let $|x| = n$, then consider the elements in the set $S = \{1, x, x^2, \ldots, x^{n-1}\}$.
All these will be *distinct* elements of G, since if $x^i = x^j$ with $0 \leq i < j \leq n-1$, then $x^{j-i} = 1$, with $j - i < n = |x|$ which contradicts the definition of the order of an element.
Hence, $|G| \geq |S| = n = |x|$.

2.2 Dihedral Groups

We now consider a family of groups that is very useful. *Dihedral groups* are used to represent the symmetries of the simplest geometric objects, regular planar figures.

A symmetry of an object is a *rigid motion* of the object, after which we can still entirely cover the original object.

For regular n-gons, an easy way to think about a specific symmetry is to label and track its vertices. If we do this, then a symmetry s is bijectively connected to σ, a permutation of the labels of its vertices, $\{1, 2, 3, \ldots, n-1, n\}$.

In order to make the set of symmetries a group we need an operation. We choose it to be function composition.

So, for symmetries s, t which effect the permutations σ, τ, we define st to be the symmetry which is the result of the rigid motion of t followed by that of s, or equivalently, the symmetry which effects the permutation $\sigma \circ \tau$.

The identity of the group is chosen to be the symmetry which does nothing to the n-gon, and the inverse of $s \equiv \sigma$ is the 'reverse' rigid motion, that is $s^{-1} \equiv \sigma^{-1}$.

We denote this group of symmetries of an n-gon by D_{2n}. The naming becomes apparent if we consider $|D_{2n}|$.

Consider the n-gon after we perform a symmetry on it. The vertex labelled 1 can now be on any of the n vertices. Moreover we have 2 choices to decide the location of its adjacent vertex 2. Once we fix the location of those 2 adjacent points, we have completely described the action of the symmetry on all vertices.

Hence, $|D_{2n}| = n \cdot 2 = 2n$.

2.3 Generators and Relations

We motivate the important concept of generators and relations through the above defined Dihedral groups.

Consider the symmetries $r, s \in D_{2n}$ defined as follows:
r rotates the n-gon by $\frac{2\pi}{n}$ anti-clockwise.
s flips the n-gon about the line joining the center and the original position of vertex 1.
Some obvious properties of these symmetries are:

- $|r| = n$, $|s| = 2$, $sr^i \neq sr^j \quad \forall \quad 0 \leq i, j \leq n-1$
- $rs = sr^{-1}$, $r^i s = sr^{-i}$
- $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$

Thus, all the group's elements can be written as finite products of r and s.

Definition 2.4. A subset S of elements of a group G with the property that every element of G can be written as a finite product of elements of S and their inverses is called a **set of generators** of G.

We shall indicate this notationally by writing $G = \langle S \rangle$ and say G is generated by S or S generates G.

eg. $D_{2n} = \langle r, s \rangle$, $\mathbb{Z} = \langle 1 \rangle$

Relations are any equations in G that the elements of S satisfy.

A *presentation* of a group is its generators combined with a collection of relations such that any relation can be deduced from the collection.

$$G = \langle S \mid R_1, R_2, \ldots, R_m \rangle$$

eg. $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$

We must however be careful with presentations since the relations given may create some hidden equalities.

eg. Consider the presentation $G = \langle u, v \mid u^4 = v^3 = 1, uv = v^2u^2 \rangle$
$uv^2 = (uv)v = v^2u^2v = v^2u(uv) = v^2u(v^2u^2) = v^2(uv^2)u^2$.
Thus, letting $uv^2 \in G$ be w gives us $w = v^2wu^2$, hence $v^2wu^2 = v^4wu^4 \implies w = v^4wu^4 = vw$
This leads to the hidden equality, $v = 1$, which again leads to $u = u^2 \implies u = 1$.
Using the definition of generators, we conclude that $G = \{1\}$.

2.4 Symmetric Groups

Definition 2.5. Let Ω be any nonempty set and let S_Ω be the set of all bijections from Ω to itself (i.e., the set of all permutations of Ω). The set S_Ω is a group under function composition: $\circ$.

The satisfiability of the group axioms follows due to the bijectivity of permutations. We can also note that $|S_\Omega| = |\Omega|!$.

The special case of the group when $\Omega = \{1, 2, \ldots, n\}$ is denoted by S_n, the symmetric group of degree n.

2.4.1 Cycle Decomposition Algorithm

Definition 2.6. A cycle is a string of integers which represents the element of S_n, which cyclically permutes these integers (and fixes all other integers). i.e. $(a_1 a_2 \ldots a_m)$ sends a_i to a_{i+1} for all $1 \leq i < m$ and sends a_m to a_1.

It is intuitively clear that any permutation is a product of cycles.

To decompose a given permutation, σ, into *disjoint* cycles, there is an algorithm.

