Contents

Part I
Group Theory

1 Symmetric Groups

Throughout the note, we let $[n] = \{1, \dots, n\}$.

1.1 Basic Definitions

Definition 1.1. The group S_n of all bijections $[n] \to [n]$ is called the **symmetric group**. The elements of S_n are called **permutations**. A permutation σ can be expressed by

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Definition 1.2. Let $a_1, \ldots, a_r$, $(r \leq n)$ be distinct elements in $[n]$. Then the r-**cycle** $(a_1 a_2 \cdots a_r)$ is the permutation $\sigma \in S_n$ defined by

$$\sigma(a_i) = a_{i+1}, \quad \forall i \in \mathbb{Z}_r,$$
$$\sigma(x) = x, \quad \forall x \notin \{a_1, \ldots, a_r\}.$$

Here, r is called the **length** of the cycle; a 2-cycle is called a **transposition**.

Definition 1.3. The permutations $\sigma_1, \ldots, \sigma_r \in S_n$ are said to be **disjoint** if for each $1 \leq i \leq r$, and every $k \in [n]$,

$$\sigma_i(k) \neq k \implies \sigma_j(k) = k \quad \forall j \neq i.$$

In particular, two cycles $(a_1 a_2 \cdots a_r)$ and $(b_1 b_2 \cdots b_s)$ are disjoint if $\{a_1, a_2, \ldots, a_r\} \cap \{b_1, b_2, \ldots, b_s\} = \emptyset$.

Proposition 1.4.

(i) $|S_n| = n!$;

(ii) $(a_1 a_2 \cdots a_r) = (a_2 a_3 \cdots a_r a_1) = \cdots = (a_r a_1 \cdots a_{r-2} a_{r-1})$;

(iii) *Any* 1*-cycle is the identity permutation, and hence it can be omitted when expressing any product of cycles;*

(iv) $|(a_1 a_2 \cdots a_r)| = r$;

(v) $(a_1 a_2 \cdots a_r)^{-1} = (a_r a_{r-1} \cdots a_1)$;

(vi) *If* $\sigma, \tau \in S_n$ *are disjoint, then* $\sigma\tau = \tau\sigma$. *Furthermore,* $\sigma\tau = Id$ *implies* $\sigma = \tau = Id$.

The action of conjugation on S_n has a nice property.

Proposition 1.5. *Let $\tau = (a_1 \cdots a_r)$ be an r-cycle and $\sigma \in S_n$. Then*

$$\sigma\tau\sigma^{-1} = \sigma(a_1 \cdots a_r)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_r)).$$

1.2 Cycle Decomposition

Theorem 1.6. *Every nonidentity permutation in S_n can be decomposed into a product of disjoint cycles, each of which has length at least 2. This decomposition is unique up to the order of the cycles in the product.*

Corollary 1.7. *The order of a permutation $\sigma \in S_n$ is the least common multiple of the orders of its disjoint cycles.*

1.3 Generators of Symmetric Groups

Proposition 1.8. *The following sets are generators of S_n:*

(i) *the set of all transpositions;*

(ii) $\{(12), (13), (14), \ldots, (1n)\}$;

(iii) $\{(12), (23), (34), \ldots, (n-1\ n)\}$;

(iv) $\{(12), (123\cdots n)\}$;

(v) $\{(12), (23\cdots n)\}$;

(vi) *if $n = p$ where p is a prime , then $\{(rs), (123\cdots p)\}$ where (rs) is any transposition.*

1.4 Sign of a Permutation

Definition 1.9. A permutation in S_n is said to be **even** (resp. **odd**) if it can be written as a product of an even (resp. odd) number of transpositions.

As discussed in the previous section, any permutation can be decomposed into a product of transpositions. The decomposition into a product of transpositions is not unique, but the numbers of transpositions appearing in these decompositions are always all even or all odd.

Theorem 1.10. *A permutation in S_n $(n \geq 2)$ cannot be both even and odd.*

Definition 1.11. The **sign** of a permutation $\tau \in S_n$ is the group homomorphism $\operatorname{sgn} : S_n \to \{-1, 1\}$ (here $\{-1, 1\}$ is a multiplicative group) defined by

$$\operatorname{sgn}(\tau) = \begin{cases} 1 & \text{if } \tau \text{ is even,} \\ -1 & \text{if } \tau \text{ is odd.} \end{cases}$$

1.5 Alternating Group

Definition 1.12. The group of all even permutations of S_n is called the **alternating group** of degree n and is denoted A_n.

Lemma 1.13. *When $n \geq 3$, A_n is generated by the set of all 3-cycles.*

Theorem 1.14. *Let $n \geq 2$. Then A_n is a normal subgroup of S_n of index 2 and order $n!/2$. Furthermore A_n is the only subgroup of S_n of index 2.*

Lemma 1.15. *Let r, s be distinct elements of $[n]$. Then A_n $(n \geq 3)$ is generated by the $n-2$ cycles (rsk), $1 \leq k \leq n$ with $k \neq r, s$.*

Lemma 1.16. *If N is a normal subgroup of A_n $(n \geq 3)$ and N contains a 3-cycle, then $N = A_n$.*

Theorem 1.17. *The alternating group A_n is simple if and only if $n \neq 4$.*

Main References. [Suz82; Lan02; Hun80; Li25]

2 Dihedral Groups and the Quaternion Group

2.1 Dihedral Groups

Definition 2.1. Let $n \geq 3$ and let $d : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}_{\geq 0}$ be the Euclidean distance. A **symmetry** s of a regular polygon P_n of n sides is a bijection that preserves distances, i.e., if $x, y \in P_n$, then $d(x, y) \implies d(s(x), s(y))$. The **dihedral group** D_n is the group of symmetries of P_n.

Proposition 2.2. *Let r be a rotations of degree $360°/n$ clockwise around the center of the polygon P_n and let s be a fixed reflection about a line through the center and one vertex v. Then $D_n = \langle r, s \rangle$ and hence $|D_n| = 2n$.*

2.2 Presentations of Dihedral Groups

A way to describe a group is by using a **presentation**. Informally, it is an expression of the form $\langle X|R\rangle$, where X is a set of "generators", and R is a set of "relations". The precise definition will be introduced after we have studied free groups. For $n \geq 1$, D_n has a usual presentation $\langle r, s \,|\, r^n = s^2 = 1, rs = sr^{-1}\rangle$. Clearly $D_1 \cong \mathbb{Z}_2$ and $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. This extends the definition of dihedral groups.

The following are some of the presentations commonly used to express D_n:

(i) A subgroup of S_n generated by $(123\cdots n)$ and $\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-2 & \cdots & 3 & 2 \end{pmatrix}$.

(ii) A subgroup of $\mathrm{GL}(2,\mathbb{C})$ generated by $\begin{pmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

(iii) A subgroup of $\mathrm{GL}(2,\mathbb{C})$ generated by $\begin{pmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

2.3 Subgroups of Dihedral Groups

We can give the complete description of subgroups of dihedral groups. The proof below depends on the following theorem (will be studied in Generators and Relations).

Theorem 2.3 (Van Dyck)**.** *Let X be a set and let Y be the set of reduced words on X. Let G be a group defined by the generators $x \in X$ and relations $w = e$ $(w \in Y)$. Then for any group H generated by X satisfying the same relations, there is an epimorphism $G \to H$.*

Theorem 2.4. *Every subgroup of a dihedral group D_n is cyclic or dihedral. In fact, every subgroup of $D_n = \langle r, s \rangle$ belongs to one of the following lists:*

(i) $\langle r^d \rangle$, where d is a positive divisor of n;

(ii) $\langle r^d, r^i s \rangle$, where d is a positive divisor of n and $0 \leq i \leq d-1$.

Theorem 2.5. *If n is odd, then the proper normal subgroups of D_n are those in Theorem 2.4.(i). If n is even, the proper normal subgroups of D_n are those in Theorem 2.4.(i), together with $\langle r^2, s\rangle$ and $\langle r^2, rs\rangle$.*

2.4 Quaternion Group

Definition 2.6. The **quaterion group** is the group $Q_8 = \langle i, j \,|\, i^4 = 1, i^2 = j^2, ij = ji^{-1} \rangle$. Another presentation is $\langle -1, i, j, k \,|\, (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$.

Proposition 2.7. *The order of Q_8 is 8.*

The following are some usual presentations of Q_8:

(i) A subgroup of $\mathrm{GL}(2,\mathbb{C})$ generated by $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(ii) A subgroup of $\mathrm{GL}(2,\mathbb{C})$ generated by $\begin{pmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Theorem 2.8. *All subgroups of Q_8 are normal.*

If a group G is abelian, then all the subgroups of G are normal in G. Theorem 2.8 provides counterexamples to the converse of this statement. Moreover, $D_4 \ncong Q_8$, which can be seen from their normal subgroups.

Theorem 2.9. *Let G be a nonabelian group of order 8. Then either $G \cong D_4$ or $G \cong Q_8$.*

Main References. [DF04; Art91; Hun80]

3 Group Actions

3.1 Basic Definitions

Definition 3.1. Let G be a group and let X be a set. The **left action** of G on X is a function $\rho : G \times X \to X$ such that

(i) $\rho(g, \rho(g', x)) = \rho(gg', x)$ for all $g, g' \in G$ and $x \in X$;

(ii) $\rho(e, x) = x$ for all $x \in X$.

3.2 Orbit-Stabilizer Theorem

Definition 3.2. Let G act on X. A subset

$$O_G(x) = \{gx \mid g \in G\}$$

is called an **orbit** containing $x \in X$. The number of elements in $O_G(x)$ is called the **length** of the orbit $O_G(x)$.

Proposition 3.3. *$O_G(x)$ $(x \in X)$ are equivalence classes with respect to the relation defined by $x \sim y$ if and only if $y = gx$ for some $g \in G$.*

Definition 3.4. Let $x \in X$. The set $S_G(x) = \{g \in G \mid gx = x\}$ is called the **stabilizer** of x. An element $g \in G$ is said to **stabilize** or **fix** x if $g \in Gx$.

