Summary for Modern Algebra I

SEUNGWOO HAN

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

Contents

Chapter **Groups** — Page 2

1.1 Definitions and Examples of Groups 2
1.2 Group Homomorphisms 4
1.3 Subgroups 5
1.4 Generators of Groups and Free Groups 7
1.5 Cyclic Groups 8
1.6 Alternating Groups 10

Chapter **Normal Subgroups and Quotient Groups** — Page 12

2.1 Lagrange Theorem 12
2.2 Normal Subgroups 14
2.3 Quotient Groups and Group Homomorphisms 16
2.4 Simple Groups and Jordan–Hölder Theorem 20

Chapter **Group Actions** — Page 25

3.1 Stabilizers and Orbits 25
3.2 Group Actions by Conjugation 27
3.3 Automorphisms 29

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 $-: G \times G \to G$ 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. □

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 $G \hookrightarrow\!\!\!\!\to G$ 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 φ 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 $\operatorname{id}_H : H \hookrightarrow G$ 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) $\to$ (ii) and (ii) $\to$ (iii) are trivial. For any $a, b \in H$, we have $1 = aa^{-1} \in H$, $a^{-1} = 1a^{-1} \in H$, and $ab = a(b^{-1})^{-1} \in H$. $\square$

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, $H \leq G$. $\square$

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. $\square$

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 φ 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 $0 \leq r < k$ 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, $k = d \mid n$. $\square$

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, $|\sigma| = \mathrm{lcm}(|\sigma_1|, |\sigma_2|, \cdots, \sigma_k)$.

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 $\sigma(\Delta) = \prod_{i \le i < j \le n}(x_{\sigma(i)} - x_{\sigma(j)})$ 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

ε 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 $\varepsilon(\sigma) = (-1)^k$. $\varepsilon(\tau\sigma)\Delta = (\tau\sigma)(\Delta) = \varepsilon(\sigma)\prod_{i \le i < j \le n}(x_{\tau(i)} - x_{\tau(j)}) = \varepsilon(\sigma)\varepsilon(\tau)\Delta$. Hence, $\varepsilon(\tau\sigma) = \varepsilon(\sigma)\varepsilon(\tau) = \varepsilon(\tau)\varepsilon(\sigma)$. $\square$

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 $K \leq G$ 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 $K \leq G$ 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 $K \leq G$.

Definition 2.1.3

Let $K \leq G$.

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

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 φ 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,

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

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 $H \le G$.

(ii) $K = \{r_0, s\} \le D_4$ 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 $H \le G$. 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 $H \le G$.

(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 π 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

$$ab = c_1(d^i c_2)d^j = (c_1c_2)(d^i d^j) = c_2(c_1 d^j)d^i = c_2 d^j c_1 d^i = ba.$$

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 $G/\ker(f) \cong \mathrm{im}(H)$.

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 φ 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, $Ka = Kb$; φ 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, $K/N \neq K'/N$. ϕ 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, ϕ 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,

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

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,

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

are the same up to permutation, and

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

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.

(⇒) 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.

(⇐) 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. □

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, $N = A_n$. □

Take any $\{(1)\} \lneq N \trianglelefteq A_n$ and fix some $\sigma \in N \setminus \{(1)\}$. Consider the cycle decomposition of σ. There are three cases: (i) some cycle has length ≥ 4, (ii) the maximum length of cycle is 3, and (iii) every cycle has length ≤ 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 τ 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 τ fixes $[3]$ and τ 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 τ fixes $[4]$ and τ 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. □

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 $N = S_n$. □

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, φ 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, $G/K(G,A) \cong \mathrm{im}(\varphi) \leq S(A)$ 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 σ and its conjugation have the same cycle type, the conjugacy class of σ is the collection of permutations with the same cycle type of σ.

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. □

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 $k \leq 1$.

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

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

Corollary 3.2.11

Let $G \curvearrowright \mathcal{P}(G)$ by conjugation; $(g,A) \mapsto gAg^{-1}$. We say $A, B \subseteq G$ are *conjugate* if $A = gBg^{-1}$ for some $g \in G$. Then, $[G{:}N_G(A)] = |G \cdot A| = |\text{orbit of } A|$.

Proof. $N_G(A) = G_A$. □

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

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 $\varphi_g(n_1 n_2) = g n_1 n_2 g^{-1} = g n_1 g^{-1} g n_2 g^{-1} = \varphi_g(n_1)\varphi_g(n_2)$; thus φ_g is a group isomorphism as it is already $\varphi_g \in S(N)$.

We have

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

□

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 $N_G(H) = N_{N_G(H)}(H)$. The result follows from Theorem 3.3.1. □

Note:-

Let $\mathrm{Inn}(G)$ be the set of all inner automorphisms of G. Then, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$ since $\forall \varphi \in \mathrm{Aut}(G)$, $\varphi \circ i_c \circ \varphi^{-1} = i_{\varphi(c)}$. We call $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ the *outer automorphism group*.

Corollary 3.3.3
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. $\square$

Example 3.3.4
- $\mathrm{Inn}(D_4) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathrm{Inn}(Q_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
- $\mathrm{Inn}(S_n) \cong S_n$ for $n \geq 3$.

Definition 3.3.5

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 a group under usual multiplication.

Theorem 3.3.6
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 $f_k : \mathbb{Z}_n \to \mathbb{Z}_n$ by $\ell \mapsto k\ell$. Then, clearly, $f_k \in \mathrm{Aut}(\mathbb{Z}_n)$.

Now, define $\Phi : (\mathbb{Z}/n\mathbb{Z}) * \to \mathrm{Aut}(\mathbb{Z}_n)$ by $k \mapsto f_k$. Then, it is easy to check Φ 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:-
- $\neg(G \text{ is abelian} \implies \mathrm{Aut}(G) \text{ is abelian})$.
- $\neg(G \text{ is cyclic} \implies \mathrm{Aut}(G) \text{ is cyclic})$.

End.