Algebra

Bruh

Contents

Preliminaries

These are definitions and results we used without proof. It is recommended to show them; should be good exercises for beginners in algebra.

Groups

(1) We start from defining a set with a binary operation.

- A set M with a binary operation $M \times M \to M$ is called a **magma**. We denote it by $(M, \cdot)$ or simply M. Note that the closure property is mentioned in the binary operation.
- A magma M is called a **semigroup** if it satisfies associative law: $(xy)z = x(yz)$ for all $x, y, z \in M$.
- A semigroup M is called a **monoid** if there is an identity element $e \in M$ (or 1) such that $ex = xe = x$ for all $x \in M$.
- A monoid G is called a **group** if every element in G has an inverse: for all $x \in G$, there exists $x^{-1} \in G$ such that $xx^{-1} = e = x^{-1}x$.

(2) Magma $\subset$ Semigroup $\subset$ Monoid $\subset$ Group.

(3) There is an optional property: x, y are **commutative** if $xy = yx$. A commutative group is called an **abelian group**.

(4) We can drop the bracket for the element $x_1 x_2 \cdots x_n$ in semigroup because of the **general associative law** (so we say the product is **uniquely determined**). It means that the ways to take the product while fixing the order of elements does not affect the outcome. Similarly, the product of elements in a commutative semigroup is uniquely determined regardless of the ways to take the product or the order of elements. This is because of the **general commutative law**.

(5) If elements x and y in a monoid is invertible, then $(x^{-1})^{-1} = e$ and $(xy)^{-1} = y^{-1}x^{-1}$. The latter is sometimes described as the **socks-shoes property**.

(6) In a group, define x^n $(n \geq 1)$ as the product of x taken n times, $x^0 = e$ and x^{-n} $(n \geq 1)$ as the product of x^{-1} taken n times. Then the following hold:

(i) $(x^{-1})^m = (x^m)^{-1}$ for all integer m;

(ii) $x^m x^n = x^{m+n}$ and $(x^m)n = x^{mn}$ for all integers m, n.

Subgroups

(1) Simply speaking, given a group with a binary operation $\cdot$, if the restriction of $\cdot$ to a subset $H \subseteq G$ makes H itself a group, then we call H a **subgroup** of G.

(2) We have a analogous criterion for sets to be subspaces of a vector space; so we call this criterion the **subgroup criterion**. A subset H is a subgroup of a group if and only if

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

This statement also equivalent to $xy \in H$ and $x^{-1} \in H$ for all $x, y \in H$.

(3) Let H be a subgroup of G. Then the identity of H is the identity of G.

(4) Clearly G and $\{e\}$ are subgroups of G. They are called **trivial subgroups**.

(5) Write $H \leq G$ for a subgroup H of G. Then we have:

(i) $K \leq H$ and $H \leq G \Rightarrow K \leq G$;

(ii) $H, K \leq G$ and $K \subseteq H \Rightarrow K \leq H$.

(6) The **intersection of subgroups** of G is a **subgroup** of G. I think that the index set is not required to be a countable set. So $\bigcap_{\lambda \in \Lambda} H_\lambda$ is also a subgroup of G.

(7) The **union of subgroups** is **not necessarily a subgroup** of G. In fact,

$$H \cup K \leq G \Leftrightarrow H \subseteq K \text{ or } K \subseteq H.$$

(8) The product $HK = \{hk \mid h \in H, k \in K\}$ is called the **product** of subgroups H and K. It is **not necessarily a subgroup** of G. In fact, we have

$$HK \leq G \Leftrightarrow HK = KH.$$

Subgroups defined by a subset

Let S be a subset of G. There are three classical subgroups that can be defined from S:

(1) the **subgroup** of G **generated by** S, denoted by $\langle S \rangle$; this is the set of all elements of G which can be written as the product of finite number of elements of S or of the inverses of elements of S, i.e., every element is of the form

$$s_1 s_2 \cdots s_n$$

where $s_i \in S$ or $s_i^{-1} \in S$.

- $\langle S \rangle$ is the intersection of all subgroups of G that contain S.
- $\langle S \rangle$ is the smallest subgroup of G that contains S.
- If $H = \langle S \rangle$, then S is called a **generating set** of H.
- If S is a finite set, then H is said to be **finitely generated**.
- In particular, if S is a singleton, then H is said to be **cyclic**.
- If we involve more than a set, say $S_1, \ldots, S_n$, then $\langle S_1, \ldots, S_n \rangle$ is the subgroup generated by the union of subsets S_i. If we have a collection of subsets $S_\lambda (\lambda \in \Lambda)$, then $\langle S_\lambda \,|\, \lambda \in \Lambda$ is the subgroup generated by $\bigcup_{\lambda \in \Lambda} S_\lambda$.

(2) the **normalizer** of S in G, denoted by $N_G(S)$; this is the set

$$N_G(S) = \{g \in G \,|\, gSg^{-1} = S\}.$$

In this case, we say g **normalizes** S.

- If H is a subgroup of G, then H is normal in $N_G(H)$.
- $N_G(H)$ is the largest subgroup of G that contains H as a normal subgroup.

(3) the **centralizer** of S in G, denoted by $C_G(S)$; this is the set

$$C_G(S) = \{g \in G \,|\, gs = sg \text{ for all } s \in S\}.$$

In this case, we say g centralizes S.

- $C_G(G)$ is called the **center** of G, and is denoted by $Z(G)$.

(4) The next subgroup is not depending on S, but it has important connection between those subgroups defined by S: If H is a subgroup of G, then xHx^{-1} (where $x \in G$ is fixed) is called a **conjugate subgroup** of H.

- Let $S \subseteq G$ and $x \in G$. Then

$$\begin{aligned} \langle xSx^{-1} \rangle &= x\langle S \rangle x^{-1}, \\ N_G(xSx^{-1}) &= xN_G(S)x^{-1}, \\ C_G(xSx^{-1}) &= xC_G(S)x^{-1}. \end{aligned}$$

As a consequence, $N_G(S) \subseteq N_G(C_G(S))$.

Cosets

(1) Let H be a subgroup of G and $x \in G$.

- xH is a **left coset** of H in G;
- Hx is a **right coset** of H in G.
- The number of distinct left cosets of H in G is called the index of H in G and denoted $[G : H]$.

When the context is clear, we will call a left coset simply a coset.

(2) $xH = yH \Leftrightarrow xy^{-1} \in H$.

(3) G can be **partitioned** into a **disjoint union of cosets** of H.

(4) Each coset has the same number of elements as in H, i.e., $|xH| = |H|$.

(5) $[G : K] = [G : H][H : K]$ for $K \leq H \leq G$.

(6) **Lagrange's Theorem.** $|G| = [G : H]|H|$.

(7) As corollary, the order of an element of a finite group G must divide the order of G.

(8) Using the concept of cosets one can establish

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

Remark that it has a weaker hypothesis than the Second Isomorphism Theorem since we don't require any subgroup to be normal.

Normal subgroups

(1) A subgroup H of G is said to be **normal** if

$$xH = Hx \text{ for all } x \in G.$$

Sometimes we denote it by $H \lhd G$. This condition can be also expressed as $xHx^{-1} = H$. So we can also define a normal subgroup as H with property $N_G(H) = G$.

(2) We have the following equivalent statements

$$xHx^{-1} = H \text{ for all } x \in G \Leftrightarrow xHx^{-1} \subseteq H \text{ for all } x \in G.$$

That is why sometimes proofs in some books only consider one direction.

(3) If $N \lhd G$ and $K \leq G$, then

- $NK \leq G$ (and so $NK = KN$);
- $NK = \langle N, K \rangle$;
- $N \cap K \lhd K$;
- $N \lhd NK$;
- if $K \supseteq N$, then $N \lhd K$.
- if $K \lhd G$, then $NK \lhd G$ and $N \cap K \lhd G$.

(4) $K \lhd H$ and $H \lhd G$ **do not imply** $K \lhd G$.

(5) Every normal subgroup is the kernel of some homomorphisms (there is an obvious one $x \mapsto xN$ after we have discussed quotient groups).

(6) A subgroup is normal in G if and only if it is a union of conjugacy classes.

(7) Some classical examples:

- $Z(G) \lhd G$;
- $C_G(S) \lhd N_G(S)$; in particular, if $N \lhd G$, then $C_G(N) \lhd G$;
- the **commutator subgroup** $[G, G] \lhd G$.
- The kernel of any homomorphism $G \to H$ is normal in G.

Quotient groups

(1) Let G/H ($H \lhd G$) be the set of all cosets of H in G. Define a binary operation on G/H by

$$aHbH = abH.$$

This forms a group and we call G/H the **quotient group** of G by H (or modulo H). When one writes down G/H without stating that H is normal, we will assume H is normal (otherwise it does not make sense; the binary operation is not well-defined for nonnormal subgroup).

(2) The map $x \mapsto xH$ of G into G/H is called the **canonical projection**. Sometimes it is denoted by $\overline{G}$.

(3) Some usual properties:

- $(xH)^{-1} = x^{-1}H$;
- $|G/H| = [G : H] = |G|/|H|$.