The Cycle Decomposition Algorithm

a. Choose the smallest number in $(1, 2, \ldots, n)$ that hasn't appeared in a previous cycle. Call it a. ($a = 1$ if no previous cycles defined)
Begin the new cycle: $(a$
$b \leftarrow \sigma(a)$
b. do while $b \neq a$:
Add b to the cycle.
$b \leftarrow \sigma(b)$
c. Here, $b = a$. Complete the cycle with a right parenthesis.
Return to **a.**
Conventionally, cycles of length 1 aren't written.
eg. We represent $\sigma \in S_5$ defined as: $\sigma(1) = 2, \sigma(2) = 5, \sigma(3) = 4, \sigma(4) = 3, \sigma(5) = 1$ as $\sigma = (1\,2\,5)(3\,4)$
Using the cycle representation, we can obtain the same for a permutation's inverse, by simply reversing the order of the elements in each cycle.
It can be seen that:

- S_n is a non-abelian group ($n \geq 3$). Consider $\sigma \in S_3 = (1\,2)$ and $\tau \in S_3 = (1\,3)$
  $\sigma \circ \tau = (1\,2) \circ (1\,3) = (1\,3\,2)$ but $\tau \circ \sigma = (1\,3) \circ (1\,2) = (1\,2\,3)$.
- Disjoint cycles commute.
- Cyclically permuting the elements of a cycle doesn't change the cycle.
- If $\sigma = (a_1 a_2 \ldots a_m) \implies |\sigma| = m$.
- If σ's cycle decomposition is $(a_{1,1}a_{1,2}\ldots a_{1,m_1})(a_{2,1}a_{2,2}\ldots a_{2,m_2})\ldots(a_{k,1}a_{k,2}\ldots a_{k,m_k})$ then $|\sigma| = \text{lcm}(m_1, m_2, \ldots, m_k)$.

2.5 The Quaternion Group

This is an important group which is isomorphic to some subsequent examples:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

And the group operation . is defined with the following relations:

$$\begin{gathered} 1.a = a.1 = a \quad (-1).a = a.(-1) = -a \quad \text{for all } a \in Q_8 \\ (-1).(-1) = 1 \\ i.i = j.j = k.k = -1 \\ i.j = -k \quad j.i = k \\ j.k = -i \quad k.j = i \\ k.i = -j \quad i.k = j \end{gathered}$$

Q_8 is clearly non-abelian.

2.6 Homomorphisms and Isomorphisms

Definition 2.7. A **homomorphism** is a map between the sets of 2 groups, $(G, \star)$ and $(H, \diamond)$, $\phi : G \to H$ such that $\forall x, y \in G$:

$$\phi(x \star y) = \phi(x) \diamond \phi(y)$$

If the map ϕ is a bijection, then we call it an **isomorphism**.

eg. $\phi : R \to R^+$ defined as $\phi(x) = e^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$, since $\phi(x + y) = e^{x+y} = e^x \times e^y = \phi(x) \times \phi(y)$

Some important points are:

- If ϕ is an isomorphism from G to H, then ϕ^{-1}, which exists since ϕ is bijective, is an isomorphism from H to G. This is denoted by $G \cong H$.
- $\cong$ is an equivalence relation.
- $G \cong H \implies$
  - $|G| = |H|$
  - G is abelian $\iff$ H is abelian
  - $\forall x \in G \ |x| = |\phi(x)|$
- If A and B are sets then $|A| = |B| \iff S_A \cong S_B$.

Since $\cong$ is an equivalence relation, we can define isomorphism classes. One of the central problems in mathematics is to determine what properties of a structure specifies its isomorphism class.

Theorems which specify such properties are known as *classification* theorems. eg:

$$\text{any non-abelian group of order 6} \cong S_3$$

$\text{Aut}(G)$ is defined to be the set of all isomorphisms from the group G to itself, called automorphisms.

Exercise 3. Prove that $\text{Aut}(G)$ is a group under function composition.

Solution.
If ϕ and τ are 2 bijections $G \to G$, then so is $\phi \circ \tau$.
$\forall x, y \in G$

$$(\phi \circ \tau)(xy) = \phi(\tau(x)\tau(y)) = (\phi \circ \tau)(x)(\phi \circ \tau)(y)$$

where the first equality follows since τ is an automorphism.

Hence, $\phi, \tau \in \text{Aut}(G) \implies \phi \circ \tau \in \text{Aut}(G)$.

The identity of the group is clearly $1 : 1(g) = g \quad \forall g \in G$

And the inverses exist because of the bijectivity of the maps.

Exercise 4. Let G be a finite group with an automorphism σ such that $\sigma(g) = g \iff g = 1$. If σ^2 is the identity map, prove that G is abelian.

Solution.
First we consider the map $\phi : G \to G$ defined as

$$\phi(x) = x^{-1}\sigma(x)$$

Also, $\sigma(x)\sigma(x^{-1}) = 1 \implies (\sigma(x))^{-1} = \sigma(x^{-1})$.
To show that ϕ is a bijection:

$$\begin{aligned} x^{-1}\sigma(x) &= y^{-1}\sigma(y) \\ \implies yx^{-1} &= \sigma(y)(\sigma(x))^{-1} \\ \implies yx^{-1} &= \sigma(yx^{-1}) \\ \implies yx^{-1} &= 1 \\ \therefore y &= x \end{aligned}$$