Proposition 3.5. *Let G act on X. Then*

(i) the stabilizer of $x \in X$ is a subgroup of G. Hence it is also called the ***isotropy group****;*

(ii) for all $g \in G$ and $x \in X$, we have

$$S_G(gx) = gS_G(x)g^{-1}.$$

Lemma 3.6. *Let G act on X. Then*

(i) the set of orbits partitions X, i.e., $X = \cup_x O_G(x)$ where x is a representative for each orbit;

(ii) for each $x \in X$, the function $O_G(x) \to \{gS_G(x) \mid g \in G\}; gx \mapsto gS_G(x)$ is bijective.

Theorem 3.7 (Orbit-Stabilizer Theorem)**.** *Let G act on a* ***finite*** *set X. Then for all $x \in X$,*

$$|O_G(x)| = [G : S_G(x)] = \frac{|G|}{|S_G(x)|}.$$

Corollary 3.8 (Orbit decomposition)**.** *Let G act on a finite set X. Let n be the total number of disjoint orbits. If x_i is a representative of $O_G(x_i)$ for $i = 1, \ldots, n$, then*

$$|X| = \sum_{i=1}^{n} [G : S_G(x_i)].$$

We end this section by counting the total number of orbits in a group action with both group and set being finite.

Definition 3.9. Let G act on a finite set X. The **character** of a permutation representation of G is the function $\chi : G \to \mathbb{Z}_{\geq 0}$ defined by

$$\chi(g) = |\{x \in X \mid gx = x\}|.$$

In other words, $\chi(g)$ is the number of points of X fixed by g.

Theorem 3.10 (Burnside's Lemma)**.** *Let G act on X. If both G and X are finite, then the total number of orbits is given by*

$$\frac{1}{|G|}\sum_{g\in G}\chi(g).$$

3.3 Kernel of Group Actions

Definition 3.11. Let G act on X and let $\rho : G \to \mathrm{Sym}(X)$ be the associated homomorphism (discussed in Proposition **??**). We say that the action is **faithful** if $\mathrm{Ker}\,\rho = \{e\}$.

Proposition 3.12. *Let G act on X. Then the kernel of the action is the intersection of all the stabilizers $\cap_{x \in X} S_G(x)$.*

3.4 Transitive Actions

Definition 3.13. Let G act on X. The action (or the G-set) is said to be **transitive** (or G is **transitive** on X) if there is only one orbit, i.e., for all $x, y \in X$, there exists $g \in G$ such that $y = gx$; otherwise, it is **intransitive**.

Proposition 3.14. *Let G act transitively on X. Then the kernel of the action is*

$$\bigcap_{g \in G} g S_G(x) g^{-1}$$

for some $x \in X$.

Proposition 3.15. *Let G act transitively on X. If G is finite and $|X| > 1$, then there exists $g \in G$ fixing no points of X.*

3.5 Conjugations

Definition 3.16. Two subsets S and T of a group G are said to be **conjugate** in G if there exists $g \in G$ such that $T = gSg^{-1}$.

Definition 3.17. We say that a group G act on a set X by **conjugation** if the action of G is given by $(g, x) \mapsto gxg^{-1}$.

Definition 3.18. Let G be a group and let H be a subgroup of G. The following table shows the notions used for orbits and stabilizers of group actions by conjugation.

Group	Set	Orbit	Stabilizer
G	G	Conjugacy class of x	Centralizer of x
H	G	-	Centralizer of x in H
H	Subsets of G	-	Normalizer of K in H

Proposition 3.19. *The number of conjugates of a subset S in a group G is the index of the normalizer of S. In particular, the number of conjugates of an element x of G is the index of the centralizer of x.*

Definition 3.20. Consider a finite group G act on itself by conjugation. The equation

$$|G| = \sum_{i=1}^{n} [G : C_G(g_i)]$$

which follows from Corollary 3.8, is called the **class equation** of G.

Proposition 3.21. *Let G be a finite group. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$

where $x_1, \ldots, x_m$ are representatives of distinct conjugacy classes such that $[G : C_G(x_i)] > 1$.

Corollary 3.22. *Let H be a subgroup of a finite group G. If $\cup_{g \in G} gHg^{-1} = G$, then $H = G$.*

Theorem 3.23 (Landau)**.** *For each positive integer k, there exists a bound $B(k)$ such that a finite group G having exactly k conjugacy classes satisfies $|G| \leq B(k)$.*

We start with a lemma.

Lemma 3.24. *Given a positive integer k and a number M, there exist at most finitely many solutions in positive integers x_i for the equation*

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_k} = M.$$

3.6 Translations

Definition 3.25. Let G be a group and let H be a subgroup of G. We say that G act on the set of all left cosets of H in G by **left translation** (or **left multiplication**) if the action of G is given by $(g, aH) \mapsto gaH$. When $H = \{e\}$, we say that G **acts on itself by left translation** since we can identify each coset $\{a\}$ as the element a.

Theorem 3.26. *Let G act on the set X of left cosets of H in G by left translation. Let $\rho : G \to \mathrm{Sym}(X)$ be the associated homomorphism. Then*

(i) G *acts transitively on* X*;*

(ii) $S_G(H) = H$*;*

(iii) $\mathrm{Ker}\,\rho = \cap_{g \in G}\, gHg^{-1}$*;*

(iv) $\mathrm{Ker}\,\rho$ *is the largest normal subgroup of* G *contained in* H*.*

In the situation of Theorem 3.26, the largest normal subgroup of G contained in H is called the **core** of H in G, and we write $N = \mathrm{Core}_G(H)$.

Corollary 3.27. *The action of a group on itself by left translation is faithful.*

Theorem 3.28 (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of some permutation group. If G is a group of order n, then G is isomorphic to a subgroup of S_n.*

Definition 3.29. The isomorphism ρ defined above is called the **left regular representation**. The **right regular representation** is defined similarly by $\rho_g(x) = xg^{-1}$ (inverse is needed in order to satisfy axioms).

Corollary 3.30. *Let G be a group and let H be a subgroup of G with finite index n. Then there exists a normal subgroup N in G such that N is a subgroup of H and $[G : N]$ divides $n!$.*

Corollary 3.31. *If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.*

Main References. [DF04; Rot95; Hun80; Isa09]

4 The Sylow Theorems

The entire study of this section can be motivated by the following question:

Question. Lagrange's Theorem states that for every subgroup H of a finite group G, we have $|H|$ divides $|G|$. Is the converse true? That is, if d divides $|G|$, then G contain a subgroup of order d.

The following provides a counterexample.

Proposition 4.1. *The alternating group A_4 has order 12 and does not contain a subgroup of order 6.*

This motivates us to add some conditions so that the converse is true. It turns out that the result is true if the divisor is a power of prime.

4.1 p-groups

Definition 4.2. Let p be a prime. A finite **p-group** is a finite group of order p^k for some $k \geq 0$. A subgroup of G is called **p-subgroup** if it is a p-group.

Lemma 4.3 (Fixed point lemma)**.** *Let G be a p-group and let X be a finite set. Suppose G acts on X. Let $X_G = \{x \in X \mid gx = x \text{ for all } g \in G\}$. Then $|X| \equiv |X_G| \mod p$.*

Theorem 4.4 (Cauchy's Theorem)**.** *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Corollary 4.5. *A finite group G is a p-group if and only if every element has order a power of the prime p.*

Proposition 4.6. *Let H be a p-subgroup of a finite group G.*

(i) $[N_G(H) : H] \equiv [G : H] \mod p$;

(ii) if $p | [G : H]$, *then* $N_G(H) \neq H$.

4.2 Sylow's Theorems

Definition 4.7. Let G be a group of order $p^k m$, where $p \nmid m$, then a subgroup of order p^k is called a **Sylow p-subgroup** of G. The set of Sylow p-subgroups of G will be denoted by $\mathrm{Syl}_p(G)$.

Theorem 4.8 (First Sylow Theorem)**.** *Let G be a group of order $p^k m$, where $k \geq 1$ and p is a prime not dividing m. Then*

(i) for each $1 \leq i \leq k$, the group G contains a subgroup of order p^i;

(ii) for each $1 \leq i < k$, every subgroup of G of order p^i is normal in some subgroup of order p^{i+1}.

In particular, Sylow p-subgroups of G exists.

Theorem 4.9 (Second Sylow Theorem)**.** *Let p be a prime. If P is a Sylow p-subgroup of a finite group G, and H is a p-subgroup of G, then H is contained in some conjugate of P, i.e., there exists $x \in G$ such that $H \leq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.*

Theorem 4.10 (Third Sylow Theorem)**.** *Let G be a finite group and let p be a prime. If n_p is the number of Sylow p-subgroups of G, then $n_p = [G : N_G(P)]$ for any Sylow p-subgroup P, and hence n_p divides $|G|$. Furthermore,*

$$n_p \equiv 1 \mod p.$$

In other words, n_p is of the form $kp+1$ for some $k \geq 0$.

4.3 Applications

As an application, one thing we might do is to determine whether a group contains a normal Sylow subgroup, and so study its simplicity. However, this section is a total mess, as there are many variants of the problems, and some require more elegant approaches to solve. In this section, I will only focus on a few problems that use common arguments. It is good to explore more ideas through textbooks and their exercises.