(4) **Correspondence Theorem.** There is a one-to-one-correspondence (a bijective function) between the set of subgroups of G/H and the set of subgroups of G which contain H.

- More precisely, For any subgroup $\overline{K}$ of G/H, there is a unique subgroup K of G such that
$$K \supseteq H \quad \text{and} \quad K/H = \overline{K}.$$
In fact, the construction is given by $K = \{x \in G \,|\, xH \in \overline{K}\}$.
- This one-to-one correspondence also gives the following properties (assume S and T are subgroups):
  (i) $\overline{S} \subseteq \overline{T} \Leftrightarrow H \subseteq S \subseteq T$; so we have $[\overline{T}, \overline{S}] = [T : S]$;
  (ii) $\overline{S} \lhd \overline{T} \Leftrightarrow S \lhd T$;
  (iii) $\overline{S}$ and $\overline{T}$ are conjugate in $G/H \Leftrightarrow S$ and T are conjugate in G.

Group homomorphisms

(1) A function $f : G \to H$ is called a **group homomorphism** if

$$f(xy) = f(x)f(y) \quad \text{for all } x, y \in G.$$

(2) An injective (resp. surjective) homomorphism is called a **monomorphism** (resp. **epimorphism**). A bijective function is called an **isomorphism**. Technically, we should not use "called" if we have already defined monomorphisms and epimorphisms in category. We can verify that the homomorphisms in group can satisfy the conditions in the sense of category if they are injective or surjective. This is also a reason why we write $f \in \hom(G, H)$ for a group homomorphism f.

(3) Usual properties:

- $f(e) = e$;
- $f(x^{-1}) = f(x)^{-1}$;

- If two subsets S and T are conjugate in G, then $f(S)$ and $f(T)$ are conjugate in H;
- $H \lhd G \Rightarrow f(H) \lhd f(G)$.

Note that $f(e) = e$ can be deduced from the fact that f is homomorphism: take $f(e)f(e) = f(e)$ and multiply by $f(e)^{-1}$. In the case of monoids, we cannot do that since not every element has an inverse. So the definition of homomorphisms between monoids are as follows: A function $g : M \to N$ is called a **monoid homomorphism** if

$$g(xy) = g(x)g(y) \quad \text{for all } x, y \in M \quad \text{and} \quad g(1) = 1.$$

(4) The common subgroups defined from a homomorphism $f : G \to H$ would be the **kernel** of f and the **image** of f.

- The kernel of f is a subgroup of G:

$$\ker f = \{x \in G \mid f(x) = e\}.$$

- The image of f is a subgroup of H:

$$\operatorname{im} f = \{f(x) \mid x \in G\}.$$

In fact, the kernel is a special case of the **preimage** of a fixed subgroup of H under f. Let $U \leq H$. It can be checked that

$$f^{-1}(U) = \{x \in G \mid f(x) \in U\}$$

is a subgroup of G.

(5) Common homomorphisms defined from f (the old one):

- The **restriction** of f to U (U is a subgroup of the domain G);
- composite mapping.

(6) Common homomorphisms defined from subgroups and quotient groups:

- The **inclusion map** of H into G (where H is a subgroup of G), usually denoted by $H \hookrightarrow G$.
- The **canonical projection** of G onto the quotient group G/N, usually denoted by $G \twoheadrightarrow G/N$.

- The **retraction** from G to H (where H is a subgroup of G). This is a homomorphism $f : G \to H$ such that $f(h) = h$ for all $h \in H$.

(7) The isomorphism theorems:

(i) **First Isomorphism Theorem.** For any $f : G \to H$,

$$\begin{aligned} G/\ker f &\xrightarrow{\sim} \operatorname{im} f, \\ x \ker f &\mapsto f(x). \end{aligned}$$

(ii) **Second Isomorphism Theorem.** If $H \leq G$ and $N \lhd G$, then

$$H \hookrightarrow HN \twoheadrightarrow HN/N$$

induces an isomorphism

$$\frac{H}{H \cap N} \cong \frac{HN}{N}.$$

(iii) **Third Isomorphism Theorem.** If $N \lhd G$ and $N \subseteq H \leq G$ (same as saying $\overline{H} \in G/N$), then

$$G \twoheadrightarrow G/N \twoheadrightarrow (G/H)/\overline{H}$$

induces an isomorphism

$$\frac{G}{H} \cong \frac{G/N}{H/N}.$$

(8) **Generalized version of Correspondence Theorem.** Let $f : G \to G'$ be a homomorphism. Then there is a one-to-one correspondence between the set of subgroups of G' and the set of subgroups of G which contain $\ker f$.

- More precisely, the function is given by

$$H' \mapsto f^{-1}(H') = \{x \in G \,|\, f(x) \in H'\}.$$

The inverse function is given by

$$H \mapsto f(H).$$

- This one-to-one correspondence also gives the following properties (assume S and T are subgroups):

(i) $f(S) \subseteq f(T) \Leftrightarrow \ker f \subseteq S \subseteq T$; so we have $[f(T) : f(S)] = [T : S]$;

(ii) $f(S) \lhd f(T) \Leftrightarrow S \lhd T$;

(iii) $f(S)$ and $f(T)$ are conjugate in $G' \Leftrightarrow S$ and T are conjugate in G.

(iv) Let $N' \lhd G'$. Then

$$\frac{G}{f^{-1}(N')} \cong \frac{G'}{N'}.$$

It provides another approach to show isomorphism theorems.

Cyclic groups

(1) Cyclic groups can be finite or infinite.

(2) In finite case, say x has order k. Then $\langle x \rangle$ consists of k elements. Note that

$$x^m = x^n \Leftrightarrow m \equiv n \mod k.$$

(3) In infinite case, say x is such that $x^m \neq x^n$ whenever $m \neq n$. Then $\langle x \rangle$ has infinitely many elements, which are of the form x^n ($n \in \mathbb{Z}$).

(4) With both cases above, one can see that the map $\mathbb{Z} \to \langle x \rangle$ given by $n \mapsto x^n$ is a **surjective** homomorphism. If x has **infinite order**, then

$$\langle x \rangle \cong \mathbb{Z}.$$

If x is has **finite order** k, then we see that the **kernel** of this map is $k\mathbb{Z}$ and we have (by the First Isomorphism Theorem)

$$\langle x \rangle \cong \mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}_k.$$

(5) The subgroups and quotient groups of a cyclic group is cyclic.

(6) There are **only two generators** for an **infinite cyclic** group $\langle x \rangle$, namely x and x^{-1}.

(7) For finite cyclic group $\langle x \rangle$ (of order k), there are $\varphi(k)$ generators. More precisely, we have the following results:

- $x^n = \frac{k}{\gcd(n,k)}$;
- the result above leads to $\langle x \rangle = \langle x^n \rangle \Leftrightarrow \gcd(n,k) = 1$, that is why the generators can be counted via **Euler's Totient function**.

(8) A cyclic group of order k has a **unique subgroup** of order d for **each divisor** d of k.

(9) Using (8), we have a stronger version of (7): For each divisor d of k, we have $\varphi(d)$ elements of order d. This immediately leads to a result on Number Theory:

$$\sum_{d|k} \varphi(d) = k.$$

Group automorphisms

(1) An isomorphism $G \to G$ is called an **automorphism** of G.

(2) An automorphism $\sigma : G \to G$ preserves a lot of properties in group:

- $\sigma(H) = H$ for all $H \leq G$;
- $[\sigma(H), \sigma(K)] = [H : K]$ for all $K \leq H \leq G$;
- $K \lhd H \Leftrightarrow \sigma(K) \lhd \sigma(H)$;
- $H/K \cong \sigma(H)/\sigma(K)$ for all $K \lhd H$;
- $\langle \sigma(S) \rangle = \sigma(\langle S \rangle)$;
- $N_G(\sigma(H)) = \sigma(N_G(H))$;
- $C_G(\sigma(H)) = \sigma(C_G(H))$.

(3) The set of automorphisms of G forms a **group under composition**. It is denoted by $\operatorname{Aut} G$.

(4) We are interested in a special kind of automophisms: The automorphism of G defined by $x \mapsto gxg^{-1}$ ($g \in G$ is fixed) is called an **inner automorphism** by g. This is also called the **conjugation** by g.

- The set of all inner automorphisms of G is a subgroup of $\operatorname{Aut} G$, and is denoted by $\operatorname{Inn} G$.
- $\operatorname{Inn} G \cong G/Z(G)$.
- In fact $\operatorname{Inn} G \lhd \operatorname{Aut} G$. The quotient group $\operatorname{Aut} G/\operatorname{Inn} G$ is called the group of **outer automorphisms** of G.

(5) **Characteristic subgroup.** This is a subgroup of G for which every automorphism of G maps H onto itself, i.e., $\sigma(H) = H$ for all $\sigma \in \operatorname{Aut} G$. Sometimes we write $H \operatorname{char} G$.

- $H \operatorname{char} G \Rightarrow H \lhd G$ (look at the inner automorphisms). The converse is not true.