Hence, $\phi(x) = \phi(y) \iff x = y$. Thus, each element $g \in G$ can be written as $x^{-1}\sigma(x)$ for some $x \in G$.
Now, consider $\sigma(g) = \sigma(x^{-1}\sigma(x)) = \sigma(x^{-1})\sigma^2(x) = (\sigma(x))^{-1}x = g^{-1}$

$$\sigma(g) = g^{-1} \quad \forall g \in G$$

Therefore $\forall a, b \in G$:

$$\begin{aligned} \sigma^2(ab) &= \sigma(\sigma(ab)) \\ \implies ab &= \sigma(b^{-1}a^{-1}) \\ \implies ab &= \sigma(b^{-1})\sigma(a^{-1}) \\ \implies ab &= ba \end{aligned}$$

2.7 Group Actions

Definition 2.8. A **group action** of a group on a set A is a map: $G \times A \to A$ denoted by $g.a \quad \forall g \in G, a \in A$, such that:

- $g_1.(g_2.a) = (g_1 g_2).a \quad \forall g_1, g_2 \in G, a \in A$
- $1.a = a \quad \forall a \in A$

If we were to take a group action and then focus on some single g in G, then the map becomes $A \to A$. We denote it by σ_g, and $\sigma_g(a) = g.a$.

Proposition. σ_g is a permutation of the set acted upon, A, for all $g \in G$.

Proof. Consider $\sigma_{g^{-1}}$. For all $a \in A$

$$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(g.a) \\ &= g^{-1}.(g.a) \\ &= (g^{-1}g).a = 1.a = a \quad \text{Using the properties of a group action}\end{aligned}$$

Similarly, $(\sigma_g \circ \sigma_{g^{-1}})(a) = a$ for all $a \in A$.

Since, the map has a two-sided inverse, it is a bijection/permutation of A. □

Proposition. The map, ϕ, from G to the symmetric group S_A, $g \to \sigma_g$ is a homomorphism.

Proof. We need to show that $\phi(g_1 g_2)$ is the same permutation as $\phi(g_1) \circ \phi(g_2)$.

For all $a \in A$:

$$\begin{aligned}\phi(g_1 g_2)(a) &= (g_1 g_2).a \\ &= g_1.(g_2.a) \\ &= \sigma_{g_1}(\sigma_{g_2}(a)) \\ &= (\phi(g_1) \circ \phi(g_2))(a)\end{aligned}$$

□

Thus, a group action can be represented by assigning a permutation of the set to each element of the group, such that the permutations obey the group structure.

Some terms related to group actions are:

- The group action which sends each $g \in G$ to the identity map of A is called the *trivial action*.
- If each element of the group induces a distinct permutation, then the action is said to be *faithful*.
- The *kernel* of an action is the set of elements of the group mapped to the identity permutation.

eg. The group action of D_{2n} on the set $\{1, 2, \ldots, n\}$ defined by $(\alpha, i) \to \sigma_\alpha(i)$. This approach also leads to the conclusion that $D_6 \cong S_3$, since the group action gives a homomorphism from D_6 to S_3, which will also be injective since they have an equal number of elements.

Chapter 3

Subgroups

3.1 Basics

Looking at smaller parts of a mathematical object that also satisfy the same axioms is an important technique. This is the motivation for the following definition:

Definition 3.1. A **subgroup** H of a group G is a non-empty subset of G which is closed under the group operation and inverses, that is:

$$x, y \in H \implies xy, x^{-1} \in H$$

this is denoted by $H \leq G$.

From the definition, it is clear that any subgroup contains the identity of the group and follows associativity over the group operation.

eg. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$, $\{1\} \leq G$ for all group and is called the *trivial subgroup*, $\{1, r, r^2, \ldots, r^{n-1}\} \leq D_{2n}$.

A non-example: $\mathbb{Z}^+$ is not a valid subgroup of $(\mathbb{Z}, +)$, since it is not closed under taking inverses.

Proposition. *The Subgroup Criterion:* A subset H is a valid subgroup of $G \iff \forall x, y \in H$, $xy^{-1} \in H$, and H is non-empty.

Proof. The forward implication is obvious. For the converse:

Since H is non-empty, we can take $x \in H \implies xx^{-1} = 1 \in H$

$1 \in H$ can be used to claim that $x \in H \implies 1x^{-1} = x^{-1} \in H \therefore H$ is closed under inverse.

$x, y \in H \implies x, y^{-1} \in H \implies x(y^{-1})^{-1} = xy \in H \therefore H$ is also closed under the group operation.

Hence, H is a subgroup of G. □

Also, a finite subgroup can only contain elements of finite order due to being closed under multiplication i.e. $\{x, x^2, x^3, \ldots\}$ has $x^a = x^b$ for some $a, b, b > a \implies x^{b-a} = 1$.

Exercise 5. *The torsion subgroup.* Let G be an abelian group. Prove that $\{g \in G \mid |g| < \infty\}$ is a subgroup of G.

Solution. 1 clearly belongs to the given set (name it H).

Let $x, y \in H$ and $|x| = n, |y| = m$. Then, $(xy)^{nm} = x^{nm}y^{nm} = 1$ since G is abelian.

Hence, $|xy| \leq nm < \infty \implies xy \in H$.

Also, $x \in H, |x| = n \implies x^{-1} \in H \because |x^{-1}| = |x| = n$.

Therefore, H is non-empty and closed under multiplication and inverse $\implies H$ is a subgroup of G.

