# Summary for Modern Algebra I

SEUNGWOO HAN

David S. Dummit, Richard M. Foote. *Abstract Algebra*.
3rd ed., Wiley, 2003.

# Contents

# Chapter 1

# Groups

## 1.1 Definitions and Examples of Groups

**Definition 1.1.1: Abelian Group**

An *abelian group* is a nonempty set $G$ equipped with a binary operation $+$ on $G$ that satisfies the following.

(i) (associative) $\forall a, b, c \in G,\ a + (b + c) = (a + b) + c$.
(ii) (commutative) $\forall a, b \in G,\ a + b = b + a$.
(iii) (identity) $\exists 0 \in G,\ \forall a \in G,\ a + 0 = 0 + a = a$.
(iv) (inverse) $\forall a \in G,\ \exists b \in G,\ a + b = b + a = 0$.

**Note:-**

One may easily show that the identity is unique, and for each $a \in G$, an inverse of $a$ is unique.

**Notation 1.1.2**

- We define $-\colon G \times G \to G$ by $a - b = a + (-b)$.
- We write, for each positive integer $n$, and for each $a \in G$,

$$na \triangleq \underbrace{a + a + \cdots + a}_{n \text{ times}}, \qquad 0a \triangleq 0_G, \qquad (-n)a \triangleq \underbrace{(-a) + (-a) + \cdots + (-a)}_{n \text{ times}}.$$

- Hence, $\forall m, n \in \mathbb{Z},\ \forall a \in G,\ (m + n)a = ma + na \wedge m(na) = (mn)a$.

**Example 1.1.3**

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, equipped with their ordinary additions, are abelian groups, while $(\mathbb{N}, +)$ is not.
(ii) $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, and $\mathbb{C} \setminus \{0\}$, equipped with their ordinary multiplications, are abelian groups.
(iii) If $G = \{1, -1, i, -i\} \subseteq \mathbb{C}$, then $(G, \cdot)$ is an abelian group. One may explicitly write the *group table* for this.
(iv) $\mathrm{GL}_n(\mathbb{C}) = \{\, n \times n \text{ invertible matrices over } \mathbb{C} \,\}$ (general linear group) equipped with $\cdot$ is not an abelian group but is a group. (See Definition 1.1.4.)

**Definition 1.1.4: Group**

An *group* is a nonempty set $G$ equipped with a binary operation $\cdot$ on $G$ that satisfies the following.

(i) (associative) $\forall a,b,c \in G,\ a\cdot(b\cdot c) = (a\cdot b)\cdot c$.
(ii) (identity) $\exists 1 \in G,\ \forall a \in G,\ a\cdot 1 = 1\cdot a = a$.
(iii) (inverse) $\forall a \in G,\ \exists b \in G,\ a\cdot b = b\cdot a = 1$.

**Theorem 1.1.5**

Let $(G,\cdot)$ be a group. Let $a,b,c \in G$.

(i) $ab = ac \implies b = c$
(ii) $(a^{-1})^{-1} = a$
(iii) $(ab)^{-1} = b^{-1}a^{-1}$

***Proof.*** Trivial. □

**Notation 1.1.6**

- We write, for each positive integer $n$, and for each $a \in G$,

$$a^n \triangleq \underbrace{a\cdot a\cdot\cdots\cdot a}_{n\text{ times}}, \qquad a^0 \triangleq 1_G, \qquad a^{-n} \triangleq \underbrace{a^{-1}\cdot a^{-1}\cdot\cdots\cdot a^{-1}}_{n\text{ times}}.$$

- Hence, $\forall m,n \in \mathbb{Z},\ \forall a \in G,\ a^m a^n = a^{m+n} \wedge (a^m)^n = a^{mn}$.

**Note:-**
We don't generally have $(ab)^n = a^n b^n$.

**Definition 1.1.7: Order**

We write $|G|$ to denote the number of elements in $G$ and call it *order* of $G$.

**Example 1.1.8** Dihedral Groups

$$\begin{aligned} D_n &\triangleq \{\, r_i : [n] \hookrightarrow\!\!\!\!\rightarrow [n] \mid \forall j \in [n],\ r_i(j) = i +_n j \,\} \cup \{\text{reflections???}\} \\ &= \{\,\text{all “rigid motions” for regular } n \text{ polygon}\,\} \end{aligned}$$

Then, $(D_n, \circ)$ is a group where $\circ$ is ordinary function composition operator. We claim that $|D_n| = 2n$ and $D_n$ is not abelian.

***Proof.*** If $r \in D_n$ is a rotation, then □

**Example 1.1.9** Symmetric Group

Let $T$ be a nonempty set. Then, the set $S(T) \triangleq \{\, f : f : T \hookrightarrow\!\!\!\!\rightarrow T \,\}$ with the function composition operator $\circ$ is a group.

We write

$$S_n \triangleq S(\{1,2,\cdots,n\})$$

and call it *symmetric group*. $S_1$ and $S_2$ are abelian, but $S_n$ with $n \geq 3$ is not abelian. $((1\,2\,3)\circ(1\,2) \neq (1\,2)\circ(1\,2\,3))$

**Definition 1.1.10: Group Action**

Let $G$ be a group and $A$ be a set. A group action $G$ on $A$ is a map $f : G \times A \to A$ such that:

(i) $\forall g_1, g_2 \in G$, $\forall a \in A$, $f(g_1, f(g_2, a)) = f(g_1 g_2, a)$.

(ii) $\forall a \in A$, $f(1, a) = a$.

We write $G \curvearrowright A$ to write $G$ acts on $A$.

**Example 1.1.11** Quaternion Group

$Q_8 \triangleq \{\pm 1, \pm i, \pm j, \pm k\}$ as usual.

**Example 1.1.12** General Linear Group

$\mathrm{GL}_n(R)$ is a group of all $n \times n$ invertible matrices over $R$.

**Definition 1.1.13: Direct Product**

If $(G, *_G)$ and $(H, *_H)$ are groups, then the binary operation $*$ on $G \times H$ defined by $(g, h) \times (g', h') \triangleq (g *_G g', h *_H h')$ forms a group $(G \times H, *)$.

## 1.2 Group Homomorphisms

**Definition 1.2.1: Group Homomorphism**

Let $G$ and $H$ be groups. A *group homomorphism* between $G$ and $H$ is a function $f : G \to H$ such that $\forall a, b \in G$, $f(ab) = f(a)f(b)$.

**Definition 1.2.2: Group Isomorphism**

Let $G$ and $H$ be groups. A *group isomorphism* is a bijective group homomorphism between $G$ and $H$. (This means that $G$ and $H$ have the same group structure.) We write $G \cong H$.

**Theorem 1.2.3**

Let $f : G \to H$ be a group homomorphism.

(i) $f(1_G) = 1_H$.

(ii) $\forall a \in G$, $f(a^{-1}) = f(a)^{-1}$.

(iii) $\operatorname{Im} f$ is a group under the group operation under $H$.

(iv) If $f$ is injective, then $G \cong \operatorname{Im} f$.

***Proof.***

(i) $f(1_G)f(1_G) = f(1_G 1_G) = f(1_G) = f(1_G)1_H$. Hence, we have $f(1_G) = 1_H$ from Theorem 1.1.5 (i).

(ii) $f(a^{-1})f(a) = f(a^{-1}a) = f(1_G) = 1_H$ by (i). Hence, $f(a^{-1}) = f(a)^{-1}$.

(iii) Direct from definition.

(iv) Direct from definition. $\square$

**Note:-**

There is only one way—the direct product—to give a group structure on $G \times H$ such that both projections are group homomorphisms.

**Definition 1.2.4: Group Automorphism**

An *automorphism* of $G$ is an isomorphism $G \hookrightarrow\!\!\!\!\rightarrow G$ between $G$ and itself. Then, the collection of all automorhpisms of $G$, $\mathrm{Aut}(G) \triangleq \{\text{automorphisms of } G\}$, equipped with $\circ$, is a group. Moreover, $\mathrm{Aut}(G) \curvearrowright G$ in the natural way $((\sigma, g) \mapsto \sigma(g))$.

**Example 1.2.5**

Fix any $c \in G$ and define $i_c : G \to G$ by $g \mapsto cgc^{-1}$. Then, $i_c \in \mathrm{Aut}(G)$. $i_c$ is called the *inner automorphism on $G$ induced by $c$.*

**Lemma 1.2.6**

Let $G \curvearrowright A$. Then, every $g \in G$ induces a map

$$\begin{aligned} \varphi_g : A &\longrightarrow A \\ a &\longmapsto ga. \end{aligned}$$

Then, $\varphi : G \to S(A)$ defined by $g \mapsto \varphi_g$ is a group homomorphism, which is called the *permutation representation of the group action of $G$ on $A$.*

*Proof.* For each $a \in A$, $(\varphi_{g^{-1}} \circ \varphi_g)(a) = g^{-1}(ga) = (g^{-1}g)a = 1a = a$. Thus, $\varphi_{g^{-1}} \circ \varphi_g = \varphi_g \circ \varphi_{g^{-1}} = \mathrm{id}$. Therefore, $\varphi_g \in S(A)$. It is easy to show that $\varphi$ is a group homomorphism. □

**Lemma 1.2.7**

Let $G$ be a group and let $A$ be a set. If $\varphi : G \to S(A)$ is a group homomorphism, Then, the map $G \times A \to A$ defined by $(g, a) \mapsto \varphi(g)(a)$ is a group action of $G$ on $A$.

*Proof.* Direct from Definition 1.1.10. □

**Theorem 1.2.8**

Let $G$ be a group and let $A$ be a nonempty set. Then, there exists one-to-one correspondence

$$\{\text{all group actions of } G \text{ on } A\} \overset{\text{1-1}}{\longleftrightarrow} \{\text{all group homomorphisms } G \to S(A)\}.$$

*Proof.* Direct from Lemmas 1.2.6 and 1.2.7. □

## 1.3 Subgroups

**Definition 1.3.1: Subgroup**

Let $G$ be a group, and $\varnothing \subsetneq H \subseteq G$. $H$ is a *subgroup* of $G$ if $H$ is a group under the binary operation of $G$. If $H$ is a subgroup of $G$, we write $H \leq G$.

**Note:-**

(i) $1, G \leq G$.
(ii) If $H, K \leq G$ and $H \subseteq K$, then $H \leq K$.
(iii) If $f : H \to G$ is a group homomorphism, then $\operatorname{im}(f) \leq G$.
(iv) If $H \leq G$, then $\mathrm{id}_H : H \hookrightarrow G$ is a group homomorphism.
(v) For all $n \in \mathbb{Z}$, $n\mathbb{Z} = \{ nz \mid z \in \mathbb{Z} \} \leq \mathbb{Z}$.
(vi) $\{ \pm 1, \pm i \} \leq \mathbb{C}^*$.
(vii) $\{ 1, r_1, \cdots, r_{n-1} \} \leq D_n \leq S_n$ and $\{ 1, s \} \leq D_n$.

**Theorem 1.3.2**

TFAE. Let $G$ be a group and $\varnothing \subsetneq H \subseteq G$.
(i) $H \leq G$.
(ii) $\forall a, b \in H, ab \in H$ and $\forall a \in H, a^{-1} \in H$.
(iii) $\forall a, b \in H, ab^{-1} \in H$.

***Proof.*** Implications (i) → (ii) and (ii) → (iii) are trivial. For any $a, b \in H$, we have $1 = aa^{-1} \in H$, $a^{-1} = 1a^{-1} \in H$, and $ab = a(b^{-1})^{-1} \in H$. □

**Definition 1.3.3: Kernel**

Let $f : G \to H$ be a group homomorphism. The *kernel* of $f$ is the set

$$\ker(f) \triangleq \{ g \in G \mid f(g) = 1_H \}.$$

**Example 1.3.4** Kernel

Let $f : G \to H$ be a group homomorphism. Then, $\ker(f) \leq G$ since, $1 \in \ker(f)$ and, for each $a, b \in \ker(f)$, $f(ab^{-1}) = f(a)f(b)^{-1} = 1_H 1_H = 1_H$.

**Corollary 1.3.5**

Let $G$ be a group and let $H$ be a nonempty finite subset of $G$. Then,

$$H \leq G \iff \forall a, b \in H,\ ab \in H.$$

***Proof.*** The direction ($\Leftarrow$) is trivial.

Take any $a \in H$. By the assumption, $a^n \in H$ for all $n \in \mathbb{Z}_+$. As $H$ is finite, there exists $m, n \in \mathbb{Z}_+$ such that $a^n = a^m$. WLOG, $m < n$. Therefore, $1 = a^{n-m} \in H$. Moreover, we have $aa^{n-m-1} = 1$, which implies $a^{-1} = a^{n-m-1} \in H$. Therefore, by Theorem 1.3.2, $H \leq G$. □

**Note:-**

The finite condition in Corollary 1.3.5 is essential since $\mathbb{N} \not\leq \mathbb{Z}$ while $\mathbb{N}$ is closed under addition. ($\mathbb{N}$ is not a group at first.)

**Corollary 1.3.6**

Let $G$ be a group and let $\langle H_i \mid i \in I \rangle$ be an indexed system of subgroups of $G$. Then, $\bigcap_{i \in I} H_i \leq G$.

***Proof.*** Since $1 \in H_i$ for all $i \in I$, $\bigcap_{i \in I} H_i \neq \varnothing$. Take any $a, b \in \bigcap_{i \in I} H_i$. Then, as $\forall i \in I$, $ab^{-1} \in H_i$, we have $ab^{-1} \in \bigcap_{i \in I} H_i$. The result follows from Theorem 1.3.2. □

**Note:-**

Even though $H_1, H_2 \leq G$, it is not guaranteed that $H_1 \cup H_2 \leq G$. For instance, $2\mathbb{Z} \cup 3\mathbb{Z} \nleq \mathbb{Z}$. ($2+3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$.)

**Theorem 1.3.7** Cayley Theorem

Let $G$ be a group. Then, $G \cong H$ for some $H \leq S(G)$.

***Proof.*** Note that $(g, g') \mapsto gg'$ is a group action of $G$ on $G$. Let $\varphi: G \to S(G)$ be the permutation representation of it. We only need to show that $\varphi$ is injective.

Take any $x, y \in G$ and assume $\varphi_x = \varphi_y$. Then, $x = x \cdot 1 = \varphi_x(1) = \varphi_y(1) = y \cdot 1 = y$. Therefore, $G \cong \operatorname{im}(\varphi) \leq S(G)$. □

**Definition 1.3.8: Center**

Let $G$ be a group. The *center* of $G$ is the set

$$Z(G) \triangleq \{\, g \in G \mid \forall a \in G,\ ag = ga \,\}.$$

**Theorem 1.3.9**

Let $G$ be a group. Then, $Z(G)$ is an abelian group.

***Proof.*** Take any $a, b \in Z(G)$. Then for all $g \in G$, $(ab)g = a(gb) = a(gb) = (ag)b = g(ab)$; hence $ab \in Z(G)$. For all $g \in G$, $ga^{-1} = a^{-1}g(aa^{-1}) = a^{-1}(ga)a^{-1} = a^{-1}g(aa^{-1}) = a^{-1}g$; hence $a^{-1} \in Z(G)$. Therefore, $Z(G) \leq G$ by Theorem 1.3.2. $Z(G)$ is abelian by definition. □

**Definition 1.3.10: Centralizer**

Let $G$ be a group and let $\varnothing \subsetneq A \subseteq G$. The *centralizer* of $A$ is the subset

$$C_G(A) = C(A) \triangleq \{\, g \in G \mid \forall a \in A,\ ag = ga \,\}.$$

We may also write $C(a)$ instead of $C(\{a\})$.

**Theorem 1.3.11**

Let $G$ be a group.

(i) $C(A) \leq G$ for any $\varnothing \subsetneq A \subseteq G$.

(ii) $Z(G) = \bigcap_{a \in G} C(a)$.

(iii) $a \in Z(G) \iff C(a) = G$.

***Proof.***

(i) □

## 1.4 Generators of Groups and Free Groups

**Theorem 1.4.1**

Let $G$ be a group and $\varnothing \subsetneq S \subseteq G$. Let $\langle S \rangle$ be the closure of $S$ under the structure $(G, \cdot, ^{-1})$.

(i) $\langle S \rangle \leq G$ and $S \subseteq \langle S \rangle$.

(ii) If $H \leq G$ and $S \subseteq H$, then $\langle S \rangle \subseteq H$.

*Proof.* Trivial. □

**Definition 1.4.2: Generator**

Let $G$ be a group and $\varnothing \subsetneq S \subseteq G$. If $G = \langle S \rangle$, then we say $G$ is *generated by* $S$ and $S$ is a *generator* of $G$. If $S$ is finite, then $G$ is *finitely generated*.

**Example 1.4.3**

(i) A finite group is finitely generated. $G = \langle G \rangle$.
(ii) $\mathbb{Z} = \langle -1 \rangle$ is finitely generated.
(iii) $\mathbb{Q}$ is not finitely generated. If $\mathbb{Q} = \langle p_i/q_i \mid i < n \rangle$, then, for a prime $p \in \mathbb{P}$ such that $\forall i < n$, $p \nmid q_i$, we have $1/p \notin \langle p_i/q_i \mid i < n \rangle$.
(iv) $D_n = \langle r_1, s \rangle$. (This is a minimal representation.)
(v) $Q_8 = \langle i, j \rangle = \langle j, k \rangle = \langle k, i \rangle$.

**Definition 1.4.4: Group Presentation**

We write

$$G = \langle S \mid R \rangle$$

as a way of representing group $G$ in terms of *generator* $S$ and a set of relations $R$.

**Example 1.4.5**

(i) $\mathbb{Z} = \langle 1 \rangle$.
(ii) $D_n = \langle r, s \mid r^n = s^2 = rsrs = 1 \rangle$.

**Theorem 1.4.6**

Let $G = \langle g_1, \cdots, g_k \mid r_1(g_1, \cdots, g_k) = \cdots = r_m(g_1, \cdots, g_k) = 1 \rangle$ be a group presentation. Let $H$ be a group. If $\varphi : \{ g_1, \cdots, g_k \} \to H$ such that $r_i(\varphi(g_1), \cdots, \varphi(g_k)) = 1$ for all $i \in [m]$, then there uniquely exists a group homomorphism $\tilde{\varphi} : G \to H$ such that $\tilde{\varphi}\big|_{\{g_1, \cdots, g_k\}} = \varphi$.

## 1.5 Cyclic Groups

**Definition 1.5.1: Order**

Let $G$ be a group and let $a \in G$. If $a^k = 1$ for some $k \in \mathbb{Z}_+$, then we say $a$ has a *finite order* and the *order of* $a$ is

$$|a| = \min\{ n \in \mathbb{Z}_+ \mid a^n = 1 \}.$$

If $a$ does not have a finite order, we write $|a| = \infty$.

**Example 1.5.2**

(i) If $f : G \xrightarrow{\approx} H$, then $\forall a \in G$, $|a| = |f(a)|$.
(ii) $\forall a \in G$, $|a| = |a^{-1}|$.

(iii) $\forall a \in G$, $(|a| = 1 \iff a = 1)$.
(iv) $\forall m \in \mathbb{Z}_n$, $|m| = n/\gcd(n,m)$.
(v) In $Q_8$, $|1| = 1$, $|-1| = 2$, $|\pm i| = |\pm j| = |\pm k| = 4$.
(vi) In $D_n$, $|r_i| = n/\gcd(n,i)$ and $|s| = 2$.

Note that (v) and (vi) shows that $Q_8 \ncong D_n$.

**Theorem 1.5.3**

Let $G$ be a group. Let $a, b \in G$.

(i) $|a| = \infty \iff \forall i, j \in \mathbb{Z}, (a^i = a^j \implies i = j)$.
(ii) Assume $|a| = n < \infty$.
  (1) $a^k = 1 \iff n \mid k$.
  (2) $a^i = a^j \iff i \equiv j \pmod n$
  (3) If $n = td$, then $|a^t| = d$.
(iii) Assume $ab = ba$, $|a| < \infty$, $|b| < \infty$, and $\gcd(a,b) = 1$. Then, $|ab| = |a|\,|b|$.

***Proof.***

(i) Trivial.
(ii) Basic number theory.
(iii) Let $\alpha \triangleq |a|$, $\beta \triangleq |b|$, and $\ell = \alpha\beta$. Since $(ab)^\ell = 1$, we have $|ab| \le \ell$.

Suppose $(ab)^m < 1$ for some $0 < m < \ell$ for the sake of contradiction. Then, we have $1 = a^{m\alpha} = b^{-m\alpha}$; thus $\beta \mid m$ as $\gcd(a,b) = 1$. Similarly, we have $\alpha \mid m$, which implies $\ell = \alpha\beta \mid m$. This contradicts $m < \ell$. □

**Note:-**

We do not have $|ab| = \operatorname{lcm}(|a|,|b|)$. In $D_3$, $|r_1 s| = 2 \neq 6 = \operatorname{lcm}(|r_1|,|s|)$.

