Abstract Algebra

Group Theory

Alex Feng

2023

Contents

Chapter 1

Introduction to Groups

1.1 Basic Axioms

Definition 1.1.1: Binary Operation

1. A binary operation $*$ on a set G is a function $* : G \times G \to G$. For any $a, b \in G$, we write $a * b$ for $*(a, b)$.

2. A binary operation $*$ on a set G is associative if

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

3. If $*$ is a binary operation on G, elements $a, b \in G$ commute if $a * b = b * a$. We say $*$ (or G) is commutative if

$$\forall a, b \in G, a * b = b * a$$

Example 1.1.1 (Binary Operations)

Commutative:
- $+$, usual addition on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$
- $\times$, usual multiplication on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$

Noncommutative:
- $-$, usual subtraction on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$ (Not a binary operation on $\mathbb{Z}^+, \mathbb{Q}^+$, or $\mathbb{R}^+$)
- Cross product of two vectors in $\mathbb{R}^3$ (also not associative)

Let $*$ be a binary operation on set G and $H \subseteq G$. H is said to be closed under $*$ if

$$\forall a, b \in H, a * b \in H$$

Additionally, if $*$ is associative or commutative on G, it retains the same property when it is restricted to H.

Definition 1.1.2: Group

An ordered pair $(G, *)$ is a group (for a set G under binary operation $*$) if:

1. $\forall a, b, c \in G, (a * b) * c = a * (b * c)$ ($*$ is associative),

2. $\exists e \in G, \forall a \in G, a * e = e * a = a$ (existence of identity element),

3. $\forall a \in G, \exists a^{-1} \in G, a * a^{-1} = a^{-1} * a = e$ (existence of inverse)

$(G, *)$ is called abelian if $\forall a, b \in G, a * b = b * a$

Note:-

We (informally) say G is a group under $*$ if $(G, *)$ is a group, or even just G is a group. G is a finite group if G is a finite set.

Example 1.1.2 (Groups)

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are groups under $+$ ($e = 0, a^{-1} = a$). $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q}^+$, and $\mathbb{R}^+$ are groups under $\times$ ($e = 1, a^{-1} = \frac{1}{a}$). $\mathbb{Z} - \{0\}$ is not a group under $\times$ because not every element has an inverse. Vector spaces are abelian groups under addition (due to their axioms).

Proposition 1.1.1

Let $(G, *)$ be a group. Then

1. the identity of G is unique
2. the inverse of each element in G is unique
3. $\forall a \in G, (a^{-1})^{-1} = a$
4. $(a * b)^{-1} = b^{-1} * a^{-1}$
5. for any $a_1, a_2, \ldots, a_n \in G$, $a_1 * a_2 * \cdots * a_n$ is independent of how it is bracketed (generalized associative law).

Proof: 1. Suppose f and g are both identities. By the group definition axiom, $f * g = f$ and $f * g = g$. Thus, $g = f$ and the identity is unique

2. Assume b and c are both inverses of a. By the group definition axiom, $a * b = e$ and $c * a = e$. Then,

$$\begin{aligned} c &= c * e \\ &= c * (a * b) \\ &= (c * a) * b \\ &= e * b \\ &= b \end{aligned}$$

3. Read part 2 with a and a^{-1} interchanged.
4. Let $c = (a * b)^{-1}$. Then,

$$\begin{aligned} (a * b) * c &= e \\ a * (b * c) &= e \\ a^{-1} * a * (b * c) &= a^{-1} * e \\ (a^{-1} * a) * (b * c) &= a^{-1} \\ e * (b * c) &= a^{-1} \\ b * c &= a^{-1} \end{aligned}$$

Repeating the process for b^{-1} shows that $c = b^{-1} * a^{-1}$

Note:-

For simplicity, abstract groups such as G and H will be written with binary operation $\cdot$ and $a \cdot b$ will be written as ab. Brackets will not be used if the generalized associative law applies. For an abstract group $(G, \cdot)$, the identity will be denoted by 1. $x \in G, n \in \mathbb{Z}^+$, the product $xx \cdots x$ (with n terms) will be denoted x^n.