The abelian nature of G was important here. Consider the non-example:

$GL_2(\mathbb{R}) = \{A | A \text{ is a } 2 \times 2 \text{ matrix with entries from } \mathbb{R} \text{ and } \det(A) \neq 0\}$.

Consider the elements of G, $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$. $A^2 = B^2 = I \implies |A| = |B| = 2$ and $A, B \in H$

Now consider $C = AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = I + X$ where $X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, and $X^2 = 0$

$\therefore C^n = (I + X)^n = I + nX = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq I$ for any $n > 0 \implies |C| = \infty \therefore C \notin H$

Hence, H is not closed under multiplication and not a subgroup.

Exercise 6. Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined as

$$a \sim b \iff a = h.b \text{ for some } h \in H$$

is an equivalence relation.

Solution.

By the property of a group action $1.a = a \implies a \sim a$.

Also, if for some $h \in H, h.a = b$ then

$$\begin{aligned} & h^{-1}.(h.a) = h^{-1}.b \\ \implies & (h^{-1}h).a = 1.a = a = h^{-1}.b \\ & \therefore b \sim a \implies a \sim b \end{aligned}$$

If there are $h_1, h_2 \in H$ such that $a = h_1.b$ and $b = h_2.c$, then

$$a = h_1.b = h_1.(h_2.c) = (h_1h_2).c$$

$$\therefore a \sim b, b \sim c \implies a \sim c$$

Hence, we can conclude that $\sim$ is an equivalence relation.

For each $x \in A$, the equivalence class of x under $\sim$ is called the *orbit* of x under the action.

Exercise 7. Let H be a subgroup of the finite group G. Let H act on G by left multiplication, i.e. $h.g : H \times G \to G$ is defined as $h.g = hg$ for all $h \in H, g \in G$. Let $x \in G$ and let $\mathcal{O}_x$ be the orbit of x under this action. Prove that the map, ϕ_x

$$H \to \mathcal{O}_x \quad \text{defined as } h \mapsto hx$$

is a bijection.

Solution.

If $\phi_x(h_1) = \phi_x(h_2)$ then $h_1x = h_2x \implies h_1 = h_2$. ϕ_x is injective.

Also, for each $a \in \mathcal{O}_x$, by definition of an orbit, there is some $h \in H$ such that $a = h.x = hx$. ϕ_x is surjective.

Hence, we can conclude that ϕ_x is a bijection.

This gives us that $|H| = |\mathcal{O}_x|$.

We also know that the orbits of the set acted upon partition it, since they are equivalence classes.

This leads to:

Theorem 1 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.*

3.2 Centralizers and Normalizers

Let A be a non-empty subset of the group G.

Definition 3.2. Let $C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the **centralizer** of A in G.

$\because gag^{-1} = a \implies ga = ag$, the centralizer can also be defined as the set of elements of G that commute with all the elements of A.

Proposition. $C_G(A)$ is a subgroup of G.

Proof. The identity commutes with all the elements by definition, so $1 \in C_G(A)$.

Let $x, y \in C_G(A)$, then for all $a \in A$

$$\begin{aligned} & xya = xay = axy \quad \text{since } x, y \text{ commute with } a \\ \implies & xy \in C_G(A) \\ & x^{-1}a = (xa^{-1})^{-1} = ax^{-1} \\ \implies & x^{-1} \in C_G(A) \end{aligned}$$

Hence, $C_G(A)$ is a subgroup. □

The *center* of G denoted by $Z(G)$ is defined as $C_G(G)$.

Definition 3.3. Define gAg^{-1} as $\{gag^{-1} \mid a \in A\}$. Then the **normalizer** of A is defined as the set $N_G(A) = \{g \in G \mid gAg^{-1} = A\}$.

This is a generalization of the centralizer since it doesn't require g to commute with all the elements of the set. $C_G(A) \leq N_G(A)$.

If G is abelian, then for any $A \subset G$, $N_G(A) = C_G(A) = G$.

eg. Consider $A = \{1, r, r^2, r^3\} \subset D_8$.

To compute $C_{D_8}(A)$, we first consider the fact that all powers of r commute with each other, hence $1, r, r^2, r^3 \in C_{D_8}(A)$.

Next consider s. $sr = r^{-1}s \neq rs$, hence $s \notin C_{D_8}(A)$. Since, $C_{D_8}(A)$ is a subgroup of D_8, if any element of the form $sr^i \in C_{D_8}(A)$, then $sr^i r^{-i} = s$ also would be in $C_{D_8}(A)$, which isn't possible.

Hence, $C_{D_8}(A) = \{1, r, r^2, r^3\} = A$

To compute $N_{D_8}(A)$, we know that $A \in N_{D_8}(A)$, so we proceed to check s.

$sAs^{-1} = \{s1s^{-1}, srs^{-1}, sr^2s^{-1}, sr^3s^{-1}\} = \{1, r^{-1}, r^{-2}, r^{-3}\} = \{1, r^3, r^2, r\} = A$

Hence, $s \in N_{D_8}(A)$. Since $N_{D_8}(A)$ is a subgroup, and closed under multiplication, all elements of the form sr^j also $\in N_{D_8}(A)$. $N_{D_8}(A) = D_8$.