- $H \operatorname{char} G \Leftrightarrow \sigma(H) \subseteq H$ for all $\sigma \in H$(an analogous result to normal subgroups).
- $H \operatorname{char} G \Rightarrow C_G(H) \operatorname{char} G$.
- If H is the unique subgroup of its order, then $H \operatorname{char} G$.
- $H \operatorname{char} K$ and $K \operatorname{char} G \Rightarrow H \operatorname{char} G$.
- $H \operatorname{char} K$ and $K \lhd G \Rightarrow H \lhd G$.
- Common examples: Trivial subgroups and $Z(G)$.

(6) Studies of automorphisms of cyclic groups (say C):

- $\operatorname{Aut} C$ is abelian.
- If σ is an automorphism of C, then σ must **send generators to generators**.
- As a consequence, we get (by counting the number of generators)

$$|\operatorname{Aut}\ \mathbb{Z}| = 2 \quad \text{and} \quad |\operatorname{Aut}\ \mathbb{Z}_k| = \varphi(k).$$

  We also have

$$\operatorname{Aut} \mathbb{Z}_k \cong (\mathbb{Z}_k)^\times.$$

- In particular, if k is a power of a prime, say p^m, then

$$|\operatorname{Aut}\ \mathbb{Z}_{p^m}| = p^{m-1}(p-1).$$

- Every subgroup of C is a characteristic of C.

Commutator subgroup

(1) The subgroup of G generated by all of the elements of the form $xyx^{-1}y^{-1}$ (called the **commutator** of x and y) is called the **commutator** subgroup (or the **derived group**) of G. We denote it by $[G, G]$ (or $D(G)$, $G^{(1)}$).

(2) Usual properties:

- $[x, y] = 1 \Leftrightarrow x$ and y commutes;
- A homomorphism f sends commutators to commutators of the images ,i.e., $f([x, y]) = [f(x), f(y)]$;
- $[G, G] \operatorname{char} G$ (and so $[G, G] \lhd G$).

(3) The quotient group $G/[G, G]$ is abelian. Moreover, $[G, G]$ is the **smallest normal subgroup** having the property that the **quotient group is abelian**, i.e., for all $H \lhd G$, if G/H is abelian, then $H \supseteq [G, G]$.

Rings

(1) A set R with two binary operations, **addition** $+$ and **multiplication** $\cdot$ is called a **ring** if

   (i) $(R, +)$ is an abelian group.

   (ii) $(R, \cdot)$ is a semigroup.

   (iii) (Distributive laws) Left (or right) multiplication distributes over addition, i.e., $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$ for all $a, b, c \in R$.

   Remark that the properties given above is defined for convenience. The commutativity in $(R, +)$ is redundant because it can be deduced from other axioms.

(2) Optional properties:

   (a) If the multiplication in R is commutative, then R is called a **commutative ring**.

   (b) If R has a multiplicative identity 1, then R is called a **ring with identity** (or **unital ring**).

   (c) If each nonzero element in a unital ring R has a multiplicative inverse, then R is called a **division ring.**

   (d) The properties (a), (b), (c) hold and $0 \neq 1 \Rightarrow R$ is a **field**.

(3) $1 = 0 \Leftrightarrow R$ is the **zero ring** $\{0\}$. Due to this result, we often impose that $1 \neq 0$ (meaning that R is not the zero ring).

(4) Usual properties: for all $a, b \in R$,

   - $0a = a0 = 0$;
   - $(-a)b = a(-b) = -(ab)$;
   - $(-a)(-b) = ab$;
   - if R has 1, then 1 is unique, $(-1)^2 = 1$ and $-a = (-1)a$.

Subrings

(1) A **subring** of R is a nonempty set that is

   (i) an additive subgroup of R

   (ii) and closed under multiplication.

(2) A subring of R need not have a multiplicative identity. E.g. $2\mathbb{Z}$ is a subring of $\mathbb{Z}$ but does not contain 1.

(3) The intersection of a nonempty collection of subrings is also a subring.

Integral domains

(1) A nonzero element x is called a **left zero divisor** (resp. **right zero divisor**) if $xa = 0$ (resp. $ax = 0$) for some $a \in R$. We call x a **zero divisor** if it is either left **or** right zero divisor.

(2) An element x of nonzero R is said to be **left invertible** (resp. **right invertible**) if $ax = 1$ (resp. $xa = 1$) for some $a \in R$. In this case, a is called a **left inverse** (resp. **right inverse**) of x.

(3) Left-invertibility **does not imply** right-invertibility.

(4) If x has left inverse y and right inverse y', then $y = y'$ and so we shall say that x is **invertible** (or a **unit**) in R and y is called the inverse of x.

(5) The set of all units in R forms a multiplicative group.

(6) x is a **zero divisor** $\Rightarrow$ x is **not a unit**. Thus fields contain no zero divisor.

(7) x is not a zero divisor $\Rightarrow$ x is **left and right cancellable**, i.e., $xa = xb \Rightarrow x = 0$ or $b = c$, and $ax = bx \Rightarrow x = 0$ or $b = c$.

(8) An **integral domain** R is

  (i) a commutative nonzero ring with 1

  (ii) which has **no zero divisors**.

(9) If the commutative property is dropped, we will call R a **domain**.

(10) Cancellation law holds for integral domains.

(11) R is an integral domain and R is finite $\Rightarrow$ R is a field.

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 $a_1, \dots, a_r$, $(r \leq n)$ 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

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

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

Definition 1.3. The permutations $\sigma_1, \dots, \sigma_r \in S_n$ 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 $\{a_1, a_2, \dots, a_r\} \cap \{b_1, b_2,$
$\dots, b_s\} = \emptyset$.

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*

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

Proof. Write $[n] = \{\sigma(a_1), \ldots, \sigma(a_r), \sigma(b_{r+1}), \ldots, \sigma(b_n)\}$ where $b_{r+1}, \ldots, b_n \notin \{a_1, \ldots, a_r\}$. The following

$$\sigma(a_i) \overset{\sigma^{-1}}{\longmapsto} a_i \overset{\tau}{\longmapsto} a_{i+1} \overset{\sigma}{\longmapsto} \sigma(a_{i+1}),$$
$$\sigma(b_i) \overset{\sigma^{-1}}{\longmapsto} b_i \overset{\tau}{\longmapsto} b_i \overset{\sigma}{\longmapsto} \sigma(b_i)$$

prove the assertion. ■

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.*

Proof. Let σ be the nonidentity permutation.

1. The set $[n]$ can be partitioned into the orbits of $\langle\sigma\rangle$ on $[n]$, i.e., $[n] = \bigcup_i \langle\sigma\rangle x_i$ (will be studied in Group Actions).

2. If $\langle\sigma\rangle x_i = \{x_i\}$, then it corresponds to the identity permutation.

3. If $\langle\sigma\rangle x_i \neq \{x_i\}$, then there must be $\sigma^{k+\ell}x_i = \sigma^\ell x_i$ for some positive integer k and some nonnegative integer ℓ, since $\langle\sigma\rangle x_i$ is finite. This implies there is the least positive integer m such that $\sigma^m x_i = x_i$. Therefore $\langle\sigma\rangle x_i = \{x_i, \sigma x_i, \sigma^2 x_i, \ldots, \sigma^{m-1}x_i\}$ and it induces a cycle $\tau_i = (x_i(\sigma x_i)\cdots(\sigma^{m-1}x_i))$.

4. The induced cycles are disjoint since the orbits are disjoint. Also, $\sigma x = \tau_i x$ if $x \in \langle\sigma\rangle x_i$, completing the proof, i.e., $\sigma = \tau_1 \cdots \tau_r$ for some r. Remark that any cycle of length 1 is omitted in the product.

5. To prove the uniqueness, consider $\sigma = \phi_1 \cdots \phi_s$ for some s. Take $x \in [n]$ such that $\sigma(x) \neq x$. Then there is a unique ϕ_j such that $\phi_j(x) = \sigma(x)$. It follows from $\phi_j \sigma = \sigma \phi_j$ that $\phi_j^k(x) = \sigma^k(x)$ and hence the orbit of x under ϕ_j is one of the orbits of σ. By Proposition 1.4.(ii), we get $\phi_j = \tau_i$. So $s = r$ and $\phi_i = \tau_i$ after reindexing. ■

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

Proof. Write $\sigma = \tau_1 \cdots \tau_r$. Then $\sigma^m = \mathrm{Id}$ if and only if $\tau_i^m = \mathrm{Id}$ (by Proposition 1.4.(vi)) if and only if $|\tau_i| | m$ for all i. By definition, $\mathrm{lcm}(|\tau_1|, \ldots, |\tau_r|)$ is the least integer that is divisible by all $|\tau_i|$. ■

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.

Proof. (i) Note that

$$(x_1) = (x_1 x_2)(x_2 x_1),$$
$$(x_1 x_2 x_3 \cdots x_r) = (x_1 x_r)(x_1 x_{r-1}) \cdots (x_1 x_3)(x_1 x_2).$$

Then use Theorem 1.6.

(ii) Note that $(ij) = (1i)(1j)(1i)$. Then use (i).

(iii) Note that $(1j) = (1\ j-1)(j-1\ j)(1\ j-1)$. Then use (ii).

(iv) Let $\tau = (12)$ and $\sigma = (123 \cdots n)$. Then use Proposition 1.5 and (iii).