**Corollary 1.5.4**

Let $f : G \to H$ be a group homomorphism. If $g \in G$ has a finite order, then $|f(g)| \mid |g|$.

**Corollary 1.5.5**

Let $G$ be an abelian group in which all elements have finite order. If $c \in G$ has the largest order, then $\forall a \in G$, $|a| \mid |c|$.

***Proof.*** Suppose there exists $a \in G$ such that $|a| \nmid |c|$ for the sake of contradiction. Then, we may write $|a| = p^r m$ and $|c| = p^s n$ where $p$ is a prime number, $\gcd(m,p) = \gcd(n,p) = 1$, and $r > s$. Then, by Theorem 1.5.3 (ii), $|a^m| = p^r$ and $|c^{p^s}| = n$. Therefore, by Theorem 1.5.3 (iii), $|a^m c^{p^s}| = |a^m|\,|c^{p^s}| = p^r n > |c|$, which contradicts the maximality of $|c|$. □

**Definition 1.5.6**

Let $G$ be a group. Then, a subgroup of $G$ of the form

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

is called a *cyclic subgroup generated by* $a$. If $G = \langle a \rangle$, then we say $G$ is a cyclic group.

**Note:-**

Every cyclic group is abelian, but the converse is not true. (e.g. Example 1.4.3 (iii))

**Corollary 1.5.7**

Let $G$ be a group and let $a \in G$.

(i) If $|a| = \infty$, then $\langle a \rangle \cong \mathbb{Z}$.

(ii) If $|a| = n$, then $\langle a \rangle \cong \mathbb{Z}_n$.

This gives the complete classification of cyclic groups.

**Corollary 1.5.8**

Let $G = \langle a \rangle$ be a cyclic group. Let $H$ be a nontrivial subgroup of $G$.

(i) $H = \langle a^k \rangle$ where $k = \min\{ n \mid a^n \in H \}$.

(ii) If $|a| = \infty$, then $\langle 1 \rangle, \langle a \rangle, \langle a^2 \rangle, \cdots$ are all the distinct subgroups of $G$.

(iii) If $|a| = n < \infty$, then $\min\{ n \mid a^n \in H \} \mid n$.

***Proof.***

(i) As $a^i \in H$ for some $i \neq 0$, we may let $k = \min\{ n \mid a^n \in H \}$.

Take any $h \in H$. Then, $h = a^m$ for some $m \in \mathbb{Z}$. There exists $q, r \in \mathbb{Z}$ such that $0 \le r < k$ and $m = kq + r$. Then, $a^r = a^m (a^k)^{-q} \in H$; thus $r = 0$ by minimality of $k$. Hence, $H = \langle a^k \rangle$.

(ii) Trivial.

(iii) Let $d = \gcd(k, n)$. As $d \mid k$, we have $\langle a^k \rangle \subseteq \langle a^d \rangle$. There exist $u, v \in \mathbb{Z}$ such that $d = mu + nv$. Then, $a^d = (a^m)^u (a^n)^v = (a^m)^u$; thus $\langle a^d \rangle \subseteq \langle a^k \rangle$. Hence, $k = d \mid n$. □

**Example 1.5.9**

Let $m, n \in \mathbb{Z}_+$. Then, $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \iff \gcd(m, n) = 1$.

($\Rightarrow$) Suppose $\gcd(m, n) > 1$ for the sake of contradiction. Take any $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Then, $|(a, b)| \mid \operatorname{lcm}(m, n) = mn / \gcd(m, n) < mn$. Hence, $\mathbb{Z}_m \times \mathbb{Z}_n$ has no element of order $mn$; thus $\mathbb{Z}_m \times \mathbb{Z}_n \ncong \mathbb{Z}_{mn}$.

($\Leftarrow$) As $|(1, 0)| = m$ and $|(0, 1)| = n$ in $\mathbb{Z}_m \times \mathbb{Z}_n$, $|(1, 1)| = |(1, 0)(0, 1)| = mn$ by Theorem 1.5.3 (iii). Therefore, $\mathbb{Z}_m \times \mathbb{Z}_n = \langle (1, 1) \rangle \cong \mathbb{Z}_{mn}$. □

## 1.6 Alternating Groups

**Definition 1.6.1: $m$-Cycle**

Permutations of the form $(a_1\, a_2\, \cdots\, a_m)$ is called *$m$-cycles*.

**Note:-**

Some basic facts:

- $S_1, S_2, S_3$ consist of cycles while $S_4$ has a non-cycle $(1\,2)(3\,4)$.
- $(a_1\, a_2\, \cdots\, a_m)^{-1} = (a_m\, a_{m-1}\, \cdots\, a_1)$.
- Every $\sigma \in S_n$ admits a disjoint cycle decomposition. In other words,

$$\sigma = (a_{i_{11}}\, \cdots\, a_{i_{1m_1}})(a_{i_{21}}\, \cdots\, a_{i_{2m_2}}) \cdots (a_{i_{k1}}\, \cdots\, a_{i_{km_k}})$$

where $a_{i_{j\ell}}$s are all different. Moreover, the cycle decomposition is unique up to permutation of the cycles.

- If $\sigma = \sigma_1 \sigma_2 \cdots \sigma_k$ is a disjoint cycle decomposition, then $\sigma^n = \sigma_1^n \sigma_2^n \cdots \sigma_k^n$. Moreover, $|\sigma| = \operatorname{lcm}(|\sigma_1|, |\sigma_2|, \cdots, \sigma_k)$.

**Example 1.6.2** Center of Symmetric Group

$Z(S_2) = S_2$ since $S_2$ is abelian. Fix $n \geq 3$ and consider $S_n$. Let $\sigma \in Z(S_n) \setminus \{(1)\}$. Let $\sigma = (a_1\, a_2\, \cdots\, a_m)\sigma_2 \cdots \sigma_k$ be a disjoint cycle decomposition with $m \geq 2$. Choose $\tau \in S_n$ such that $\tau(a_1) = a_1$ and $\tau(a_2) \neq a_2$. Then, $\sigma(a_1) = \tau\sigma\tau^{-1}(a_1) = \tau\sigma(a_1) = \tau(a_2) \neq a_2$, which is a contradiction. Hence, $Z(S_n) = \{(1)\}$.

**Definition 1.6.3: Transposition**

A *transposition* is a 2-cycle $(a\, b)$.

**Note:-**

- $(a_1\, a_2\, \cdots\, a_m) = (a_1\, a_m)(a_1\, a_{m-1}) \cdots (a_1\, a_2)$.
- By the cyclic decomposition and the equation above, we get the fact that every $\sigma \in S_n$ is a product of transpositions.

**Definition 1.6.4: Parity of Permutation**

For each $\sigma \in S_n$, define $\sigma(\Delta) = \prod_{i \leq i < j \leq n}(x_{\sigma(i)} - x_{\sigma(j)})$ be a polynomial on independent variables $x_1, \cdots, x_n$. Let $\Delta \triangleq (1)(\Delta)$. Then, $\sigma(\Delta) = \pm\Delta$. We define $\varepsilon : S_n \to \{1, -1\}$ by

$$\varepsilon(\sigma) \triangleq \begin{cases} 1 & \text{if } \sigma(\Delta) = \Delta \\ -1 & \text{if } \sigma(\Delta) = -\Delta. \end{cases}$$

**Theorem 1.6.5**

$\varepsilon$ in Definition 1.6.4 is a surjective group homomorphism.

***Proof.*** Take any $\sigma, \tau \in S_n$. Suppose $\sigma(\Delta)$ has exactly $k$ factors of $(x_j - x_i)$ with $j > i$ so that $\varepsilon(\sigma) = (-1)^k$. $\varepsilon(\tau\sigma)\Delta = (\tau\sigma)(\Delta) = \varepsilon(\sigma)\prod_{i \leq i < j \leq n}(x_{\tau(i)} - x_{\tau(j)}) = \varepsilon(\sigma)\varepsilon(\tau)\Delta$. Hence, $\varepsilon(\tau\sigma) = \varepsilon(\sigma)\varepsilon(\tau) = \varepsilon(\tau)\varepsilon(\sigma)$. □

**Definition 1.6.6: Alternating Group**

$$A_n \triangleq \ker(\varepsilon : S_n \to \{\pm 1\})$$

# Chapter 2

# Normal Subgroups and Quotient Groups

## 2.1 Lagrange Theorem

**Definition 2.1.1: Congruence**

Let $K \le G$ and $a, b \in G$. We say *$a$ is congruent to $b$ modulo $K$* if $ab^{-1} \in K$, and write $a \equiv b \pmod{K}$.

**Definition 2.1.2: Coset**

Let $K \le G$ and $a \in G$.
- $Ka \triangleq \{ ka \mid k \in K \}$ is a *right coset of $K$ in $G$*.
- $aK \triangleq \{ ak \mid k \in K \}$ is a *left coset of $K$ in $G$*.

**Note:-**

The relation $\equiv \pmod{K}$ is reflexive, symmetric, and transitive; hence it is a equivalence relation. Then, the equivalence class of $a \in G$ is

$$[a]_K = \{ b \in G \mid b \equiv a \pmod{K} \} = \{ b \in G \mid \exists k \in K,\ b = ka \} = Ka.$$

In other words, $a \equiv b \pmod{K} \iff Ka = Kb$.

One may define $\equiv_l$ by $a \equiv_l b$ iff $a^{-1}b \in K$ so that $[a] = aK$.

**Note:-**

One may note that, if $K$ is just a nonempty subset of $G$, then $\equiv \pmod{K}$ is an equivalence relation if and only if $K \le G$.

**Definition 2.1.3**

Let $K \le G$.

$$G/K \triangleq \{ Ka \mid a \in G \}.$$

**Definition 2.1.4: Index**

The *index of $K$ in $G$* is

$$[G:K] \triangleq |G/K|.$$

**Example 2.1.5**

(i) $n\mathbb{Z} \leq \mathbb{Z}$; $[\mathbb{Z}:n\mathbb{Z}] = n$.

(ii) $\mathbb{Z} \leq \mathbb{Q}$; $[\mathbb{Q}:\mathbb{Z}] = \infty$.

**Theorem 2.1.6**

Let $K \leq G$. Let $L$ and $R$ be sets of left and right cosets, respectively. Then, the map

$$\begin{aligned} \varphi : R &\longrightarrow L \\ Ka &\longmapsto a^{-1}K \end{aligned}$$

is a (well-defined) bijection.

***Proof.*** Take any $a, b \in G$ and assume $Ka = Kb$. Then, we have $b = ka$ for some $k \in K$. Hence, $a^{-1} = b^{-1}k$; thus we have $a^{-1}K = b^{-1}K$. Therefore, the function is well-defined. Moreover, by a similar argument, $a^{-1}K = b^{-1}K \implies Ka = Kb$; thus $\varphi$ is injective. The surjectivity is evident. □

**Note:-**

Theorem 2.1.6 implies that $[G:K] = |\{ aK \mid a \in G \}|$.

**Lemma 2.1.7**

Let $K \leq G$. For each $a \in G$, the function

$$\begin{aligned} f : K &\longrightarrow Ka \\ k &\longmapsto ka \end{aligned}$$

is a bijection.

***Proof.*** $f$ is evidently surjective. If $ka = f(k) = f(k') = k'a$, then we have $k = k'$. □

**Theorem 2.1.8** Lagrange Theorem

Let $K$ be a finite group and $K \leq G$. Then, $[G:K] = |G|/|K|$. (In particular, $|K| \mid |G|$.)

***Proof.*** Let $n = [G:K]$ and write $G/K = \{Ka_1, Ka_2, \cdots, Ka_n\}$. By Lemma 2.1.7, $|Ka_i| = |K|$ for all $i \in [n]$. Therefore, $|G| = \sum_{i=1}^{n} |Ka_i| = n|K| = [G:K]|K|$. □

**Example 2.1.9**

$A_n(1\,2) = \{\text{all odd permutations}\}$. Therefore, $[S_n:A_n] = 2$; thus by Lagrange Theorem, $|A_n| = n!/2$.

**Note:-**

The converse of Lagrange Theorem (if $d \mid |G|$, there exists a subgroup of order $d$) does not hold.

$|A_4| = 12$. Suppose $K \leq A_4$ with $|K| = 6$. Then, there are two right cosets $K$ and $Ka$ where $a \in A_4 \setminus K$. (Note that $Ka = A_4 \setminus K$.) Take any $b \in A_4 \setminus K$. If $b^2 \in Ka = Kb$, then $b^2 = kb$ for some $k \in K$, which implies $b = k \in K$. Thus, $b^2 \in K$. Therefore, $\forall g \in G, g^2 \in K$. Hence, for all $g \in G$ with $|g| = 3$, then $g = g^4 = (g^2)^2 \in K$ while there are 8 elements in $A_4$ whose order is 3, which contradicts $|K| = 6$.

**Corollary 2.1.10**

Let $G$ be a finite group.

(i) If $a \in G$, then $|a| \mid |G|$.

(ii) If $a^{|G|} = 1$.

***Proof.*** Direct from Lagrange Theorem. $\square$

**Corollary 2.1.11**

Let $p$ be a prime number. Then, every group of order $p$ is cyclic.

***Proof.*** Fix any $a \in G \setminus \{1\}$. Then, $1 < |a| \mid p$; thus $|a| = p$; thus $G = \langle a \rangle$. $\square$

**Corollary 2.1.12**

Let $G$ be a finite group and let $K \leq H \leq G$. Then, $[G{:}K] = [G{:}H][H{:}K]$.

***Proof.*** $[G{:}K]|K| = |G| = [G{:}H]|H| = [H{:}K][G{:}H]|K|$. $\square$

## 2.2 Normal Subgroups

**Lemma 2.2.1**

Let $G$ be a group and let $N \leq G$. Then,

$$\forall a, a', b, b' \in G, (Na = Na' \wedge Nb = Nb' \implies Nab = Na'b') \iff \forall g \in G, gNg^{-1} \subseteq N.$$

***Proof.***

($\Rightarrow$) Take any $g \in G$ and $n \in N$. Since $N1 = Nn^{-1}$, we have $Ng = Ngn^{-1}$. Hence, there exists $n' \in N$ such that $ng = n'gn^{-1}$. Therefore, $gng^{-1} = g(gn^{-1})^{-1} = n^{-1}n' \in N$.

($\Leftarrow$) Take any $a, a', b, b' \in G$ and assume $Na = Na'$ and $Nb = Nb'$. Then, $n' \triangleq a'a^{-1} \in N$ and $b'b^{-1} \in N$. Hence, $a' = n'a$; thus $(a'b')(ab)^{-1} = n'(a(b'b^{-1})a^{-1}) \in N$ (by $b'b^{-1} \in N$ and the assumption). Therefore, $Nab = Na'b'$. $\square$

**Definition 2.2.2: Normal Subgroup**

Let $G$ be a group and let $N \leq G$. $N$ is a *subgroup* if $\forall g \in G$, $gNg^{-1} \in N$. If $N$ is a normal subgroup of $G$, we write $N \trianglelefteq G$.

**Example 2.2.3**

(i) If $G$ is abelian, then every subgroup is normal.

(ii) If $f : G \to H$ is a group homomorphism, then $\ker(f) \trianglelefteq G$.

**Lemma 2.2.4**

Let $G$ be a group and $N \leq G$. Then, $aNa^{-1} \leq G$ and $aNa^{-1} \cong N$.

*Proof.* For each $ana^{-1}, an'a^{-1} \in aNa^{-1}$, we have $(ana^{-1})(an'a^{-1})^{-1} = (ana^{-1})(a(n')^{-1}a^{-1}) = a(n(n')^{-1})a^{-1} \in aNa^{-1}$. Therefore, $aNa^{-1} \leq G$.

Moreover, $f : N \to aNa^{-1}$ defined by $n \mapsto ana^{-1}$ is a bijective group homomorphism; thus $aNa^{-1} \cong N$. □

**Theorem 2.2.5**

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

(i) $N \trianglelefteq G$

(ii) $\forall a \in G$, $aNa^{-1} = N$

(iii) $\forall a \in G$, $Na = aN$

*Proof.*

(i)⇒(ii) For each $n \in N$ and $a \in G$, we have $a^{-1}na = a^{-1}n(a^{-1})^{-1} \in N$; thus $n = a(a^{-1}na)a^{-1} \in aNa^{-1}$. Therefore, $N \subseteq aNa^{-1}$.

(ii)⇒(iii) Take any $n \in N$ and $a \in G$. Then, $ana^{-1} = n'$ for some $n' \in N$. Hence, $an = n'a \in Na$; thus $aN \subseteq Na$. Similarly, we may show $Na \subseteq aN$.

(iii)⇒(i) Take any $n \in N$ and $a \in G$. Then, $an = n'a$ for some $n' \in N$. Thus, $ana^{-1} = n' \in N$; thus $aNa^{-1} \subseteq N$. □

**Lemma 2.2.6**

Let $G$ be a group and $N \leq G$. If $[G{:}N] = 2$, then $N \trianglelefteq G$.

*Proof.* $\{N, Na\}$ and $\{N, aN\}$ are partitions of $G$; thus $Na = aN$. The result follows from Theorem 2.2.5. □

**Example 2.2.7**

(i) If $N \leq Z(G)$, then $N \trianglelefteq G$. (In particular, $Z(G) \trianglelefteq G$).

(ii) By (i) and Lemma 2.2.6, $A_n \trianglelefteq S_n$.

(iii) $\{r_0, s\} \trianglelefteq \{r_0, s, r_2, sr_2\} \trianglelefteq D_4$ but $\{r_0, s\} \ntrianglelefteq D_4$.

**Definition 2.2.8: Normalizer**

Let $G$ be a group and let $\varnothing \subsetneq A \subseteq G$. Then, the *normalizer of A* is the set

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

**Theorem 2.2.9**

Let $G$ be a group and let $\varnothing \subsetneq A \subseteq G$. Then, $C(A) \leq N(A) \leq G$.

*Proof.* As $C(A) \subseteq N(A)$, it is enough to show $N(A) \leq G$. Note that $1 \in A$ by definition. Take any $x, y \in N(A)$. Then, $(xy^{-1})A(xy^{-1})^{-1} = xy^{-1}Ayx^{-1} = xy^{-1}(yAy^{-1})yx^{-1} = xAx^{-1} = A$. Therefore, $xy^{-1} \in N(A)$; thus $N(A) \leq G$ by Theorem 1.3.2. □

**Theorem 2.2.10**

Let $G$ be a group and let $H \leq G$.

(i) $H \trianglelefteq N(H)$

(ii) If $H \trianglelefteq K \leq G$, then $K \leq N(H)$.

*Proof.* (i) is trivial since $H \subseteq N(H)$. Take any $k \in K$. From $kHk^{-1} = H$, we have $k \in N(H)$; $K \subseteq N(H)$. □

**Note:-**

Theorem 2.2.10 essentially says that $N(H)$ is the largest subgroup of $G$ of which $H$ is a normal subgroup.

**Example 2.2.11**

(i) If $G$ is abelian, then $N(H) = G$ for all $H \leq G$.
(ii) $K = \{r_0, s\} \leq D_4$ but $K \ntrianglelefteq D_4$. $N(K) = \{r_0, r_2, s, r_2\}$.

**Definition 2.2.12: Characteristic Subgroup**

Let $G$ be a group and let $H \leq G$. $H$ is called a *characteristic subgroup of* $G$ if $\forall \sigma \in \mathrm{Aut}(G)$, $\sigma(H) = H$. If $H$ is a characteristic characteristic subgroup of $G$, we write $H \operatorname{char} G$.

**Theorem 2.2.13**

Let $G$ be a group and let $H \leq G$.
(i) If $H \operatorname{char} G$, then $H \trianglelefteq G$.
(ii) If $H$ is a unique subgroup of $G$ of a given order, then $H \operatorname{char} G$.
(iii) If $K \operatorname{char} H \trianglelefteq G$, then $K \trianglelefteq G$.

*Proof.*
(i) For all $g \in G$, we have $gHg^{-1} = i_g(H) = H$.
(ii) For any automorphism $\sigma \in \mathrm{Aut}(G)$, we have $|\sigma(H)| = |H|$ but the condition asserts that $H = \sigma(H)$.
(iii) Take any $g \in G$. Note that $i_g\big|_H \in \mathrm{Aut}(H)$. Then, $gKg^{-1} = i_g\big|_H(K) = K$; thus $K \trianglelefteq G$. □

## 2.3 Quotient Groups and Group Homomorphisms

**Definition 2.3.1: Quotient Group**

Let $G$ be a group and $N \trianglelefteq G$. Then, by Lemma 2.2.1, $G/N$ equipped with operation $(Na, Nb) \mapsto (Nab)$ is a group.

$\pi : G \to G/N$ defined by $a \mapsto Na$ is a surjective group homomorphism. We call $\pi$ the *natural projection*.

**Note:-**

If $G$ is abelian/cyclic/finite, then $G/N$ is also abelian/cyclic/finite.