Proposition 1.1.2

For a group G, with $a, b \in G$,

$$au = av \implies u = v$$

and

$$ub = vb \implies u = v.$$

Definition 1.1.3: Order of Element

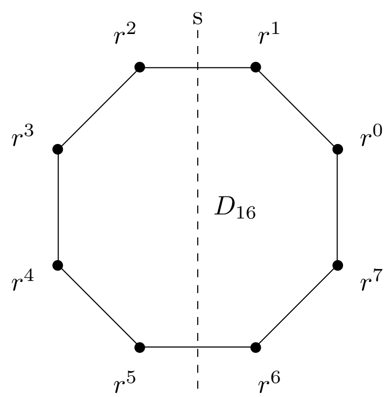
For a group G and $x \in G$, the order of x, denoted $|x|$, is the smallest positive integer n such that $x^n = 1$. x is said to be of infinite order if no such n exists.

1.2 Dihedral Groups

Definition 1.2.1: Dihedral Group

For each $n \in \mathbb{Z}^+, n \geq 3$, D_{2n} is the set of symmetries r and s of a regular n-gon (rotation by $\frac{2\pi}{n}$ and flipping over a line of symmetry).

The symmetries are represented by permutations on $\{1, 2, \ldots, n\}$, and D_{2n} is a group under function composition.



Proposition 1.2.1

1. $|r| = n$
2. $|s| = 2$
3. $s \neq r^i$ for any i
4. $D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$
5. $rs = sr^{-1}$ (which shows that D_{2n} is not abelian)
6. $r^i = sr^{-i}$

For a group G, $S \subseteq G$ with the property that every element of G can be written as as (finite) product of elements in S and their inverses is a set of generators of G (S generates G). The equations that the generators satisfy are called relations (in G). For some collection of relations, $R_1, R_2, \ldots, R_m$ such that the relation among any element can be deduced, the presentation of G is written

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

Example 1.2.1 (Presentation of Dihedral Group)

The presentation of Dihedral group of order $2n$ is

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

1.3 Symmetric Groups

Definition 1.3.1: Set of all Permutations

Let Ω be any nonempty set. S_Ω is the set of all permuations of Ω. It is denoted S_n in the special case when $\Omega = \{1, 2, \ldots, n\}$.

Under function composition, S_Ω is called the symmetric group on the nonemptyset Ω. For symmetric groups, we now use cycle decomposition notation, which is much more efficient. If $a_i \mapsto a_{i+1}$ for $1 \leq i \leq m-1$ and $a_m \mapsto a_1$, with k cycles, we write

$$(a_1 \ a_2 \ \ldots \ a_{m_1})(a_{m_1+1} \ a_{m_1+2} \ \ldots \ a_{m_2}) \ldots (a_{m_{k-1}+1} \ a_{m_{k-1}+2} \ \ldots \ a_{m_k})$$

The length of a cycle is the number, t, of integers appearing in it, called a $t-cycle$. Two cycles are disjoint if they have no numbers in common. Elements that are mapped to themselves aren't written in cycle decomposition.

Note:-

Since the binary operation is function composition, the product of two cycles $(1\ 2) \circ (2\ 3)$, shortened to $(1\ 2)(2\ 3)$ when the context is clear, is equal to $(1\ 2\ 3)$ since function composition is read right to left.

1.4 Matrix Groups

Definition 1.4.1: Field

A field is a set F under two binary operations $+$ and $\cdot$ such that $(F, +)$ and $(F - \{0\}, \cdot)$ are an abelian groups following the distributive law:

$$\forall a, b, c \in F, a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Let $F^\times = F - \{0\}$ for any field F.

Example 1.4.1 (Fields)

A few examples of fields include

- $\mathbb{Q}$
- $\mathbb{R}$
- For a prime p, $\mathbb{Z}/p\mathbb{Z}$, which will be denoted $\mathbb{F}_p$

Definition 1.4.2: General Linear Group of Degree n

Let $M_{n\times n}$ be the set of all $n \times n$ matrices. For any $n \in \mathbb{Z}^+$,

$$\mathrm{GL}_n(F) = \{A \in M_{n\times n} \mid \det(A) \neq 0\}$$

The order of a finite field is equal to p^m for some prime p and integer m. Additionally, for a field F,

$$|F| = q < \infty \implies |\mathrm{GL}_n(F)| = \prod_{m=0}^{n-1} (q^n - q^m)$$

1.5 The Quaternion Group

Definition 1.5.1: The Quaternion Group

The quaternion group, Q_8, is defined by

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

with product $\cdot$ computed as follows:

$$\forall a \in Q_8, 1 \cdot a = a \cdot 1 = a$$

$$(-1) \cdot (-1) = 1$$

$$\forall a, \in Q_8 (-1) \cdot a = a, a \cdot (-1) - a$$

$$i \cdot i = j \cdot j = k \cdot k = -1$$

$$\begin{aligned} i \cdot j &= k, & j \cdot i &= -k \\ j \cdot k &= i, & k \cdot j &= -i \\ k \cdot i &= j, & i \cdot k &= -j. \end{aligned}$$