(v) Let $\tau = (12)$ and $\sigma = (23 \cdots n)$. Then use Proposition 1.5 and (ii).

(vi) Let $\tau = (rs)$ and $\sigma = (123\cdots p)$. Set $d = s - r$. By Proposition 1.5, $\langle \tau, \sigma \rangle$ contains $\{(k\ k+d) \mid k \in \mathbb{Z}_p\}$. Note that $(k+d\ k+2d)(k\ k+d)(k+d\ k+2d) = (k\ k+2d)$ for all $k \in \mathbb{Z}_p$. Inductively, $(k+id\ k+(i+1)d)(k\ k+id)(k+id\ k+(i+1)d) = (k\ k+(i+1)d)$ for all $k \in \mathbb{Z}_p$ and $i \in \mathbb{Z}_p \setminus \{0, p-1\}$. Since $d \in \mathbb{Z}_p^*$, there exists $d^{-1} \in \mathbb{Z}_p^*$ such that $d^{-1}d = 1$. In particular, $\langle \tau, \sigma \rangle$ contains $(k, k+d^{-1}d) = (k, k+1)$ for all $k \in \mathbb{Z}_p$. Hence the assertion is proved by (iii). ■

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.*

Proof. A permutation $\sigma \in S_n$ induces a permutation matrix $P_\sigma \in \mathrm{GL}(n, \mathbb{R})$, i.e. $P_\sigma = (p_{ij})$ where

$$p_{ij} = \begin{cases} 1 & \text{if } \sigma(j) = i, \\ 0 & \text{if } \sigma(j) \neq i. \end{cases}$$

So the map $S_n \to \mathrm{GL}(n, \mathbb{R}); \sigma \mapsto P_\sigma$ is a group homomorphism. The transposition τ is mapped to a matrix formed by swapping two columns of the identity matrix, and thus $\det P_\tau = -1$. Hence σ cannot be both even and odd, since $\det P_\sigma$ can only take one value. ■

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

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

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.*

Proof. Any $\sigma \in A_n$ is a product of terms of the form $(ab)(cd)$. Observe that

$$(ab)(cd) = \begin{cases} 1 & \text{if } \{a,b\} = \{c,d\}, \\ \text{3-cycle} & \text{if } |\{a,b\} \cap \{c,d\}| = 1, \\ (acb)(acd) & \text{if } \{a,b\} \cap \{c,d\} = \emptyset. \end{cases}$$ ■

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.*

Proof. The first assertion is proved by the First Isomorphism Theorem on the homomorphism sgn. To prove the second assertion, suppose that $H \neq A_n$ is a subgroup of index 2. By Lemma 1.13, there exists a 3-cycle $(abc) \notin H$ (otherwise $A_n \subseteq H$ and thus $A_n = H$ because $|A_n| = |H|$). However H, $(abc)H$ and $(abc)^{-1}H$ are distinct cosets, a contradiction. ■

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 $k \neq r, s$.*

Proof. Let a, b, c be distinct elements and $a, b, c \neq r, s$. The decompositions of any 3-cycles into a product of the $n-2$ cycles mentioned above are presented without any motivation:

$$\begin{aligned} (rsa) &\text{ is trivial,} \\ (ras) &= (rsa)^2, \\ (rab) &= (rsb)(rsa)^2, \\ (sab) &= (rsb)^2(rsa), \\ (abc) &= (rsa)^2(rsc)(rsb)^2(rsa). \end{aligned}$$

Hence the result follows from Lemma 1.13. ■

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

Proof. Without loss of generality, assume that $(123) \in N$. Then $(213) = (123)^2 \in N$. Since N is normal in A_n, N contains all the conjugates $\sigma(213)\sigma^{-1}$ $(\sigma \in A_n)$. In particular, if we choose $\sigma = (12)(3k)$, where $k \geq 4$, then $\sigma(213)\sigma^{-1} = (12k)$. The result follows by Lemma 1.15. ■

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

Proof.

1. A_2 only contains the identity permutation.

2. The order of A_3 is 3 (which is a prime) and hence a cyclic group.

3. $\{(1), (12)(34), (13)(24), (14)(23)\} \lhd A_4$ provides a counterexample.

4. For $n \geq 5$, let N be a nontrivial normal subgroup of A_n. For any $\sigma \in S_n$, we say that $i \in [n]$ is a **fixed point** of σ if $\sigma(i) = i$. The number of fixed points of σ is denoted by $[n]_\sigma$.

   (a) Take a permutation $\sigma \in N$ so that $[n]_\sigma$ is the largest among the permutations in N. Two cases to consider: σ is a product of disjoint transpositions; and σ is a cycle of length at least 3.

   (b) For the first case, we can find two disjoint transpositions (ab) and (cd). Then we take $x \neq a, b, c, d$ and define

   $$\begin{aligned} \tau &= (cdx) \in A_n, \\ \sigma' &= [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1} \in N. \end{aligned}$$

   It can be checked that we see that $\sigma'(c) = x$ (and thus nontrivial) and σ' fixes a, b and $[n]_\sigma \setminus \{x\}$. This means that $[n]_{\sigma'} > [n]_\sigma$, a contradiction.

   (c) For the second case, if it is of length 3, then we are done. If it is of length 4, then we arrive at a contradiction because it is an odd permutation. If it is of length at least 5, i.e., $\sigma = (abcdx\cdots)$, then using the same construction in (b) one can see that $\sigma'(c) = d$ and σ' fixes b and $[n]_\sigma$. So $[n]_{\sigma'} > [n]_\sigma$, again a contradiction.

5. Therefore σ is a cycle of length 3. Hence Lemma 1.16 gives the result. ■

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 $|D_n| = 2n$.*

Proof. Let σ be a symmetry of $P_n = \{1, 2, \ldots, n\} \subseteq \mathbb{Z}_n$, labelled in clockwise direction and assume that $n = v$. We observe the following:

(i) $r^\ell(k) = k + \ell$ for all $k, \ell \in \mathbb{Z}_n$;

(ii) $s(k) = -k$ for all $k \in \mathbb{Z}_n$.

Suppose that σ maps 1 to some i. The possible values of $\sigma(2)$ are $i - 1$ and $i + 1$. If $\sigma(2) = i + 1$, then $\sigma(k) = k + i - 1$ for all $k \in \mathbb{Z}_n$ and thus σ is equal to r^{i-1}. If $\sigma(2) = i - 1$, then $\sigma(k) = i + 1 - k$ for all $k \in \mathbb{Z}_n$. This implies $\sigma(k) = r^{i+1}(-k) = r^{i+1}s(k)$ for all $k \in \mathbb{Z}_n$ and thus $\sigma = r^{i+1}s$. Since $s^2 = e$, the first assertion is proved. For the second assertion, it suffices to verify that

(i) $|r| = n$ and $|s| = 2$;

(ii) $r^i s = sr^{-i}$ for all $0 \leq i \leq n$;

(iii) $s \neq r_i$ for all i.

This leads to $D_n = \{1, r, r^2 \cdots, r^{n-1}, s, sr, sr^2 \cdots, sr^{n-1}\}$ where the elements in the set are distinct. ■

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 $0 \le i \le d-1$.

Proof. Clearly D_n contains a cyclic group C of order n consisting of rotations. Let H be any subgroup of D_n. If $H \le C$, then H is cyclic. If not, then note that $H \cap C$ is a proper subgroup of C. Let $C = \langle r\rangle$. Then $H \cap C = \langle r^d\rangle$ for some positive divisor d of n. Take $r^i s \in H$. Then we can verify that $H = \langle r^d, r^i s\rangle$. Since $|H| = 2|r^d|$, $|r^d| = n/d$, $|r^i s| = 2$ and $r^{d+i}s = sr^{-i-d} = r^i s r^{-d}$, we have $H \cong D_{n/d}$. ∎

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 $\langle r^2, rs\rangle$.*

Proof. If H is a cyclic subgroup of G that is normal in G, then the subgroups of H is also normal in G (see Hungerford Exercises I.5.11). So the subgroups in Theorem 2.4.(i) are normal in D_n.

Note that for all $k \in \mathbb{Z}$, we have $r(r^k s)r^{-1} = r^{k+2}s$. So $r^k s$ and $r^{k+2}s$ must belong to the same conjugacy class (will be studied in Group Actions). Let N be a normal

subgroup in D_n containing at least a reflection (those without reflections have been classified in the first paragraph). Now we argue in two cases.

Case I. If n is odd, then the conjugacy classes containing a reflection is $[s] = \{r^k s \mid k \in \mathbb{Z}\}$. So N must contain this entire set. So $|N| > n$ since there are n reflections and an identity element. Hence we have $N = D_n$ by Lagrange's Theorem.