**Theorem 2.3.2**

Let $G$ be a group. If $G/Z(G)$ is a cyclic group, then $G$ is an abelian group.

*Proof.* Let $C \triangleq Z(G)$. There exists $d \in G$ such that $G/C = \langle Cd \rangle$. Take any $a, b \in G$. Then, $Ca = Cd^i$ and $Cb = Cd^j$ for some $i, j \in \mathbb{Z}$. Hence, $a = c_1 d^i$ and $b = c_2 d^j$ for some $c_1, c_2 \in C$. Then, we have

$$ab = c_1(d^i c_2)d^j = (c_1 c_2)(d^i d^j) = c_2(c_1 d^j)d^i = c_2 d^j c_1 d^i = ba.$$

Hence, the result follows. □

**Theorem 2.3.3**

Let $f: G \to H$ be a group homomorphism. Then, $\ker(f) = \{1\}$ if and only if $f$ is injective.

***Proof.***
($\Rightarrow$) Take any $a, b \in G$ with $f(a) = f(b)$. Then, we have $1 = f(a)f(b)^{-1} = f(ab^{-1})$; thus $ab^{-1} \in \ker(f)$. Therefore, we have $ab^{-1} = 1$, which implies $a = b$.
($\Leftarrow$) Trivial. □

**Theorem 2.3.4** First Isomorphism Theorem

If $f: G \to H$ is a group homomorphism, then $G/\ker(f) \cong \operatorname{im}(H)$.

***Proof.*** WLOG, $f$ is surjective. Put $K \triangleq \ker(f)$. Define $\varphi: G/K \to H$ by $Ka \mapsto f(a)$. It is well-defined since, if $Ka = Kb$, then we have $a = kb$ for some $k \in \ker(f)$ and thus $f(a) = f(k)f(b) = f(b)$. Moreover, it is evidently surjective.

It is clear that $\varphi$ is a group homomorphism. Take any $Ka, Kb \in G/K$ and assume $f(a) = f(b)$. Then, $1 = f(ab^{-1})$; thus $ab^{-1} \in K$. Therefore, $Ka = Kb$; $\varphi$ is injective. □

**Corollary 2.3.5**

Let $N \leq G$ be a subgroup of a finite group $G$. If $[G:N]$ is the smallest prime divisor of $|G|$, then $N \trianglelefteq G$.

***Proof.*** Let $L$ be the set of left cosets of $N$ in $G$ and let $p \triangleq [G:N] = |L|$. (See Theorem 2.1.6.) Note that $G \curvearrowright L$ by $(g, aN) \mapsto (ga)N$. Then, by Lemma 1.2.6, the map $\varphi: G \to S(L)$ defined by $g \mapsto \varphi_g$ is a group homomorphism. Let $K \triangleq \ker(\varphi)$. By First Isomorphism Theorem and Lagrange Theorem, we have $|G/K| \mid p!$.

On the other hand, for each $k \in K$, since $\varphi(k) = \mathrm{id}_L$, $kN = \varphi(k)(N) = N$; thus $k \in N$. Hence, we have $K \leq N$. By Corollary 2.1.12, $p[N:K] = [N:K][G:N] = [G:K] \mid p!$. Now, we have $[N:K] \mid (p-1)!$. As $p$ is the smallest prime divisor of $|G|$, and as $[N:K]$ divides $|G|$, we have $[N:K] = 1$; that is to say $N = K = \ker(\varphi) \trianglelefteq G$. □

**Theorem 2.3.6**

If $H, K \leq G$ and $G$ is a finite group, then

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

***Proof.*** Note that, for each $h_1, h_1 \in H$,

$$h_1K = h_2K \iff h_2^{-1}h_1 \in K \iff h_2^{-1}h_1 \in H \cap K \iff h_1(H \cap K) = h_2(H \cap K).$$

Therefore,

$$|\{hK \mid h \in H\}| = |\{h(H \cap K) \mid h \in H\}| = [H:H \cap K] = |H|/|H \cap K|$$

by Lagrange Theorem and Theorem 2.1.6. Therefore, $|HK| = |\{hK \mid h \in H\}||K| = |H||K|/|H \cap K|$. □

**Theorem 2.3.7**

Let $H, K \leq G$. Then, $HK \leq G$ if and only if $HK = KH$.

***Proof.***
($\Rightarrow$) Take any $kh \in KH$. Since $H, K \leq HK$, we have $kh \in HK$; thus $KH \subseteq HK$. Now, take any $x \in HK$. Then, since $x^{-1} \in HK$, $x^{-1} = hk$ for some $h \in H$ and $k \in K$. Therefore, $x = (x^{-1})^{-1} = k^{-1}h^{-1} \in KH$; thus $HK \subseteq KH$.
($\Leftarrow$) $HK$ is evidently nonempty. Take any $h_1k_1, h_2k_2 \in HK$. Since $k_1k_2^{-1}h_2^{-1} \in KH = HK$, we have $k_1k_2^{-1}h_2^{-1} = h_3k_3$ for some $h_3 \in H$ and $k_3 \in K$. Therefore, $(h_1k_1)(h_2k_2)^{-1} = h_1(k_1k_2^{-1}h_2^{-1}) = h_1h_3k_3 \in HK$. Thus, $HK \leq G$ by Theorem 1.3.2. $\square$

**Corollary 2.3.8**

Let $H, K \leq G$. Then, $H \leq N(K)$ implies $HK \leq G$. In particular, if $H \leq G$ and $K \trianglelefteq G$, then $HK \leq G$.

***Proof.*** Take any $hk \in HK$. Since $hkh^{-1} \in K$, we have $hk = (hkh^{-1})h \in KH$; thus $HK \subseteq KH$. On the other hand, for each $kh \in KH$, we have $kh = h(h^{-1}kh) \in HK$ by the same reason. Hence, $HK = KH$. The result follows from Theorem 2.3.7. $\square$

**Theorem 2.3.9** Second Isomorphism Theorem

Let $N \trianglelefteq G$ and $K \leq G$. Then, $NK \leq G$, $N \trianglelefteq NK$, $N \cap K \trianglelefteq K$, and $K/(N \cap K) \cong NK/N$.

***Proof.*** By Corollary 2.3.8 and Theorem 2.3.7, we have $KN = NK \leq G$. Moreover, $N \trianglelefteq G$ and $N \leq NK$ straightforwardly implies $N \trianglelefteq NK$. Consider a group homomorphism $f : K \to NK/N$ defined by $k \mapsto Nk$. As $Nnk = Nk$ for each $n \in N$ and $k \in K$, $f$ is surjective. Now,

$$\ker(f) = \{k \in K \mid Nk = N\} = \{k \in K \mid k \in N\} = K \cap N.$$

Therefore, $K \cap N \trianglelefteq K$. First Isomorphism Theorem implies $K/(K \cap N) \cong NK/N$. $\square$

**Theorem 2.3.10** Third Isomorphism Theorem

Let $N, K \trianglelefteq G$ and $N \leq K$. Then, $K/N \trianglelefteq G/N$ and $(G/N)/(K/N) \cong G/K$.

***Proof.*** Define

$$\begin{aligned} f : G/N &\longrightarrow G/K \\ Na &\longmapsto Ka. \end{aligned}$$

To show well-definedness, take any $a, b \in G$ and assume $ab^{-1} \in N$. Then, since $N \subseteq K$, we also have $ab^{-1} \in K$, i.e., $Ka = Kb$. Now, clearly $f$ is a surjective group homomorphism.

$$\ker(f) \triangleq \{Na \in G/N \mid Ka = K\} = \{Na \in G/N \mid a \in K\} = K/N.$$

Therefore, $(G/N)/(K/N) \cong G/K$ by First Isomorphism Theorem. $\square$

**Theorem 2.3.11** Fourth Isomorphism Theorem

Let $N \trianglelefteq G$ and let $\pi : G \twoheadrightarrow G/N$ be the natural projection. Then, there is a natural one-to-one correspondence between

$$\{\text{subgroups of } G \text{ containing } N\} \overset{1:1}{\longleftrightarrow} \{\text{subgroups of } G/N\}$$

with $K \mapsto K/N$. Furthermore, for each $K \leq G$ such that $N \leq K$, we have $K \trianglelefteq G \iff K/N \trianglelefteq G/N$.

***Proof.*** Let $\phi(K) = K/N$ for each subgroup $K \leq G$ containing $N$.

- Assume $N \leq K, K' \leq G$ with $K \neq K'$. WLOG, fix $k \in K \setminus K'$. If $Nk = Nk'$ for some $k' \in K'$, then we have $k \in Nk' \subseteq K'$. Therefore, $\forall k' \in K$, $Nk \neq Nk'$; we get $Nk \in K/N$ while $Nk \notin K'/N$. Thus, $K/N \neq K'/N$. $\phi$ is injective.
- Take any $\overline{K} \leq G/N$ and let $K = \pi^{-1}(\overline{K}) = \{g \in G \mid Ng \in \overline{K}\}$. Then, we immediately have $N \leq K \leq G$ and $\phi(K) = K/N = \overline{K}$.

Therefore, $\phi$ is bijective.

We are now left with the last assertion.

($\Rightarrow$) Third Isomorphism Theorem

($\Leftarrow$) Assume $K/N \trianglelefteq G/N$. Take any $a \in G$ and $k \in K$. Then, we have $Na^{-1}ka = (Na)^{-1}(Nk)(Na) \in K/N$. Therefore, $Na^{-1}ka = Nt$ for some $t \in K$, and thus $a^{-1}ka = nt$ for some $n \in N$. Since $N \subseteq K$, we have $a^{-1}ka \in K$. □

**Definition 2.3.12: Commutator**

Let $G$ be a group and let $x, y \in G$. Then, the *commutator* of $x$ and $y$ is

$$[x, y] \triangleq x^{-1}y^{-1}xy.$$

Moreover, for $A, B \leq G$, the *commutator* of $A$ and $B$ is

$$[A, B] \triangleq \langle [a, b] \mid a \in A \wedge b \in B \rangle.$$

The *commutator subgroup of $G$* is $[G, G]$.

**Note:-**

- Let $x, y \in G$. From the fact that $xy = yx[x, y]$, we have $[x, y] = 1 \iff xy = yx$.
- $G$ is abelian if and only if $[G, G] = \{1\}$.
- We do not have $\{[a, b] \mid a \in A \wedge b \in B\} \leq G$ in general. However, the smallest counterexample requires $|G| = 96$; so we do not consider it.

**Example 2.3.13**

- In $D_n$, $[r_1^i, r_1^j] = r_0$, $[sr_1^i, r_1^j] = r_1^{2j}$, $[r_1^i, sr_1^j] = r_1^{-2i}$, and $[sr_1^i, sr_1^j] = r_1^{-2i+2j}$. In particular, $[D_4, D_4] = \{r_0, r_1^2\}$.

**Theorem 2.3.14**

Let $G$ be a group and let $H \leq G$.

(i) $H \trianglelefteq G \iff [H, G] \leq H$.
(ii) $\forall \sigma \in \mathrm{Aut}(G)$, $\forall x, y \in G$, $\sigma([x, y]) = [\sigma(x), \sigma(y)]$.
(iii) $[G, G]$ char $G$, and $G/[G, G]$ is abelian.
(iv) $H \trianglelefteq G$ and $G/H$ is abelian if and only if $[G, G] \leq H$.

***Proof.***

(i) Take any $g \in G$ and $h \in H$. Then, $[h, g] = h^{-1}(g^{-1}hg) \in H \iff g^{-1}hg \in H$.
(ii) Take any $\sigma \in \mathrm{Aut}(G)$ and $x, y \in G$. Then, $\sigma([x, y]) = \sigma(x^{-1}y^{-1}xy) = \sigma(x)^{-1}\sigma(y)^{-1}\sigma(x)\sigma(y) = [\sigma(x), \sigma(y)]$.

(iii) Take any $\sigma \in \mathrm{Aut}(G)$. Then, we have $\sigma([G,G]) \leq [G,G]$ and $\sigma^{-1}([G,G]) \leq [G,G]$ by (ii). Hence, $\sigma([G,G] = G)$.

Now, take any $x, y \in G$. Then, $[G,G]xy = [G,G][y^{-1}, x^{-1}]xy = [G,G]yx$. Hence, $G/[G,G]$ is abelian.

(iv) (⇒) Take any $x, y \in G$. Then, $H = (Hx)^{-1}(Hy)^{-1}(Hx)(Hy) = H(x^{-1}y^{-1}xy) = H[x,y]$. Therefore, $[x,y] \in H$. This shows $[G,G] \leq H$.

(⇐) By (iii) and Theorem 2.2.13 (i), we have $[G,G] \trianglelefteq G$; and thus $[G,G] \trianglelefteq H$. Moreover, since $G/[G,G]$ is abelian, every subgroup of $G/[G,G]$ is normal. In particular, $H/[G,G] \trianglelefteq G/[G,G]$. Hence, by Fourth Isomorphism Theorem, $H \trianglelefteq G$. By Third Isomorphism Theorem, $G/H \cong (G/[G,G])/(H/[G,G])$ is abelian. □

**Note:-**

From Theorem 2.3.14 (iii) and Theorem 2.3.14 (iv), we get the fact that $G/[G,G]$ is the *largest* abelian quotient of $G$.

## 2.4 Simple Groups and Jordan–Hölder Theorem

**Definition 2.4.1: Simple Group**

A nontrivial group $G$ is *simple* if $G$ has only two normal subgroups.

**Example 2.4.2**

Let $G$ be a group and let $M$ be a proper normal subgroup of $G$. Then, $M$ is a maximal normal subgroup if and only if $G/M$ is simple.

(⇒) Let $N \trianglelefteq G/M$. Let $H \triangleq \{h \in G \mid Mh \in N\}$ so that $M \leq H \trianglelefteq G$. By maximality of $M$, we have $H = M$ or $H = G$, that is to say $N = \{M\}$ or $N = G/M$.

(⇐) Let $M \trianglelefteq N \trianglelefteq G$. Then, by Third Isomorphism Theorem, $N/M \trianglelefteq G/M$; thus $N/M = \{M\}$ or $N/M = G/M$ as $G/M$ is simple. Therefore, $N = M$ or $N = G$. □

**Definition 2.4.3: Composition Series**

Let $G$ be a group. A sequence of subgroups

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_k = G$$

of $G$ is called a *composition series of* $G$ if $N_i/N_{i-1}$ is simple for each $i \in [k]$. Each $N_{i+1}/N_i$ is called a *composition factor of* $G$.

**Example 2.4.4**

(i) $\{r_0\} \trianglelefteq \langle s \rangle \trianglelefteq \langle s, r_1^2 \rangle \trianglelefteq D_4$ and $\{r_0\} \trianglelefteq \langle r_1^2 \rangle \trianglelefteq \langle s, r_1^2 \rangle \trianglelefteq D_4$ are two composition series of $D_4$.

(ii) $\mathbb{Z}$ has no composition series because every proper subgroup of $\mathbb{Z}$ is an infinite cyclic group.

**Theorem 2.4.5** Jordan–Hölder Theorem

Let $G$ be a nontrivial finite group.

(i) $G$ has a composition series.
(ii) If $(N_0, \cdots, N_r)$ and $(M_0, \cdots, M_s)$ are composition series of $G$, then $r = s$ and $\exists \sigma \in S_r$ such that $\forall i \in [r]$, $M_{\sigma(i)}/M_{\sigma(i)-1} \cong N_i/N_{i-1}$.

***Proof.***

(i) We prove (i) by induction on $|G|$. It is trivial when $|G| = 2$. Let $G$ be a finite group with $|G| \geq 3$. If $G$ is simple, we are done; assume $G$ is not simple. Then, $G$ has a proper normal subgroup $N$ which is maximal so that $G/N$ is simple. By induction hypothesis, $N$ admits a composition series.

(ii) WLOG, $s \geq r$. We proceed with induction on $r$. Since $r = 1$ implies $G$ is simple and $s = 1$, we are done; hence assume $r \geq 2$. If $N_{r-1} = M_{s-1}$, then we are done by induction hypothesis.

Now, assume $N_{r-1} = M_{s-1}$. Then, $N_{r-1}, M_{s-1} \trianglelefteq N_{r-1}M_{s-1} \leq G$ by Corollary 2.3.8. Moreover, since $g(nm)g^{-1} = (gng^{-1})(gmg^{-1}) \in N_{r-1}M_{s-1}$ for all $g \in G$, $n \in N_{r-1}$, and $m \in M_{s-1}$, we have $N_{r-1}M_{s-1} \trianglelefteq G$. Hence, as $N_{r-1}$ and $M_{s-1}$ are maximal proper normal subgroups of $G$, and as $N_{r-1} \neq M_{s-1}$, we have $N_{r-1}M_{s-1} = G$. Define $H \triangleq H_{r-1} \cap M_{s-1}$ so that $H \trianglelefteq N_{r-1}, M_{s-1}$. Then, by Second Isomorphism Theorem, $G/N_{r-1} = N_{r-1}M_{s-1}/N_{r-1} \cong M_{s-1}/H$ and $G/M_{s-1} = N_{r-1}M_{s-1}/M_{s-1} \cong N_{r-1}/H$, and they are simple groups.

Let $\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_h = H$ be a composition series of $H$. Then,

$$\begin{aligned} \{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_h = H \trianglelefteq N_{r-1} \\ \{1\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_h = H \trianglelefteq M_{s-1} \end{aligned}$$

are composition series of $N_{r-1}$ and $M_{s-1}$, respectively. Therefore, by induction hypothesis, $r - 1 = h + 1 = s - 1$; thus $r = s$. By induction hypothesis again,

$$\begin{aligned} H_1/H_0, H_2/H_1, \cdots, H_h/H_{h-1}, N_{r-1}/H_h \cong G/M_{s-1} \\ \text{and } N_1/N_0, N_2/N_1, \cdots, N_{r-2}/N_{r-1}, N_{r-1}/N_{r-2} \end{aligned}$$

are the same up to permutation, and

$$\begin{aligned} H_1/H_0, H_2/H_1, \cdots, H_h/H_{h-1}, M_{s-1}/H_h \cong G/N_{r-1} \\ \text{and } M_1/M_0, M_2/M_1, \cdots, M_{s-2}/M_{s-1}, M_{s-1}/M_{s-2} \end{aligned}$$

are the same up to isomorphism. Hence, the result follows. □

**Theorem 2.4.6**

Let $G$ be an abelian group. Then, $G$ is simple if and only if $G \cong \mathbb{Z}_p$ for some prime number $p$.

***Proof.***

($\Rightarrow$) Take any $a \in G \setminus \{1\}$. Then, $\langle a \rangle \trianglelefteq G$ since $G$ is abelian. As $G$ is simple, we have $\langle a \rangle = G$. Therefore, by Corollary 1.5.7, $\langle a \rangle \cong Z_p$ for some prime $p$.

($\Leftarrow$) Trivial. □

**Theorem 2.4.7**

$A_n$ is simple for $n \geq 5$.

***Proof.***

**Claim 1.** For $n \geq 3$, $A_n$ is generated by 3-cycles.

***Proof.*** There are three types of products of two transpositions.
- $(a\,b)(c\,d) = (a\,d\,b)(a\,d\,c)$
- $(a\,b)(a\,c) = (a\,c\,b)$
- $(a\,b)(a\,b) = (1)$

This is sufficient since every $\sigma \in A_n$ is a product of even number of transpositions. $\square$

**Claim 2.** Let $n \geq 3$ and $N \trianglelefteq A_n$ such that $N$ contains a 3-cycle. Then, $N = A_n$.

***Proof.*** WLOG, $(1\,2\,3) \in N$. Then, $(1\,3\,2) = (1\,2\,3)^2 \in N$. Take any $k \geq 4$. Then,
- $(1\,2\,k) = (2\,k\,1) = \tau(1\,3\,2)\tau^{-1} \in N$ where $\tau = (1\,2)(3\,k)$, and
- $(2\,1\,k) = (1\,k\,2) = \tau'(1\,2\,3)(\tau')^{-1} \in N$ where $\tau' = (3\,2\,k)$.

All other 3-cycles can be generated by:
- $(1\,a\,b) = (1\,2\,b)(1\,2\,a)(1\,2\,a) \in N$,
- $(2\,a\,b) = (2\,1\,b)(2\,1\,a)(2\,1\,a) \in N$, and
- $(a\,b\,c) = (1\,2\,a)(1\,2\,a)(1\,2\,c)(1\,2\,b)(1\,2\,b)(1\,2\,a) \in N$.

Therefore, by Claim 1, $N = A_n$. $\square$

Take any $\{(1)\} \lneq N \trianglelefteq A_n$ and fix some $\sigma \in N \setminus \{(1)\}$. Consider the cycle decomposition of $\sigma$. There are three cases: (i) some cycle has length $\geq 4$, (ii) the maximum length of cycle is 3, and (iii) every cycle has length $\leq 2$.