3.3 Stabilizers, Kernels of Group Actions

These concepts deal with inferring the structure of a group based on the *sets it acts on.*

Definition 3.4. If G is a group which acts on a set S, then the **stabilizer** of $s \in S$ is the set

$$G_s = \{g \in G \mid g.s = s\}$$

From the property of a group action, $1 \in G_s$.
Also, if $y \in G_s$, then $y^{-1}.s = y^{-1}.(y.s) = (y^{-1}y)s = s \implies y^{-1} \in G_s$
if $x, y \in G_s$, then $(xy).s = x.(y.s) = x.s = s \implies xy \in G_s$
Hence, G_s is a subgroup of G.

We can also show that the kernel of a group action is a subgroup:
$1.s = s$ for all $s \in S$, so $1 \in$ the kernel.
$x.s = s$ for all $s \in S \implies x^{-1}.s = x^{-1}.(x.s) = s$ for all $s \in S$, hence, $x^{-1} \in$ the kernel.
$x.s = y.s = s$ for all $s \in S \implies (xy).s = x.(y.s) = x.s = s$ for all $s \in S$, hence, $xy \in$ the kernel.

The following example provides some geometric intuition for these concepts for the case of D_8.
Consider the set $A = \{\{1, 3\}, \{2, 4\}\}$ of the unordered pairs of the opposite vertices of a square.
D_8 acts on A:
Let $a = \{1, 3\}, b = \{2, 4\}$
As can be geometrically seen, $(1, r^2, s, sr^2)$ send a, b to themselves, while (r, r^3, sr, sr^3) send a to b, and b to a.
From here, we can confirm that:
$g_1.(g_2.x) = (g_1g_2).x$ for all $g_1, g_2 \in D_8, x \in A$.
And, the stabilizer for both a and b is (the subgroup) $\{1, r^2, s, sr^2\}$, which is also the kernel for the group action.

Now, we show that $C_G(A), N_G(A)$ being subgroups of G is a special case of the stabilizer and kernel being subgroups.
Consider the power set of the group, $S = \mathcal{P}(G)$, and let G act on S by conjugation, i.e. for $g \in G, B \in S$

$$g.B = gBg^{-1} = \{gbg^{-1} \mid b \in B\} \in S$$

Now, for any $A \in S$, $N_G(A)$ is the stabilizer of A under this action, which is a subgroup of G.
Now, let $N_G(A)$ act on the set A by conjugation, i.e. for $g \in N_G(A), a \in A$:

$$g.a = gag^{-1}$$

Here, $C_G(A)$ is precisely the kernel of the above action, hence $C_G(A) \leq N_G(A) \leq G$.

3.4 Cyclic groups and Cyclic subgroups

Definition 3.5. A group H is **cyclic** if it can be generated by a single element $\in H$. i.e. $H = \{x^n | n \in \mathbb{Z}\}$. This is denoted by $H = \langle x \rangle$.

It can be noted that a cyclic group is necessarily abelian.

Proposition. If $H = \langle x \rangle$, then $|H| = |x|$. Specifically,

1. if $|H| = n < \infty$, then $x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements of H.
2. if $|H| = \infty$, then $x^n \neq 1$ for any $n \neq 0$.

Proof. Let $|x| = n < \infty$, then $1, x, x^2, \ldots, x^{n-1}$ are necessarily distinct elements, since $x^a = x^b$ for some $0 \leq a < b < n \implies x^{b-a} = 1$ with $b - a < n$ which contradicts the definition of the order of an element.
Now, consider x^t, $t \in \mathbb{Z}$. By the Division Algorithm: $t = nq + r$ where $n, q, r \in \mathbb{Z}$ and $0 \leq r < n$
Hence, $x^t = (x^n)^q x^r = x^r \in \{1, x, x^2, \ldots, x^{n-1}\}$.
$\implies H = \{1, x, x^2, \ldots, x^{n-1}\}$ and $|H| = n$.
If $|x| = \infty$, then distinct powers of x will be distinct elements of H, hence $|H| = \infty$.
□

Theorem 2. *Any 2 cyclic groups of the same order are isomorphic.*

1. *For $n \in \mathbb{Z}^+$ and with $\langle x \rangle$, $\langle y \rangle$ two cyclic subgroups of order n, the map:*

$$\phi : \langle x \rangle \to \langle y \rangle \equiv \phi(x^k) = y^k$$

is an isomorphism.

2. *For $\langle x \rangle$, an infinte cyclic group, consider the cyclic group $\mathbb{Z} = \langle 1 \rangle$. Then the map:*

$$\phi : \mathbb{Z} \to \langle x \rangle \equiv \phi(k) = x^k$$

is an isomorphism.

Proposition. Let G be a group, and let $x \in G$, $a \in \mathbb{Z} - \{0\}$:

1. If $|x| = \infty$, then $|x^a| = \infty$.
2. If $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$.

Proof. For 1: If the $|x^a| = m < \infty$, then $x^{am} = 1 \implies |x| | |am|$ which cannot be true.
For 2: Let $(n, a) = d$, then $n = db, a = dc$, where $(b, c) = 1$.
Then, $(x^a)^b = x^{dbc} = (x^n)^c = 1 \implies |x^a|$ divides b.
But, $(x^a)^k = 1 \implies x^{ak} = 1 \implies n$ divides ak, hence, db divides $dc \cdot |x^a|$.
Since, $(b, c) = 1$, we have b divides $|x^a|$. Given the 2 equations, we have $|x^a| = b = \dfrac{n}{(n, a)}$. □

Proposition. Let $H = \langle x \rangle$.