1.6 Homomorphisms and Isomorphisms

Definition 1.6.1: Homomorphism

Let $(G, *)$ and $(H, \cdot)$ be groups. A homomorphism is a map $\varphi : G \to H$ such that

$$\forall x, y \in G, \varphi(x * y) = \varphi(x) \cdot \varphi(y)$$

Definition 1.6.2: Isomorphism

An isomorphism is a bijective homomorphism. Two isomorphic groups G and H can be written $G \cong H$.

Example 1.6.1 (Isomorphisms)

- The identity map is an obvious isomorphism.
- $\exp : \mathbb{R} \to \mathbb{R}^+$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}^+, \times)$.

It is easy to see if two groups are not isomorphic. For an isomorphism $\varphi : G \to H$,

- $|G| = |H|$
- G is abelian iff H is abelian
- $\forall x \in G, |x| = |\varphi(x)|$

1.7 Group Actions

Definition 1.7.1: Group Action

A group action of a group G on a set A is a map from $G \times A$ to A, written as $g \cdot a$ for all $g \in G$ and $a \in A$, that satisfies the following properties:

1. $\forall g_1, g_2 \in G, a \in A, g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, and
2. $\forall a \in A, 1 \cdot a = a$.

Note:-

We say that G is a group acting on a set A.

Let the group G act on the set A. For each fixed $g \in G$, we get a map $\sigma_g : A \to A$ defined by

$$\sigma_g(a) = g \cdot a.$$

Proposition 1.7.1

1. For each fixed $g \in G$, σ_g is a permutation of A, and
2. The map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism (and it is called the permutation representation associated to the given action).

Proof:

1. σ_g is a map from A to A, and it can be shown to be a permutation if it is bijective (and has a two-sided inverse).

$$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \\ &= g^{-1} \cdot (g \cdot a) \\ &= (g^{-1} g) \cdot a \\ &= 1 \cdot a = a\end{aligned}$$

Then $\sigma_{g^{-1}} \circ \sigma_g : A \to A$ is the identity map. g was arbitrary and we can interchange the roles of g and g^{-1} to obtain $\sigma_g \circ \sigma_{g^{-1}}$ is also the identity map. Then, σ_g has a two-sided inverse, hence is a permuatation of A.

2. Let $\varphi : G \to S_A$ be defined by $g \mapsto \sigma_g$ (and note that we just proved $\sigma_g \in S_A$). For all $a \in A$,

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

Thus, φ is a homomorphism.

Chapter 2

Subgroups

2.1 Definitions

Definition 2.1.1: Subgroup

Let G be a group. $H \subseteq G$ is a subgroup of G if $H \neq \emptyset$ and

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

$H \leq G$ denotes that H is a subgroup of G. $H < G$ denotes proper containment.

If G is a group and $H \leq G$, H has the same binary operation on G and is a group.

Example 2.1.1 (Subgroups)

- $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ under addition.
- All groups have trivial subgroup $\{1\}$ called the trivial subgroup, henceforth denoted by 1.
- Let $H = \{1, r, r^2, \ldots, r^{n-1}\}$. H is closed under the binary operation of D_{2n} and $H \subseteq D_{2n}$ so $H \leq D_{2n}$.
- The set of all even integers is a subgroup of $\mathbb{Z}$ under addition.

Proposition 2.1.1 The Subgroup Criterion

Let G be a group. $H \subseteq G$ is a subgroup if and only if

1. $H \neq \emptyset$
2. $\forall x, y \in H, xy^{-1} \in H$.

Proof: 1. and 2. must obviously hold if $H \leq G$.
To show that the converse holds, let $x \in H$ (since $H \neq \emptyset$). Letting $y = x$ implies that $xx^{-1} \in H$, so $1 \in H$. Then, H must contain the elements 1 and x, so it must also contain $1x^{-1}$ and $x^{-1} \in H$, implying that H is closed under taking inverses.
Finally, if $x, y, y^{-1} \in H \implies x(y^{-1})^{-1} \in H$. Then, $xy \in H$. Hence, H is a subgroup of G.