Corollary 4.11. *Let G be a group and let p be a prime. Let P be the Sylow p-subgroup of G. Then P is unique if and only if P is normal in G.*

Proposition 4.12. *Let G be a group of order pm, where p is a prime not dividing the integer $m \geq 1$. If the only factor of m, whose remainder is 1 when divided by p, is 1, then G is not simple.*

Proposition 4.13. *Let G be a group of order pq, where $p > q$ are primes. Then G has a normal Sylow p-subgroup. Also, if G is nonabelian, then $q|(p-1)$ and $n_q = p$.*

Proposition 4.14. *Let G be a group of order p^2q, where p and q are distinct primes. Then G has a normal Sylow subgroup (either p or q).*

Main References. [Hun80; DF04; Isa09]

5 Series

This series is not the series in analysis okay. One approach to studying the structure of groups is by breaking them down using composition series. It turns out that any two composition series of a group have the same of composition factors (Jordan–Hölder Theorem). These composition factors thus form an invariant of the group.

5.1 Basic Definitions and Examples

Definition 5.1. Let G be a group. A finite sequence of subgroups

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = \{e\}$$

is called a **series** of G. The **length** of the series is the number of strict inclusions. Furthermore, we say that it is

(i) **proper** if $G_i \neq G_{i+1}$ for all $i = 0, 1, \ldots, n-1$;

(ii) **subnormal** if $G_i \lhd G_{i-1}$ for all $i = 1, 2, \ldots, n$;

(iii) **normal** if $G_i \lhd G$ for all $i = 0, 1, \ldots, n$.

When the series is subnormal, the quotient groups G_i/G_{i+1} are called the **factors** of the series. In this case, the length of the series can be defined as the number of nontrivial factors.

Note that we are not concerned with series without any additional properties. Instead, we focus on certain types of series which involve the concept of normality, simplicity and abelian group.

Definition 5.2. Given a subnormal series $G = G_0 \geq G_1 \geq \cdots \geq G_n = \{e\}$. We say that the series is a **composition series** if each factor G_i/G_{i+1} is simple. In this case, we may write $G_0 > G_1 > \cdots > G_n$ and the factors are called **composition factors**.

Definition 5.3. Let

$$S: \quad G = G_0 \geq G_1 \geq \cdots \geq G_n = \{e\}$$

be a subnormal series of a group G. A **refinement** of S is a subnormal series S' of G such that G_i is a term in S' for each i. A refinement of S is said to be **proper** if its length is larger than the length of S; otherwise it is said to be **trivial**.

Simply speaking, refinement is just another subnormal series obtained by inserting a subgroup into the given subnormal series, and it is trivial if we insert a subgroup that already appears in the subnormal series. We do not define refinement for a series because it becomes redundant in this context.

Let us first characterize simple abelian groups before showing examples.

Proposition 5.4. *Every abelian group is simple if and only if it is of prime order.*

Example 5.5. Let G be a simple group. Then $G > \{e\}$ is a composition series.

Example 5.6. Let C be a cyclic group of order p^k, where p is a prime and $k \geq 1$. Let x be a generator of C. Then

$$C = \langle x \rangle > \langle x^p \rangle > \langle x^{p^2} \rangle > \cdots > \langle x^{p^k} \rangle = \{e\}$$

is a composition series. Note that every composition factor in this series is isomorphic to $\mathbb{Z}_p$.

Example 5.7. Let $n \geq 2$ be an integer. Let the prime factorization of n be $p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell}$. Then the following

$$\mathbb{Z}_n > \langle q_1 \rangle > \langle q_1 q_2 \rangle > \cdots > \langle q_1 q_2 \cdots q_m \rangle = \langle n \rangle = \{0\}.$$

is a composition series, where $q_1, \ldots, q_m$ is any ordering of prime factors of n and $m = k_1 + \cdots + k_\ell$. In fact, the number of composition series for $\mathbb{Z}_n$ is given by $\frac{m!}{k_1! k_2! \cdots k_\ell!}$. For example, let $n = 2025$. Then

$$\mathbb{Z}_{2025} > \langle 3 \rangle > \langle 9 \rangle > \langle 45 \rangle > \langle 135 \rangle > \langle 675 \rangle > \{0\}$$

is a composition series.

Example 5.8. As discussed in Section 1, we obtain composition series for S_n, where $n \geq 2$.

$$S_2 > \{e\},$$
$$S_3 > A_3 > \{e\},$$
$$S_4 > A_4 > \langle (1,2),(3,4),(1,3),(2,4) \rangle > \langle (1,2),(3,4) \rangle > \{e\},$$
$$S_n > A_n > \{e\}, \quad n \geq 5.$$

Example 5.9. In view of Theorem 2.5, we can determine composition series for D_4 as follows.

$$
\begin{gathered}
D_4 > \langle r \rangle > \langle r^2 \rangle > \{1\}, \\
D_4 > \langle s, r^2 \rangle > \langle s \rangle > \{1\}, \\
D_4 > \langle s, r^2 \rangle > \langle r^2 \rangle > \{1\}, \\
D_4 > \langle s, r^2 \rangle > \langle sr^2 \rangle > \{1\}, \\
D_4 > \langle r^2, rs \rangle > \langle r^3 s \rangle > \{1\}, \\
D_4 > \langle r^2, rs \rangle > \langle rs \rangle > \{1\}, \\
D_4 > \langle r^2, rs \rangle > \langle r^2 \rangle > \{1\}.
\end{gathered}
$$

Example 5.10. In view of Theorem 2.8, we can determine composition series for Q_8 as follows.

$$Q_8 > \langle i \rangle > \langle -1 \rangle > \{1\},$$
$$Q_8 > \langle j \rangle > \langle -1 \rangle > \{1\},$$
$$Q_8 > \langle ij \rangle > \langle -1 \rangle > \{1\}.$$

5.2 Basic Properties

Before we begin to study the properties of composition series, let us recall some definitions and their basic results that will be used later.

Definition 5.11. Let M be a proper subgroup of a group G is said to be **maximal** (resp. **maximal normal**) if $M \leq H \leq G$ (resp. $M \lhd H \lhd G$) implies $H = M$ or $H = G$.

Proposition 5.12. *Let G be a finite group. Then a maximal (resp. maximal normal) subgroup of G exists.*

Proposition 5.13. *Let G be a group. Then H is a maximal normal subgroup of G if and only if G/H is simple.*

Proposition 5.14. *Every finite group has a composition series.*

Proposition 5.14 is not true for infinite group. For example, $\mathbb{Z}$ has no composition series because every nontrivial proper subgroup of $\mathbb{Z}$ (which is of the form $m\mathbb{Z}$, $m > 1$) is not simple.

Proposition 5.15. *Every composition series has no proper refinement.*

5.3 Schreier Refinement Theorem and Jordan–Hölder Theorem

Definition 5.16. Two subnormal series of a group G

$$H_0 = G \geq H_1 \geq \cdots \geq H_s = \{e\},$$
$$K_0 = G \geq K_1 \geq \cdots \geq K_t = \{e\}$$

are said to be **isomorphic** if there exists a one-to-one correspondence between the set of factors $\{H_0/H_1, H_1/H_2, \ldots, H_{s-1}/H_s\}$ and $\{K_0/K_1, K_1/K_2, \ldots, K_{t-1}/K_t\}$ such that the corresponding factors are isomorphic.

Lemma 5.17 (Dedekind Law)**.** *Let U and V be two subsets of a group G and let L be a subgroup of G. If U is a subset of L, then*

$$U(V \cap L) = UV \cap L.$$

Lemma 5.18 (Zassenhaus Lemma / Butterfly Lemma)**.** *Let U, V be subgroups of a group. Let u, v be normal subgroups of U and V, respectively. Then*

$$u(U \cap v) \lhd u(U \cap V) \quad \text{and} \quad (u \cap V)v \lhd (U \cap V)v.$$

Moreover,

$$\frac{u(U \cap V)}{u(U \cap v)} \cong \frac{(U \cap V)v}{(u \cap V)v}.$$

Theorem 5.19 (Schreier Refinement Theorem)**.** *Let G be a group. Then any two subnormal series of G have isomorphic subnormal refinements.*

Definition 5.20. Let S and T be subnormal series of a group G. We say that S and T are **equivalent** if there is a one-to-one correspondence between the nontrivial factors of S and the nontrivial factors of T such that the corresponding factors are isomorphic.

Theorem 5.21 (Jordan–Hölder Theorem)**.** *Any two composition series of a group G are equivalent.*

By Theorem 5.21, we can conclude that composition factors of a group are unique determined up to isomorphism.

Corollary 5.22. *If a group G possesses a composition series, then any subnormal series of G can be refined to a composition series.*

Corollary 5.23. *Let H be a normal subgroup of a group G which has a composition series. Then both H and G/H have a composition series.*

We end the section by giving a new fancy proof of Fundamental Theorem of Arithmetic.

Corollary 5.24 (Fundamental Theorem of Arithmetic)**.** *Every integer $n \geq 2$ can be represented uniquely as a product of prime numbers, up to the order of the factors.*

Main References. [Lan02; Suz82; DF04; Li25; Rot15]

6 Direct Products

6.1 Direct Products of Finitely Many Groups

Definition 6.1. Let $H_1, H_2, \ldots, H_n$ be groups. The **direct product** of these groups is the cartesian product set $H_1 \times H_2 \times \cdots \times H_n$, equipped with the following binary operation

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1 y_1, x_2 y_2, \ldots, x_n y_n).$$

Sometimes we write $\prod_{i=1}^{n} H_i = H_1 \times H_2 \times \cdots \times H_n$.

Proposition 6.2. *Let $H_1, H_2, \ldots, H_n$ be groups.*

(i) *The direct product $\prod_{i=1}^{n} H_i$ is a group. If 1_i denotes the identity of the group H_i, then the element $(1_1, 1_2, \ldots, 1_n)$ is the identity of $\prod_{i=1}^{n} H_i$. The inverse of $(x_1, x_2, \ldots, x_n)$ is $(x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1})$. For each $(x_1, x_2, \cdots, x_n) \in \prod_{i=1}^{n} H_i$, $|(x_1, x_2, \cdots, x_n)| = \operatorname{lcm}(|x_1|, |x_2|, \ldots, |x_n|)$.*

(ii) $H_1 \times H_2 \times \cdots \times H_n \cong (H_1 \times \cdots \times H_m) \times (H_{m+1} \times \cdots \times H_n)$.