(i) WLOG, $\sigma = (1\,2\,\cdots\,r)\tau$ where $r \geq 4$ where $\tau(i) = i$ for each $i \in [r]$. Let $\delta = (1\,2\,3) \in A_n$. Then, we have $(2\,3\,1\,4\,5\,\cdots\,r)\tau = \delta\sigma\delta^{-1} \in N$. Moreover, we have

$$\sigma^{-1}(2\,3\,1\,4\,5\,\cdots\,r)\tau = (r\,r-1\,\cdots\,1)(2\,3\,1\,4\,5\,\cdots\,r)\tau^{-1}\tau = (1\,3\,r) \in N;$$

thus $N = A_n$ by Claim 2.

(ii) We have two subcases: (1) there are (at least) two 3-cycles and (2) there are only one 3-cycle.

(1) WLOG, $\sigma = (1\,2\,3)(4\,5\,6)\tau$ where $\tau$ fixes $[6]$. Let $\delta = (1\,2\,4) \in A_n$. Then, $(2\,4\,3)(1\,5\,6)\tau = \delta\sigma\delta^{-1} \in N$. Hence, we have

$$\sigma^{-1}(2\,4\,3)(1\,5\,6)\tau = (3\,2\,1)(6\,5\,4)(2\,4\,3)(1\,5\,6)\tau^{-1}\tau = (1\,4\,2\,6\,3) \in N,$$

which reduces to case (i). Hence, we have $N = A_n$ in this case.

(2) WLOG, $\sigma = (1\,2\,3)\tau$ where $\tau$ fixes $[3]$ and $\tau$ is a product of disjoint transpositions so that $\tau^2 = 1$. Then, we have $\sigma^2 = (1\,3\,2) \in N$; thus $N = A_n$ by Claim 2.

(iii) WLOG, $\sigma = (1\,2)(3\,4)\tau$ where $\tau$ fixes $[4]$ and $\tau$ is a product of disjoint transpositions. Let $\delta = (1\,2\,3) \in A_n$. Then, $(2\,3)(1\,4)\tau = \delta\sigma\delta^{-1} \in N$. Therefore,

$$\beta \triangleq \sigma^{-1}(2\,3)(1\,4)\tau = (1\,2)(3\,4)(2\,3)(1\,4)\tau^{-1}\tau = (1\,3)(2\,4) \in N.$$

As $n \geq 5$ we may fix $5 \leq k \leq n$ and let $\alpha = (1\,3\,k) \in A_n$. Then, $(3\,k)(2\,4) = \alpha\beta\alpha^{-1} \in N$. Hence,

$$\beta(3\,k)(2\,4) = (1\,3)(2\,4)(3\,k)(2\,4) = (1\,3\,k) \in N,$$

which implies $N = A_n$ by Claim 2. $\square$

**Note:-**
- $A_4$ is not simple.
- We have two infinite series of simple groups: $\mathbb{Z}_p$'s ($p$ is prime) and $A_n$'s $n \geq 5$.

**Corollary 2.4.8**

For $n \geq 5$, $S_n$ has only three normal subgroups $\{1\}$, $A_n$, and $S_n$.

***Proof.*** By Lemma 2.2.6, we have $A_n \trianglelefteq S_n$.

Let $N \trianglelefteq S_n$ be a nontrivial normal subgroup of $S_n$. Then, $N \cap A_n \trianglelefteq A_n$. By Theorem 2.4.7, we have (i) $N \cap A_n = \{(1)\}$ or (ii) $N \cap A_n = A_n$.

(i) If $N \cap A_n = \{1\}$, then $N \cong N/(N \cap A_n) \cong A_n N/A_n$ by Second Isomorphism Theorem. As $|A_n N| | n!$ and $|A_n| = n!/2$, we have $|N| = |A_n N|/|A_n| = 2$ as we assumed $N$ is nontrivial. Then, $N = \{(1), \sigma\}$ where $\sigma^2 = (1)$. By Theorem 2.2.5, $\tau N = N\tau$ for all $\tau \in S_n$; that is to say $\sigma\tau = \tau\sigma \in S_n$ for all $\tau \in S_n$. This means $N \leq Z(S_n) = \{(1)\}$, which is a contradiction.

(ii) Assume $N \cap A_n = A_n$, i.e., $A_n \leq N$. However, by Lagrange Theorem, $n!/2 \mid |N| \mid n!$ so that $N = A_n$ or $N = S_n$. $\square$

**Definition 2.4.9: Solvable Group**

Let $G$ be a group. We say $G$ is *solvable* if there is a sequence

$$\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

of subgroups of $G$ such that $G_{i-1}/G_i$ is abelian for each $i \in [n]$.

**Example 2.4.10**

- Every abelian group is solvable. ($G_0 = \{1\}, G_1 = G$)
- $\{1\} \trianglelefteq A_3 \trianglelefteq S_3$ and $A_3$ is abelian; thus $S_3$ is solvable.
- $\{1\} \trianglelefteq \{(1), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \trianglelefteq A_4 \trianglelefteq S_4$; $S_4$ is solvable.
- $S_n$ is not solvable for $n \geq 5$.

**Theorem 2.4.11**

Let $G$ be a group and $N \trianglelefteq G$. Then, $G$ is solvable if and only if $N$ and $G/N$ are solvable.

***Proof.***

($\Rightarrow$) There exists a sequence $\{1\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$ such that $G_{i-1}/G_i$ is abelian for each $i \in [n]$. Then, we have $N \cap G_i \trianglelefteq G_{i-1}$ and thus $N \cap G_i \trianglelefteq N \cap G_{i-1}$ for each $i \in [n]$. Moreover,

$$(N \cap G_{i-1})/(N \cap G_i) \leq G_{i-1}/(N \cap G_i).$$

By Third Isomorphism Theorem, $G_i/(N \cap G_i) \trianglelefteq G_{i-1}/(N \cap G_i)$ and $(G_{i-1}/(N \cap G_i))/(G_i/(N \cap G_i)) \cong G_{i-1}/G_i$.

Considering the existence of natural projection

$$G_{i-1}/(N \cap G_i) \twoheadrightarrow (G_{i-1}/(N \cap G_i))/(G_i/(N \cap G_i)) \cong G_{i-1}/G_i,$$

there is a group homomorphism

$$\varphi : (N \cap G_{i-1})/(N \cap G_i) \longrightarrow G_{i-1}/G_i$$

whose kernel $\ker(\varphi) = (N \cap G_{i-1})/(N \cap G_i) \cap G_i/(N \cap G_i) = (N \cap G_i)/(N \cap G_i)$ is trivial. Therefore, $\varphi$ is injective by Theorem 2.3.3. Hence, $(N \cap G_i)/(N \cap G_i)$ is isomorphic to a subgroup of $G_{i-1}/G_i$, which is abelian. Therefore, the sequence

$$\{1\} = N \cap G_n \trianglelefteq N \cap G_{n-1} \trianglelefteq \cdots \trianglelefteq N \cap G_0 = N$$

witnesses that $N$ is solvable.

Let $\pi\colon G \to G/N$ be the natural projection. Then, $\pi(G_i) \trianglelefteq \pi(G_i)$ for all $i \in [n]$. The map $G_{i-1}/G_i \mapsto \pi(G_{i-1})/\pi(G_i)$ defined by $G_i g_{i-1} \mapsto \pi(G_i)\pi(g_{i-1})$ is a surjective group homomorphism; thus $\pi(G_{i-1})/\pi(G_i)$ is abelian. Hence, the sequence

$$\{1\} = \pi(G_n) \trianglelefteq \pi(G_{n-1}) \trianglelefteq \cdots \trianglelefteq \pi(G_0) = G/N$$

witnesses that $G/N$ is solvable.

($\Leftarrow$) Let

$$\{1\} = N_s \trianglelefteq N_{s-1} \trianglelefteq \cdots \trianglelefteq N_0 = N$$

and

$$\{N\} = \overline{G}_r \trianglelefteq \overline{G}_{r-1} \trianglelefteq \cdots \trianglelefteq \overline{G}_0 = G/N$$

be sequences that witnesses the solvability of $N$ and $G/N$. By Fourth Isomorphism Theorem, for each $j \in [r]$, there (uniquely) exists $G_j \leq G$ such that $N \trianglelefteq G_j$ and $G_j/N = \overline{G}_j$. Then, for each $j \in [r]$, we have $G_j \trianglelefteq G_{j-1}$ by Fourth Isomorphism Theorem. By Third Isomorphism Theorem, $G_{j-1}/G_j \cong (G_{j-1}/N)/(G_j/N) = \overline{G}_{j-1}/\overline{G}_j$ is abelian; thus

$$\{1\} = N_s \trianglelefteq N_{s-1} \trianglelefteq \cdots \trianglelefteq N_0 = N = G_r \trianglelefteq G_{r-1} \trianglelefteq \cdots G_0 = G$$

shows that $G$ is solvable. $\square$

# Chapter 3

# Group Actions

## 3.1 Stabilizers and Orbits

**Definition 3.1.1: Stabilizer**

Let $G \curvearrowright A$. The *stabilizer of* $a \in A$ is the set

$$G_a \triangleq \{ g \in G \mid ga = a \}.$$

**Definition 3.1.2: Kernel of Group Action**

Let $G \curvearrowright A$. The *kernel of* $G \curvearrowright A$ is the set

$$K(G,A) \triangleq \{ g \in G \mid \forall a \in A,\ ga = a \} = \bigcap_{a \in A} G_a.$$

**Note:-**

$K(G,A)$ is the kernel of the permutation representation of the group action. Therefore, $K(G,A) \trianglelefteq G$.

**Theorem 3.1.3**

Let $G \curvearrowright A$. Then, $\forall a \in G,\ G_a \leq G$.

***Proof.*** $G_a \neq \varnothing$ since $1 \in G_a$. If $x, y \in G_a$, then $(xy^{-1})a = (xy^{-1})(ya) = xa = a$; thus $xy^{-1} \in G_a$. Hence, $G_a \leq G$ by Theorem 1.3.2. □

**Example 3.1.4**

(i) Let $G$ be a group and let $S \triangleq \mathcal{P}(G)$. Define a group action of $G$ on $S$ by $(g, A) \mapsto gAg^{-1}$. Then, for each $A \in \mathcal{P}(G)$, $G_A = \{ g \in G \mid gAg^{-1} = A \} = N(A)$.

(ii) Let $G$ be a group and let $A \subseteq G$. Define a group action of $N(A)$ on $A$ by $(g, a) \mapsto gag^{-1}$. Then, $K(N(A), A) = \{ g \in N(A) \mid \forall a \in A,\ gag^{-1} = a \} = C(A)$.

(iii) Let $G$ be a group and define a group action of $G$ on $G$ by $(g, a) \mapsto gag^{-1}$. Then, $G_a = \{ g \in G \mid gag^{-1} = a \} = C(a)$ for each $a \in G$ and $K(G, G) = \{ g \in G \mid \forall a \in A,\ gag^{-1} = a \} = Z(G)$.

**Definition 3.1.5: Faithful Group Action**

If $G \curvearrowright A$, we say the group action is *faithful* if $K(G,A) = \{1\}$.

**Note:-**
Let $\varphi: G \to S(A)$ be the permutation representation. Then, $G/K(G,A) \cong \operatorname{im}(\varphi) \leq S(A)$ so we may consider injective group homomorphism $G/K(G,A) \hookrightarrow S(A)$ so that $G/K(G,A) \curvearrowright A$ is faithful.

**Lemma 3.1.6**
Define $a \sim b \iff \exists g \in G,\ a = g \cdot b$. Then, $\sim$ is an equivalence relation.

**Definition 3.1.7: Orbit**

Let $G \curvearrowright A$. The *orbit of $a \in A$* is the set

$$Ga \triangleq \{\, g \cdot a \mid g \in G \,\}.$$

**Note:-**
By Lemma 3.1.6, the collection of orbits forms a partition of $A$. Moreover, $G \curvearrowright Ga$ for each $a \in A$.

**Theorem 3.1.8** Orbit-Stabilizer Theorem
Let $G \curvearrowright A$ and $a \in A$. Then, the function

$$\begin{aligned} f : Ga &\longrightarrow \{\text{left cosets of } G_a \text{ in } G\} \\ ga &\longmapsto gG_a \end{aligned}$$

is well-defined and is a bijection. In particular, if $Ga$ is finite, then $|Ga| = [G{:}G_a]$.

***Proof.*** For each $g, g' \in G$, we have

$$ga = g'a \iff a = g^{-1}g'a \iff g^{-1}g' \in G_a \iff gG_a = g'G_a$$

Therefore, $f$ is well-defined and is injective. The surjectivity of $f$ is evident. $\square$

**Definition 3.1.9: Transitive Group Action**

Let $G \curvearrowright A$. The group action is *transitive* if $\forall a \in A,\ A = Ga$.

**Note:-**
By Orbit-Stabilizer Theorem and Lagrange Theorem, if $G$ and $A$ are finite, and if the group action is transitive, then $|A| \mid |G|$.

**Definition 3.1.10**

Let $G \curvearrowright A$. Then, for each $g \in G$, we define

$$A_g \triangleq \{\, a \in A \mid g \cdot a = a \,\}.$$

**Example 3.1.11**

(i) Let $S_n \curvearrowright [n]$. Then, $(S_n)_i \cong S_{n-1}$ for each $i \in [n]$. Moreover, $K(S_n,[n]) = \bigcap_{i\in[n]}(S_n)_i = \{(1)\}$. By Orbit-Stabilizer Theorem, $|S_n \cdot i| = |S_n|/|(S_n)_i| = n$; thus $S_n \cdot i = [n]$.

**Theorem 3.1.12** Burnside's Lemma

Let $G \curvearrowright A$ and let $|G|$ and $|A|$ be finite. Then,

$$(\text{\# of orbits of } G) = \frac{1}{|G|}\sum_{a\in A}|G_a| = \frac{1}{|G|}\sum_{g\in G}|A_g|.$$

***Proof.*** Let $S \triangleq \{(g,a) \in G \times A \mid g \cdot a = a\}$. Then, by double counting, $|S| = \sum_{a\in A}|G_a| = \sum_{g\in G}|A_g|$. By Orbit-Stabilizer Theorem,

$$\sum_{a\in A}|G_a| = \sum_{a\in A}\frac{|G|}{|Ga|} = |G|\sum_{a\in A}\frac{1}{|Ga|}.$$

Since $\sum_{a'\in Ga}|Ga|^{-1} = 1$, we have $\sum_{a\in A}\frac{1}{|Ga|} = (\text{\# of orbits of } G)$. Therefore, we have

$$(\text{\# of orbits of } G) = \frac{1}{|G|}\sum_{a\in A}|G_a| = \frac{1}{|G|}\sum_{g\in G}|A_g|.$$

□

## 3.2 Group Actions by Conjugation

**Definition 3.2.1: Conjugate**

Let $G$ be a group. We say $a, b \in G$ are *conjugate* if

$$\exists g \in G,\ b = gag^{-1}.$$

In other words, if $G$ acts on $G$ by conjugation $g \cdot a = gag^{-1}$, $a, b \in G$ are conjugate if they are in the same orbit. The orbit of $a$ in this case is called *conjugacy class* of $a$.

**Note:-**

Under conjugation, the stabilizer of $a$ is the centralizer of $a$.

**Example 3.2.2**

(i) The conjugacy class of $a$ is $\{1\}$ if and only if $a \in Z(G)$.

(ii) Let $\sigma \in S_n$ has the *cycle type* $(n_1, n_2, \cdots, n_r)$. Then, as $\sigma$ and its conjugation have the same cycle type, the conjugacy class of $\sigma$ is the collection of permutations with the same cycle type of $\sigma$.

**Corollary 3.2.3**

Let $G \curvearrowright A$ and let $a \in A$. If $[G{:}C_G(a)]$ is finite, then

$$|\text{conjugacy class of } a| = [G{:}C_G(a)].$$

***Proof.*** Direct consequence of Orbit-Stabilizer Theorem. □

**Example 3.2.4**

Let $1 \leq m \leq n$. Let $\sigma = (1\,2\cdots m)$ be an $m$-cycle in $S_n$. Then, there are $n(n-1)\cdots(n-m+1)/m$ number of $m$-cycles in $S_n$. Therefore, $|C_{S_n}(\sigma)| = |G|/[n(n-1)\cdots(n-m+1)/m] = m\cdot(n-m)!$. One may note that $C_{S_n}(\sigma) = \{\,\sigma^i\tau \mid 0 \leq i \leq m-1 \text{ and } \tau \in S_{n-m}\,\}$.

**Theorem 3.2.5** Class Equation

Let $G$ be a finite group. If $C_1, C_2, \cdots, C_r$ are all the distinct conjugacy classes of $G$ such that $\forall i \in [r]$, $C_i \nsubseteq Z(G)$, and if $a_i \in C_i$ for each $i \in [r]$, then

$$|G| = |Z(G)| + \sum_{i=1}^{r}[G{:}C_G(a_i)].$$

***Proof.*** $Z(G)$ is the union of all singleton conjugacy classes by Example 3.2.2 (i). The result follows from Corollary 3.2.3 and the fact that conjugacy classes partition $G$. □

**Example 3.2.6**

- $|S_3| = 1+2+3$
- $|Q_8| = 2+2+2+2$
- $|D_4| = 2+2+2+2$

**Corollary 3.2.7**

Let $G$ be a group of order $p^n$ where $p$ is a prime number and $n \geq 1$. Then, $|Z(G)| = p^k$ for some $k \geq 1$.

***Proof.*** In Class Equation, each $[G{:}C_G(a_i)]$ is a multiple of $p$. Therefore, we must have $p \mid |Z(G)|$ while $Z(G) \neq \varnothing$. □

**Corollary 3.2.8**

Let $G$ be a group of order $p^2$ where $p$ is a prime number, then $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

***Proof.*** By Corollary 3.2.7, we have $|Z(G)| = p^2$ or $|Z(G)| = p$.

If $|Z(G)| = p^2$, then If $G$ has an element of order $p^2$, then $G \cong \mathbb{Z}_{p^2}$. If every nonidentity element of $G$ has order $p$, then $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Then, $f : \mathbb{Z}_p \times \mathbb{Z}_p \to G$ defined by $(i, j) \mapsto x^i y^j$ where $x \in G \setminus \{1\}$ and $y \in G \setminus \langle x \rangle$ is a group isomorphism.

Now, assume $|Z(G)| = p$. Then, $G/Z(G) \cong \mathbb{Z}_p$. By Theorem 2.3.2, we get $Z(G) = G$, which is a contradiction. □

**Theorem 3.2.9**

Let $G$ be a group and let $N \trianglelefteq G$. Let $K$ be a conjugacy class of $G$. Then, we have $K \subseteq N$ or $K \cap N = \varnothing$. In particular, $N$ is union of some conjugacy classes of $G$.

***Proof.*** Assume $K \cap N \neq \varnothing$ and take any $x \in K \cap N$. Then, for any $g \in G$, $gxg^{-1} \in gNg^{-1} = N$; thus $K \subseteq N$. □

**Example 3.2.10**

There are four cycle types of $A_5$; $(1), (1\,2\,3), (1\,2\,3\,4\,5), (1\,2)(3\,4)$. Note that, even if

$\sigma$ and $\sigma'$ have the same cycle type so that $\sigma' = \tau\sigma\tau^{-1}$ for some $S_5$, $\sigma$ and $\sigma'$ may not be in the same conjugacy class since $\tau$ may not be an element of $A_5$.

- $C_{S_5}((1\,2\,3)) = \langle(1\,2\,3),(4\,5)\rangle$ and $C_{A_5}((1\,2\,3)) = \langle(1\,2\,3)\rangle \cong \mathbb{Z}_3$; thus the conjugacy class consists of 20 elements; which are all the 3-cycles in $A_5$.
- $C_{S_5}((1\,2\,3\,4\,5)) = \langle(1\,2\,3\,4\,5)\rangle$ and $C_{A_5}((1\,2\,3\,4\,5)) = \langle(1\,2\,3\,4\,5)\rangle \cong \mathbb{Z}_5$; the conjugacy class of $(1\,2\,3\,4\,5)$ consists of 12 elements while $A_5$ has 24 5-cycles. The conjugacy class of $(1\,3\,5\,2\,4)$ consists of 12 elements.
- $|C_{S_5}((1\,2)(3\,4))| = 8$ and $|C_{A_5}((1\,2)(3\,4))| = 4$; the conjugacy class of $(1\,2)(3\,4)$ consists of all 15 elements.

Therefore, the class equation of $A_5$ is $|A_5| = 1 + 12 + 12 + 15 + 20$; thus by Theorem 3.2.9, if there is a nontrivial normal subgroup then its order is sum of orders of some conjugacy classes but there is no way to make it divisible by $|A_5| = 60$. Therefore, $A_5$ is simple.

**Definition 3.2.11: Conjugate Subsets**

Let $G$ be a group. We say $A, B \subseteq G$ are *conjugate* if $A = gBg^{-1}$ for some $g \in G$.

**Corollary 3.2.12**

Let $G \curvearrowright \mathcal{P}(G)$ by conjugation; Then, $[G{:}N_G(A)] = |G \cdot A| = |\text{orbit of } A|$.