2.2 Centralizers, Normalizers, Stabilizers, and Kernels

Definition 2.2.1: Centralizer

The centralizer of nonempty $A \subseteq G$ in group G is the subset of G

$$C_G(A) = \{g \in G \mid \forall a \in A, gag^{-1} = a\}$$

$C_G(A)$ contains all elements of G that commute with every element in A.

To show that $C_G(A) \leq G$, we first see that $1 \in C_G(A) \implies G_G \neq \emptyset$. Secondly, assume that $x, y \in C_G(A)$, or

$$\forall a \in A, xax^{-1} = a, yay^{-1} = a$$

$$\begin{aligned}(xy)a(xy)^{-1} &= (xy)a(y^{-1}x^{-1}) \\ &= x(yay^{-1})x^{-1} \\ &= xax^{-1} \\ &= a\end{aligned}$$

Then, $x, y \in C_G(A) \implies xy \in C_G(A)$. Observe that $xax^{-1} = a \implies a = x^{-1}ax$ so $\forall x \in C_G(A), x^{-1} \in C_G(A)$. Therefore, $C_G(A)$ is a subgroup.

Example 2.2.1 (Centralizers of Groups)

- If G is an abelian group, $\forall A \subseteq G, C_G(A) = G$
- $C_{Q_8}(i) = \{\pm 1, \pm i\}$

Definition 2.2.2: Center

The center of G is the subset

$$Z(G) = C_G(G) = \{g \in G \mid \forall x \in G, gx = xg\}$$

This is the set of all elements commuting with all elements of G.

Definition 2.2.3: Normalizer

Define

$$gAg^{-1} = \{gag^{-1} \mid a \in A\}.$$

The normalizer of A in G is the set

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

If G is a group acting on set S, for some fixed $s \in S$ the stabilizer of s in G is the set

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

The kernel of the action of G on S is defined as

$$\{g \in G \mid \forall s \in S, g \cdot s = s\}$$

2.3 Cyclic Groups and Cyclic Subgroups

Definition 2.3.1: Cyclic Group

A group H is cyclic if

$$\exists x \in H, H = \{x^n \mid n \in \mathbb{Z}\}$$

Equivalently, H is cyclic if it can be generated by a single element.

Observe that $H = \langle x \rangle \implies H = \langle x^{-1} \rangle$. Additionally, note that all cyclic groups are abelian.

Proposition 2.3.1

$$H = \langle x \rangle \implies |H| = |x|$$

(one side being infinite implies that the other is too.)
More specifically,

1. $|H| = n < \infty \implies x^n = 1$ and $1, x, x^2, \ldots, x^{n-1}$ are all distinct elements in H
2. $|H| = \infty \implies (\forall n \neq 0, x^n \neq 1) \wedge (\forall a \neq b \in \mathbb{Z}, x^a \neq x^b)$

Proposition 2.3.2

Let G be an arbitrary group, $x \in G$, and $m, n \in Z$.

$$x^n = 1 \wedge x^m = 1 \implies x^{(m,n)} = 1.$$

In particular,

$$x^m = 1 \implies (|x|) \mid m.$$

Proof: By the Euclidean Algorithm, $\exists r, s \in \mathbb{Z}, (m, n) = mr + ns$. Thus,

$$x^{(m,n)} = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1.$$

Theorem 2.3.1 Cyclic Group Isomorphism

1. If $n \in \mathbb{N}$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n, there exists a well defined isomorphism

$$\varphi : \langle x \rangle \to \langle y \rangle$$
$$x^k \mapsto y^k$$

2. If $\langle x \rangle$ is an infinite cyclic group, there exists a well defined isomorphism

$$\varphi : \mathbb{Z} \to \langle x \rangle$$
$$k \mapsto x^k$$

Proof: Let $\langle x \rangle$ and $\langle y \rangle$ be cyclic groups of order n and $\varphi : \langle x \rangle \to \langle y \rangle, x^k \mapsto y^k$. To prove φ is well defined