(iii) $H_1 \times H_2 \cong H_2 \times H_1$.

Definition 6.3. The direct product above is called an **external direct product**. If the operations in H_i are written additively, then we call $\prod_{i=1}^{n} H_i$ the **external direct sum** of these groups and write $H_1 \oplus H_2 \oplus \cdots \oplus H_n$ or $\oplus_{i=1}^{n} H_i$.

Proposition 6.4. *Let G be the direct product of the groups $H_1, \ldots, H_n$. For each $i = 1, \ldots, n$, let*

$$\overline{H}_i = \{(1_1, 1_2, \ldots, 1_{i-1}, x_i, 1_{i+1}, \ldots, 1_n) \,|\, x_i \in H_i\}.$$

In other words, $\overline{H}_i$ is the image of H_i under canonical injection. Then the following propositions hold.

(i) The subgroup $\overline{H}_i$ is isomorphic to H_i.

(ii) The subgroup $\overline{H}_i$ is normal in G.

*(iii) Each element in $\overline{H}_i$ commutes with each element in $\overline{H}_j$ for $i \neq j$. In this case, we say that $\overline{H}_i$ and $\overline{H}_j$ **commute elementwise**.*

(iv) $G = \overline{H}_1 \overline{H}_2 \cdots \overline{H}_n$ and every element of G can be written uniquely as $x_1 x_2 \cdots x_n$ with $x_i \in \overline{H}_i$ for all i.

(v) For each $k = 1, \ldots, n$, we have $\overline{H}_k \cap (\overline{H}_1 \cdots \overline{H}_{k-1} \overline{H}_{k+1} \cdots \overline{H}_n) = \{1\}$.

Corollary 6.5. *Let $H_1, H_2, \ldots, H_n$ be groups. Then*

$$|H_1 \times H_2 \times \cdots \times H_n| = |H_1| \cdot |H_2| \cdots |H_n|.$$

Let G be an arbitrary group. We wish to know the characterization of G if we have normal subgroups satisfying the properties in Proposition 6.4. This leads to the definition of internal direct product.

Lemma 6.6. *Let H and K be normal subgroups of a group G such that $H \cap K = \{1\}$. Then $hk = kh$ for every $h \in H$, $k \in K$.*

Theorem 6.7. *Let $H_1, H_2, \ldots, H_n$ be normal subgroups of a group G such that $G = H_1 H_2 \cdots H_n$. Then the following are equivalent.*

(1) The subgroups H_i and H_j commute elementwise for $i \neq j$, and every element of G can be written uniquely as $x_1 x_2 \cdots x_n$ with $x_i \in H_i$ for all i.

(2) For each $k = 1, \ldots, n$, we have $H_k \cap (H_1 \cdots H_{k-1} H_{k+1} \cdots H_n) = \{1\}$.

(3) For each $k = 2, \ldots, n$, we have $H_k \cap (H_1 \cdots H_{k-1}) = \{1\}$.

(4) There is an isomorphism $G \cong \prod_{i=1}^{n} H_i$ such that the subgroup H_i of G corresponds to the subgroup $\overline{H_i}$ of the direct product.

Definition 6.8. The group $G = H_1 H_2 \cdots H_n$ is called the **internal direct product** of the normal subgroups H_i if the conditions in Theorem 6.7 are satisfied. The normal subgroups $H_1, \ldots, H_n$ of are said to be **independent** if they satisfy condition (2) in Theorem 6.7.

Corollary 6.9. *Let $H_1, \ldots, H_n$ be normal subgroups of a group such that $|H_i|$ is relatively prime to $|H_j|$ for $i \neq j$. Then*

$$H_1 H_2 \cdots H_n \cong H_1 \times H_2 \times \cdots \times H_n.$$

Corollary 6.10. *Let G be the direct product of the subgroups $H_1, H_2, \ldots, H_m$. Then*

$$Z(G) = Z(H_1) \times Z(H_2) \times \cdots \times Z(H_m).$$

Proposition 6.11. *Suppose that a group G is the direct product of the subgroups $H_1, \ldots, H_n$. Let N_i be a normal subgroup of H_i for each i. Let $N = N_1 N_2 \ldots N_n$. Then the following propositions hold.*

(i) Each N_i is a normal subgroup of G.

(ii) The group N is the direct product of the subgroups $N_1, N_2, \ldots, N_n$, i.e.,

$$N_1 N_2 \cdots N_n \cong N_1 \times N_2 \times \cdots \times N_n.$$

(iii) The group G/N is isomorphic to the direct product of the groups $H_1/N_1, \ldots, H_n/N_n$, i.e.,

$$\frac{H_1 \times H_2 \times \cdots \times H_n}{N_1 N_2 \cdots N_n} \cong H_1/N_1 \times H_2/N_2 \times \cdots \times H_n/N_n.$$

6.2 Direct Products of Infinitely Many Groups

We have considered the direct product of a finite number of groups. The direct product of infinitely many groups may be defined similarly.

Definition 6.12. Let $\{H_\lambda \mid \lambda \in \Lambda\}$ be a family of groups indexed by a set Λ. Consider the set $\prod_{\lambda\in\Lambda} H_\lambda$ of functions $f : \Lambda \to \bigcup_{\lambda\in\Lambda} H_\lambda$ defined on Λ such that $f(\lambda) \in H_\lambda$ for all $\lambda \in \Lambda$, and define the product of two such functions f and g by the formula

$$(fg)(\lambda) = f(\lambda)g(\lambda).$$

Then $\prod_{\lambda\in\Lambda} H_\lambda$ equipped with the operation defined above forms a group, and is called the **unrestricted direct product** (or **complete direct product**) of the groups H_λ $(\lambda \in \Lambda)$. The subgroup $\prod^{w}_{\lambda\in\Lambda} H_\lambda$ of $\prod_{\lambda\in\Lambda} H_\lambda$ consisting of functions such that $f(\lambda)$ is the identity of H_λ for all but a finite number of λ's is called the **restricted direct product** (or **weak direct product**) of the groups H_λ $(\lambda \in \Lambda)$.

Theorem 6.13. *Let $\prod_{\lambda\in\Lambda} H_\lambda$ be the unrestricted direct product of the groups H_λ ($\lambda \in \Lambda$). Then $(\prod_{\lambda\in\Lambda} H_\lambda, \{\pi_\lambda \mid \lambda \in \Lambda\})$ is a product in the category of groups, where each $\pi_\mu : \prod_{\lambda\in\Lambda} H_\lambda \to H_\mu$ is the canonical projection.*

Proposition 6.14. *Let G be the restricted direct product of a family of groups $\{H_\lambda \mid \lambda \in \Lambda\}$. For each $\lambda \in \Lambda$, let $\overline{H}_i$ be the image of H_i under canonical injection. Then the following propositions hold.*

(i) *The subgroup $\overline{H}_\lambda$ is isomorphic to H_i.*

(ii) *The subgroup $\overline{H}_\lambda$ is normal in G.*

(iii) *The subgroups $\overline{H}_\lambda$ and $\overline{H}_\mu$ commute elementwise.*

(iv) *$G = \langle \overline{H}_\lambda \mid \lambda \in \Lambda \rangle$, and for every nonidentity element g of G, there exists a unique finite subset $\{\lambda_1, \ldots, \lambda_n\}$ of Λ such that g can be written uniquely as $x_1 x_2 \cdots x_n$ with $x_i \in \overline{H}_{\lambda_i} \setminus \{1\}$ for all i.*

We also have **internal direct product** of a family of normal subgroups as follows.

Theorem 6.15. *Let $\{H_\lambda \mid \lambda \in \Lambda\}$ be a family of normal subgroups a group G such that $G = \langle H_\lambda \mid \lambda \in \Lambda \rangle$. Then the following are equivalent.*

(1) The subgroups H_λ and H_μ commute elementwise for $\lambda \neq \mu$, and for every nonidentity element g of G, there exists a unique finite subset $\{\lambda_1, \ldots, \lambda_n\}$ of Λ such that g can be written uniquely as $x_1 x_2 \cdots x_n$ with $x_i \in H_{\lambda_i} \setminus \{1\}$ for all i.

(2) For each $\lambda \in \Lambda$, we have $H_\lambda \cap \langle H_\mu \mid \mu \neq \lambda \rangle = \{1\}$.

(3) There is an isomorphism $G \cong \prod^w_{\lambda \in \Lambda} H_i$ such that the subgroup H_λ of G corresponds to the subgroup $\overline{H}_\lambda$ of the direct product.

Main References. [Suz82; Hun80; Isa09; Rob82]

7 Structure Theorem for Finitely Generated Abelian Groups

Throughout this section we write abelian groups additively.

7.1 Free Abelian Groups

Definition 7.1. A **basis** of an abelian group F is a nonempty subset X of F such that $F = \langle X \rangle$ and X is **linearly independent**, i.e., for distinct $x_1, x_2, \ldots, x_k \in X$ and $n_i \in \mathbb{Z}$,

$$n_1x_1 + n_2x_2 + \cdots + n_kx_k = 0 \implies n_i = 0 \text{ for every } i.$$

The abelian group F is said to be **free** on the set X if X is a basis of F.

Lemma 7.2. *Let I be an index set. For each $j \in I$, let θ_j be the element $(u_i)_{i \in I}$ of $\oplus_{i \in I} \mathbb{Z}$, where*

$$u_i = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

Then $\{\theta_i \,|\, i \in I\}$ is a basis of $\oplus_{i \in I} \mathbb{Z}$. Furthermore, $\oplus_{i \in I} \mathbb{Z}$ is a free object on $\{\theta_i \,|\, i \in I\}$.

Proposition 7.3. *The following conditions on an abelian group F are equivalent.*

(1) F has a basis X.