***Proof.*** $N_G(A) = \{g \in G \mid gAg^{-1} = A\} = G_A$ by definition. The result follows from Orbit-Stabilizer Theorem. □

## 3.3 Automorphisms

**Note:-**

Let $G$ be a group and let $N \trianglelefteq G$. We may let $G \curvearrowright N$ by conjugation. Then, the permutation representation evaluated at $g \in G$ is defined by $\varphi_g : N \to N$ and $n \mapsto gng^{-1}$

**Theorem 3.3.1**

Let $G$ be a group and let $N \trianglelefteq G$. Let $G \curvearrowright N$ by conjugation. Then, for each $g \in G$, we have $\varphi_g \in \mathrm{Aut}(N)$. Moreover, $\ker(\varphi) = C_G(N)$. In particular, $G/C_G(N)$ is isomorphic to a subgroup of $\mathrm{Aut}(N)$.

***Proof.*** For each $n_1, n_2 \in N$, we have $\varphi_g(n_1n_2) = gn_1n_2g^{-1} = gn_1g^{-1}gn_2g^{-1} = \varphi_g(n_1)\varphi_g(n_2)$; thus $\varphi_g$ is a group isomorphism as it is already $\varphi_g \in S(N)$.

We have

$$\ker(\varphi) = \{g \in G \mid \forall n \in \mathbb{N},\ \varphi_g(n) = n\} = \{g \in G \mid \forall n \in \mathbb{N},\ ng = gn\} = C_G(N).$$

Moreover, by First Isomorphism Theorem, $G/C_G(N) \cong \mathrm{im}(\varphi) \leq \mathrm{Aut}(N)$. □

**Corollary 3.3.2**

Let $G$ be a group and let $H \leq G$. Then, $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(G)$.

***Proof.*** We have $H \trianglelefteq N_G(H)$, $C_G(H) = C_{N_G(H)}(H)$, and $N_G(H) = N_{N_G(H)}(H)$ by definition. The result follows from Theorem 3.3.1. The last assertion is obtained by letting $H := G$. □

**Definition 3.3.3: Inner Automorphism Group**

For each $c \in G$, mapping $i_c : G \to G$ defined by $g \mapsto cgc^{-1}$ is an automorphism and is called an *inner automorphism on $G$ induced by $c$*. We define

$$\mathrm{Inn}(G) \triangleq \{\, i_c \in \mathrm{Aut}(G) \mid c \in G \,\}$$

and call it the *inner automorphism group of $G$*.

**Lemma 3.3.4**

Let $G$ be a group. Then, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

***Proof.*** $\mathrm{id}_G = i_1 \in \mathrm{Inn}(G)$. For each $c \in G$, $(i_c)^{-1} = i_{c^{-1}}$ is already an automorphism on $G$. Take any $c, c' \in G$. Then, for all $g \in G$,

$$(i_c \circ i_{c'})(g) = i_c(c'g(c')^{-1}) = cc'g(c')^{-1}c^{-1} = (cc')g(cc')^{-1} = i_{cc'}(g).$$

Therfore, $i_c \circ i_{c'} = i_{cc'}$; $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

Take any $c \in G$ and $\sigma \in \mathrm{Aut}(G)$. Then, for each $g \in G$,

$$(\sigma \circ i_c \circ \sigma^{-1})(g) = \sigma(c\sigma^{-1}(g)c^{-1}) = \sigma(c)g\sigma(c^{-1}) = \sigma(c)g\sigma(c)^{-1} = i_{\sigma(c)}(g).$$

Therefore, $\sigma \circ i_c \circ \sigma^{-1} = i_{\sigma(c)} \in \mathrm{Inn}(G)$. Hence, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. □

**Definition 3.3.5: Outer Automorphism Group**

Let $G$ be a group. Justified by Lemma 3.3.4, we

$$\mathrm{Aut}(G)/\,\mathrm{Inn}(G).$$

the *outer automorphism group of $G$*.

**Corollary 3.3.6**

Let $G$ be a group. Then, $\mathrm{Inn}(G) \cong G/Z(G)$.

***Proof.*** Let $G \curvearrowright G$ by conjugation so that $\varphi : G \twoheadrightarrow \mathrm{Inn}(G)$ is a permutation representation. Then, $\ker(\varphi) = Z(G)$; the result follows from First Isomorphism Theorem. □

**Example 3.3.7**

- $\mathrm{Inn}(D_4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathrm{Inn}(Q_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathrm{Inn}(S_n) \cong S_n$ for $n \geq 3$.

**Definition 3.3.8**

For each integer $n \geq 1$, define

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\, k \in \mathbb{Z}_n \mid \gcd(k, n) = 1 \,\}$$

so that $(\mathbb{Z}/n\mathbb{Z})^*$ is an abelian group under usual multiplication.

**Theorem 3.3.9**

For each $n \in \mathbb{Z}_+$, $\mathrm{Aut}(\mathbb{Z}_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

***Proof.*** Take any $k \in \mathbb{Z}_+$ such that $\gcd(k, n) = 1$. Consider the map $f_k \colon \mathbb{Z}_n \to \mathbb{Z}_n$ by $\ell \mapsto k\ell$. Then, clearly, $f_k \in \mathrm{Aut}(\mathbb{Z}_n)$.

Now, define $\Phi \colon (\mathbb{Z}/n\mathbb{Z}) * \to \mathrm{Aut}(\mathbb{Z}_n)$ by $k \mapsto f_k$. Then, it is easy to check $\Phi$ is an injective group homomorphism. Take any $f \in \mathrm{Aut}(\mathbb{Z}_n)$ and let $k \triangleq f(1)$. Then, $f = f_k$. $\square$

**Note:-**

- $\neg(G$ is abelian $\implies \mathrm{Aut}(G)$ is abelian).
- $\neg(G$ is cyclic $\implies \mathrm{Aut}(G)$ is cyclic).

## 3.4 Sylow Theorems

**Definition 3.4.1: Sylow $p$-Subgroup**

Let $G$ be a group of order $p^n m$ where $p$ is a prime and $\gcd(p, m) = 1$. A subgroup of $G$ of order $p^\alpha$ where $1 \leq \alpha \leq n$ is called a *$p$-subgroup* of $G$. A subgroup of $G$ of order $p^n$ (or, equivalently, a maximal $p$-subgroup) is called a *Sylow $p$-subgroup* of $G$. Write

$$\mathrm{Syl}_p(G) = \{\, \text{Sylow } p\text{-subgroups of } G \,\}$$

to denote the set of all Sylow $p$-subgroups of $G$. Write

$$n_p = n_p(G) \triangleq |\,\mathrm{Syl}_p(G)|.$$

**Lemma 3.4.2**

Let $G$ be a group. Then, if $P \in \mathrm{Syl}_p(G)$ and $Q$ is a $p$-subgroup of $G$, then $Q \cap N(P) = Q \cap P$.

***Proof.*** Let $H \triangleq Q \cap N(P)$. We already have $Q \cap P \leq H$. As $H \leq N(P)$ and $P \trianglelefteq N(P)$, we have $HP = PH \leq N(P) \leq G$ by Corollary 2.3.8. As $|PH| = |P||H|/|P \cap H|$ is a power of $p$ and $P \leq PH$, we have $|PH| = p^n$; thus $|H| = |P \cap H|$, i.e., $Q \cap N(P) = H \leq P$. $\square$

**Lemma 3.4.3**

Let $G$ be an abelian group and let $p$ be a prime. Then, $p \mid |G|$ implies that $G$ has an element of order $p$.

***Proof.*** Write $|G| = pk$. We shall conduct induction on $k$. If $k = 1$, then $G$ is cyclic by Corollary 2.1.11; thus it is done.

Now, fix $k \geq 2$ and take $x \in G \setminus \{1\}$. We have two cases: $p \mid |x|$ and $p \nmid |x|$.

- If $p \mid |x|$, then $|x| = pn$ for some $n \in \mathbb{Z}_+$, and we have $|x^n| = p$; we are done.
- Assume $p \nmid |x|$ and let $N \triangleq \langle x \rangle$. As $G$ is abelian, $N \trianglelefteq G$. Then, $p \mid |G|/|N| = |G/N| < |G|$ and $G/N$ is abelian. By induction hypothesis, $\exists y \in G$, $|Ny| = p$. Then, $y \notin N$ while $y^p \in N$. Put $m \triangleq |y^p|$. Then, as $y^{mp} = (y^p)^m = 1$, we have $m \mid |y| \mid mp$ while $y \notin \langle y^p \rangle \subseteq N$. Therefore, the only option is $|y| = mp$; this reduces to the first case. □

**Theorem 3.4.4** Sylow Theorems

Let $G$ be a group and let $|G| = p^n m$ where $p$ is a prime and $\gcd(p,m) = 1$.

(i) For each $0 \le k \le n$, $G$ has a subgroup of order $p^k$. In particular, $\mathrm{Syl}_p(G) \neq \varnothing$.

(ii) For each $P \in \mathrm{Syl}_p(G)$, and for each $p$-subgroup $Q$ of $G$, we have $Q \le gPg^{-1}$ for some $g \in G$. In particular, if $Q \in \mathrm{Syl}_p(G)$, then $Q = gPg^{-1}$ for some $g \in G$.

(iii) $\forall P \in \mathrm{Syl}_p(G)$, $n_p = [G{:}N(P)] \equiv 1 \pmod{p}$, and $n_p \mid m$.

***Proof.***

(i) The assertion trivially holds when $|G| = 1$ or $k = 0$. Hence, we conduct induction on $|G|$. Fix any $G$ and assume (i) holds for all groups of order less than $|G|$. Take any $1 \le k \le n$. There are two cases: $p \mid |Z(G)|$ and $p \nmid |Z(G)|$.

- Assume $p \mid |Z(G)|$. Then, by Lemma 3.4.3, $Z(G)$ has a subgroup $N$ of order $p$. As $N \le Z(G)$, $N$ is a normal subgroup of $G$; thus we may let $\overline{G} \triangleq G/N$. Since $|\overline{G}| = |G|/|N| = p^{n-1}m < |G|$ by Lagrange Theorem, by induction hypothesis, $\overline{G}$ has a subgroup $\overline{P}$ of order $p^{k-1}$. By Fourth Isomorphism Theorem, there exists a subgroup $P$ of $G$ containing $N$ such that $P/N = \overline{P}$. Then, $|P| = |\overline{P}||N| = p^k$ by Lagrange Theorem.
- Assume $p \nmid |Z(G)|$. By Class Equation, there exists $g \in G$ such that $p \nmid [G{:}C_G(g)]$. As $|G| = |C_G(g)|[G{:}C_G(g)]$ by Lagrange Theorem, $p^n \mid |C_G(g)|$. Moreover, as $C_G(g) \lneq G$, by induction hypothesis, there exists a subgroup of $C_G(g)$ of order $p^k$, which is also a subgroup of $G$.

(ii) Fix $P \in \mathrm{Syl}_p(G)$ and let

$$\mathcal{S} \triangleq \{\, gPg^{-1} \mid g \in G \,\}.$$

Then, $G \curvearrowright \mathcal{S}$ by conjugation. Note that $\forall P' \in \mathcal{S}$, $|P'| = |P| = p^n$ by Lemma 2.2.4.

Take any $p$-subgroup $Q$ of $G$. Then, $Q$ also acts on $S$ by conjugation. Fix $P' \in \mathcal{S}$. The stabilizer of $P'$ of the group action $Q \curvearrowright \mathcal{S}$ is

$$\{\, q \in Q \mid qP'q^{-1} = P' \,\} = N_Q(P').$$

Hence, by Orbit-Stabilizer Theorem, we have $|Q \cdot P'| = [Q{:}N_Q(P')]$. On the other hand, by Lemma 3.4.2, $N_Q(P') = N_G(P') \cap Q = P' \cap Q$. Hence, $|Q \cdot P'| = [Q{:}P' \cap Q]$ for each $P' \in \mathcal{S}$.

> **Claim 1.** $|\mathcal{S}| \equiv 1 \pmod{p}$.
>
> ***Proof.*** Fix any $P' \in \mathcal{S}$. Let $\mathcal{O}_1, \cdots, \mathcal{O}_s$ be the orbits of $P' \curvearrowright \mathcal{S}$ with $P' \in \mathcal{O}_1$. Then, by the previous discussion, $|\mathcal{O}_1| = |P' \cdot P'| = [P'{:}P' \cap P'] = 1$. Moreover, for each $P'' \in \mathcal{S} \setminus \{P'\}$, as $P' \cap P'' \lneq P'$, $|P' \cdot P''| = [P'{:}P' \cap P'']$ is a power of $p$; thus $p \mid |\mathcal{O}_i|$ for each $i \in \{2, 3, \cdots, s\}$. Hence, $|\mathcal{S}| = \sum_{i=1}^{s} |\mathcal{O}_i| \equiv |\mathcal{O}_1| = 1 \pmod{p}$. □

Suppose there exists a $p$-subgroup $Q$ such that $Q \nsubseteq P'$ for all $P' \in \mathcal{S}$. Therefore, $|Q \cap P'| < |P'|$; hence $p \mid [Q{:}P' \cap Q] = |Q \cdot P'|$ for each $P' \in \mathcal{S}$. However, this implies $p \mid |\mathcal{S}|$, which contradicts Claim 1.

(iii) By (ii), $\mathcal{S}$ (defined in the proof of (ii)) equals $\mathrm{Syl}_p(G)$. Hence, $n_p = |\mathcal{S}| \equiv 1 \pmod{p}$ by Claim 1. Moreover, $\mathcal{S}$ is the orbit of $P$ under the group action $G \curvearrowright \mathcal{P}(G)$ by conjugation.

Therefore, by Corollary 3.2.12, $n_p = |G\cdot P| = [G{:}N_G(P)] = |G|/|N_G(P)|$ while $p^n = |P| \mid |N_G(P)|$. Therefore, $n_p \mid m$. $\square$

**Example 3.4.5**

(i) Assume $|G| = 200 = 2^3\cdot 5^2$. Then, $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 8$ by Sylow Theorems (iii); thus $n_5 = 1$; thus $G$ is not simple by Corollary 3.4.6.

(ii) Assume $|G| = 30 = 2\cdot 3\cdot 5$. Then, $n_3 = 10$ and $n_5 = 6$ for the sake of contradiction.

**Corollary 3.4.6**

Let $K \in \mathrm{Syl}_p(G)$. Then, $K \trianglelefteq G \iff n_p = 1$.

***Proof.***

($\Rightarrow$) We have $gKg^{-1} = K$ for all $g \in G$; hence $\mathrm{Syl}_p(G) = \{K\}$ by Sylow Theorems (ii).

($\Leftarrow$) As $gKg^{-1} \in \mathrm{Syl}_p(G)$ for each $g \in G$, this implies $\forall g \in G$, $gKg^{-1} = K$; that is to say $K \trianglelefteq G$. $\square$

**Corollary 3.4.7** Cauchy Theorem

If $G$ is a finite group and $p \mid |G|$ for some prime $p$, then $G$ has an element of order $p$.

***Proof.*** By Sylow Theorems (i), $G$ has a subgroup of order $p$, which is cyclic by Corollary 2.1.11. Any nonidentity element of the cyclic subgroup has order $p$. $\square$

**Corollary 3.4.8**

Let $G$ be a group of order $pq$ where $p$ and $q$ are primes with $p < q$. Let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$.

(i) $Q \trianglelefteq G$

(ii) If $P \trianglelefteq G$, then $G \cong \mathbb{Z}_{pq}$. In particular, if $p \nmid q-1$, then $G \cong \mathbb{Z}_{pq}$.

***Proof.***

(i) By Sylow Theorems (iii), we have $n_q \equiv 1 \pmod q$ and $n_q = p$. Therefore, $n_q = 1$ as $p < q$. By Corollary 3.4.6, $Q \trianglelefteq G$.

(ii) We have $P = \langle x\rangle \cong \mathbb{Z}_p$ and $Q = \langle y\rangle \cong \mathbb{Z}_q$ for some $x, y \in G$. As $G/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P) \cong \mathrm{Aut}(\mathbb{Z}_p) \cong (\mathbb{Z}/p\mathbb{Z})^*$ by Theorems 3.3.1 and 3.3.9, we have $|G/C_G(P)| \mid p-1$. At the same time, $|G/C_G(P)| \mid |G| = pq$. Hence, the only option is $|G/C_G(P)| = 1$, i.e., $G = C_G(P)$; thus $xy = yx$. Therefore, $|xy| = pq$ by Theorem 1.5.3 (iii); $G \cong \mathbb{Z}_{pq}$.

Now, assume $p \nmid q-1$. We have $n_p \equiv 1 \pmod p$ and $n_p \mid q$ by Sylow Theorems (iii). Then, $n_p = 1$ as $p \nmid q-1$; thus $P \trianglelefteq G$ by Corollary 3.4.6. $\square$

**Corollary 3.4.9**

Let $G$ be a group of order 12. Then, $G$ has a normal Sylow 3-subgroup or $G \cong A_4$. When $G = A_4$, $G$ has a unique Sylow 2-subgroup. In particular, $G$ is not simple.

***Proof.*** If $n_3 = 1$, then there (uniquely) exists a normal Sylow 3-subgroup by Corollary 3.4.6. Now, assume $n_3 \neq 1$.

Then, by Sylow Theorems (iii), we have $n_3 = 4 = [G{:}N(P)]$; thus $P = N(P)$ by Lagrange Theorem. Let $G$ act on $\mathrm{Syl}_3(G)$ by conjugation. Let $\varphi\colon G \hookrightarrow S_4$ be a permutation representation of the group action. Note that the stabilizer of $P \in \mathrm{Syl}_3(G)$ is $G_P = N(P) = P$. Therefore,

$\ker(\varphi) = K(G, \mathrm{Syl}_3(G)) = \bigcap_{P\in\mathrm{Syl}_3(G)} G_P = \bigcap_{P\in\mathrm{Syl}_3(G)} P = \{1\}$ as the intersection of two distinct subgroups of order 3 is trivial. Hence, by Theorem 2.3.3, $\varphi$ is injective. Therefore, $|\mathrm{im}(\varphi)| = 12$; thus $\mathrm{im}(\varphi) \trianglelefteq S_4$ by Lemma 2.2.6. As $G$ has an element $x$ of order 3 by Cauchy Theorem, $|\varphi(x)| = 3$ for some $x \in G$. Then, as $\varphi(x) \in \varphi(G) \cap A_4 \trianglelefteq A_4$, by Claim 2 in the proof of Theorem 2.4.7, $\varphi(G) \subseteq A_4$; that is to say $\varphi(G) = A_4$. Moreover, if $V \in \mathrm{Syl}_2(G)$, then there cannot be another Sylow-2 subgroup by simple counting of elements. (Note that there are already 4 distinct Sylow-3 subgroups.) □

**Corollary 3.4.10**

Let $G$ be a group of order $p^2q$ where $p$ and $q$ are distinct prime numbers. Then, $G$ has a normal Sylow $p$-subgroup or a normal Sylow $q$-subgroup. In particular, $G$ is not simple.

***Proof.*** Fix any $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. There are two cases: $p > q$ and $p < q$.

- Assume $p > q$. By Sylow Theorems (iii), $n_p \equiv 1 \pmod p$ and $n_p \mid q$, which implies $n_p = 1$. Hence, by Corollary 3.4.6.
- Assume $p < q$. If $n_q = 1$, then we immediately have $Q \trianglelefteq G$ by Corollary 3.4.6. Hence, assume $n_q > 1$. By Sylow Theorems (iii), $n_q \equiv 1 \pmod q$ and $n_q \mid p^2$. As $n_q \geq q + 1 > p$, we have $n_q = p^2$. Now, we are left with $q \mid p^2 - 1 = (p+1)(p-1)$, which implies $q = p + 1$ as $p < q$. Hence, $p = 2$ and $q = 3$; $|G| = 12$. The result follows from Corollary 3.4.9. □

**Example 3.4.11**

(i) Let $G$ be a group of order $200 = 2^3 \cdot 5^2$. By Sylow Theorems (iii), $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 8$, which implies $n_5 = 1$. Hence, by Corollary 3.4.6, $G$ has a normal Sylow-5 subgroup; $G$ is not simple.

(ii) Let $G$ be a group of order $30 = 2 \cdot 3 \cdot 5$. We have $n_3 \equiv 1 \pmod 3$, $n_3 \mid 10$, $n_5 \equiv 1 \pmod 5$, and $n_5 \mid 6$ by Sylow Theorems (iii). Suppose $n_3 \neq 1$ and $n_5 \neq 1$ for the sake of contradiction. The only option if $n_3 = 10$ and $n_5 = 6$. Then, we have ten Sylow 3-subgroups and six Sylow 5-subgroups and they mutually intersect only at 1. Therefore, $|G| \geq 1 + 2 \cdot 9 + 5 \cdot 5 = 44$, which is a contradiction. Therefore, $n_3 = 1$ or $n_5 = 1$; thus $G$ is not simple by Corollary 3.4.6.