Case II. If n is even, we have two conjugacy classes containing reflections, i.e., $[s] = \{r^k s \mid k \in \mathbb{Z} \text{ is even}\}$ and $[rs] = \{r^k s \mid k \in \mathbb{Z} \text{ is odd}\}$. If N contains $[s]$ and $[rs]$, then $N = D_n$. If N contains exactly one of them, then $|N| > n/2$. So $[D_n : N] < 4$. Also, the element $r^i s \notin N$ implies that $r^i s N$ has order two in the quotient group D_n/N. Thus $|D_n/N| = [D_n : N]$ must be even and we get $|D_n/N| = 2$. In particular, $r^2 \in N$ since $N = rNrN = r^2 N$. If $r \in N$, then $N = D_n$. If $r \notin N$, then

$$N = \begin{cases} \langle r^2, s \rangle & \text{if } N \text{ contains } [s], \\ \langle r^2, rs \rangle & \text{if } N \text{ contains } [rs]. \end{cases}$$

■

2.4 Quaternion Group

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

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

Proof. Let $Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, ij = ji^{-1} \rangle$. The relation $ij = ji^{-1}$ forces every elements in Q_8 can be written as the form $i^s j^t$ $(s, t \in \mathbb{Z})$. From $i^4 = 1$ and $i^2 = j^2$, one can restrict s, t to $s \in \{0, 1, 2, 3\}$ and $t \in \{0, 1\}$. Observe that $\langle i \rangle \cap \langle j \rangle = \langle i^2 \rangle$. If $i^{s_1} j^{t_1} = i^{s_2} j^{t_2}$, then $j^{t_1 - t_2} \in \langle i^2 \rangle$ and so $t_1 = t_2$. Hence $s_1 = s_2$. This shows that $i^s j^t$ $(s \in \{0, 1, 2, 3\}, t \in \{0, 1\})$ are distinct elements in Q_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.*

Proof. Let $Q_8 = \langle i, j \mid i^4 = 1, i^2 = j^2, ij = ji^{-1} \rangle$. Direct verification shows that $\langle i \rangle$, $\langle j \rangle$ and $\langle ij \rangle$ are the only subgroups of order 4, and hence they are normal. Also, the only subgroup of order 2 is $\langle i^2 \rangle = \langle j^2 \rangle = \langle (ij)^2 \rangle$. We can check that $\langle i^2 \rangle$ is 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 $G \cong Q_8$.*

Proof. There are no elements of order 8, and there is an element g of order 4 (otherwise $x^2 = 1$ for all $x \in G$ implies G is abelian). So $N = \langle g \rangle$ is a subgroup of index 2, and hence a normal subgroup in G.

Take a nonidentity element $h \notin N$. Then $h^2 \in N$, otherwise, $h^2 \notin N$ implies $h^2 \in hN$ and so $h \in N$. Also, $h^{-1}gh = g^{-1}$ since N is normal and G is not abelian.

If $|h| = 2$, then $h^2 = 1$ and hence $G \cong D_4$.

If $|h| = 4$, then $h^2 = g^2$ (g^2 is the only element of order 2 in N) and hence $G \cong Q_8$. ■

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 $x \in X$.

Remark. To emphasize the set X, we can talk about an action without explicitly mentioning ρ. In this case, (i) and (ii) can be rewritten as

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

(ii) $ex = x$ for all $x \in X$.

Sometimes, we say that

- G **acts** on X;
- X is a G-**set**;
- The action is a G-**action** on X.

Note that the action of G is implicitly given so as to make X a G-set. Also, the action is also called a **left action**. A right action $X \times G \to X$ is defined analogously. Based on (i) and (ii), we can define **semigroup action** and **monoid action** accordingly, but these are not our main focus.

Proposition 3.2. *Let G be a group and let X be a set.*

(i) A group action $G \times X \to X$ induces a group homomorphism $G \to \mathrm{Sym}(X)$.

(ii) A group homomorphism $G \to \mathrm{Sym}(X)$ induces a group action $G \times X \to X$.

Proof. (i) For each $g \in G$, the map $\pi_g : X \to X$; $x \mapsto gx$ is bijective (a permutation of X). So $g \mapsto \pi_g$ is a homomorphism of G into $\mathrm{Sym}(X)$.

(ii) Let $g \mapsto \pi_g$ be such group homomorphism. Then the mapping $G \times X \to X$; $(g, x) \mapsto \pi_g(x)$ is a group action. ■

Based on Proposition 3.2, (ii) is another way to define a group action. One can use both definitions interchangeably. For example, we can view gx $(g \in G, x \in X)$ as an element $\rho(g)(x)$ when we emphasize the homomorphism $\rho : G \to \mathrm{Sym}(X)$. In fact, we have the following definition.

Definition 3.3. Let G be a group and let X be a set. A **permutation representation** of G is a group homomorphism $\rho : G \to \mathrm{Sym}(X)$ where X is a nonempty set.

Remark. Left action and **right action** are not the same. In right action $X \to G \to X$, we need

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

(ii) $xe = x$ for all $x \in X$.

When we have a left action (denoted $\cdot$), the action is not a right action because it does not satisfy (i) in the sense of right action. However, we can induce a right action by defining $xg = g^{-1} \cdot x$.

3.2 Orbit-Stabilizer Theorem

Definition 3.4. Let G act on X. A subset

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

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

Proof. Routine. ■

Definition 3.6. Let $x \in X$. The set $S_G(x) = \{g \in G \,|\, gx = x\}$ is called the **stabilizer** of x. An element $g \in G$ is said to **stabilize** or **fix** x if $g \in Gx$.

Proposition 3.7. *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

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

Proof. Routine. ■

Lemma 3.8. *Let G act on X. Then*

(i) the set of orbits partitions X, i.e., $X = \bigcup_x O_G(x)$ 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.

Proof. (i) By Proposition 3.5.

(ii) Routine. ■

Theorem 3.9 (Orbit-Stabilizer Theorem)**.** *Let G act on a **finite** set X. Then for all $x \in X$,*

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

Proof. By Lemma 3.8.(ii). ■

Corollary 3.10 (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*

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

Proof. By Lemma 3.8.(i) and Theorem 3.9. ■

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

Definition 3.11. 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 3.12 (Burnside's Lemma)**.** *Let G act on X. If both G and X are finite, then the total number of orbits is given by*

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

Proof. We use double counting argument on the set

$$\mathcal{S} = \{(x, g) \mid x \in X, g \in G, gx = x\}.$$

Fix $x \in X$, we see that there are $|S_G(x)|$ elements in G that fixes x, and so $|\mathcal{S}| = \sum_{x\in X} |S_G(x)|$. On the other hand, fix $g \in G$, we see that there are $\chi(g)$ elements in X fixed by g, and so $|\mathcal{S}| = \sum_{g\in G} \chi(g)$.

By Theorem 3.9,

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{|G|}\sum_{x\in X}|S_G(x)| = \sum_{x\in X}\frac{1}{|O_G(x)|}.$$

To calculate $\sum_{x\in X}\frac{1}{|O_G(x)|}$, choose representatives $x_1, \ldots, x_m$ of orbits so that

$$\sum_{x\in X}\frac{1}{|O_G(x)|} = \sum_{i=1}^{m}\sum_{y\in O_G(x_i)}\frac{1}{|O_G(x_i)|}.$$

Fix i. The number of elements in $O_G(x_i)$ is $|O_G(x_i)|$. Each element $y \in O_G(x_i)$ contributes $\frac{1}{|O_G(x_i)|}$ to the sum $\sum_{y\in O_G(x_i)}\frac{1}{|O_G(x_i)|}$. Hence $\sum_{y\in O_G(x_i)}\frac{1}{|O_G(x_i)|} = 1$ and thus $\sum_{x\in X}\frac{1}{|O_G(x)|} = m$. Note that m is the total number of orbits. ■

3.3 Kernel of Group Actions

Definition 3.13. Let G act on X and let $\rho : G \to \mathrm{Sym}(X)$ be the associated homomorphism (discussed in Proposition 3.2). We say that the action is **faithful** if $\operatorname{Ker}\rho = \{e\}$.

Proposition 3.14. *Let G act on X. Then the kernel of the action is the intersection of all the stabilizers $\bigcap_{x\in X} S_G(x)$.*

Proof. Note that

$$g \in \operatorname{Ker}\rho \iff \rho(g) = \mathrm{Id} \iff gx = x \text{ for all } x \in X \iff g \in S_G(x) \text{ for all } x \in X.$$

■

3.4 Transitive Actions

Definition 3.15. 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 3.16. *Let G act transitively on X. Then the kernel of the action is*

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

for some $x \in X$.

Proof. Choose a representative $x \in X$ so we can write $X = \{gx \mid g \in G\}$. Then for each $gx \in X$, we have $S_G(gx) = gS_G(x)g^{-1}$ by Proposition 3.7.(ii). Hence the result follows from Proposition 3.14. ■

Proposition 3.17. *Let G act transitively on X. If G is finite and $|X| > 1$, then there exists $g \in G$ fixing no points of X.*

Proof. We use Theorem 3.12. Since $\chi(e) = |X| > 1$, it follows that there exists $g \in G$ such that $\chi(g) = 0$, otherwise the sum $\sum_{h \in G} \chi(h)$ will exceed $|G|$. ■

3.5 Conjugations

Definition 3.18. 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 3.19. We say that a group G act on a set X by **conjugation** if the action of G is given by $(g, x) \mapsto gxg^{-1}$.