1. If $|x| = \infty$, then $H = \langle x^a \rangle \iff a = \pm 1$.
2. If $|x| = n < \infty$, then $H = \langle x^a \rangle \iff (a, n) = 1 \implies$ the number of generators of $H = \varphi(n)$.

Proof. If $|x| = \infty$ and $\langle x^a \rangle = \langle x \rangle$, then $x^a \neq x^b$ for all $a \neq b \implies \exists m \in \mathbb{Z}$ for all $n \in \mathbb{Z}$ such that $(x^a)^m = x^n \implies am = n \implies a|n$. The only integers which divide all integers are $1, -1$.

The reverse implication is obvious from the definition of a cyclic group.

For the second case: If $\langle x^a \rangle = H$ then $|x^a| = |x| = n \implies \frac{n}{(n,a)} = n$. Hence, $(n, a) = 1$.

For the converse, we already have that $|\langle x^a \rangle| = |\langle x \rangle| = n$, and we also have that $\langle x^a \rangle \leq \langle x \rangle$, hence the 2 groups must be the same. □

Theorem 3. *Let $H = \langle x \rangle$*

1. *$K \leq H \implies K = \{1\}$ or $K = \langle x^k \rangle$ where k is the* minimum positive integer *such that $x^k \in K$.*
2. *If $|H| = n < \infty$, then for each positive integer a which divides n there is a* unique *subgroup of H of order a. This subgroup is $\langle x^d \rangle, d = \dfrac{n}{a}$.*

   And for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that the subgroups of H are in bijection with the positive divisors of n.
3. *If $|H| = \infty$, then for distinct non-negative integers a, b: $\langle x^a \rangle \neq \langle x^b \rangle$, and for any integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$. So, the subgroups of H are in bijection with $\{0, 1, 2, 3, \ldots\}$.*

Proof. (1) Consider the non-trivial case when $K \neq \{1\}$. If this is the case, then $x^a, x^{-a} \in K$ for some $a \in \mathbb{Z} - \{0\}$.

Now consider the non-empty set $S = \{p \mid x^p \in K, p \in \mathbb{Z}^+\}$. By the Well-Ordering Principle of positive integers, there is a $k = \min(S)$.

K being a subgroup $\implies \langle x^k \rangle \leq K$.

$K \leq \langle x \rangle$ tells us that $z \in K \implies z = x^a$ for some $a \in \mathbb{Z}$.

By the division principle, $a = nk + r$ with $0 \leq r < k$, hence:

$$z(= x^a) \in K \implies z(x^k)^{-n} = x^{nk+r}x^{-nk} = x^r \in K$$

If $r \in S$ then $k = \min(S)$ is contradicted $\implies r = 0$, and $z \in K \implies z = x^{nk}$.

This gives us $K \leq \langle x^k \rangle$. And we can conclude that $K = \langle x^k \rangle$

□

Proof. (2) $\langle x^d \rangle$ is a valid subgroup since, $|\langle x^d \rangle| = \dfrac{n}{(n, a)} = \dfrac{n}{a} = d$, $(n, a) = a$ since $a|n$.

For $a = 1$, the unique subgroup is clearly $\{1\} = \langle 1 \rangle = \langle x^n \rangle$.

For $a > 1$, let there be a subgroup $K \leq H$ such that $|K| = a$. From (1), we have that $K = \langle x^k \rangle$ where k is the smallest positive integer such that $x^k \in K$.

We have that $|K| = \dfrac{n}{(n, k)} = \dfrac{n}{d} \implies (n, k) = d$, $d|k$. This gives us that $x^k \in \langle x^d \rangle \implies K \leq \langle x^d \rangle$. But, $|K| = |\langle x^d \rangle| = a \implies K = \langle x^d \rangle$, hence it is the unique subgroup of order a.

For any integer m, since $(n, m)|m$, we have that $x^m \in \langle x^{(n,m)} \rangle \implies \langle x^m \rangle \leq \langle x^{(n,m)} \rangle$.

$\dfrac{n}{(n, m)} = \dfrac{n}{(n, (n, m))}$, hence $|\langle x^m \rangle| = |\langle x^{(n,m)} \rangle|$. And so, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$. □