$(x^r = x^s \implies \varphi(x^r) = \varphi(x^s))$, $x^{r-s} = 1$ so, by proposition 2.3.2, $n \mid r - s$. Then,

$$\begin{aligned} r &= tn + s \\ \varphi(x^r) &= \varphi(x^{tn+s}) \\ &= y^{tn+s} \\ &= (y^n)^t y^s \\ &= y^s = \varphi(x^s) \end{aligned}$$

Thus, φ is well defined. $\varphi(x^a x^b) = \varphi(x^a)\varphi(x^b)$ so φ is a homomorphism. All elements y^k have a preimage x^k so the map is surjective. The groups have the same finite order so φ must be bijective if it is a surjection. Thus, φ is an isomorphism. If $\langle x \rangle$ has infinite order, let well defined map $\varphi : \mathbb{Z} \to \langle x \rangle, k \mapsto x^k$. $\forall a \neq b \in \mathbb{Z}, x^a \neq x^b$ so it is injective. φ is surjective by the definition of a cyclic group. Then, φ is an isomorphism.

Now, let $\langle x \rangle$ be an infinite cyclic group, and $\varphi : \mathbb{Z} \to \langle x \rangle, k \mapsto x^k$. φ is obviously well defined, and since $a \neq b \implies x^a \neq x^b$, φ is injective. φ is surjective by the definition of a cyclic group, and it can be verified to be a homomorphism. Thus, φ is an isomorphism.

From now on, let for each $n \in \mathbb{N}$, let Z_n denote the cyclic group of order n, written multiplicatively.

Proposition 2.3.3

Let G be a group, $x \in G$, $z \in \mathbb{Z} - \{0\}$

1. $|x| = \infty \implies |x^a| = \infty$
2. $|x| = n < \infty \implies |x^a| = \frac{n}{(n,a)}$
3. $|x| = n < \infty \wedge (a \in \mathbb{Z}^+, a \mid n) \implies |x^a| = \frac{n}{a}$

Proof: Suppose that $|x| = \infty$ but $|x^a| = m < \infty$. By the definition of order,

$$1 = (x^a)^m = x^{am}$$

$$x^{-am} = (x^{am})^{-1} = 1$$

Either am is positive or $-am$ is, so there exists a positive power of x equal to the identity, which is a contradiction.

Let $y = x^a, (n,a) = d, n = db, a = dc$ for $b, c \in \mathbb{Z}, b > 0$. d is the gcd of n and a so $(b,c) = 1$. To show that $|y| = b$,

$$y^b = x^{ab} = x^{dcb} = (x^n)^c = 1$$

so $(|y|) \mid b$. Then,

$$x^{a|y|} = y^{|y|} = 1$$

It follows that $n \mid (a|y|)$ so $b \mid (c|y|)$. $(b,c) = 1$ so $b \mid (|y|)$. $b \mid (|y|)$ and $(|y|) \mid b$ implies that $|y| = b$. Thus, $n = d|y|$ and $|y| = \frac{n}{d}$

Proposition 2.3.4

Let $H = \langle x \rangle$.

1. $|x| = \infty \implies (H = \langle x^a \rangle \iff a = \pm 1)$
2. $|x| = n < \infty \implies (H = \langle x^a \rangle \iff (a,n) = 1)$. Note that the number of generators of H is $\varphi(n)$ (where φ is Euler's φ-function)

Proof: If $|x| = n < \infty$, x^a generates a subgroup of H of order $|x^a|$. This subgroup equals H if and only if $|x^a| = |x|$.

$$|x^a| = |x| \iff \frac{n}{(a,n)} = n$$

Then $(a,n) = 1$, and by definition $\varphi(n)$ is the number of such generators.

Theorem 2.3.2

Let $H = \langle x \rangle$ be a cyclic group.

1. $K \leq H \implies (K = \{1\}) \vee (K = \langle x^d \rangle)$, where d is the smallest positive integer such that $x^d \in K$.
2. $|H| = \infty \implies \forall a \neq b \in \mathbb{N}, \langle x^a \rangle \neq \langle x^b \rangle$. Additionally, $\forall m \in \mathbb{Z}, \langle x^m \rangle = \langle x^{|m|} \rangle$, so the nontrivial subgroups of H correspond bijectively with $\mathbb{N}$.
3. $|H| = n < \infty$ implies that for each $a \in \mathbb{N}, a|n$ there is a unique subgroup of H of order a, $\langle x^d \rangle, d = \frac{n}{a}$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so the subgroups of H correspond bijectively with the positive divisors of n.