(iii) Let $G$ be a group of order $36 = 2^3 \cdot 3^2$. By Sylow Theorems (i), we have $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 8$. Hence, $n_3 = 1$ or $n_3 = 4$. If $n_3 = 1$, then $G$ is not simple by Corollary 3.4.6. Now, assume $n_3 = 4$ and let $H$ and $K$ be two distinct Sylow 3-subgroups. Then, by Theorem 2.3.6, $|HK| = 81/|H \cap K| \leq |G|$; thus we must have $|H \cap K| = 3$. Moreover, as $H$ and $K$ are abelian by Corollary 3.2.8, $H \cap K \trianglelefteq H, K \leq G$, which implies that $G$ is not simple. Therefore, $G$ is simple in either case.

# Chapter 4

# Product of Groups

## 4.1 Direct Products

**Definition 4.1.1: Direct Product**

(See Definition 1.1.13.)
Let $G_1, G_2, \cdots, G_n$ be groups. Then, the operation on $G_1 \times \cdots \times G_n$ given by

$$(g_1, \cdots, g_n) * (g_1', \cdots, g_n') = (g_1 g_1', \cdots, g_n g_n')$$

is a group operation. We call the group $(G_1 \times \cdots \times G_n, *)$ the *direct product* of $G_1, \cdots, G_n$.

**Notation 4.1.2**

Let $G_1, G_2, \cdots, G_n$ be groups and consider their direct product $G_1 \times G_2 \times \cdots, G_n$. For each $i \in [n]$, define

$$\tilde{G}_i \triangleq \{(1_{G_1}, \cdots, 1_{G_{i-1}}, g_i, 1_{G_{i+1}}, \cdots, 1_{G_n}) \mid g_i \in G_i\} \leq G_1 \times G_2 \times \cdots, G_n$$

so that $G_1 \cong \tilde{G}_i$ and

$$(G_1 \times G_2 \times \cdots \times G_n)/\tilde{G}_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

Abusing the notation, we may write $G_i$ instead of $\tilde{G}_i$.

**Note:-**

Let a group structure is given for $G_1 \times G_2$. If both projections are group homomorphisms, then the group structure is the direct product.

**Lemma 4.1.3**

Let $G$ be a group and let $H, K \trianglelefteq G$ and $H \cap K = \{1\}$. Then, $\forall a \in M$, $\forall b \in N$, $ab = ba$.

***Proof.*** Take any $h \in H$ and $k \in K$. Then, $h^{-1}kh \in K$ and $khk^{-1} \in H$ by normality; thus $h^{-1}khk^{-1} \in H \cap K$, which implies $h^{-1}khk^{-1} = 1$. Therefore, we have $kh = hk$. $\square$

**Theorem 4.1.4**

Let $G$ be a group and let $N_1, N_2, \cdots, N_k$ be normal subgroups of $G$. Let $f : N_1 \times \cdots \times N_k \to G$ be defined by $(a_1, \cdots, a_k) \mapsto a_1 \cdots a_k$. If $f$ is bijective, then $f$ is a group isomorphism.

*Proof.* If $\{1\} \subsetneq N_i \cap N_j$ for some $i \neq j$, then it contradicts the injectivity of $f$. Hence, by Lemma 4.1.3, $a_i a_j = a_j a_i$ for all $a_i \in N_i$ and $a_j \in N_j$.

Take any $(a_1, \cdots, a_k), (b_1, \cdots, b_k) \in N_1 \times \cdots \times N_k$. Then,

$$\begin{aligned} f((a_1, \cdots, a_k)(b_1, \cdots, b_k)) &= f(a_1 b_1, a_2 b_2, \cdots, a_k b_k) \\ &= a_1 b_1 a_2 b_2 \cdots a_k b_k \\ &= a_1 a_2 \cdots a_k b_1 b_2 \cdots b_k \\ &= f(a_1, \cdots, a_k) f(a_2, \cdots, a_k). \end{aligned}$$

Hence, the result follows. □

### Corollary 4.1.5

Let $G$ be a group and let $N_1, N_2, \cdots, N_k$ be normal subgroups of $G$. If

(i) $G = N_1 N_2 \cdots N_k$ and

(ii) $\forall i \in [k]$, $N_i \cap (N_1 \cdots N_{i-1} N_{i+1} \cdots N_k) = \{1\}$,

then $G \cong N_1 \times N_2 \times \cdots \times N_k$.

*Proof.* (i) essentially says that $f$ in Theorem 4.1.4 is surjective.

Suppose $a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_k$ but $(a_1, \cdots, a_k) \neq (b_1, \cdots, b_k)$. Then,

$$\begin{aligned} b_1^{-1} a_1 &= (b_2 \cdots b_k)(a_2 \cdots a_k)^{-1} \\ &= b_2 \cdots b_{k-1} b_k a_k^{-1} a_{k-1}^{-1} \cdots a_2^{-1} \end{aligned}$$

As $b_k a_k^{-1} N_k \trianglelefteq G$, $(b_k a_k^{-1})(a_{k-1}^{-1} \cdots a_2^{-1}) = (a_{k-1}^{-1} \cdots a_2^{-1}) n_k$ for some $n_k \in N_k$. Therefore, this continues to

$$= b_2 \cdots b_{k-1} a_{k-1}^{-1} \cdots a_2^{-1} n_k$$

This continues and we yield

$$= n_2 n_3 \cdots n_k \in N_2 N_3 \cdots N_{k-1}$$

for some $n_2, n_3, \cdots, n_{k-1}$ where $n_i \in N_i$ for each $i \in \{2, 3, \cdots, k-1\}$. By (ii), we have $a_1 = b_1$; and thus $a_2 a_3 \cdots a_k = b_2 b_3 \cdots b_k$. We may repeat this and obtain $a_i = b_i$ for all $i \in [k]$. Hence, the function $f$ in Theorem 4.1.4 is injective; the result follow from Theorem 4.1.4. □

### Definition 4.1.6: Decomposable Group

Let $G$ be a group. We say $G$ is *decomposable* if $G \cong M \times N$ for some nontrivial groups $M$ and $N$.

**Note:-**

If $G$ is decomposable, then $G$ has at least four normal subgroups.

### Corollary 4.1.7

Let $G$ be a group of order $p^2 q$ where $p$ and $q$ are distinct primes with $q \not\equiv 1 \pmod{p}$ and $p^2 \not\equiv 1 \pmod{q}$. Then, $G \cong \mathbb{Z}_{p^2 q}$ or $G \cong \mathbb{Z}_{pq} \times \mathbb{Z}_p$.

*Proof.* By Sylow Theorems (iii), we have $n_p \equiv 1 \pmod{p}$, $n_p \mid q$, $n_q \equiv 1 \pmod{q}$, and $n_q \mid p^2$. By the constraints, we have $n_p = 1$ and $n_q = 1$. By Corollary 3.4.6, the unique $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$ are normal in $G$. Moreover, $P \cap Q = \{1\}$ by Lagrange Theorem. By Theorem 2.3.6, $PQ = G$. Hence, $G \cong P \times Q$ by Corollary 4.1.5. By Corollary 3.2.8, $P \cong \mathbb{Z}_{p^2}$ and $P \cong \mathbb{Z}_p \times \mathbb{Z}_p$. The result follows from Example 1.5.9. □

**Example 4.1.8**

(i) Suppose $\mathbb{Z} \cong N \times H$ for some nontrivial normal subgroups $N, H \trianglelefteq \mathbb{Z}$. However, any intersection of two nontrivial subgroups of $\mathbb{Z}$ is nontrivial; thus $\mathbb{Z}$ is indecomposable.

(ii) The image of the natural projection $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/6\mathbb{Z}$ is decomposable ($\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_2 \times \mathbb{Z}_3$) while $\mathbb{Z}$ is indecomposable.

(iii) $S_n$ for $n \geq 5$ is indecomposable.

(iv) Let $n$ be an odd positive integer and consider $D_{2n}$. Let $M \triangleq \langle s, r_1^2 \rangle$ and $N \triangleq \langle r_1^n \rangle$. Then, they are nontrivial normal subgroups whose intersection is trivial and $MN = D_{2n}$. Therefore, $D_{2n} \cong D_n \times \mathbb{Z}_2$.

## 4.2 Fundamental Theorem of Finitely Generated Abelian Groups

**Lemma 4.2.1**

Let $G$ be an abelian group generated by $g_1, \cdots, g_k$. For any nonnegative integers $c_1, c_2, \cdots, c_k$ with $\gcd(c_1, \cdots, c_k) = 1$, there exists generators $x_1, \cdots, x_k$ for $G$ such that $x_1 = c_1 g_1 + \cdots + c_k g_k$.

***Proof.*** We conduct the induction on $S := c_1 + \cdots + c_k$. If $S = 1$, then simply changing the order suffices.

If $S > 1$, then there exist at least two nonzero $c_i$. WLOG, $c_1 \geq c_2 > 0$. As

(i) $g_1, g_1 + g_2, g_3, g_4, \cdots, g_k$ generate $G$,

(ii) $\gcd(c_1 - c_2, c_2, \cdots, c_k) = 1$, and

(iii) $(c_1 - c_2) + c_2 + \cdots, c_k < S$,

by induction hypothesis, there exist generators $x_1, \cdots, x_k$ such that $x_1 = (c_1 - c_2)g_1 + c_2(g_1 + g_2) + c_3 g_3 + \cdots c_k g_k$. The result follows from $(c_1 - c_2)g_1 + c_2(g_1 + g_2) = c_1 g_1 + c_2 g_2$. □

**Definition 4.2.2: Basis of Group**

Let $G$ be a group. Then, $\{g_1, g_2, \cdots, g_k\} \subseteq G$ is a *basis* of $G$ if $G = \langle g_1, \cdots, g_k \rangle$ and

$$\forall m_1, \cdots, m_k \in \mathbb{Z}, (m_1 g_1 + \cdots + m_k g_k = 0 \iff m_1 g_1 = \cdots = m_k g_k = 0).$$

**Lemma 4.2.3**

If $G$ is a finitely generated abelian group, then $G$ has a basis.

***Proof.*** Let $g_1, g_2, \cdots, g_k$ be generators of $G$ with minimum $|g_1|$ among generators with minimum size. We shall conduct induction on $k$. If $k = 1$, then $G$ is cycle; $\{g_1\}$ is a basis. Assume $k > 1$.

WLOG, $|g_1| \leq |g_2| \leq \cdots \leq |g_k|$. Note that $g_2, \cdots, g_k$ are minimal generators of $\langle g_2, \cdots, g_k \rangle$. Hence, by induction hypothesis, $\langle g_2, \cdots, g_k \rangle$ has a basis $\{h_1, \cdots, h_{k-1}\}$. Note that $\langle g_1, h_1, \cdots, h_{k-1} \rangle = G$.

Suppose $\{g_1, h_1, \cdots, h_{k-1}\}$ is not a basis of $G$ for the sake of contradiction. Then, there exist $n_1, m_1, \cdots, m_{k-1} \in \mathbb{Z}$ such that $n_1 g_1 + m_1 h_1 + \cdots + m_{k-1} h_{k-1} = 0$ but $n_1 g_1 \neq 0$. Possibly replacing $g_1$ with $-g_1$ and $h_i$ with $-h_i$, WLOG, $0 < n_1 < |g_1|$ and $m_i \geq 0$ for all $i \in [k-1]$.

Let $d \triangleq \gcd(n_1, m_1, \cdots, m_{k-1})$ and let $c_0 \triangleq n_1/d$ and $c_i \triangleq m_i/d$ for each $i \in [k-1]$. By Lemma 4.2.1, there exist generators $x_1, \cdots, x_k$ of $G$ such that $x_1 = c_0 g_1 + c_1 h_1 + \cdots + c_{k-1} h_{k-1}$. Then, as $dx_1 = 0$, we have $|x_1| \leq d \leq n_1 < |g_1|$, which contradicts the minimality of initial choice of $g_1, g_2, \cdots, g_k$. Therefore, $\{g_1, h_1, \cdots, h_{k-1}\}$ is a basis of $G$. □

**Lemma 4.2.4**

Let $G$ be a finitely generated abelian group. If $\{g_1, \cdots, g_k\}$ is a basis of $G$, then $G \cong \langle g_1 \rangle \times \cdots \times \langle g_k \rangle$.

***Proof.*** As $G$ is abelian, $\langle g_i \rangle \trianglelefteq G$ for all $i \in [k]$. Assume

$$m_1 g_1 + m_2 g_2 + \cdots + m_k g_k = n_1 g_1 + n_2 g_2 + \cdots + n_k g_k$$

for some $m_i, n_i \in \mathbb{Z}$. Then, we have $(m_1 - n_1)g_1 + \cdots + (m_k - n_k)g_k = 0$; as $\{g_1, \cdots, g_k\}$ is a a basis, $m_i g_i = n_i g_i$ for all $i \in [k]$. Therefore, by Theorem 4.1.4, $G \cong \langle g_1 \rangle \times \cdots \times \langle g_k \rangle$. □

**Lemma 4.2.5**

Let $p$ be a prime number. If

$$\mathbb{Z}_{p^{u_1}} \times \cdots \times \mathbb{Z}_{p^{u_r}} \cong \mathbb{Z}_{p^{v_1}} \times \cdots \times \mathbb{Z}_{p^{v_s}},$$

for some integers $u_1 \geq \cdots \geq u_r \geq 1$ and $v_1 \geq \cdots \geq v_s \geq 1$, then $r = s$ and $u_i = v_i$ for each $i \in [r]$.

***Proof.*** WLOG, $u_1 \geq v_1$ Note that

$$p^n \mathbb{Z}_{p^m} \cong \begin{cases} \mathbb{Z}_{p^{m-n}} & \text{if } n \leq m \\ \{1\} & \text{otherwise} \end{cases}$$

for each $m, n \in \mathbb{Z}_{\geq 0}$. Therefore, we have

$$\mathbb{Z}_{p^{u_1 - v_1}} \cong p^{v_1}\left(\mathbb{Z}_{p^{u_1}} \times \cdots \times \mathbb{Z}_{p^{u_r}}\right) \cong p^{v_1}\left(\mathbb{Z}_{p^{v_1}} \times \cdots \times \mathbb{Z}_{p^{v_s}}\right) \cong \{1\},$$

which implies $u_1 = v_1$. We continue this process of multiplying $p^{\min\{u_i, v_i\}}$ for $i = 2, 3, \cdots, \min\{r, s\}$ so we obtain the result. □

**Theorem 4.2.6** Fundamental Theorem of Finitely Generated Abelian Group

If $G$ is a finitely generated abelian group, then

$$G \cong \mathbb{Z}^r \times \underbrace{\left(\mathbb{Z}_{p_1^{\beta_{1,1}}} \times \cdots \times \mathbb{Z}_{p_1^{\beta_{1,k_1}}}\right) \times \cdots \times \left(\mathbb{Z}_{p_t^{\beta_{t,1}}} \times \cdots \times \mathbb{Z}_{p_t^{\beta_{t,k_t}}}\right)}_{\textit{torsion part}}$$

for some $r \in \mathbb{Z}_{\geq 0}$, $\beta_{i,j} \geq 1$, distinct primes $p_1, \cdots, p_t$, and $\beta_{i,j} \geq \beta_{i,j'}$ if $j \geq j'$. Furthermore, the expression is unique. $r$ is the expression is called the *rank* of $G$.

***Proof.*** Let $\{g_1, \cdots, g_k\}$ be a basis of $G$. Then, $G \cong \langle g_1 \rangle \times \cdots \times \langle g_k \rangle$ by Lemma 4.2.3. By Corollary 1.5.7, $G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$ where $r \geq 0$ and $n_i \geq 2$. The existence of such expression in the theorem is given by Example 1.5.9.

To prove the uniqueness of the rank, suppose

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s} \cong \mathbb{Z}^{r'} \times \mathbb{Z}_{n'_1} \times \cdots \times \mathbb{Z}_{n'_{s'}}$$

for some $r' \in \mathbb{Z}_{\geq 0}$ and $n'_i \geq 2$. Let $p$ be a prime number which is greater than any of $n_1, \cdots, n_s, n'_1, \cdots, n'_{s'}$. Then,

$$p\mathbb{Z}_{n_i} = \mathbb{Z}_{n_i} \text{ and } p\mathbb{Z}_{n'_i} = \mathbb{Z}_{n'_i} \text{ for each } i$$

so

$$pG \trianglelefteq G \text{ and } G/pG \cong (\mathbb{Z}_p)^r \cong (\mathbb{Z}_p)^{r'}.$$

Therefore, $r = r'$ by Lemma 4.2.5.

Moreover, we have

$$G/\mathbb{Z}^r \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s} \cong \mathbb{Z}_{n'_1} \times \cdots \times \mathbb{Z}_{n'_{s'}}.$$

Therefore, the uniqueness follows from Example 1.5.9 and Lemma 4.2.5. □

**Theorem 4.2.7** Fundamental Theorem of Finite Abelian Group

Let $G$ be a finite abelian group.

(i) If the prime factorization of $|G|$ is given by $|G| = p_1^{r_1} \cdots p_t^{r_t}$, then

$$G \cong \left(\mathbb{Z}_{p_1^{\beta_{1,1}}} \times \cdots \times \mathbb{Z}_{p_1^{\beta_{1,k_1}}}\right) \times \cdots \times \left(\mathbb{Z}_{p_t^{\beta_{t,1}}} \times \cdots \times \mathbb{Z}_{p_t^{\beta_{t,k_t}}}\right)$$

for some $\beta_{i,j} \geq 1$ where $\beta_{i,j} \geq \beta_{i,j'}$ if $j \geq j'$ and $\beta_{i,1} + \cdots + \beta_{i,k_i} = r_i$. $p_i^{\beta_{i,j}}$'s are called *elementary divisors of* $G$.

(ii) For some $m_1, \cdots, m_s \in \mathbb{Z}_{>1}$ such that $m_1 m_2 \cdots m_s = |G|$ and $m_s \mid \cdots \mid m_2 \mid m_1$,

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_s}.$$

$m_i$'s are called *invariant factors of* $G$.

Moreover, the representations in (i) and (ii) are unique.

***Proof.***

(i) A direct consequence of Fundamental Theorem of Finitely Generated Abelian Group.

(ii) It is equivalent to (i) by Example 1.5.9 and Lemma 4.2.5. □

## 4.3 Semidirect Products

**Theorem 4.3.1**

Let $H, K$ be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a group homomorphism. We define a binary operation on $G = H \times K$ (simple Cartesian product) by

$$(h_1, k_1) \cdot (h_2, k_2) \triangleq (h_1 \varphi(k_1)(h_2), k_1 k_2).$$

Let $\tilde{H} \triangleq H \times \{1\} \cong H$ and $\tilde{K} \triangleq \{1\} \times K \cong K$. Then,

(i) $G$ is a group.

(ii) $\tilde{H} \trianglelefteq G$ and $\tilde{K} \leq G$ with $\tilde{H} \cap \tilde{K} = \{(1,1)\}$.

(iii) $G = \tilde{H}\tilde{K}$.

***Proof.***

(i) $(1,1)$ is the identity of the group. Take any $h_1, h_2, h_3 \in H$ and $k_1, k_2, k_3 \in K$. We have

$$\begin{aligned}\big((h_1,k_1)(h_2,k_2)\big)(h_3,k_3) &= (h_1\varphi(k_1)(h_2), k_1k_2)(h_3,k_3)\\ &= (h_1\varphi(k_1)(h_2)\varphi(k_1k_2)(h_3), k_1k_2k_3)\\ (h_1,k_1)\big((h_2,k_2)(h_3,k_3)\big) &= (h_1,k_1)(h_2\varphi(k_2)(h_3), k_2k_3)\\ &= (h_1\varphi(k_1)(h_2\varphi(k_2)(h_3)), k_1k_2k_3)\end{aligned}$$

while

$$\begin{aligned}\varphi(k_1)(h_2\varphi(k_2)(h_3)) &= \varphi(k_1)(h_2)\varphi(k_1)(\varphi(k_2)(h_3)) && \triangleright\ \varphi(k_1) \in \mathrm{Aut}(H)\\ &= \varphi(k_1)(h_2)\varphi(k_1k_2)(h_3). && \triangleright\ \varphi \text{ is a group homomorphism}\end{aligned}$$

Hence, the operation is associative.

Moreover, for each $(h,k) \in G$,

$$\begin{aligned}(h,k)(\varphi(k^{-1})(h^{-1}), k^{-1}) &= (h\varphi(k)(\varphi(k^{-1})(h^{-1})), kk^{-1})\\ &= (h \cdot \mathrm{id}_H(h^{-1}), 1) && \triangleright\ \varphi \text{ is a group homomorphism}\\ &= (1,1)\end{aligned}$$

and

$$\begin{aligned}(\varphi(k^{-1})(h^{-1}), k^{-1})(h,k) &= (\varphi(k^{-1})(h^{-1})\varphi(k^{-1})(h), k^{-1}k)\\ &= (\varphi(k^{-1})(1), 1) && \triangleright\ \varphi(k^{-1}) \in \mathrm{Aut}(H)\\ &= (1,1);\end{aligned}$$

hence $(h,k)^{-1} = (\varphi(k^{-1})(h^{-1}), k^{-1})$. We conclude that $G$ is a group.