Remark. We require that gxg^{-1} makes sense for all $x \in X$. So the set X cannot be arbitrary chosen. The next definition presents some typical sets involved.

Definition 3.20. 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 3.21. *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.*

Proof. Trivial. ■

Definition 3.22. 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 3.10, is called the **class equation** of G.

Proposition 3.23. *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 $[G : C_G(x_i)] > 1$.

Proof. Note that

$$[G : C_G(x)] = 1 \overset{\text{Theorem 3.9}}{\iff} O_G(x) = \{x\} \iff x \in Z(G). \qquad \blacksquare$$

Corollary 3.24. *Let H be a subgroup of a finite group G. If $\bigcup_{g \in G} gHg^{-1} = G$, then $H = G$.*

Proof. Consider the action of G on the set of subsets of G by conjugation. Then there are $|O_G(H)| = [G : N_G(H)]$ distinct conjugates of H. Since $|gHg^{-1}| = |H|$ for all $g \in G$, we have the bound

$$|G| - 1 \leq [G : N_G(H)](|H| - 1)$$

which can be obtained by counting the nonidentity elements in G. Note that H is a subgroup of $N_G(H)$ and so $[G : N_G(H)] \leq [G : H]$. Hence we get $|G| - 1 \leq |G| - [G : H]$ and thus $[G : H] \leq 1$. $\blacksquare$

Theorem 3.25 (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 3.26. *Given a positive integer k and a number M, there exist at most finitely many solutions in positive integers x_i for the equation*

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

Proof. When $M < 0$, there is no solutions (still considered at most finitely many solutions).

Assume that $M > 0$. We rearrange x_i's so that x_k is the smallest among $x_1, \ldots, x_k$. Then $\frac{k}{x_k} \geq M$. This restricts the choices of x_k because $1 \leq x_k \leq k/M$. If $k = 1$, then we are done. If $k > 1$, we write $\frac{1}{x_1} + \cdots + \frac{1}{x_{k-1}} = M - \frac{1}{x_k}$ and apply induction on k. $\blacksquare$

Proof of Theorem 3.25. Suppose G has k conjugacy classes. Multiply the class equation of G of $1/|G|$. By the lemma above, there are finitely many solutions (we treat $|C_G(x_i)|$ as positive integers in the lemma). So there exists a bound $B(k)$ such that $|C_G(x_i)| \leq B(k)$ for all $i = 1, \ldots, k$. In particular, one element x_j of the x_i's is the identity element and so $|G| = |C_G(x_j)| \leq B(k)$. ■

3.6 Translations

Definition 3.27. 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 3.28. *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) $\mathrm{Ker}\,\rho = \bigcap_{g \in G} gHg^{-1}$;

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

Proof. (i) Let $aH, bH \in X$. Then we see that $aH = (ab^{-1})bH$. Hence aH and bH lie in the same orbit.

(ii) $S_G(H) = \{g \in G \,|\, gH = H\} = \{g \in G \,|\, g \in H\} = H$.

(iii) By (i), (ii) and Proposition 3.16.

(iv) Let N be a normal subgroup of G such that $N \leq H$. Then $N = gNg^{-1} \leq gHg^{-1}$ for all $g \in G$. So $N \leq \bigcap_{g \in G} gHg^{-1} = \mathrm{Ker}\,\rho$. ■

In the situation of Theorem 3.28, 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 3.29. *The action of a group on itself by left translation is faithful.*

Proof. By Proposition 3.28.(iii). ■

Theorem 3.30 (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.*

Proof. Let G act on itself by left translation and let $\rho : G \to \mathrm{Sym}(G)$ be the associated homomorphism. By Corollary 3.29, we see that ρ is a monomorphism. Hence $G \cong \mathrm{Im}\,\rho \leq \mathrm{Sym}(G)$. To prove the second assertion, note that $\mathrm{Sym}(G) \cong S_n$. ■

Definition 3.31. 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 3.32. *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 $n!$.*

Proof. Consider the action of G on the set of left cosets of H in G by left translation and use Theorem 3.30. ■

Corollary 3.33. *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.*

Proof. Let H be a subgroup of index p. By Corollary 3.32, we take a normal subgroup N of H such that $[G : N]$ divides $p!$ and consider $[G : N] = [G : H][H : N]$. ■

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.*

Proof. Let H be a subgroup of A_4 with $|H| = 6$. Then $[A_4 : H] = 2$. We claim that $a^2 \in H$ for all $a \in A_4$. If $a \in H$, then clearly $a^2 \in H$. If $a \notin H$, then $A_4 = H \cup aH$. If $a^2H = aH$, then $aH = H$, a contradiction. Thus $a^2H = H$ and so $a^2 \in H$.

Note that every 3-cycle (abc) is a square, i.e., $(abc) = (abc)^4 = ((abc)^2)^2$ and thus they are contained in H. But there are more than six 3-cycles, while $|H| = 6$. ■

Remark. In case you want to count the number of r-cycles in S_n, there are $\binom{n}{r}(r-1)!$ of them. It is found by choosing r elements from n elements and counting the number of cyclic permutations.

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 $|X| \equiv |X_G| \mod p$.*

Proof. Since $x \in X_G$ if and only if $|O_G(x)| = 1$, it follows from Lemma 3.8.(i) that

$$X = \bigcup_{\substack{x \\ |O_G(x)|=1}} O_G(x) \cup \bigcup_{\substack{x \\ |O_G(x)|>1}} O_G(x) = X_G \cup \bigcup_{\substack{x \\ |O_G(x)|>1}} O_G(x).$$

If $|O_G(x)| > 1$, then p divides $|O_G(x)|$ by Theorem 3.9. This proves the lemma. ■

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.*

Proof. (**McKay's Construction**) Define

$$X = \{(a_1, a_2, \ldots, a_p) \,|\, a_i \in G \text{ and } a_1 a_2 \cdots a_p = e\}.$$

Note that for every $k \in \mathbb{Z}_p$, $(a_{k+1}, a_{k+2}, \ldots, a_p, a_1, \ldots, a_k) \in X$ (use the fact that $ab = e$ implies $ba = e$). It can be verified that the following function

$$\begin{aligned} \mathbb{Z}_p \times X &\to X \\ (k, (a_1, a_2 \cdots, a_p)) &\mapsto (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, \ldots, a_k) \end{aligned}$$

is a well-defined action of $\mathbb{Z}_p$ on X.

Let $X_{\mathbb{Z}_p} = \{(a_1, \ldots, a_p) \in X \,|\, k(a_1, \ldots, a_p) = (a_1, \ldots, a_p) \text{ for all } k \in \mathbb{Z}_p\}$. Then we can check that

$$X_{\mathbb{Z}_p} = \{(a, \ldots, a) \,|\, a^p = e\}.$$

Note that the set $X_{\mathbb{Z}_p}$ is nonempty since $(e, \ldots, e) \in X_{\mathbb{Z}_p}$.

Since $\mathbb{Z}_p$ is a p-group, it follows from Lemma 4.3 that $|X_{\mathbb{Z}_p}| \equiv |X| \mod p$. Now we claim that $|X| \equiv 0 \mod p$. In fact, we have $|X| = |G|^{p-1}$. This is established by observing that a_p is uniquely determined by $(a_1 a_2 \cdots a_{p-1})^{-1}$. The claim follows since p divides $|G|$.

Consequently, since $|X_{\mathbb{Z}_p}| \equiv 0 \mod p$ and $X_{\mathbb{Z}_p}$ is nonempty, there must be at least p elements in $X_{\mathbb{Z}_p}$. In particular, there exists $a \neq e$ such that $a^p = e$. Since p is prime, the order of a is p. ■

Remark. The McKay's trick is famous that it has even appeared in Putnam 2007 A5: Suppose that a finite group has exactly n elements of order p, where p is a prime. Prove that either $n = 0$ or p divides $n + 1$.

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.*

Proof. If G is a p-group, then the result immediately follows by Lagrange's Theorem.

Suppose that every element has order a power of the prime p. Let q be a prime such that $q||G|$. By Theorem 4.4, G contains an element of order q. So $q = p$, since q is a power of the prime p. Hence $|G|$ is a power of 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 $N_G(H) \neq H$.

Proof. Let X be the set of left cosets of H in G. Let H act on X by left translation. By Lemma 4.3, $|X_H| \equiv |X| \mod p$. Since $|X| = [G:H]$ it suffices to show that $|X_H| = [N_G(H):H]$. To see this,

$$xH \in X_H \iff hxH = xH \quad \forall h \in H \iff x^{-1}Hx = H \iff x \in N_G(H).$$

So X_H contains xH where $x \in N_G(H)$. This proves (i).

If $p|[G:H]$, then we have $[N_G(H):H] \equiv 0 \mod p$. Since $[N_G(H):H] \geq 1$, we must have $[N_G(H):H] > 1$ and so $N_G(H) \neq H$. ■

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.

Proof. By Theorem 4.4, G contains an element x of order p, and hence a subgroup of order p (namely $\langle x \rangle$).