(2) F is the direct sum of a family of infinite cyclic subgroups.

(3) F is isomorphic to a direct sum of copies of $\mathbb{Z}$.

(4) F is a free object on X in the category of abelian groups.

Theorem 7.4. *Any two bases of a free abelian group F have the same cardinality.*

Definition 7.5. The number of elements in a basis of G will be called the **rank** of G.

Theorem 7.6. *If G is a subgroup of a free abelian group F, then G is a free abelian group. Moreover,* $\operatorname{rank} G \leq \operatorname{rank} F$.

Corollary 7.7. *Let F_1 be the free abelian group on the set X_1 and F_2 the free abelian group on the set X_2. Then $F_1 \cong F_2$ if and only if F_1 and F_2 have the same rank.*

Corollary 7.8. *Every abelian group G is the homomorphic image of a free abelian group of rank $|X|$, where X is a set of generators of G.*

Corollary 7.9. *Every subgroup of finitely generated abelian group is finitely generated.*

7.2 Structure Theorem

Definition 7.10. Let G be an abelian group. An element $x \in G$ is said to be **torsion** if it has finite order. The subset G_t of all torsion elements of G is a subgroup of G called the **torsion subgroup** of G. An abelian group is said to be **torsion free** if the only torsion element is the identity.

Lemma 7.11. *Let G be a finitely generated torsion-free abelian group. Then G is a free abelian group of finite rank.*

Lemma 7.12. *Let $\varphi : G \to F$ be a surjective homomorphism of abelian groups, where F is free. Then there exists a subgroup H of G such that the restriction of φ to H induces an isomorphism of H with F , i.e., $H \cong F$, and*

$$G = \ker \varphi \oplus H.$$

Theorem 7.13. *If G is a finitely generated abelian group, then G_t is finite and $G = G_t \oplus F$, where F is a free abelian group of finite rank and $F \cong G/G_t$.*

Lemma 7.14. *For each positive integer m, let G_m be the subgroup of a group G consisting of elements $x \in G$ such that $mx = 0$. Then for any positive coprime integers r and s,*

$$G_{rs} = G_r \oplus G_s.$$

Theorem 7.15. *Let G be a torsion abelian group. For each prime p, let $G(p)$ be the set of elements of G whose order is a power of p, i.e., $G(p) = \{x \in G \,|\, |x| = p^n$ for some $n \geq 0\}$.*

(i) $G(p)$ is a subgroup of G for each prime p. If $G(p)$ is finite, then it is a p-group.

(ii) (Primary Decomposition) $G = \oplus_{p \text{ is prime}} G(p)$. If G is finitely generated, then only finitely many of the $G(p)$ are nonzero.

Lemma 7.16. *Let G be an abelian p-group. Let g be a nonzero element of G. If $p^k g$ is nonzero and has order p^ℓ, then g has order $p^{k+\ell}$.*

Lemma 7.17. *Let G be a p-group and let x be an element of maximal order in G. Let $\bar{g}$ be an element of $G/\langle x \rangle$, of order p^r. Then there exists a representative g of $\bar{g}$ in G which also has order p^r.*

Lemma 7.18. *Let m and n be integers such that $1 \leq m < n$. Let p be a prime number. Then*

$$p^m \mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-m}}.$$

Lemma 7.19. *Let G an abelian group and let m be an integer. If G is the direct sum of subgroups G_i $(i \in I)$ then*

$$mG = \bigoplus_{i \in I} mG_i.$$

Theorem 7.20. *Let G be a finite abelian p-group. Then G is an (internal) direct sum of cyclic groups of orders $p^{n_1}, \ldots, p^{n_k}$ respectively, with $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$. In particular,*

$$G \cong \mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_k}}.$$

In this case, we say that G is of type $(p^{n_1}, \ldots, p^{n_k})$. The integers $n_1, \ldots, n_k$ are uniquely determined.

By Theorems 7.13, 7.15 and 7.20, we have the following decomposition of finitely generated abelian groups.

Theorem 7.21. *A finitely generated abelian group G is the direct sum of a free abelian group F of finite rank and a finite number of cyclic groups. The cyclic summands (if any) are of orders $p_1^{s_1}, \ldots, p_k^{s_k}$ where $p_1, \ldots, p_k$ are (not necessarily distinct) prime numbers and $s_1, \ldots, s_k$ are (not necessarily distinct) positive integers. The rank of F and the prime powers $p_1^{s_1}, \ldots, p_k^{s_k}$ are uniquely determined by G, up to their order). In particular,*

$$\begin{aligned} G &= \langle x_1 \rangle \oplus \cdots \oplus \langle x_k \rangle \oplus F \\ &\cong \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k}} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{\text{rank } F \text{ summands}} \end{aligned}$$

where $x_1, \ldots, x_k \in G$ with $|x_i| = p_i^{s_i}$ for all $i = 1, \ldots, k$.

Definition 7.22. The prime powers $p_1^{s_1}, \ldots, p_k^{s_k}$ in Theorem 7.21 are called the **elementary divisors** of G.

Since the order of the primary cyclic factors may vary, the decomposition is not entirely unique. To resolve this issue, there is another way to decompose a group without introducing elementary divisors.

Theorem 7.23. *A finitely generated abelian group G is the direct sum of a free abelian group F of finite rank and a finite number of cyclic groups. The cyclic summands (if any) are of orders $m_1, \ldots, m_r$ where $m_1, \ldots, m_r$ are integers greater than 1 such that $m_1 | m_2 | \cdots | m_r$. The rank of F and the integers $m_1, \ldots, m_r$ are uniquely determined by G. In particular,*

$$\begin{aligned} G &= \langle x_1 \rangle \oplus \cdots \oplus \langle x_r \rangle \oplus F \\ &\cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{\text{rank } F \text{ summands}} \end{aligned}$$

where $x_1, \ldots, x_r \in G$ with $|x_i| = m_i$ for all $i = 1, \ldots, r$.

Definition 7.24. The integers $m_1, \ldots, m_r$ in Theorem 7.23 are called the **invariant factors** of G.

The isomorphism between finitely generated abelian groups can be studied using invariant factors (resp. elementary divisors).

Corollary 7.25. *Let G and H be finitely generated abelian groups. Then $G \cong H$ if and only if* $\operatorname{rank}(G/G_t) = \operatorname{rank}(H/H_t)$ *and G and H have the same invariant factors (resp. elementary divisors).*

Main References. [Lan02; Hun80; Kap54; Kap77; Rob82]

8 Semidirect Products

Important Note. Throughout this section, we will use **right action** $X \times G \to X$ where the image of $x \in X$ under $g \in G$ is denoted by x^g. Following the axioms of right action, we have $(x^g)^{g'} = x^{gg'}$ for all $g, g' \in G$. In accordance with this, function composition will be written as fg to mean that f is applied first, followed by g, i.e., $(fg)(x) = g(f(x))$. In conjugation by g on x, we define $x \mapsto g^{-1}xg$ to make it consistent with the right actions. To summarize, we can just "switch" the side from the corresponding left actions and replace the symbols s with s^{-1}.

8.1 Definitions and Properties

Definition 8.1. Let G and H be two groups. If a homomorphism $\varphi : G \to \operatorname{Aut} H$ is given, then we say that G acts on H via φ and G is an **operator group** on H. The homomorphism φ is called an **action** of G on H. We denote the image $\varphi(g)(h)$ of an element h of H simply by h^g.

Proposition 8.2. *Let φ be a function from a group G into the set of all functions on the subgroup H. Then φ is an action of G on H if and only if for all $u, v \in H$ and $x, y \in G$,*

$$(uv)^x = u^x v^x,$$
$$u^{xy} = (u^x)^y,$$
$$u^1 = u$$

where 1 is the identity of G.

Proposition 8.3. *Let φ be an action of a group G on another group H. Let L be the cartesian product set of H and G. Define the product of two elements of L by*

$$(h_1, g_1)(h_2, g_2) = (h_1 h_2^{g_1^{-1}}, g_1 g_2).$$

Then L forms a group with respect to this operation.

Definition 8.4. The group L in Proposition 8.3 is called the **semidirect product** H by G with respect to the action φ and is denoted by $H \rtimes_\varphi G$.

We set

$$\overline{H} = \{(h, 1) \mid h \in H\}, \quad \overline{G} = \{(g, 1) \mid g \in G\}.$$

Obviously they are just image sets under canonical injections. We summarize all the properties in a proposition.

Proposition 8.5. *Let $H \rtimes G$ be the semidirect product. Then the following propositions hold.*

(i) $\overline{H} \cong H$ *and* $\overline{G} \cong G$.

(ii) $\overline{H} \lhd H \rtimes G$.

(iii) $H \rtimes G = \overline{H}\,\overline{G}$.

(iv) $\overline{H} \cap \overline{G} = \{(1, 1)\}$.

(v) $|H \rtimes G| = |H||G|$ *if* G *and* H *are finite.*

(vi) For any $h \in H$ *and* $g \in G$, *we have* $(1, g)^{-1}(h, 1)(1, g) = (h^g, 1)$.

Corollary 8.6. *Every element of $H \rtimes G$ can be written uniquely as hg with $h \in H$ and $g \in G$.*

Proposition 8.7. *Let G act on another group H via φ. Let X and Y be two groups such that $X \cong G$ and $Y \cong H$. Then*

$$H \rtimes_{\varphi} G \cong Y \rtimes_{\theta} X$$

for some action θ of X on Y.

Definition 8.8. A group G is called an **internal semidirect product** of H by K (where H, K are subgroups of G), if

$$G = HK, \quad H \lhd G, \quad H \cap K = \{1\}.$$

Any internal semidirect product is isomorphic to the semidirect product with respect to some action. For this reason, "internal" is often omitted.