(ii) For each $(h_1,1), (h_2,1) \in \tilde{H}$ and $(1,k_1), (1,k_2) \in \tilde{K}$, we have

$$(h_1,1)(h_2,1)^{-1} = (h_1,1)(h_2^{-1},1) = (h_1h_2^{-1},1) \in \tilde{H}$$

and

$$(1,k_1)(1,k_2)^{-1} = (1,k_1)(1,k_2^{-1}) = (1,k_1k_2^{-1}) \in \tilde{K}.$$

Hence, by Theorem 1.3.2, $\tilde{H}$ and $\tilde{K}$ are subgroups of $G$. For normality of $\tilde{H}$, take any $(h,k) \in G$ and $(h',1) \in \tilde{H}$. Then, we have

$$\begin{aligned}(h,k)(h',1)(h,k)^{-1} &= (hh',k)(\varphi(k^{-1})(h^{-1}), k^{-1})\\ &= (\text{something complex}, 1) \in \tilde{H}.\end{aligned}$$

Hence, $\tilde{H} \trianglelefteq G$. $\tilde{H} \cap \tilde{K} = \{(1,1)\}$ is clear.

(iii) For each $(h,k) \in G$, $(h,k) = (h,1)(1,k) \in \tilde{H}\tilde{K}$. □

**Definition 4.3.2: Semidirect Product**

Let $H$ and $K$ be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a group homomorphism. Then, the group $G$ on $H \times K$ equipped with the operation defined in Theorem 4.3.1 is called the *semidirect product of $H$ and $K$ with respect to $\varphi$* and is written

$$G = H \rtimes_\varphi K.$$

**Theorem 4.3.3**

Let $G$ be a group with $H \trianglelefteq G$ and $K \le G$ with $H \cap K = \{1\}$.

(i) Let $\varphi : K \to \mathrm{Aut}(H)$ be defined by $k \mapsto i_k\big|_H$. Then, $\varphi$ is a group homomorphism.

(ii) Moreover, $HK \cong H \rtimes_\varphi K$.

***Proof.***

(i) Note that the well-definedness of $\varphi$ follows from normality of $H$. For each $k, k' \in K$, we have

$$\varphi(kk') = i_{kk'}\big|_H = (i_k \circ i_{k'})\big|_H = i_k\big|_H \circ i_{k'}\big|_H = \varphi(k) \circ \varphi(k').$$

(ii) Let $f : HK \to H \rtimes_\varphi K$ be defined by $hk \mapsto (h,k)$. It is well-defined since, for each $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $h_1 k_1 = h_2 k_2$, we have $H \ni h_2^{-1} h_1 = k_2 k_1^{-1} \in K$; thus $h_1 = h_2$ and $k_1 = k_2$. This further shows that $f$ is injective (and surjective indeed).

Moreover, for each $h_1 k_1, h_2 k_2 \in HK$,

$$\begin{aligned}
f\big((h_1k_1)(h_2k_2)\big) &= f\big((h_1k_1h_2k_1^{-1})(k_1k_2)\big) && \triangleright \text{ inserting } k_1^{-1}k_1 \\
&= (h_1k_1h_2k_1^{-1}, k_1k_2) && \triangleright\ h_1k_1h_2k_1^{-1} \in H \text{ and } k_1k_2 \in K \\
&= (h_1 i_{k_1}(h_2), k_1k_2) \\
&= (h_1, k_1)(h_2, k_2) \\
&= f(h_1k_1) f(h_2k_2).
\end{aligned}$$

Hence, $f$ is a group isomorphism. $\square$

**Corollary 4.3.4**

Let $H$ and $K$ be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a group homomorphism. TFAE.

(i) $\varphi$ is trivial (is a constant map).

(ii) $H \rtimes K = H \times K$

(iii) $\tilde{K} \trianglelefteq H \rtimes_\varphi K$.

***Proof.*** (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (iii) are direct.

We show (ii) $\Rightarrow$ (i) first. Then, we have $h_1 \varphi(k_1)(h_2) = h_1 h_2$ for all $h_1, h_2 \in H$ and $k_1 \in K$. In other words, $\varphi(k_1) = \mathrm{id}_H$ for all $k_1 \in K$. Hence, $\varphi$ is trivial.

Now, we show (iii) $\Rightarrow$ (ii). We have $\tilde{H}, \tilde{K} \trianglelefteq H \rtimes_\varphi K$, $\tilde{H}\tilde{K} = H \rtimes_\varphi K$, and $\tilde{H} \cap \tilde{K} = \{(1,1)\}$ by Theorem 4.3.1. Hence, by Corollary 4.1.5, we have $H \rtimes_\varphi K \cong \tilde{H} \times \tilde{K} \cong H \times K$. This implies that $f : H \rtimes_\varphi K \to H \times K$ defined by $(h,k) \mapsto (h,k)$ is a group isomorphism. $\square$

**Lemma 4.3.5**

$\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_3) \cong S_3$

***Proof.*** $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$ is exactly the set of bijections on $\mathbb{Z}_2 \times \mathbb{Z}_2$ which fix $(0,0)$. $\square$

**Example 4.3.6**

(i) Let $p$ and $q$ be primes such that $p \mid q-1$. Let $H \triangleq \mathbb{Z}_q$ and $K \triangleq \mathbb{Z}_p$. $\mathrm{Aut}(H) \cong \mathbb{Z}_{q-1}$ has a unique subgroup of order $p$. There exists a nontrivial group homomorphism $\varphi : K \to \mathrm{Aut}(H)$. Then, $G \triangleq H \rtimes_\varphi K$ is nonabelian as $\tilde{K}$ is not normal.

(ii) $H \triangleq \mathbb{Z}_3$ and $K \triangleq \mathbb{Z}_4$. Then, there uniquely exists a group homomorphism $\varphi : K \to \mathrm{Aut}(H)$. Then, $T_{12} \triangleq \mathbb{Z}_3 \rtimes_\varphi \mathbb{Z}_4$ is a nonabelian group of order 12. Moreover, $\mathbb{Z}_4 \cong \tilde{K} \le T_{12}$; thus $T_{12}$ has an element of order 4. This implies that $T_{12} \ncong A_4$ and

$T_{12} \not\cong D_6$.

(iii) $H \triangleq \mathbb{Z}_3$ and $K \triangleq \mathbb{Z}_2 \times \mathbb{Z}_2$. Note that $\operatorname{Aut}(H) \cong \mathbb{Z}_2$. There are three nontrivial group homomorphisms $\varphi_1, \varphi_2, \varphi_3 \colon K \to \operatorname{Aut}(H)$ with $\varphi_1(0,1) = 0$, $\varphi_2(1,0) = 0$, and $\varphi_3(1,1) = 0$. However, $H \rtimes_{\varphi_1} K \cong H \rtimes_{\varphi_2} K \cong H \rtimes_{\varphi_3} K$. For instance, the function $H \rtimes_{\varphi_1} K \to H \rtimes_{\varphi_3} K$ defined by

$$(h,(0,0)) \mapsto (h,(0,0)), (h,(1,0)) \mapsto (h,(1,0))$$
$$(h,(0,1)) \mapsto (h,(1,1)), (h,(1,1)) \mapsto (h,(0,1))$$

is a group isomorphism.

Let $G \triangleq H \rtimes_{\varphi_3} K$. Let $M \triangleq \langle (0,(1,0)) \rangle \tilde{H}$ and $N \triangleq \langle (0,(1,1)) \rangle$. Let $a \triangleq (1,(0,0)) \in M$ and $b \in (0,(1,0)) \in M$. Then,

$$ab = (1,(0,0))(0,(1,0)) = (1,(1,0)) = (0,(1,0))(2,(0,0)) = ba^{-1},$$

hence $M \cong D_3$. Moreover, $M \trianglelefteq G$ by Lemma 2.2.6.

In addition, $N \trianglelefteq G$ as, for each $(h,(k_1,k_2)) \in G$,

$$\begin{aligned}
&(h,(k_1,k_2))(0,(1,1))(h,(k_1,k_2))^{-1} \\
&= (h,(k_1+1,k_2+1))(\varphi_3(-k_1,-k_2)(-h),(-k_1,-k_2)) \\
&= (h+\varphi_3(k_1+1,k_2+1)(\varphi_3(-k_1,-k_2)(-h)),(1,1)) \\
&= (h+\varphi_3(1,1)(-h),(1,1)) \\
&= (0,(1,1)) \in N.
\end{aligned}$$

Hence, by Corollary 4.1.5, $G \cong M \times N \cong D_3 \times \mathbb{Z}_2 \cong D_6$. (See Example 4.1.8 (iv).)

(iv) Let $H \triangleq \mathbb{Z}_2 \times \mathbb{Z}_2$ and $K \triangleq \mathbb{Z}_3$. By Lemma 4.3.5, $\operatorname{Aut}(H) \cong S_3$. Then, there are two homomorphisms $\varphi_1, \varphi_2 \colon K \to \operatorname{Aut}(H)$ defined by $\varphi_1(1) = (1\,2\,3)$ and $\varphi_2(1) = (1\,3\,2)$. However, they give the same semiproduct since $\varphi_1(2) = \varphi_2(1)$. Let $G \triangleq H \rtimes_{\varphi_1} K$. Then, $K$ is a Sylow-3 subgroup of $G$ but is not normal in $H$. Hence, Corollary 3.4.9 shows that $G \cong A_4$.

## 4.4 Classification of Finite Groups of Small Orders

**Theorem 4.4.1**

If $G$ is a group of order $2p$ where $p$ is an odd prime, then $G \cong \mathbb{Z}_{2p}$ or $G \cong D_p$.

***Proof.*** By Cauchy Theorem, there exists $a, b \in G$ such that $|a| = p$ and $|b| = 2$. Let $H \triangleq \langle a \rangle$. By Lemma 2.2.6, $H \trianglelefteq G$. As $bab = bab^{-1} \in H$, there exists $t \in \mathbb{Z}$ such that $bab^{-1} = a^t$. Then, we have

$$a^{t^2} = (a^t)^t = (bab^{-1})^t = ba^tb^{-1} = bbab^{-1}b^{-1} = a.$$

Hence, $t^2 \equiv 1 \pmod{p}$ by Theorem 1.5.3 (ii), so we have $t \equiv \pm 1 \pmod{p}$.

- Assume $t \equiv 1 \pmod{p}$. Then, $bab^{-1} = a^t = a$, i.e., $ba = ab$. By Theorem 1.5.3 (iii), $|ab| = 2p$, i.e., $G \cong \mathbb{Z}_{2p}$.
- Assume $t \equiv -1 \pmod{p}$. Then, $bab = a^t = a^{-1}$, i.e., $abab = 1$. Hence, by Theorem 1.4.6, there exists a group homomorphism $f : D_p \to G$ with $f(r_1) = a$ and $f(s) = b$. By Lagrange Theorem, $\operatorname{im}(f) = G$, i.e., $f$ is a group isomorphism. $\square$

**Lemma 4.4.2**

Let $G$ be a group. If $a^2 = 1$ for all $a \in G$, then $G$ is abelian.

***Proof.*** Take any $a, b \in G$. Then, $1 = (ab)^2 = abab$, and thus $ab = (bab)b = ba$. $\square$

**Theorem 4.4.3**

If $G$ is a group of order 8, then $G$ is isomorphic to one of $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2^3$, $D_4$, and $Q_8$.

***Proof.*** If $G$ is abelian, then Fundamental Theorem of Finite Abelian Group asserts that $G \cong \mathbb{Z}_8$, $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, or $G \cong \mathbb{Z}_2^3$. Now, assume that $G$ is nonabelian. By Lemma 4.4.2, there exists $a \in G$ such that $|a| = 4$. Fix $b \in G \setminus \langle a \rangle$. Then, $G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\} = \langle a, b \rangle$. There are three possibilities: $ba = ab$, $ba = a^2b$, and $ba = a^3b$.

- If $ba = ab$, then $G$ is abelian.
- Assume $ba = a^2b$. Then,
$$a^2ba = a^2(a^2b) = a^4b = b$$
so that
$$ba^2 = a^4ba^2 = a^2(a^2ba)a = a^2ba.$$
Thus, $b = a^2ba = ba^2$, so $a^2 = 1$, which is a contradiction. Thus, $ba = a^3b$.

Now, we have four possibilities: $b^2 = 1$, $b^2 = a$, $b^2 = a^2$, and $b^2 = a^3$. If $b^2 = a$ or $b^2 = a^3$, then $|b| = 8$, which is a contradiction.

- Assume $b^2 = 1$. Then, we have $abab = a(a^3b)b = a^4b^2 = 1$. Hence, $G \cong D_4$.
- Assume $b^2 = a^2$. Then, $G \cong Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, ji = i^{-1}j \rangle$. $\square$

**Theorem 4.4.4**

If $G$ is a group of order 12, then $G$ is isomorphic to one of $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, $T_{12}$, $D_6$, or $A_4$.

***Proof.*** If $G$ is abelian, then Fundamental Theorem of Finite Abelian Group asserts that $G \cong \mathbb{Z}_{12}$ or $G \cong \mathbb{Z}_6 \times \mathbb{Z}_2$. Assume $G$ is nonabelian.

Fix some $P \in \mathrm{Syl}_2(G)$ and $Q \in \mathrm{Syl}_3(G)$. Then, $P \cong \mathbb{Z}_4$ or $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ by Corollary 3.2.8, and $Q \cong \mathbb{Z}_3$ by Corollary 2.1.11. By Corollary 3.4.9, $P$ or $Q$ is normal in $G$. Note that $PQ = G$ and $P \cap G = \{1\}$. Hence, one cannot have both $P \trianglelefteq G$ and $Q \trianglelefteq G$ by Corollary 4.1.5.

- Assume $P \trianglelefteq G$ and $Q \ntrianglelefteq G$. Then, $G \cong P \rtimes Q$. If $P = \mathbb{Z}_4$, then the trivial group homomorphism $Q \to \mathrm{Aut}(P)$ is the only homomorphism, hence $G \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ by Corollary 4.3.4. If $P = \mathbb{Z}_2 \times \mathbb{Z}_2$, then $G \cong A_4$ by Example 4.3.6 (iv).
- Assume $P \ntrianglelefteq G$ and $Q \trianglelefteq G$. Then, $G \cong Q \rtimes P$. If $P = \mathbb{Z}_4$, then $G \cong T_{12}$ by Example 4.3.6 (ii). If $P = \mathbb{Z}_2 \times \mathbb{Z}_2$, then $G \cong D_6$ by Example 4.3.6 (iii). $\square$

**Note:-**

Now, we have complete classification of groups of order less than 16.

# Chapter 5

# Rings

## 5.1 Definitions and Examples of Rings

**Definition 5.1.1: Ring**

A *ring* is a nonempty set equipped with two binary operations "+" and "·" such that for all $a, b, c \in R$, the following are satisfied:

(i) $(R, +)$ is an abelian group.
(ii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$.

The additive identity of ring $R$ is usually denoted 0, and the additive inverse of $a \in R$ is usually denoted $-a$.

A *commutative ring* is a ring $(R, +, \cdot)$ such that the following condition is additionally satisfied.

(iv) $a \cdot b = b \cdot a$ for all $a, b \in R$.

A *ring with identity* is a ring $(R, +, \cdot)$ such that the following condition is additionally satisfied.

(v) There exists $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

A *commutative ring with identity* is a ring $(R, +, \cdot)$ such that (iv) and (v) are both satisfied.

**Theorem 5.1.2**

Let $R$ be a ring. Then, the following hold.

(i) $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$.
(ii) $a \cdot (-b) = (-a) \cdot b = -ab$ for all $a, b \in R$.
(iii) $(-a) \cdot (-b) = ab$ for all $a, b \in R$.
(iv) If $R$ is a ring with identity, then $(-1) \cdot a = -a$ for all $a \in R$.

***Proof.***

(i) We have $0 \cdot a + 0 \cdot a = (0 + 0) \cdot a = 0 \cdot a$; hence $0 \cdot a = 0$. We have $a \cdot 0 = 0$ similarly.
(ii) $a \cdot b + a \cdot (-b) = a \cdot (b - b) = a \cdot 0 = 0$ by (i). Hence, $a \cdot (-b)$ is the additive inverse of $a \cdot b$. Similarly, $(-a) \cdot b = -ab$.
(iii) $(-a)(-b) = -(-a)b = -(-ab) = ab$ by (ii).
(iv) $a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 - 1) \cdot a = 0 \cdot a = 0$ by (i). Hence, $(-1) \cdot a$ is the additive inverse of $a$. $\square$

**Theorem 5.1.3**

Let $R$ be a commutative ring with identity. If $1 = 0$, then $R$ is the trivial ring $\{0\}$.

***Proof.*** For any $a \in R$, then $a = 1 \cdot a = 0 \cdot a = 0$ by Theorem 5.1.2 (i). □

**Definition 5.1.4: Unit**

Let $R$ be a ring with identity. An element $a \in R$ is a *unit* if $a$ has a multiplicative inverse, i.e., there exists $u \in R$ such that $au = ua = 1$.

**Definition 5.1.5: Zero Divisor**

Let $R$ be a ring.

- An element $a \in R \setminus \{0\}$ is a *zero divisor* if there exists $b \in R$ such that $ab = 0$ or $ba = 0$.
- An element $a \in R \setminus \{0\}$ is a *nonzero divisor* if $a$ is not a zero divisor.

**Definition 5.1.6: Integral Domain**

Let $R$ be a nontrivial commutative ring with identity. If $R$ has no zero divisor, then $R$ is called an *integral domain*.

**Theorem 5.1.7**

Let $R$ be a ring with identity. Then, the following hold.

(i) If $u \in R$ is a unit, then it is not a zero divisor.
(ii) A multiplicative inverse $u^{-1}$ of a unit $u$ is unique.
(iii) If $a$ is a nonzero divisor and $ab = ac$ (or $ba = ca$), then $b = c$.

***Proof.***

(i) There is an element $w \in R$ such that $uw = wu = 1$. Suppose $uv = 0$ for some $u \in R$. Then, $0 = w0 = w(uv) = (wu)v = 1v = v$, which is a contradiction. It is similar for the case in which $vu = 0$ for some $u \in R$.
(ii) Assume $vu = wu = 1$ for some $v, w \in R$. Then, $0 = vu - wu = (v - w)u$. By (i), $u$ is not a zero divisor, hence $v - w = 0$, i.e., $v = w$.
(iii) We have $a(b - c) = 0$ (or $(b - c)a = 0$). As $a$ is a nonzero divisor, we have $b - c = 0$, i.e., $b = c$. □

**Theorem 5.1.8**

Every element of a finite commutative ring with identity is 0, a unit, or a zero divisor.

***Proof.*** Let $R = \{a_1, \cdots, a_n\}$ be a finite commutative ring with identity. Take any $a_t \in R \setminus \{0\}$ and assume $a_t$ is a nonzero divisor. If $a_i a_t = a_j a_t$, then $a_i = a_j$ by Theorem 5.1.7 (iii), i.e., $i = j$. Therefore, $a_1 a_t, a_2 a_t, \cdots, a_n a_t$ are all distinct; hence

$$R = \{a_1 a_t, a_2 a_t, \cdots, a_n a_t\}.$$

Thus, there exists $a_i \in R$ such that $a_i a_t = 1$; hence $a_t$ is a unit. □

**Corollary 5.1.9**

A finite integral domain is a field[1].

A *field* is a nontrivial commutative ring $(R,+,\cdot)$ with identity in which every nonzero element is a unit.

***Proof.*** Direct from Theorem 5.1.8. □

**Definition 5.1.10: Subring**

Let $R$ be a ring and let $S \subseteq R$ be nonempty. Then, $S$ is a *subring* of $R$ if $S$ is a ring under the binary operations $+$ and $\cdot$.

**Theorem 5.1.11**

Let $R$ be a ring and let $S \subseteq R$ be nonempty. Then, $S$ is a subring of $R$ if and only if $S$ is closed under subtraction and multiplication.

## 5.2 Ring Homomorphisms

**Definition 5.2.1: Ring Homomorphism**

Let $R$ and $S$ be groups. A *ring homomorphism* between $R$ and $S$ is a function $f : R \to S$ such that

$$f(a+b) = f(a) + f(b) \text{ and } f(ab) = f(a)f(b)$$

for all $a, b \in R$. The *kernel* of a ring homomorphism $f$ is the set

$$\ker(f) \triangleq \{r \in R \mid f(r) = 0\}.$$

**Definition 5.2.2: Ring isomorphism**

Let $R$ and $S$ be groups. A *ring isomorphism* between $R$ and $S$ is a bijective ring homomorphism between $R$ and $S$. We write $R \cong S$ if there is a ring isomorphism between $R$ and $S$. "$\cong$" is an equivalence relation.