We proceed by induction. Assume that H is a subgroup of order p^i $(1 \leq i < k)$. Then $[G:H] = |G|/|H| = p^{k-i}m$. Since $k - i > 1$, we have $p|[G:H]$. From the argument in Proposition 4.6, we know that H is normal in $N_G(H)$ and $|N_G(H)/H| \equiv 0 \mod p$. Then p divides $|N_G(H)/H|$. By Theorem 4.4, $N_G(H)/H$ contains a subgroup of order p. By Correspondence Theorem, this subgroup of order p is of the form K/H where K is a subgroup of $N_G(H)$ containing H. Note that $|K| = |K/H||H| = p \cdot p^i = p^{i+1}$. Hence K is the desired subgroup. For (ii), recall that H is normal in $N_G(H)$ and $H \leq K \leq N_G(H)$. Thus H is normal in K. ■

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.*

Proof. Consider the set X of left cosets of P in G. Let H act on X by left translation. By Lemma 4.3, $|X_H| \equiv |X| \mod p$. Now we claim that $|X_H| \geq 1$. Since $|X| = [G : P]$, it suffices to show that p does not divide $[G : P]$. To see this, note that $|G| = [G : P]|P|$ by Lagrange's Theorem. Let $|G| = p^k m$ where p does not divide m. Then w e have $|P| = p^k$ and so $[G : P] = m$. Consequently, $|X_H| \geq 1$. Let $xP \in X_H$ where $x \in G$. By the definition of X_H, we have $hxP = xP$ for all $h \in H$. Hence $H \leq xPx^{-1}$.

If H is a Sylow p-subgroup, then $|H| = |P| = |xPx^{-1}|$. Since $H \leq xPx^{-1}$, we obtain $H = xPx^{-1}$. ■

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 $k \geq 0$.

Remark. We also see that $\gcd(n_p, p) = 1$, will be useful later.

Proof. Since any two Sylow p-subgroups of G are conjugate by Theorem 4.9, we can choose a Sylow p-subgroup P and consider the action of G on $\mathrm{Syl}_p(G)$ by conjugation to obtain $n_p = |O_G(P)|$. By Theorem 3.9 and Definition 3.20, we have $n_p = [G : N_G(P)]$ and hence n_p divides $|G|$.

Let P act on $\mathrm{Syl}_p(G)$ by conjugation. Let $X = \mathrm{Syl}_p(G)$. By Lemma 4.3, $n_p = |X| \equiv |X_P| \mod p$. We now claim that $X_P = \{P\}$. Let $Q \in X_P$. Note that

$$Q \in X_P \iff xQx^{-1} = Q \quad \forall x \in P \iff P \leq N_G(Q).$$

Since Q is also a subgroup in $N_G(Q)$, we can view P and Q as Sylow p-subgroups in $N_G(Q)$. By Theorem 4.9, there exists $x \in N_G(Q)$ such that $P = xQx^{-1}$. Since Q is normal in $N_G(Q)$, we have $xQx^{-1} = Q$. Hence $P = Q$. This completes the proof. ■

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.*

Proof. This follows from Theorem 4.9. ■

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.*

Proof. By Theorem 4.10, $n_p \equiv 1 \mod p$ and $n_p | m$. So $n_p \in \{\text{divisors of } m\}$. But the only factor d of m which satisfied $d \equiv 1 \mod p$ is $d = 1$, and so $n_p = 1$. Therefore there is only one p-Sylow subgroup, which is therefore normal by Corollary 4.11. Consequently, 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 $n_q = p$.*

Proof. By Theorem 4.10, we have two informations:

(i) n_p divides pq;

(ii) $n_p \equiv 1 \mod p$.

From (i) and $\gcd(n_p, p) = 1$, we have $n_p = 1$ or q. Since $1 < q < p$, it follows from (ii) that $n_p = 1$. So the results follows from Corollary 4.11.

Let P be the only Sylow p-subgroup of G. Note that $G/P \cong \mathbb{Z}_q$ and hence G/P is abelian. This implies that the commutator subgroup $[G, G] \leq P$.

We claim that $n_q > 1$. Suppose on the contrary that $n_q = 1$. Then there is a normal Sylow q-subgroup Q of G. Hence $[G, G] \leq Q$. Therefore, $[G, G] \leq P \cap Q = \{e\}$, which means that G is abelian, a contradiction. Hence $n_q > 1$. Since $n_q = 1$ or p, we have $n_q = p$. By Theorem 4.10, we obtain $p = n_q \equiv 1 \mod q$ ■

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).*

Proof. Let $P \in \mathrm{Syl}_p(G)$ and let $Q \in \mathrm{Syl}_q(G)$.

When $p > q$, we have $n_p | q$ and $n_p \equiv 1 \mod p$. Hence $n_p = 1$ and thus P is normal in G.

Consider now the case $p < q$. If $n_q = 1$, then we are done. If $n_q > 1$, Then $n_q = 1 + kq$ for some $k \geq 1$. Since n_q divides p^2, we have $n_q = p$ or p^2. Since $q > p$, we see that $n_q = 1 + kq > p$. So we must have $n_q = p^2$. We count the elements. Note that for distinct Sylow q-subgroups Q_1 and Q_2, we have $Q_1 \cap Q_2 = 1$. So they do not

share any nonidentity element. Since there are p^2 Sylow q-subgroups, each containing $q-1$ nonidentity elements, we have a total of $p^2(q-1)$ nonidentity elements of order q. So there are p^2 elements which are not of order q. Then P must contain these p^2 elements, since P does not have an element of order q. Hence P is unique and thus normal in G. ■

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.*

Proof. Let G be a group with $|G| = p$ where p is a prime number. Then Lagrange's Theorem shows that G has no subgroups other than $\{e\}$ and G. So G is simple.

Conversely, let G be a simple group. Since G is abelian, every subgroup is normal. Since G is simple, it follows that G has no subgroups other than $\{e\}$ and G. If $G \neq \{e\}$, choose $x \in G$ with $x \neq e$ and consider the subgroup $\langle x \rangle$ of G. We see immediately that $\langle x \rangle = G$. Now we claim that G is finite. If x has infinite order, then all the powers of x are distinct, and so $\langle x^2 \rangle \subset \langle x \rangle$ is a proper nontrivial subgroup of $\langle x \rangle$, a contradiction. Therefore G has finite order. If $|G|$ is not a prime, then $|G| = mn$ with $m, n > 1$ and $\langle x^m \rangle$ is a proper nontrivial subgroup of G, a contradiction. Consequently, $|G|$ is a prime number. ■

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.

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

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.*

Proof. Let H be a proper subgroup of G. If H is a maximal normal subgroup, then we are done. If not, there exists a subgroup H_1 with $H < H_1 < G$. Continuing this process, we can obtain a chain of subgroups $H < H_1 < H_2 < \cdots$. Since G is finite, the chain must terminate at H_k, that is, H_k is maximal. ■

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.*

Proof. Suppose H is a maximal normal subgroup of G. Let $K' = K/H$ be a normal subgroup of G/H. Then $H \lhd K \lhd G$. This implies $K = H$ or $K = G$, equivalently, $K' = H/H = \{H\}$ or $K' = G/H$.

Conversely, suppose that G/H is simple. Let K be such that $H \lhd K \lhd G$. Then $\{H\} \lhd K/H \lhd G/H$. Therefore $K/H = \{H\}$ or $K/H = G/H$, equivalently, $K = H$ or $K = G$. ■

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

Proof. Let G be a finite group. We prove by contradiction. If G is a group having the smallest order that does not have a composition series, then G is not simple by Example 5.5. Since G is finite, we can find a maximal normal subgroup H of G. Since $|H| < |G|$ and G was assumed to be a counterexample with the smallest order, H must have a composition series. Let this series be $H > H_1 > \cdots > H_k > \{e\}$. However, G/H is simple by Proposition 5.13. This implies $G > H > H_1 > \cdots > H_k > \{e\}$ is a composition series of G, a contradiction. ■

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.*

Proof. If it does, then there is a subgroup H such that $G_{i+1} \lhd_{\neq} H \lhd_{\neq} G_i$ for some i. By Correspondence Theorem, H/G_{i+1} is a proper normal subgroup of G_i/G_{i+1}, which contradicts the fact that G_i/G_{i+1} is simple. ■

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.

Remark. Some authors consider only nontrivial factors to be isomorphic, and they simply say that the series are equivalence (Definition 5.20). It is important to note that our definition allows for trivial factors.

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*

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

Proof. We want to show that $U(V \cap L) \subseteq UV \cap L$ and $U(V \cap L) \supseteq UV \cap L$.

Let $x \in U(V \cap L)$. Then $x = uv$ where $u \in U$ and $v \in V \cap L$. Clearly $x \in UV$. Since $U \subset L$, we have $x = uv \in L$. Hence $U(V \cap L) \subseteq UV \cap L$.

Let $x \in UV \cap L$. Then $x \in L$ and $x = uv$ where $u \in U$ and $v \in V$. We show that $v \in L$. To see this, note that $u \in L$ and thus $v = u^{-1}x \in L$. Hence $UV \cap L \subseteq U(V \cap L)$. ■

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,

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

Proof. Since $u \lhd U$, the sets $u(U \cap v)$ and $u(U \cap V)$ are subgroups. Since $v \lhd V$, we have $U \cap v = (U \cap V) \cap v \lhd U \cap V$. Hence $u(U \cap v) \lhd u(U \cap V)$. Similarly, we obtain $(u \cap V)v \lhd (U \cap V)v$.