Proof: Let $K \leq H$. The proposition is true for $K = \{1\}$, so assume $K \neq \{1\}$. Thus, $\exists a \neq 0, x^a \in K$.

$$a < 0 \implies x^{-a} = (x^a)^{-1} \in K$$

so K always contains a positive power of x. Let

$$\mathcal{P} = \{b \mid b \in \mathbb{Z}^+ \wedge x^b \in K\}$$

There must exist a minimum element $d \in \mathcal{P}$. K is a subgroup and $x^d \in K$ so $\langle x^d \rangle \leq K$. $K \leq H$ so any element in K is of the form x^a for some integer a.

$$a = qd + r, \quad 0 \leq r < d$$

$$x^r = x^a (x^d)^{-q} \in K$$

since both $x^a, x^d \in K$. By minimality of d, $r = 0$ so $x^a = (x^d)^q \in \langle x^d \rangle$. Thus, $K \leq \langle x^d \rangle$, and since $\langle x^d \rangle \leq K$, $\langle x^d \rangle = K$

Assume $|H| = n < \infty$ and $a \mid n$. Let $d = \frac{n}{a}$ so $\langle x^d \rangle$ so is a subgroup of order a, showing its existence. To show uniqueness, suppose K is any order a subgroup of H, with

$$K = \langle x^b \rangle$$

for the minimum positive integer b such that $x^b \in K$.

$$\frac{n}{d} = a = |K| = |x^b| = \frac{n}{(n,b)}$$

so $d = (n, b)$ and $d \mid b$. Then, $x^b \in \langle x^d \rangle$, hence

$$K \leq \langle x^d \rangle$$

$|\langle x^d \rangle| = a = |K|$ so $K = \langle x^d \rangle$. $\langle x^m \rangle$ and $\langle x^{(n,m)} \rangle$ have the same order and $(n, m) \mid n$. Thus, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$

Chapter 3

Quotient Groups and Homomorphisms

3.1 Definitions

Definition 3.1.1: Kernel

The kernel of homomorphism $\varphi : G \to H$ is the set

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

Proposition 3.1.1

Let G and H be groups and $\varphi : G \to H$ be a homomorphism.

1. $\varphi(1_G) = 1_H$ (1_G and 1_H are identities of G and H, respectively)
2. $\forall g \in G, \varphi(g^{-1}) = \varphi(g)^{-1}$
3. $\forall n \in \mathbb{Z}, \varphi(g^n) = \varphi(g)^n$
4. $\ker \varphi \leq G$
5. The image of G under φ, $\text{im}(\varphi) \leq H$

Definition 3.1.2: Quotient Group

Let $\varphi : G \to H$ be a homomorphism with kernel K. The quotient group, G/K (read G modulo K) is the group whose elements are fibers (set of preimages) of φ, with group operation such that if X and Y are the fibers above a and b respectively, the product of X and Y is the fiber above the product ab.

Proposition 3.1.2

Let $\varphi : G \to H$ be a homomorphism of groups with kernel K. Let $X = \varphi^{-1}(a)$. Then,

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

Proof: Let $u \in X$. By definition of X, $\varphi(u) = a$. Let

$$uK = \{uk \mid k \in K\}$$

To prove $uK \subseteq X$,

$$\begin{aligned}\forall k \in K, \varphi(uk) &= \varphi(u)\varphi(k) \\ &= \varphi(u)1 \\ &= a\end{aligned}$$

so $uk \in X \implies uK \subseteq X$. To prove the reverse inclusion, let $g \in X$ and $k = u^{-1}g$.

$$\begin{aligned}\varphi(k) = \varphi(u^{-1})\varphi(g) &= \varphi(u)^{-1}\varphi(g) \\ &= a^{-1}a = 1\end{aligned}$$

So $k \in \ker\varphi$, and $g = uk \in uK$, establishing $X \subseteq uK$. Therefore, $X = uK$.

Definition 3.1.3: Coset

For any $N \leq G$ and $g \in G$,

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

are the left and right cosets of N in G, respectively. Any element of a coset is called a representative for it.

Theorem 3.1.1

Let G be a group and K be the kernel of some homomorphism from G to another group. The set of left cosets of K in G with operation defined by

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

forms a group, G/K. This operation is well defined in the sense that $u_1 \in uK \wedge v_1 \in vK \implies u_1v_1 \in uvK$. Additionally, $u_1v_1K = uvK$ so the multiplication doesn't depend on choice of representatives (element in coset) for the cosets. This statement is true when "left coset" is interchanged "right coset."