Exercise 8. Let p be an odd prime, and $n > 1$ be a positive integer. First show that $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ and $(1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$. Hence $|1+p| = p^{n-1}$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Solution.
Call $s_p(x)$ as the highest power of the prime p dividing x.
First observe that if $z \equiv 1 \pmod{p}$ and $s_p(z-1) = \beta$, then

$$\begin{aligned} z^p - 1 &= \sum_1^{p-1} \binom{p}{r} (z-1)^r + (z-1)^p \\ &= \sum_1^{p-1} p^{r\beta+1}\gamma_r + p^{p\beta}\gamma_p \\ &= p^{\beta+1}\left(\sum_1^{p-1} \gamma_r p^{(r-1)\beta} + \gamma_p p^{(p-1)\beta-1}\right) = p^{\beta+1}(\gamma_1 + kp) \end{aligned}$$

where $s_p(\gamma_i) = 0$. This follows because $s_p(\binom{p}{r}) = s_p(p!) - s_p((p-r)!) - s_p(r!) = 1 - 0 - 0 = 1$ for $0 < r < p$.
Hence for $p > 2$, $s_p(z^p - 1) = \beta + 1 = s_p(z-1) + 1$.
Now, consider $1 + p$. We thus have, $s_p((1+p)^p - 1) = 2 \implies (1+p)^p \equiv 1 \pmod{p^2} \equiv 1 \pmod{p}$.
Repeating this,

$$s_p((1+p)^{p^2} - 1) = s_p((1+p)^p - 1) + 1 = 3 \implies (1+p)^{p^2} \equiv 1 \pmod{p^3} \equiv 1 \pmod{p}$$

And so on, hence

$$s_p((1+p)^{p^{n-2}} - 1) = n - 1 \implies (1+p)^{p^{n-2}} \equiv 1 \pmod{p^{n-1}} \not\equiv 1 \pmod{p^n}$$

$$s_p((1+p)^{p^{n-1}} - 1) = n \implies (1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$$

Using this in the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$, we have: $|1+p|$ divides p^{n-1}, but doesn't divide p^{n-2}.
Hence, $|1+p| = p^{n-1}$.

3.5 Subgroups generated by subsets of a group

As we defined the cyclic subgroups generated by an element, we can do the same for multiple elements of a general group. The idea is to define a *minimal* subgroup, such that any other subgroup containing the given subset also contain the minimal subgroup.

Definition 3.6. If $A \subseteq G$, then:

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

is called the subgroup *generated* by A.

It is a subgroup since the intersection of any collection of subgroup is one.
Moreover, if we call $\mathcal{A}$ as the set of all the subgroups containing A, then their intersection will be the unique minimal subgroup containing A, i.e. $H \in \mathcal{A} \implies \langle A \rangle \leq H$
A clear but unweildy method to construct $\langle A \rangle$ for a finite A is to take the set of all finite products of the elements and their inverses (called *words*).
For $A = \{a_1, a_2, \ldots, a_n\}$:

$$\langle A \rangle = \{b_1^{\epsilon_1} b_2^{\epsilon_2} \ldots b_l^{\epsilon_l} \,|\, l \in \mathbb{Z},\ l \geq 0,\ b_i \in A,\ \epsilon_i = \pm 1\ \forall i\}$$

Chapter 4

Quotient Groups and Homomorphisms

4.1 Basics

The basic idea of this concept is to again try and create smaller groups from a given one, to study its structure.

As it turns out, if we have a homomorphism between G and H and we consider the *set of the sets* of elements in G that the homomorphism maps to the same element in H (the fibers of the map), then the set has the properites of a group.

Say, elements in X_a get mapped to $a \in H$ and the same happens for X_b, b, then the intuitive group operation for the set of fibers we can guess is: $X_a.X_b = X_{ab}$, which satisfies the group axioms.

It is this set of fibers of a homomorphism that we term a **quotient group.**

Definition 4.1. If $\varphi : G \to H$ is a homomorphism, then the **kernel** of φ is the set:

$$\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}$$

Proposition. For the groups G, H and the homomorphism $\varphi : G \to H$:

1. $\varphi(1_G) = 1_H$.
2. $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.
3. $\varphi(g^n) = \varphi(g)^n$
4. $\ker \varphi$ is a subgroup of G
5. $\text{im}(\varphi)$ is a subgroup of H

Proof. (1) $\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)\varphi(1_G) \implies \varphi(1_G)^{-1}\varphi(1_G) = 1_H = \varphi(1_G)$.

(2) $\varphi(g)\varphi(g^{-1}) = \varphi(1_G) = 1_H \implies \varphi(g^{-1}) = \varphi(g)^{-1}$.

(3) Base case: $\varphi(g^1) = \varphi(g)^1$
Assume: $\varphi(g^{n-1}) = \varphi(g)^{n-1}$ for some $n > 1$
$\varphi(g^n) = \varphi(g.g^{n-1}) = \varphi(g)\varphi(g^{n-1}) = \varphi(g)^n$. Hence proved.

(4) From (1), $1_G \in \ker \varphi$ hence it is non-empty.
If $x, y \in \ker \varphi$, then $\varphi(xy) = \varphi(x)\varphi(y) = 1_H 1_H = 1_H \implies xy \in \ker \varphi$
Also, $\varphi(x^{-1}) = \varphi(x)^{-1} = 1_H^{-1} = 1_H \implies x^{-1} \in \ker \varphi$, hence $\ker \varphi$ is closed under multiplication and inverse, hence it is a subgroup of G.

(5) $1_H \in \text{im}(\varphi)$, hence it is non-empty. If $x, y \in \text{im}(\varphi)$ then there exist $a, b \in G$ such that $\varphi(a) = x, \varphi(b) = y$.