Proposition 8.9. *Let G be an internal semidirect product of two subgroups H and K such that $H \lhd G = HK$ and $H \cap K = \{1\}$. Let $\varphi(k)$ be the automorphism of H induced by the conjugation of $k \in K$, i.e., $h^k = k^{-1}hk$. Then φ is an action of K on H, and $H \rtimes K \cong G$.*

The definition of an internal semidirect product is not symmetric with respect to H and K. So it should be stated clearly which subgroup is normal in G when it is important to distinguish between them. In fact, if both subgroups are normal, then we recover direct product. More specifically, we have the following result.

Proposition 8.10. *Let φ be an action of a group G on a group H. Then the following are equivalent.*

(1) The identity map between $H \rtimes G$ and $H \times G$ is a group isomorphism.

(2) φ is the trivial homomorphism from G into $\operatorname{Aut} H$.

(3) The subgroup G is normal in $H \rtimes G$.

8.2 Examples

Example 8.11. By Proposition 4.14, a group G of order p^2q (p and q are distinct prime) has a normal Sylow subgroup. Let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. Then we can check that $|PQ| = |G|$ and $P \cap Q = \{1\}$. If $P \lhd G$, then $G \cong P \rtimes Q$. If $Q \lhd G$, then $G \cong Q \rtimes P$.

Example 8.12. Let H be any abelian group and let $K = \langle k \rangle \cong \mathbb{Z}_2$ be the group of order 2. Define $\varphi : K \to \operatorname{Aut} H$ by mapping k to the automorphism of inversion on H, i.e., $h^k = h^{-1}$ for all $h \in H$. Then $H \rtimes K$ contains the subgroup H of index 2, since every element $g \in H \rtimes K$ is either in H or in kH. Let $H = \langle h \rangle$. Then we have

$$k^{-1}hk = h^{-1}.$$

If $H = \mathbb{Z}_n$, one recognizes $H \rtimes K$ as the dihedral group D_n. Since D_n has presentation

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

by Van Dyck's Theorem (Theorem 2.3), we get

$$D_n \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$$

since both groups have the same order.

If $H = \mathbb{Z}$, then we get a group D_∞ having the presentation

$$D_\infty = \langle r, s \,|\, s^2 = 1, s^{-1}rs = r^{-1} \rangle = \langle x, y \,|\, x^2 = y^2 = 1 \rangle.$$

The group D_∞ is called the **infinite dihedral group**. By Van Dyck's Theorem, there is an epimorphism $\theta : D_n \to H \rtimes K$ in which $\theta(r) = h$ and $\theta(s) = k$. Every element of D_n is the form $s^m r^\ell$ where $m = 0, 1$. Suppose that $s^m r^\ell \in \ker \theta$. Then we have $k^m h^\ell = \theta(s^k r^\ell) = 1$, which implies that $k = 0 = \ell$. Thus

$$D_\infty \cong \mathbb{Z} \rtimes \mathbb{Z}_2.$$

Example 8.13. Let H be any abelian group and to let $K = \langle k \rangle \cong \mathbb{Z}_{2n}$ be cyclic of order $2n$. Define φ again by mapping k to inversion, i.e., $h^k = h^{-1}$, so that k^2 acts as the identity on H. In $H \rtimes K$, we have $k^{-1}hk = h^{-1}$ and $k^{-2}hk^2 = h$ for all $h \in H$. Thus $k^2 \in Z(H \rtimes K)$. For instances, set $H = \mathbb{Z}_3$ and $K = \mathbb{Z}_4$. Then $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ is a nonabelian group of order 12 which is not isomorphic to A_4 or D_6, since its Sylow 2-subgroup, is cyclic of order 4.

Example 8.14. Let $H = \langle h \rangle \cong \mathbb{Z}_{2^n}$ and let $K = \langle k \rangle \cong \mathbb{Z}_4$ with $k^{-1}hk = h^{-1}$ in $H \rtimes K$. As noted above, $k^2 \in Z(H \rtimes K)$. Since k inverts h (i.e., inverts H), k inverts the unique subgroup $\langle z \rangle$ of order 2 in H, where $z = h^{2^{n-1}}$. Thus $k^{-1}zk = z^{-1} = z$, so k centralizes z. It follows that $z \in Z(H \rtimes K)$. Thus $k^2 z \in Z(H \rtimes K)$ and hence $\langle k^2 z \rangle \lhd H \rtimes K$. Let $G = (H \rtimes K)/\langle k^2 z \rangle$. Note that

$$|k^2 z| = \operatorname{lcm}(|k^2|, |z|) = \operatorname{lcm}(2, 2) = 2.$$

So

$$|G| = \frac{|H \rtimes K|}{|\langle k^2 z \rangle|} = \frac{2^{n+2}}{2} = 2^{n+1}.$$

Let $\bar{k}$ and $\bar{h}$ be images of k and h under canonical projections, respectively. Then we see that

$$\bar{k}^4 = 1, \quad \bar{h}^{2^n} = 1, \quad \bar{k}^{-1}\bar{h}\bar{k} = \bar{h}^{-1}, \quad \bar{h}^{2^{n-1}} = \bar{k}^2.$$

The last equality follows from $\bar{k}^2\bar{z} = 1$. Therefore, by Van Dyck's Theorem, we have

$$Q_{2^{n+1}} \cong \frac{H \rtimes K}{\langle k^2 z \rangle} \cong \frac{\mathbb{Z}_{2^n} \rtimes \mathbb{Z}_4}{\langle (2^{n-1}, 2) \rangle}$$

where the group $Q_{2^{n+1}}$ is called the **generalized quaternion group** of order 2^{n+1} which have the presentation

$$Q_{2^{n+1}} = \langle x, y \,|\, x^4 = 1, y^{2^n} = 1, x^{-1}yx = y^{-1}, y^{2^{n-1}} = x^2 \rangle.$$

In particular, when $n = 2$, we obtain the quaternion group Q_8.

Example 8.15. Let $\mathrm{GL}(n, \mathbb{F})$ be the group of $n \times n$ invertible matrices over a field $\mathbb{F}$. Let $\mathrm{SL}(n, \mathbb{F})$ be the subgroup of $\mathrm{GL}(n, \mathbb{F})$ consisting of matrices with determinant 1. Let $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ and let

$$K = \{\mathrm{diag}(a, 1, 1, \ldots, 1) \in \mathrm{GL}(n, \mathbb{F}) \,|\, a \in \mathbb{F}^*\}.$$

We now claim that $\mathrm{GL}(n, \mathbb{F})$ is an internal semidirect product of $\mathrm{SL}(n, \mathbb{F})$ and K. Clearly $\mathrm{SL}(n, \mathbb{F}) \cap K = \{I_n\}$ and $\mathrm{SL}(n, \mathbb{F}) \lhd \mathrm{GL}(n, \mathbb{F})$ (consider the kernel of determinant function). It remains to show that $\mathrm{GL}(n, \mathbb{F}) = \mathrm{SL}(n, \mathbb{F})K$. Let $A \in \mathrm{GL}(n, \mathbb{F})$ and $\det A = a$. Then we have

$$A = A\,\mathrm{diag}(a^{-1}, 1, \ldots, 1)\,\mathrm{diag}(a, 1, \ldots, 1) \in \mathrm{SL}(n, \mathbb{F})K$$

since $\det[A\,\mathrm{diag}(a^{-1}, 1, \ldots, 1)] = 1$. This proves the claim. By $K \cong \mathbb{F}^*$, Propositions 8.7 and 8.9, we obtain

$$\mathrm{GL}(n, \mathbb{F}) \cong \mathrm{SL}(n, \mathbb{F}) \rtimes K \cong \mathrm{SL}(n, \mathbb{F}) \rtimes \mathbb{F}^*.$$

Note that $\mathrm{GL}(n, \mathbb{F}) \ncong \mathrm{SL}(n, \mathbb{F}) \times \mathbb{F}^*$ in general. Let $n = 2$ and $\mathbb{F} = \mathbb{R}$. Then $\mathrm{GL}(2, \mathbb{R})$ has infinitely many elements of order 2, for example, each matrix of the form

$$\begin{pmatrix} 0 & x \\ x^{-1} & 0 \end{pmatrix}, \quad x \neq 0$$

is of order 2. However, $\mathrm{SL}(2, \mathbb{R}) \times \mathbb{R}^*$ contains only three elements of order 2, namely $(-I_2, 1)$, $(I_2, -1)$ and $(-I_2, -1)$.

8.3 Some Classifications of Groups

Proposition 8.16. *Let C be a cyclic group and let H be an arbitrary group. Let φ_1 and φ_2 be homomorphisms from C into $\mathrm{Aut}(H)$ such that $\operatorname{im}\varphi_1$ and $\operatorname{im}\varphi_2$ are conjugate subgroups of $\mathrm{Aut}(H)$. Then the following propositions hold.*

(i) If C is finite, then $H \rtimes_{\varphi_1} C \cong H \rtimes_{\varphi_2} C$.

(ii) If C is infinite, φ_1 and φ_2 are injective, then $H \rtimes_{\varphi_1} C \cong H \rtimes_{\varphi_2} C$.

Example 8.17. There are only two isomorphism types of groups of order pq, where $p > q$ are primes.

Let G be any group of order pq, let $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. By Proposition 4.13, we have $G \cong P \rtimes_\varphi Q$ with respect to some action φ. Clearly $P \cong \mathbb{Z}_p$ and $Q \cong \mathbb{Z}_q$ are cyclic. The group $\mathrm{Aut}(P) \cong \mathbb{Z}_{p-1}$ is also cyclic.