Proof: Let $X, Y \in G/K$ and $Z = XY \in G/K$ (by definition). Then, X, Z, and Z are (left) cosets of K. Assume K is the kernel of some homomorphism $\varphi : G \to H$ so $X = \varphi^{-1}(a)$ and $Y = \varphi^{-1}(b)$ for some $a, b \in H$. By the definition of the G/K operation, $Z = \varphi^{-1}(ab)$. Let $u \in X$ and $v \in Y$ be arbitrary representatives their cosets, so $\varphi(u) = a, \varphi(v) = b, X = uK, Y = vK$.

$$\begin{aligned}uv \in Z &\iff uv \in \varphi^{-1}(ab) \\ &\iff \varphi(uv) = ab \\ &\iff \varphi(u)\varphi(v) = ab\end{aligned}$$

The latter equality holds so $uv \in Z \implies Z = uvK$. Thus, $XY = uvK$ for any representatives $u \in X, v \in Y$. The last statement follows since $\forall u \in G, uK = Ku$.

It is important to note that multiplication is independent of the representative chosen. $\overline{u}$ can be used to denote a coset uK, and $\overline{G}$ can denote G/K. Then, $\overline{u} \cdot \overline{v} = \overline{uv}$.

Example 3.1.1

- If $\varphi : G \to H$ is an isormorphism, $K = 1$ and the fibers of φ each contain one element, so $G/1 \cong G$.
- Let G be any group and $H = 1$ be a group of order 1. $\varphi : G \to H, g \in G \mapsto 1$ is the trivial homomorphism. $\ker\varphi = G$ and $G/G \cong Z_1 = \{1\}$.
- Define $\varphi : Q_8 \to V_4$ by
$$\pm 1 \mapsto 1, \ \ \pm i \mapsto a, \ \ \pm j \mapsto b, \ \ \pm k \mapsto c$$
$\ker\varphi = \{\pm 1\}$ and $Q_8/\langle \pm 1\rangle$ can be thought of as the "absolute value" of Q_8.

Proposition 3.1.3

Let $N \leq G$. The set of left cosets of N in G form a partition of G. Additionally,

$$\forall u, v \in G, uN = vN \iff v^{-1}u \in N$$

$$uN = vN \iff u \in vN \wedge v \in uN$$

Proof:

$$N \leq G \implies 1 \in N$$
$$\forall g \in G, g = g \cdot 1 \in gN$$
$$G = \bigcup_{g \in G} gN$$

To show that $uN \cap vN \neq \emptyset$, let $x \in uN \cap vN$, for some $n, m \in N$,

$$x = un = vm$$

$$u = vmn^{-1} = vm_1$$
$$\forall ut \in uN, ut = (vm_1)t = v(m_1 t) \in vN.$$

Thus, $uN \subseteq vN$. u and v can be interchanged to obtain that $vN \subseteq uN$. Therefore, $uN \cap vN \neq \emptyset \implies uN = vN$.

$$uN = vN \iff u \in vN \iff n \in N, u = vn \iff v^{-1}u \in N$$

Proposition 3.1.4

Let G be a group and $N \leq G$.

1. The operation described by
$$uN \cdot vN = (uv)N$$
is well defined if and only if $\forall g \in G, n \in N, gng^{-1} \in N$.

2. If the operation is well defined then the set of left cosets of N in G is a group. The identity is $1N$ and $(gN)^{-1} = g^{-1}N$.

Proof: First assume

$$\forall u, v \in G, u, u_1 \in uN \wedge v, v_1 \in vN \implies uvN = u_1 v_1 N.$$