**Theorem 5.2.3**

Let $R$ be a ring with identity and let $S$ be a ring. Let $f : R \twoheadrightarrow S$ be a surjective ring homomorphism. Then, the following hold.

(i) $f(1)$ is the multiplicative identity of $S$.
(ii) If $u$ is a unit in $R$, then $f(u)$ is a unit in $S$ and $f(u)^{-1} = f(u^{-1})$.

***Proof.***

(i) Take any $s \in S$. Then, there exists $r \in R$ such that $f(r) = s$. Then, $sf(1) = f(r)f(1) = f(r) = s$ and $f(1)s = f(1)f(r) = f(r) = s$. Hence, the result follows.
(ii) $f(u)f(u^{-1}) = f(1) = 1$ and $f(u^{-1})f(u) = f(1) = 1$ by (i). Hence, $f(u^{-1}) = f(u)^{-1}$. □

**Theorem 5.2.4**

Let $R$ and $S$ be groups and let $f : R \to S$ be a group homomorphism. Then, $\mathrm{im}(f)$ is a subring of $S$ and $\ker(f)$ is a subring of $R$.

***Proof.*** $\operatorname{im}(f)$ and $\ker(f)$ are a subgroup of $(R,+)$ and $(S,+)$, respectively.

Take any $s, s' \in \operatorname{im}(f)$. Then, there exist $r, r' \in R$ such that $f(r) = s$ and $f(r') = s'$, then $ss' = f(r)f(r') = f(rr') \in \operatorname{im}(f)$. Hence, $\operatorname{im}(f)$ is closed under multiplication.

Take any $r, r' \in \ker(f)$. Then, $f(rr') = f(r)f(r') = 0 \cdot 0 = 0$. Hence, $\ker(f)$ is closed under multiplication. Ther result follows from Theorem 5.1.11. □

# Chapter 6

# Ideals and Quotient Rings

## 6.1 Ideals

**Definition 6.1.1: Congruence**

Let $R$ be a ring and let $S$ be a subring of $R$. For $a, b \in R$, We say *$a$ is congruent to $b$ modulo $S$* if $a - b \in S$, and write $a \equiv b \pmod{S}$.

**Definition 6.1.2: Coset**

Let $R$ be a ring and let $S$ be a subring of $R$. Let $a \in R$. As $(R, +)$ is abelian, the left coset $a + S$ equals the right coset $S + a$. Hence, we call either of them just a *coset* of $S$.

**Definition 6.1.3**

Let $R$ be a ring and let $S$ be a subring of $R$. We define $R/S$ by

$$R/S \triangleq \{a + S \mid a \in R\}.$$

**Lemma 6.1.4**

Let $R$ be a ring and let $S$ be a subring of $R$. Then,

$$\begin{aligned}\forall a, a', b, b' \in R,\ (a + S = a' + S \wedge b + S = b' + S \implies ab + S = a'b' + S)\\ \iff \forall r \in R,\ \forall s \in S,\ (rs \in S \wedge sr \in S).\end{aligned}$$

***Proof.***

($\Rightarrow$) Take any $r \in R$ and $s \in S$. Then, we have $0 + S = s + S$ and $r + S = r + S$. Hence, by assumption, $0 + S = 0 \cdot r + S = sr + S$, i.e., $sr \in S$. Similarly, $rs \in S$.

($\Leftarrow$) Take any $a, a', b, b' \in R$ such that $a + S = a' + S$ and $b + S = b' + S$. This means $a - a' \in S$ and $b - b' \in S$ so that

$$(a - a')b' = ab' - a'b' \in S \text{ and } a(b - b') = ab - ab' \in S,$$

which implies $ab - a'b' = (ab - ab') + (ab' - a'b') \in S$. Hence, $ab + S = a'b' \in S$. □

**Definition 6.1.5: Ideal**

Let $R$ be a ring and let $I \subseteq R$ be nonempty. Then, $I$ is an *ideal* of $R$ if $I$ is a subring of $R$ and $ir, ri \in I$ for all $i \in I$ and $r \in R$.

**Example 6.1.6**

(i) For any ring $R$, then the trivial subring $\{0\}$ is an ideal in $R$, which is called the *trivial ideal* of $R$.

(ii) For any ring $R$ with identity and an ideal $I$ in $R$, $I = R$ if and only if $u \in I$ for some unit $u \in R$. For if $u \in I$ where $u$ is a unit of $R$, then $r = (ru^{-1})u \in I$ for all $r \in R$.

**Corollary 6.1.7**

Let $R$ be a group and let $\langle I_i \mid i \in I \rangle$ be an indexed system of ideals of $R$. Then, $\bigcap_{i\in I} I_i$ is an ideal in $R$.

***Proof.*** Trivial. □

**Theorem 6.1.8**

Let $R$ be a commutative ring and let $c_1, c_2, \cdots, c_n \in R$. Then,

$$I \triangleq \{ r_1c_1 + r_2c_2 + \cdots + r_nc_n \mid r_1, r_2, \cdots, r_n \in R \}$$

is an ideal in $R$.

***Proof.*** Simply check. □

**Definition 6.1.9**

In the case of Theorem 6.1.8, In this case, $I$ is said to be *(finitely) generated by* $c_1, c_2, \cdots, c_n$ and is denoted by $(c_1, c_2, \cdots, c_n)$. When $n = 1$, $I$ is called a *principal ideal* generated by $c_1$.

**Note:-**

The *smallest ideal* of $R$ containing $a \in R$ is

$$\{ na + ra \mid n \in \mathbb{Z} \wedge r \in R \},$$

which equals $(a)$ when $R$ has an identity. If $R$ a commutative ring without identity, then $a \notin (a)$.

## 6.2 Quotient Rings and Ring Homomorphisms

**Definition 6.2.1: Quotient Ring**

Let $R$ be a ring and let $I \subseteq R$ be an ideal in $R$. Then, $R/I$ equipped with operations

$$(a+I)+(b+I)=(a+b)+I$$
$$(a+I)\cdot(b+I)=ab+I$$

is a ring and is called the *quotient ring of $R$ by $I$*. This is justified by Lemma 6.1.4. If

$R$ is commutative, then so is $R/I$. If $R$ has a multiplicative identity, then $1+I$ is the multiplicative identity of $R/I$. There is a surjective ring homomorphism

$$\begin{aligned}\pi: R &\longrightarrow R/I\\ r &\longmapsto r+I\end{aligned}$$

which is called the *natural projection from $R$ to $R/I$*.

**Lemma 6.2.2**

Let $R$ and $S$ be rings. Let $f: R \to S$ be a ring homomorphism. Then, $\ker(f)=\{0\}$ if and only if $f$ is injective.

***Proof.*** This is a special case of Theorem 2.3.3 noting that $f$ is a group homomorphism from $(R,+)$ to $(S,+)$. □

**Theorem 6.2.3** First Isomorphism Theorem

Let $R$ and $S$ be rings. Let $f: R \to S$ be a ring homomorphism. Then, $R/\ker(f) \cong \operatorname{im}(f)$.

***Proof.*** Let $K \triangleq \ker(f)$. Define a function

$$\begin{aligned}\varphi: R/K &\longrightarrow \operatorname{im}(f)\\ r+K &\longmapsto f(r).\end{aligned}$$

For each $r, r' \in R$, we have $r+K=r'+K$ if and only if $f(r)=f(r')$ as $f$ is a ring homomorphism. Hence, $\varphi$ is well-defined and injective. $\varphi$ is evidently surjective. Therefore, $\varphi$ is a bijective ring isomorphism. □

**Definition 6.2.4**

Let $R$ be a ring and let $I$ and $J$ be ideals of $R$. Then, we define

$$I+J \triangleq \{i+j \mid i \in I \wedge j \in J\}$$
$$IJ \triangleq \{i_1j_1+i_2j_2+\cdots+i_nj_n \mid n \in \mathbb{N} \wedge \forall k \in [n], (i_k \in I \wedge j_k \in J)\}.$$

**Lemma 6.2.5**

Let $R$ be a ring and let $I$ and $J$ be ideals of $R$. Then, $I+J$ and $IJ$ are ideals of $R$.

***Proof.***

(i) Take any $i+j, i'+j' \in I+J$ and $r \in R$. Then,

$$(i+j)-(i'+j') = (i-i')+(j+j') \in I+J$$

and

$$\begin{aligned} r(i+j) &= ri+rj \in I+J, \\ (i+j)r &= ir+jr \in I+J. \end{aligned}$$

Hence, $I+J$ is an ideal in $R$.

(ii) Take any $i_1j_1+\cdots+i_mj_m, i'_1j'_1+\cdots+i'_nj'_n \in IJ$ and $r \in J$. Then,

$$(i_1j_1+\cdots+i_mj_m)-(i'_1j'_1+\cdots+i'_nj'_n) = i_1j_1+\cdots+i_mj_m+(-i'_1)j'_1+\cdots+(-i'_n)j'_n \in IJ$$

and

$$\begin{aligned} r(i_1j_1+\cdots+i_mj_m) &= (ri_1)j_1+\cdots(ri_m)j_m \in IJ, \\ (i_1j_1+\cdots+i_mj_m)r &= i_1(j_1r)+\cdots i_m(j_mr) \in IJ \end{aligned}$$

Hence, $IJ$ is an ideal in $R$. □

**Theorem 6.2.6** Second Isomorphism Theorem

Let $R$ be a ring and let $I$ and $J$ be ideals in $R$. Then, $I \cap J$ is an ideal in $I$, $J$ is an ideal in $I+J$, and $I/(I\cap J) \cong (I+J)/J$.

***Proof.*** $J$ is clearly an ideal in $I+J$. Define a ring homomorphism

$$\begin{aligned} \varphi : I &\longrightarrow (I+J)/J \\ i &\longmapsto i+J. \end{aligned}$$

Then, for any $i+j \in I+J$, we have $(i+j)+J = i+(j+J) = i+J = \varphi(i)$; hence $\varphi$ is surjective. We also have $\ker(\varphi) = I\cap J$; $I \cap J$ is an ideal in $I$. Hence, by First Isomorphism Theorem, $I/(I\cap J) \cong (I+J)/J$. □

**Theorem 6.2.7** Third Isomorphism Theorem

Let $R$ be a ring and let $I$ and $J$ be ideals in $R$ such that $J \subseteq I$. Then, $I/J$ is an ideal in $R/J$. Furthermore, $(R/J)/(I/J) \cong R/I$.

***Proof.*** Define a function

$$\begin{aligned} \varphi : R/J &\longrightarrow R/I \\ r+J &\longmapsto r+I. \end{aligned}$$

For each $r, r' \in R$ such that $r+J = r'+J$, then $r-r' \in J \subseteq I$; thus $r+I = r'+I$, hence $\varphi$ is well-defined. It is evident that $\varphi$ is a surjective ring homomorphism. Simply computing the kernel, we have $\ker(\varphi) = I/J$ and $I/J$ is an ideal in $R/J$. Hence, by First Isomorphism Theorem, $(R/J)/(I/J) \cong R/I$. □

**Lemma 6.2.8**

Let $R$ and $S$ be rings. Let $f : R \to S$ be a ring homomorphism. If $I \subseteq S$ is an ideal in $S$, then $f^{-1}(I)$ is an ideal in $R$.

***Proof.*** Take any $a, b \in f^{-1}(I)$. Then, $f(a-b) = f(a)-f(b) \in I$; hence $a-b \in f^{-1}(I)$. Moreover, for any $r \in R$, we have $f(ra) = f(r)f(a) \in I$ and $f(ar) = f(a)f(r) \in I$; hence $ar, ra \in f^{-1}(I)$. Hence, $f^{-1}(I)$ is an ideal in $R$. □

**Theorem 6.2.9** Fourth Isomorphism Theorem

Let $R$ be a ring and let $I$ be an ideal in $R$. Let $\pi\colon R \twoheadrightarrow R/I$ be the natural projection. Then, there is a natural one-to-one correspondence between

$$\{\text{ideals of } R \text{ containing } I\} \overset{1:1}{\longleftrightarrow} \{\text{ideals of } R/I\}$$

with $K \mapsto K/I$.

***Proof.*** Define a function

$$\begin{aligned} \varphi\colon \{\text{ideals of } R \text{ containing } I\} &\longrightarrow \{\text{ideals of } R/I\} \\ K &\longmapsto K/I. \end{aligned}$$

By Third Isomorphism Theorem, if $K \subseteq R$ is an ideal containing $I$, then $\varphi(K) = K/I$ is an ideal in $R/I$. Hence, $\varphi$ is well-defined.

Let $K, K' \subseteq R$ be ideals in $R$ containing $I$ such that $K \neq K'$. Then, there exists $k \in K \setminus K'$. If $k + I = k' + I$ for some $k' \in K'$, then $k = k' + i$ for some $i \in I$, which implies $k \in K'$, which is a contradiction. Hence, $k + I \neq k' + I$ for all $k' \in K'$, i.e., $k + I \in \varphi(K) \setminus \varphi(K')$. Therefore, $\varphi$ is injective.

Let $\overline{K}$ be an ideal in $R/I$. then, by Lemma 6.2.8, $K \triangleq \varphi^{-1}(\overline{K})$ is an ideal in $R$. Clearly, $I = \ker(\varphi) = \varphi^{-1}(\{0\}) \subseteq K$ and $\varphi(K) = K/I = \overline{K}$. Hence, $\varphi$ is surjective. □

## 6.3 Prime and Maximal Ideals

**Definition 6.3.1: Prime Ideal**

Let $R$ be a commutative ring. A proper ideal $P$ in $R$ is a *prime ideal* if $ab \in P$ implies $a \in P \vee b \in P$.

**Theorem 6.3.2**

Let $R$ and $S$ be commutative rings with identity. Let $f : R \to S$ be a ring homomorphism. If $P \subseteq S$ is a prime ideal in $S$, then $f^{-1}(P)$ is a prime ideal in $R$.

***Proof.*** By Lemma 6.2.8, $f^{-1}(P)$ is an ideal in $R$. Moreover, as $1 \notin P$ by Example 6.1.6 (ii), $1 \notin f^{-1}(P)$ by Theorem 5.2.3 (i), and thus $f^{-1}(P) \subsetneq R$.

Take any $a, b \in R$ such that $ab \in f^{-1}(P)$. Then, as $f(a)f(b) = f(ab) \in P$, we have $f(a) \in P$ or $f(b) \in P$, i.e., $a \in f^{-1}(P)$ or $b \in f^{-1}(P)$. □

**Theorem 6.3.3**

Let $R$ be a commutative ring with identity and let $P$ be an ideal in $R$. Then, $P$ is a prime ideal if and only if $R/P$ is an integral domain.

***Proof.***

($\Rightarrow$) $R/P$ is a commutative ring with identity. $R/P$ is not trivial as $P \subsetneq R$. Take any $a, b \in R$ such that $(a+P)(b+P) = 0+P$. Then, $ab \in P$ and thus $a \in P$ or $b \in P$, i.e., $a+P = 0+P$ or $b+P = 0+P$.

($\Leftarrow$) $P \subsetneq R$ as $R/P$ is not trivial. Take any $a, b \in R$ such that $ab \in P$. Then, we have $(a+P)(b+P) = ab+P = 0+P$. Hence, $a+P = 0+P$ or $b+P = 0+P$, i.e., $a \in P$ or $b \in P$. □

**Definition 6.3.4: Maximal Ideal**

Let $R$ be a ring. A proper ideal $M$ in $R$ is called a *maximal ideal* if $M$ is maximal with respect to inclusion among proper ideals in $R$. In other words, if $I$ is an ideal in $R$ such that $M \subseteq I$, then $I = M$ or $I = R$.

**Theorem 6.3.5**

Let $R$ be a ring and let $I$ be a proper ideal in $R$. There exists a maximal ideal $M$ of $R$ such that $I \subseteq M$.

***Proof.*** Let

$$\mathcal{J} \triangleq \{J \subsetneq R \mid J \text{ is an ideal in } R \text{ and } I \subseteq J\}.$$

Then, $(\mathcal{J}, \subseteq)$ is a poset. Let $\mathcal{C}$ be a nonempty chain[1] in $(\mathcal{J}, \subseteq)$. Let $M_{\mathcal{C}} \triangleq \bigcup \mathcal{C}$.

**Claim 1.** $M_{\mathcal{C}} \in \mathcal{J}$

***Proof.*** It is clear that $I \subseteq M_{\mathcal{C}}$. Take any $a, b \in M_{\mathcal{C}}$. Then, there exists $J_a, J_b \in \mathcal{C}$ such that $a \in J_a$ and $b \in J_b$. WLOG, $J_a \subseteq J_b$. Then, $a - b \in J_b \subseteq M_{\mathcal{C}}$.

Take any $m \in M_{\mathcal{C}}$ and $r \in R$. Then, $m \in J$ for some $J \in \mathcal{C}$ so that $mr, rm \in J \subseteq M_{\mathcal{C}}$. Hence, $M_{\mathcal{C}}$ is an ideal in $R$. Moreover, $M_{\mathcal{C}}$ is proper since $1 \notin M_{\mathcal{C}}$. □

Claim 1 says that $M_{\mathcal{C}}$ is an upper bound of $\mathcal{C}$. Therefore, by Zorn's lemma, $\mathcal{J}$ has a maximal element $M$ with respect to the inclusion, which is evidently a maximal ideal in $R$ containing $I$. □

**Theorem 6.3.6**

Let $R$ be a commutative ring with identity and let $M$ be a ideal. Then, $M$ is a maximal ideal if and only if $R/M$ is a field.

***Proof.***

($\Rightarrow$) As $M$ is proper, $R/M$ is nontrivial commutative ring with identity. Take any nonzero element $a + M \in R/M$. Then, $a \in R \setminus M$. Define

$$J \triangleq \{m + ra \mid r \in R \wedge m \in M\}.$$

Take any $m + ra, m' + r'a \in J$. Then,

$$(m + ra) - (m' + r'a) = (m - m') + (r - r')a \in J$$

and

$$r(m' + r'a) = rm' + (rr')a \in J,$$
$$(m' + r'a)r = m'r + r'ra \in J.$$

Hence, $J$ is an ideal such that $M \subsetneq J$ as $a \in J \setminus M$. As $M$ is maximal, $J = R$; thus $1 \in J$.

There exist $m \in M$ and $r \in R$ such that $1 = m + ra$. Then,

$$(r + M)(a + M) = ra + M = 1 + M;$$

hence $a + M$ is a unit.

[1]A *chain* in a poset $(P, \leq)$ is a totally ordered subset of $P$.

($\Leftarrow$) As $1 + M \neq 0 + M$, $1 \notin M$, i.e., $M$ is a proper ideal by Example 6.1.6 (ii). Let $J$ be an ideal in $R$ such that $M \subsetneq J$. There exists some $a \in J \setminus M$ so that $a + M \neq 0 + M$. Hence, there exists $b + M \in R/M$ such that $ab + M = (a + M)(b + M) = 1 + M$, i.e., $m \triangleq ab - 1 \in M \subseteq J$. As $ab \in J$ as $a \in J$, we have $1 = ab - m \in J$; hence $J = R$ by Example 6.1.6 (ii). ☐

**Corollary 6.3.7**

Let $R$ be a commutative ring with identity. Then, every maximal ideal in $R$ is a prime ideal in $R$.

***Proof.*** Let $M$ be a maximal ideal in $R$. Then, $R/M$ is a field by Theorem 6.3.6. In particular, $R/M$ is an integral domain. Hence, by Theorem 6.3.3, $M$ is a prime ideal. ☐

**Corollary 6.3.8**

Let $R$ be a commutative ring with identity. Then, $(0)$ is a maximal ideal if and only if $R$ is a field.

***Proof.*** This directly follows from $R \cong R/(0)$ and Theorem 6.3.6. ☐

## 6.4 Rings of Fractions

**Definition 6.4.1: Multiplicative Set**

Let $R$ be a commutative ring. Then, $D \subseteq R$ is said to be *multiplicative* if every element of $D$ is a nonzero divisor and $D$ is closed under multiplication.

**Lemma 6.4.2**

Let $R$ be a commutative ring and let $D \subseteq R$ be a multiplicative set. Then, the relation $\sim$ on $R \times D$ defined by

$$(r, d) \sim (s, e) \iff re = sd$$

is an equivalence relation. Moreover, if $Q \triangleq \{[a] \mid a \in R \times D\}$ is the set of equivalence classes, then the structure $(Q, +, \cdot)$ defined by

$$\frac{a}{b} + \frac{c}{d} \triangleq \frac{ad + bc}{bd}$$

and

$$\frac{a}{b} \cdot \frac{c}{d} \triangleq \frac{ac}{bd}$$

where $a/b$ denote the equivalence class $[(a, b)]$ is well-defined and is a commutative ring with identity such that every element of form $d/d'$ where $d, d' \in D$ is a unit.

***Proof.*** ☐

***End.***