Consider $\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = xy^{-1}$. Hence, $xy^{-1} \in \text{im}(\varphi)$ and by the subgroup criterion, $\text{im}(\varphi)$ is a subgroup of H. □

Definition 4.2. For the usual G, H, φ with $\ker\varphi = K$, the **quotient group** or the factor group, G/K, read as G modulo K, is the group whose elements are the fibers of φ, with the group operation defined as $X_a.X_b = X_{ab}$, where $X_i \subseteq G$ is the fiber mapped by φ to $i \in H$

eg. consider $\varphi : \mathbb{Z} \to Z_n = \langle x \rangle$ (the cyclic group of order n), $\varphi(a) = x^a$

Here the fiber over x^a is $\varphi^{-1}(a) = \{m \mid m \in \mathbb{Z},\ x^m = x^a \implies x^{m-a} = 1\}$
$= \{m \mid m \in \mathbb{Z},\ n|(m-a)\} = \bar{a}$

Hence, the elements are exactly the residue classes modulo n. The group operation between them is $\bar{a}.\bar{b} = \bar{a} \circ \bar{b} = \overline{a+b}$ where we replaced $\circ$ with the group operation of $\mathbb{Z}$. And the kernel of this map is $\bar{0}$.

Hence, $\mathbb{Z}/\bar{0} = (\mathbb{Z}/n\mathbb{Z}, +)$, where $\bar{0}$ is the residue class of 0 modulo n.

Now, we show that the fibers of a homomorphism are a special type of subsets of the group.

Proposition. For the usual G, H, φ with the kernel, K, let $X \in G/K$ be the fiber above $a \in H$, then:

1. For any $u \in X$, $X = \{uk \mid k \in K\}$
2. For any $u \in X$, $X = \{ku \mid k \in K\}$

Proof. Let $uK = \{uk \mid k \in K\}$.

Consider any $x \in X \implies \varphi(x) = a$. If we let $k = u^{-1}x$, then $\varphi(k) = \varphi(u^{-1})\varphi(x) = a^{-1}a = 1_H$.

Hence, $k \in K$, and $x = uk \implies X \subseteq uK$.

Now, take any $uk \in uK$. $\varphi(uk) = \varphi(u)\varphi(k) = a1_H = a \implies uk \in X$. Hence, $uK \subseteq X$.

Combining the 2, $uK = X$.

Using the same notation, and similar arguments, we can show $Ku = X$. □

4.2 Cosets

The idea of forming sets using a subgroup and an element from the group ($\ker\varphi$ and u above), using left and right multiplication can be made more general through the following:

Definition 4.3. For any $N \leq G$ and $g \in G$ define:

$$gN = \{gn \mid n \in N\}$$
$$Ng = \{ng \mid n \in N\}$$

These are called the **left and right coset** of N in G, and any element of these is called a representative.

The reason the element g need not be specifically specified follows because:

Proposition. For $N \leq G$: the set of left cosets of N in G form a partition of G.

And $\forall\ u, v \in G,\ uN = vN \iff v^{-1}u \in N \iff u, v$ are the representatives of the same coset ($uN = vN$)

Proof. Since N is a subgroup, it contains 1, hence for all $g \in G$, $g \in gN$.

Let uN and vN be 2 intersecting cosets. This implies $\exists\, n, m \in N$ such that:

$$\begin{aligned} un &= vm \\ \implies u &= vmn^{-1} = vz \end{aligned}$$

where due to N being a subgroup $z = mn^{-1} \in N$

Hence, for any $ux \in uN$ $(x \in N)$, $ux = vzx = vy \in vN$ since $y = zx \in N$. This gives $uN \subseteq vN$.

Similarly, $v = unm^{-1} = uz', z' \in N$. And for any $vx' \in vN$ $(x' \in N)$, $vx' = uz'x' = uy' \in uN \because y' = z'x' \in N$. This gives $vN \subseteq uN$.

Which leads to $uN = vN$. Hence, there are no intersecting left cosets of N in G i.e. they form a partition of G.

For the next part, $uN = vN \implies un = vm$ where $n, m \in N \implies v^{-1}u = mn^{-1} \in N$

For the reverse implication, if $v^{-1}u \in N$, then $u \in vN$. But $u = u1 \in uN$, hence uN and vN intersect $\implies uN = vN$.

$u \in vN$ is the same as saying that u, v are the representatives of the same left coset $= vN = uN$ $\square$

What this means is that, given a coset, we can use *any* of its elements to generate the entire coset by left/right multiplication with the subgroup. This gives us:

Theorem 4. *Let G be a group and let K be the kernel of some homomorphism from G to another group. Then the set whose elements are the left cosets of K (which has been proven to be a subgroup) in G, with the operation defined by:*

$$uK \circ vK = (uv)K$$

forms a group, G/K.

For the operation to be well defined we need to show that taking any 2 elements from the 2 cosets gives a member of the resulting coset:

Fix $u, v \in G$, $\forall\, u' = uk_1 \in uK, v' = vk_2 \in vK$:

$\varphi(u'v') = \varphi(uk_1vk_2) = \varphi(u)1\varphi(v)1 = \varphi(uv)$.

Thus, $u'v'$ belongs to the same fiber as uv, which by a previous proposition is nothing but uvK.