If q does not divide $p-1$, then G is abelian by Proposition 4.13. By Proposition 8.10, the only homomorphism from Q to $\mathrm{Aut}(P)$ is the trivial homomorphism, hence the only semidirect product in this case the direct product, i.e., $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

Consider now the case when q divides $p-1$. Let $Q = \langle y \rangle$. Since $\mathrm{Aut}(P)$ is cyclic it contains a unique subgroup of order q, say $\langle \gamma \rangle$. Hence any homomorphism $\varphi : Q \to \mathrm{Aut}(P)$ must map y to a power of γ. Therefore there are q homomorphisms $\varphi_i : Q \to \mathrm{Aut}(P)$ given by $\varphi_i(y) = \gamma^i$ where $0 \leq i \leq q-1$. Since φ_0 is the trivial homomorphism, $P \rtimes_{\varphi_0} Q \cong P \times Q$ as before. Each nontrivial homomorphism φ_i $(i \neq 0)$ gives rise to a semidirect product of order pq, which is a nonabelian group. It is straightforward to check that $\varphi_i(Q) = \langle \gamma \rangle$ for each $i > 0$. So these groups are all isomorphic by Proposition 8.16.

Lemma 8.18. *Let $G = PQ$ where p and q are distinct primes, $P \in Syl_p(G)$ is a normal abelian subgroup in G and $Q \in Syl_q(G)$. Let φ_1 and φ_2 be homomorphisms from Q into $\mathrm{Aut}(P)$. If $P \rtimes_{\varphi_1} Q \cong P \rtimes_{\varphi_2} Q$, then $\ker \varphi_1 \cong \ker \varphi_2$.*

Example 8.19. There are thirteen isomorphism types of groups of order $56 = 2^3 \cdot 7$. Let G be a group of order 56.

Before proceed to the classification, we shall show that G must contain a normal Sylow subgroup. If there is a normal Sylow 7-subgroup, then we are done. If all Sylow 7-subgroups are not normal, then Theorem 4.10 and Corollary 4.11 show that there are eight Sylow 7-subgroups. Then we count the number of elements of order 7 in G. There are $6 \cdot 8 = 48$ of them, leaving $56 - 48 = 8$ elements that are not of order 7. This eight elements must form a unique Sylow 2-subgroup, which is normal in G. Remark that the argument was modified from Proposition 4.14. For now, we let P and Q be a Sylow 7-subgroup and a Sylow 2-subgroup respectively.

If P is normal in G, then we want to construct nonisomorphic semidirect products $P \rtimes Q$. To do this, we consider all homomorphisms $\varphi : Q \to \operatorname{Aut} P$ and identify which isomorphic types the corresponding semidirect products belong to. By the First Isomorphism Theorem, we have $Q/\ker\varphi \cong \operatorname{im}\varphi$. Since $\operatorname{Aut} P \cong \mathbb{Z}_6$ and the order of $Q/\ker\varphi$ must be a power of 2, we get $Q/\ker\varphi \cong \mathbb{Z}_1$ or $Q/\ker\varphi \cong \mathbb{Z}_2$. Then the order of $\ker\varphi$ is either 4 or 8. Now we can find homomorphisms by determining all

nonisomorphic normal subgroups of Q with order 4 or 8. In view of Lemma 8.18, the corresponding semidirect products are not isomorphic.

By Theorems 2.9 and 7.21, there are only five nonisomorphic groups of order 8: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_8$, D_4 and Q_8. So we obtain the following isomorphism types.

- φ is trivial (the kernel has order 8):

  (1) $\mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$;

  (2) $\mathbb{Z}_7 \times \mathbb{Z}_4 \times \mathbb{Z}_2$;

  (3) $\mathbb{Z}_7 \times \mathbb{Z}_8$;

  (4) $\mathbb{Z}_7 \times D_4$;

  (5) $\mathbb{Z}_7 \times Q_8$.

- φ is nontrivial (the kernel has order 4):

  (6) $\mathbb{Z}_7 \rtimes_\varphi (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)$, $\ker \varphi \cong \langle 1 \rangle \oplus \langle 1 \rangle$;

(7) $\mathbb{Z}_7 \rtimes_\varphi (\mathbb{Z}_4 \times \mathbb{Z}_2)$, $\ker\varphi \cong \langle (1,0) \rangle$;

(8) $\mathbb{Z}_7 \rtimes_\varphi (\mathbb{Z}_4 \times \mathbb{Z}_2)$, $\ker\varphi \cong \langle 2 \rangle \oplus \langle 1 \rangle$;

(9) $\mathbb{Z}_7 \rtimes_\varphi \mathbb{Z}_8$, $\ker\varphi \cong \langle 2 \rangle$;

(10) $\mathbb{Z}_7 \rtimes_\varphi D_4$, $\ker\varphi \cong \langle r \mid r^4 = 1 \rangle$;

(11) $\mathbb{Z}_7 \rtimes_\varphi D_4$, $\ker\varphi \cong \langle r^2, s \mid r^4 = s^2 = 1,\ s^{-1}rs = r^{-1} \rangle$;

(12) $\mathbb{Z}_7 \rtimes_\varphi Q_8$, $\ker\varphi \cong \langle i \mid i^4 = 1 \rangle$;

If P is not normal, then Q is normal. By Proposition 8.9, we have a semidirect product $Q \rtimes_\theta P$ where θ is the conjugation of P on Q. We claim that $Q \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. By Proposition 8.10, the homomorphism θ must be nontrivial, whence $\ker\theta < P$. Let $P = \langle x \rangle \cong \mathbb{Z}_7$. Since P is cyclic, we have $\ker\theta = \{1\}$. Note that $S_P(y) = \{1\}$ or P for all $y \in Q$. If $S_P(y) = P$ for all $y \in Q$, then $x^{-1}yx = y$ for all $x \in P$ and $y \in Q$. This implies $\ker\theta = P$, a contradiction. Hence there exists $y \in Q$ with $S_P(y) = \{1\}$. By Orbit-Stabilizer Theorem (Theorem 3.7), $|O_P(y)| = |P| = 7$. This means that every other nonidentity element in Q can be expressed as a conjugate of y. These all

have the same order as y. Since Q is a 2-subgroup, by Cauchy's theorem (Theorem 4.4), there exists an element of order 2 in Q. Therefore the argument above shows that Q must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. By Proposition 8.7, we can conclude that

$$Q \rtimes_\theta P \cong (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\varphi \mathbb{Z}_7$$

for some action φ.

Finally, we show that every semidirect product with respect to a nontrivial action φ is isomorphic to $Q \rtimes_\theta P$. Note that

$$\begin{aligned} |\mathrm{Aut}\ Q| &= |\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2)| \\ &= |\mathrm{GL}_3(\mathbb{Z}_2)| \\ &= (2^3 - 1)(2^3 - 2)(2^3 - 2^2) \\ &= 168 = 2^3 \cdot 3 \cdot 7. \end{aligned}$$

Since P is cyclic of order 7 and both φ and θ are nontrivial, the images $\mathrm{im}\,\varphi$ and $\mathrm{im}\,\theta$ are of order 7, whence they are Sylow 7-subgroup of $\mathrm{Aut}\,Q$. By the Second Sylow

Theorem (Theorem 4.9), there exists $\sigma \in \operatorname{Aut} Q$ such that $\sigma^{-1} \operatorname{im} \varphi \sigma = \operatorname{im} \theta$. By Proposition 8.16, we have $Q \times_\varphi P \cong Q \times_\theta P$. Therefore we have established the last isomorphism type.

(13) $(\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \rtimes_\varphi \mathbb{Z}_7$, $\ker \varphi = \{1\}$.

8.4 Sylow Theorems for Groups with Operator Groups

As an application of semidirect product, we generalize Sylow's Theorem to cover groups with operator groups. Throughout the section, unless otherwise stated, let Q be an operator group on a group H. Let L be the semidirect product of Q and H with respect to the given action φ.

Definition 8.20. A subgroup U of H is said to be **Q-invariant** if $\varphi(x)U = U$ for all $x \in Q$.

Proposition 8.21. *Let U be a Q-invariant subgroup of H.*

(i) The group Q act on U via the restriction $\varphi(x)|_U$ of $\varphi(x)$ to U.

(ii) If U is normal, then Q acts on the quotient group H/U via the action defined by $(Uh)^x = Uh^x$.

Lemma 8.22. *A subgroup U of H is Q-invariant if and only if $Q \subseteq N_L(U)$.*

Lemma 8.23. *If U is a Q-invariant subgroup of H, then $N_H(U)$ is a Q-invariant subgroup of H.*

Lemma 8.24 (Frattini's Argument)**.** *Let H be a normal subgroup of a group G. If S is a Sylow p-subgroup of H, then we have $G = N_G(S)H$.*

Lemma 8.25. *Let P be a p-subgroup of a group G. If P is a Sylow p-subgroup of $N_G(P)$, then P is a Sylow p-subgroup of G.*

Lemma 8.26. *Let G be an internal semidirect product of H by K (so that H is normal in G). Then $N_G(K) \cap H$ commutes elementwise with K, and we have*

$$N_G(K) \cap H = C_H(K), \quad N_G(K) = KC_H(K).$$

Lemma 8.27. *Let $G = HK$ be a product of the subgroups H and K. Then for any conjugate subgroup $x^{-1}Hx$ ($x \in G$), there exists an element k of K such that $x^{-1}Hx = k^{-1}Hk$.*

Theorem 8.28. *Let q be a prime number. Assume that the operator group Q is a q-group and that q does not divide $|H|$. Then the following hold.*

(i) There exists a Q-invariant Sylow p-subgroup of H.

(ii) Any Q-invariant p-subgroup is contained in a Q-invariant Sylow p-subgroup of H.

(iii) Two Q-invariant Sylow p-subgroups are conjugate by an element of $C_H(Q)$.

Main References. [DF04; Suz82; Rot95; AB95; DM96]

9 Introduction to Permutation Group Theory

9.1 Notations

A **permutation group** of a set Ω is a subgroup of $\operatorname{Sym}\Omega$. If G is a permutation group on Ω, then G acts on Ω via the canonical injection and this is a faithful action. The **degree** of such an action is $|\Omega|$. Conversely, if G is a faithful action on Ω, then G can be identified as a permutation group of Ω. For simplicity, we reintroduce notations for notions in group actions. Let G act on Ω.