Let $g \in G$ and $n \in N$. If $u = 1, u_1 = n, v = v_1 = g^{-1}$ then

$$1g^{-1}N = ng^{-1}N$$

$$1 \in N \implies ng^{-1} \cdot 1 \in ng^{-1}N$$
$$ng^{-1} \in g^{-1}N \implies ng^{-1} = g^{-1}n_1$$

for some $n_1 \in N$. Thus, $gng^{-1} = n_1 \in N$. Now assume $\forall g \in G, n \in N, gng^{-1} \in N$. Let $u, u_1 \in uN$ and $v, v_1 \in vN$. For some $n, m \in N$,

$$u_1 = un$$

$$v_1 = vm$$

To prove $u_1 v_1 \in uvN$,

$$\begin{aligned} u_1 v_1 &= (un)(vm) = u(vv^{-1})nvm \\ &= (uv)(v^{-1}nv)m = (uv)(n_1 m) \end{aligned}$$

where $n_1 = v^{-1}nv \in N$. Now N is closed under products so $n_1 m \in N$ and $u_1 v_1 = (uv)n_2$ for some $n_2 \in N$. Thus, uvN and $u_1 v_1 N$ contain the common element $u_1 v_1$.

Definition 3.1.4: Normal Subgroup

gng^{-1} is the conjugate of $n \in N$ by g. $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is the conjugate of N by g. g is said to normalize N if $gNg^{-1} = N$. A subgroup N of G is said to be normal (denoted $N \trianglelefteq G$) if $\forall g \in G, gNg^{-1} = N$.

Theorem 3.1.2

Let $N \trianglelefteq G$. The following are equivalent:

1. $N \trianglelefteq G$
2. $N_G(N) = G$
3. $\forall g \in G, gN = Ng$
4. The set of left cosets form a group under the operation described in proposition 3.1.4
5. $\forall g \in G, gNg^{-1} \subseteq N$

Proposition 3.1.5

For some $N \leq G$ and homomorphism φ,

$$N \trianglelefteq G \iff N = \ker \varphi$$

Proof: $N = \ker \varphi \implies \forall g \in G, gN = Ng$ so N will be normal. Conversely, let $H = G/N$ and $\pi : G \to G/N$ defined by $\forall g \in G, g \mapsto gN$.

$$\pi(g_1 g_2) = (g_1 g_2)N = g_1 N g_2 N = \pi(g_1)\pi(g_2)$$

so π must be a homomorphism.

$$\begin{aligned} \ker \pi &= \{g \in G \mid \pi(g) = 1N\} \\ &= \{g \in G \mid gN = 1N\} \\ &= \{g \in G \mid g \in N\} = N \end{aligned}$$

Definition 3.1.5: Natural Projection

Let $N \trianglelefteq G$. The homomorphism $\pi : G \to G/N$ defined by $g \mapsto gN$ is called the natural projection (homomorphism) of G onto G/N. If $\overline{H} \leq G/N$, the complete preimage of $\overline{H}$ in G is the preimage of $\overline{H}$ under the natural projection homomorphism.

Example 3.1.2

Let G be a group

- $G/1 \cong G, \quad G/1 \trianglelefteq G$
  $G/G \cong 1, \quad G/G \trianglelefteq G$
- If G is abelian, $\forall N \leq G, N \trianglelefteq G$, because

  $$\forall g \in G, n \in N, gng^{-1} = gg^{-1}n = n \in N$$

  Note that only N being abelian is not sufficient.
  Suppose $G = Z_k$. Let x be a generator of G and $N \leq G$. $N = \langle x^d \rangle$, where d is the smallest power of x that lies in N.

  $$G/N = \{gN \mid g \in G\} = \{x^\alpha \mid \alpha \in \mathbb{Z}\}$$

and since $x^\alpha N = \langle xN \rangle^\alpha$, $G/N = \langle xN \rangle$.

$$|xN| = d = \frac{|G|}{|N|}.$$

Thus, quotient groups of a cyclic group are cyclic.

- Generalizing the previous example, $N \leq Z(G) \implies N \trianglelefteq G$.

3.2 Lagrange's Theorem

Theorem 3.2.1 Lagrange's Theorem
If G is a finite group and $H \leq G$, $|H| \mid |G|$, and the number of left cosets of H in G equals $|G|/|H|$.

Proof: Let $|H| = n$ and let the number of left cosets of H in G equal k. The set of left cosets of H in G partition G. The map

$$H \to gH \quad \text{defined by} \quad h \mapsto gh$$

is surjective. This map is injective because $gh_1 = gh_2 \implies h_1 = h_2$. Thus,

$$|gH| = |H| = n.$$

G is partitioned into k disjoint subsets each with cardinality n, so $|G| = kn$. Thus,

$$k = \frac{|G|}{n} = \frac{|G|}{|H|}.$$

Chapter 4

Group Actions

Chapter 5

Direct and Semidirect Products