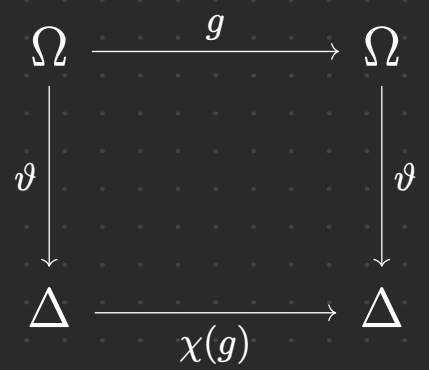
$$\omega^G = O_G(\omega) = \{\omega^g \mid g \in G\}, \qquad (\textbf{Orbit} \text{ of } \omega \in \Omega)$$
$$G_\omega = \operatorname{Stab}_G(\omega) = \{g \in G \mid \omega^g = \omega\}, \qquad (\textbf{Point stabilizer} \text{ of } \omega \in \Omega)$$
$$G_X = \{g \in G \mid X^g = X\}, \qquad (\textbf{Setwise stabilizer} \text{ of } X \subseteq \Omega)$$
$$G_{(X)} = \{g \in G \mid x^g = x \text{ for all } x \in X\}. \qquad (\textbf{Elementwise stabilizer} \text{ of } X \subseteq \Omega)$$

9.2 Isomorphic actions

Definition 9.1. Let G and H be groups acting on the sets Ω and Δ, respectively. The two actions (or the pairs (G, Ω) and (H, Δ)) are said to be **permutationally isomorphic** if there exist a bijection $\vartheta : \Omega \to \Delta$ and an isomorphism $\chi : G \to H$ such that

$$\vartheta(\omega^g) = \vartheta(\omega)^{\chi(g)}$$

for all $\omega \in \Omega, g \in G$. In other words, for every $g \in G$ the following diagram commutes.



If such conditions hold, the pair (ϑ, χ) is said to be a **permutational isomorphism**. Similarly, the pair (ϑ, χ) is a **permutational embedding** of the permutation group

G on Ω into the permutation group H on Δ, if $\chi : G \to H$ is a monomorphism and $(\vartheta, \hat{\chi})$ is a permutational isomorphism, where $\hat{\chi} : G \to \operatorname{im} \chi$ is obtained from χ by simply restricting the range of χ.

Proposition 9.2. *Let G act on a set Ω. Let Δ be a set and let $\vartheta : \Omega \to \Delta$ be a bijection. Define a G-action on Δ by $\delta^g = \vartheta((\vartheta^{-1}(\delta))^g)$. Then $(\vartheta, \mathrm{Id}_G)$ is a permutational isomorphism from the G-action on Ω to the G-action on Δ.*

Proposition 9.3. *Let G and H be groups acting transitively on Ω and Δ, respectively. Then the following are equivalent.*

(1) The actions of G and H on Ω and Δ, respectively, are permutationally isomorphic.

(2) There exist $\omega \in \Omega$ and $\delta \in \Delta$ and an isomorphism $\varphi : G \to H$ such that $\varphi(G_\omega) = H_\delta$.

(3) For all $\omega \in \Omega$ and $\delta \in \Delta$, there exists an isomorphism $\varphi : G \to H$ such that $\varphi(G_\omega) = H_\delta$.

Proposition 9.4. *Let Ω be a set and let $G_1, G_2 \leq \operatorname{Sym}\Omega$. Then G_1 and G_2 are permutationally isomorphic if and only if they are conjugate in $\operatorname{Sym}\Omega$. Moreover, if (ϑ, φ) is a permutational isomorphism, then $\vartheta \in \operatorname{Sym}\Omega$ and $\varphi(g) = \vartheta^{-1} g \vartheta$, for all $g \in G_1$.*

Recall that if H is a subgroup of a group G, then the right coset action of G on the set Γ_H of right cosets of H is defined by $(Hh)^g = Hhg$ for $h, g \in G$. In view of Theorem 3.26, this action is transitive. In fact, every transitive action is permutationally isomorphic to a coset action.

Proposition 9.5. *Let G act transitively on Ω and let $\omega \in \Omega$. Then the G-action on Ω is permutationally isomorphic to the G-action on Γ_{G_ω}.*

Corollary 9.6. *Let G act transitively on Ω and let $\omega \in \Omega$. Then a subgroup H of G is transitive if and only if $G = G_\omega H$.*

9.3 Blocks

Definition 9.7. Let G act transitively on Ω. The nonempty subset Δ of Ω is called a **block** if for every $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$. All the singletons of Ω and the set Ω itself are blocks, and so they are said to be **trivial**.

Proposition 9.8. *Let G act transitively on Ω. Then the following propositions hold.*

(i) If Δ is a block of Ω, then G_Δ acts transitively on Δ.

(ii) If Δ is a block, then $|\Delta^g| = |\Delta|$ and Δ^g is a block for each $g \in G$.

(iii) If Δ is a subset of Ω, then Δ is a block if and only if $\{\Delta^g \mid g \in G\}$ forms a partition of Ω.

Definition 9.9. Let G act on Ω. An equivalence relation $\sim$ on Ω is called a G-**congruence** if

$$\omega_1 \sim \omega_2 \iff \omega_1^g \sim \omega_2^g$$

for all $\omega_1, \omega_2 \in \Omega$ and $g \in G$. We also say that G preserves the relation.

Proposition 9.10. *Let G act transitively on Ω.*

(i) If $\sim$ is a G-congruence on Ω, then each equivalence class is a block of Ω.

(ii) If Δ is a block, then $\Sigma = \{\Delta^g \mid g \in G\}$ is the set of equivalence classes of a G-congruence on Ω. Hence G acts transitively on Σ.

Definition 9.11. Let G act transitively on Ω. A partition Σ of Ω is called a **system of blocks** (or a **system of imprimitivity**) if each $\Delta \in \Sigma$ is a block.

9.4 Primitive Actions

Definition 9.12. Let G act transitively on Ω. The action (or G-set) is said to be **primitive** (or G is **primitive** on Ω) if G has no nontrivial blocks; otherwise, it is **imprimitive**.

Proposition 9.13. *Let G acts transitively on Ω. Let $\omega \in \Omega$ be fixed. Then there is a one-to-one correspondence between the set of blocks of Ω containing ω and the set of subgroups which contains the stabilizer G_ω of ω.*

Corollary 9.14. *Let G act transitively on Ω. Then G is primitive if and only if the stabilizers are maximal subgroups.*

9.5 Centralizers and Normalizers of Transitive Permutation Groups

Definition 9.15. Let G act on a set Ω. We say that G acts **semiregularly** on Ω (G or the G-set Ω is **semiregular**) if nonidentity elements fix no point, i.e., $G_\omega = 1$ for all $\omega \in \Omega$. We say that G acts **regularly** on Ω if G is transitive and semiregular.

Lemma 9.16. *Let G be a group with a subgroup H, and put $K := N_G(H)$. Let Γ_H denote the set of right cosets of H in G, and let ρ and λ denote the right and left actions of G and K, respectively, on Γ_H as defined above. Then the following hold.*

(i) $\ker \lambda = H$ *and* $\lambda(K)$ *is semiregular.*

(ii) The centralizer C of $\rho(G)$ in $\operatorname{Sym} \Gamma_H$ *equals $\lambda(K)$.*

(iii) $H \in \Gamma_H$ has the same orbit under $\lambda(K)$ as under $\rho(K)$.

(iv) If $\lambda(K)$ is transitive, then $K = G$, and $\lambda(G)$ and $\rho(G)$ are conjugate in $\operatorname{Sym} \Gamma_H$.

Theorem 9.17. *Let G be a transitive subgroup of $\operatorname{Sym}\Omega$, and α a point in Ω. Let C be the centralizer of G in $\operatorname{Sym}\Omega$. Then the following hold.*

(i) C is semiregular, and $C \cong N_G(G_\alpha)/G_\alpha$. In particular, $|C| = |fix(G_\alpha)|$.

(ii) C is transitive if and only if G is regular.

(iii) If C is transitive, then it is conjugate to G in $\operatorname{Sym}\Omega$ and hence C is regular.

(iv) $C = 1$ if and only if G_α is self-normalizing in G, i.e., $N_G(G_\alpha) = G_\alpha$.

(v) If G is abelian, then $C = G$.

(vi) If G is primitive and nonabelian, then $C = 1$.

Theorem 9.18. *Let G be a transitive subgroup of $\operatorname{Sym}\Omega$, let N be the normalizer of G in $\operatorname{Sym}\Omega$ and let $\alpha \in \Omega$. If $\Psi : N \to \operatorname{Aut} G$ is the homomorphism defined by conjugation, and $\sigma \in \operatorname{Aut} G$, then $\sigma \in \operatorname{im}\Psi$ if and only if $(G_\alpha)^\sigma$ is a point stabilizer for G, i.e., $(G_\alpha)^\sigma = G_\beta$ for some $\beta \in \Omega$.*

Definition 9.19. Let G be a group. The **holomorph** of G, denoted by $\operatorname{Hol} G$, is the semidirect product $G \rtimes \operatorname{Aut} G$ with respect to the natural action of $\operatorname{Aut} G$ on G.

In the case where G is regular, the normalizer of G in the symmetric group is the holomorph of G.

Corollary 9.20. *Let G be a transitive subgroup of $\operatorname{Sym}\Omega$ and let N be the normalizer of G in $\operatorname{Sym}\Omega$. If G is regular, then $\operatorname{im}\Psi = \operatorname{Aut} G$. In this case $N_\alpha \cong \operatorname{Aut} G$, and N is isomorphic to $\operatorname{Hol} G$.*

Main References. [PS18; DM96; Cam99]