Set $H = u(U \cap v)$ and $K = U \cap V$. By the Second Isomorphism Theorem, we have $HK/H \cong K/(H \cap K)$. Now we simply HK and $H \cap K$. By Lemma 5.17, we see that

$$\begin{aligned} HK &= u(U \cap v)(U \cap V) \\ &= u((U \cap v)U \cap V) \\ &= u(U \cap V), \\ H \cap K &= u(U \cap v) \cap (U \cap V) \end{aligned}$$

$$
\begin{aligned}
&= (U \cap v)u \cap (U \cap V) \\
&= (U \cap v)(u \cap (U \cap V)) \\
&= (U \cap v)(u \cap V).
\end{aligned}
$$

Hence we obtain

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

A similar isomorphism involving the terms in the right hand side of the formula above can be obtained by exchanging U and V. This completes the proof. ■

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

Proof. Let

$$
\begin{aligned}
S: &\quad H_0 = G \geq H_1 \geq \cdots \geq H_s = \{e\}, \\
T: &\quad K_0 = G \geq K_1 \geq \cdots \geq K_t = \{e\}
\end{aligned}
$$

be two subnormal series. Let $H_{ij} = H_i(H_{i-1} \cap K_j)$ for $i \in \{1, 2 \ldots, s\}$ and $j \in \{0, 1, \ldots, t\}$. We first claim that $\{H_{ij}\}$ is a refinement of S. Let $i \in \{1, \ldots, s\}$ be a fixed integer. Since $H_i \lhd H_{i-1}$ and $K_j \lhd K_{j-1}$, it follows from Lemma 5.18 that $H_i(H_{i-1} \cap K_j) \lhd H_i(H_{i-1} \cap K_{j-1})$ for $j \in \{1, \ldots, t\}$. This implies

$$H_{it} \lhd H_{i,t-1} \lhd \cdots \lhd H_{i1} \lhd H_{i0}.$$

Recall that $K_t = \{e\}$ and $K_0 = G$. So we have $H_{it} = H_i(H_{i-1} \cap K_t) = H_i(H_{i-1} \cap \{e\}) = H_i$ and $H_{i0} = H_i(H_{i-1} \cap K_0) = H_i(H_{i-1} \cap G) = H_i H_{i-1} = H_{i-1}$. This proves the first claim.

Let $K_{ji} = K_j(K_{j-1} \cap H_i)$ for $j \in \{1, 2 \ldots, t\}$ and $k \in \{0, 1, \ldots, s\}$. By using a similar argument, one can immediately see that $\{K_{ji}\}$ is a refinement of T.

There are st factors (not necessarily distinct) in both refinements when we regard $H_{i0} = H_{i-1} = H_{i-1,t}$ (resp. $K_{j0} = K_{j-1} = K_{js}$) as a single term. Also, Lemma 5.18 shows that

$$\frac{H_{i,j-1}}{H_{ij}} \cong \frac{K_{j,i-1}}{K_{ji}}$$

for all $i \in \{1 \ldots, s\}$ and $j \in \{1, \ldots, t\}$. Thus two refinements are isomorphic. ■

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.*

Proof. Let

$$\begin{aligned} S: &\quad H_0 = G > H_1 > \cdots > H_s = \{e\}, \\ T: &\quad K_0 = G > K_1 > \cdots > K_t = \{e\} \end{aligned}$$

be two composition series. By Proposition 5.15, any composition series has no proper refinement. Consequently, there is exactly one nontrivial factor in a refinement between H_{i-1} and H_i (resp. K_{i-1} and K_i), and this factor is isomorphic to H_{i-1}/H_i (resp. K_{i-1}/K_i). Clearly there are exactly s nontrivial factors in S and t nontrivial factors in T. By Theorem 5.19, S and T have isomorphic refinements. In particular, they have the same number of nontrivial factor groups, since the nontrivial factors of the two series can be paired up such that the factors in each pair are isomorphic. This proves the theorem. ■

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.*

Proof. Let S be a composition series and let T be a subnormal series. By Theorem 5.19, S has a refinement S' which is isomorphic to a refinement T' of T. Since T and T' are equivalent, S' becomes a composition series after removing repeated terms. ■

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.*

Proof. In view of Corollary 5.22, the subnormal series $G \geq H \geq \{e\}$ can be refined to a composition series $G > G_1 > \cdots > G_k = H > H_1 > \cdots > H_n = \{e\}$. Omitting terms before H giving a composition series of H. Omitting terms after H and consider the series $G/H > G_1/H > \cdots > G_k/H$. By the Third Isomorphism Theorem, it can be verified that this is a composition series of G/H. ■

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.*

Proof. Since the group $\mathbb{Z}_n$ is finite, it follows from Proposition 5.14 that $\mathbb{Z}_n$ has a composition series. Let $S_1, \ldots, S_t$ be the factor groups. Moreover, since $|\mathbb{Z}_n| = |S_1||S_2| \cdots |S_t|$, together with Proposition 5.4 we see that n is a product of primes. Then Theorem 5.21 gives the uniqueness of the prime orders of the factor groups and their multiplicities. ■

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

Proof. (i) Trivial.
(ii) and (iii) Construct appropriate isomorphisms. ∎

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 $\bigoplus_{i=1}^n H_i$.

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

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

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* $x_1x_2\cdots x_n$ *with* $x_i \in \overline{H}_i$ *for all* i.

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

Proof. Routine. ■

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

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

Proof. Note that $|XY| = |X| \cdot |Y|/|X \cap Y|$. Use induction. ■

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* $h \in H$, $k \in K$.

Proof. Let $h \in H$ and $k \in K$. Note that

$$[h, k] = h(kh^{-1}k^{-1}) = (hkh^{-1})k.$$

Since $H, K \lhd G$, we get $[h, k] \in H \cap K = \{1\}$. So we obtain $[h, k] = 1$ and thus $hk = kh$. ■

Theorem 6.7. *Let* $H_1, H_2, \ldots, H_n$ *be normal subgroups of a group* G *such that* $G = H_1H_2\cdots H_n$. *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* $x_1x_2\cdots x_n$ *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 $G = H_1H_2\cdots H_n$ 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.

Proof. (1) $\Rightarrow$ (2) Fix k and suppose $g \in H_k \cap (H_1 \cdots H_{k-1}H_{k+1} \cdots H_n)$. Since $g \in H_1 \cdots H_{k-1}H_{k+1} \cdots H_n$, we can write $g = x_1x_2 \cdots x_n$ where $x_i \in H_i$ for all i and $x_k = 1$. Since $g \in H_k$, we can also write $g = y_1y_2 \cdots y_n$, with $y_i \in H_i$, $y_k = g$ and $y_i = 1$ for $i \neq k$. The uniqueness of expression implies that $x_i = y_i$ for all i. In particular, $g = y_k = x_k = 1$.

(2) $\Rightarrow$ (3) Since $H_k \cap (H_1 \cdots H_{k-1}) \subseteq H_k \cap (H_1 \cdots H_{k-1}H_{k+1} \cdots H_n)$, the result follows immediately.

(3) $\Rightarrow$ (1) The first assertion follows from Lemma 6.6. Since $G = H_1H_2 \cdots H_n$, every element of G can be written as $x_1x_2 \cdots x_n$ with $x_i \in H_i$ for all i. Suppose that $x_1x_2 \cdots x_n = y_1y_2 \cdots y_n$ where $x_i, y_i \in H_i$ for all i. Hence

$$x_ny_n^{-1} = (x_1x_2 \cdots x_{n-1})^{-1}y_1y_2 \cdots y_{n-1} = (x_1^{-1}y_1)(x_2^{-1}y_2) \cdots (x_{n-1}^{-1}y_{n-1}).$$

Let $w = x_ny_n^{-1}$. Then we see that $w \in H_n \cap H_1H_2 \cdots H_{n-1}$. Since $H_n \cap H_1 \cdots H_{n-1} = \{1\}$, we have $w = 1$ and thus $x_n = y_n$. By repeating this argument, we prove the second assertion.

(1) $\Rightarrow$ (4) Let g be an element of G. We can write the element g uniquely as $g = x_1x_2 \cdots x_n$, where $x_i \in H_i$ for all i. Let the function $\psi : G \to \prod_{i=1}^n H_i$ be defined by

$$\psi(g) = (x_1, x_2, \ldots, x_n).$$

Let $h = y_1 \cdots y_n$ be another element of G where $y_i \in H_i$ for all i. Since H_i and H_j commutes elementwise for $i \neq j$, we get

$$gh = (x_1y_1)(x_2y_2) \cdots (x_ny_n).$$

Thus

$$\psi(gh) = (x_1y_1, x_2y_2, \ldots, x_ny_n) = f(g)f(h)$$

and this proves that ψ is a homomorphism. It is clear that ψ is bijective and $\psi(H_i) = \overline{H}_i$ for all i.

(4) $\Rightarrow$ (3) We can verify that $\overline{H}_k \cap (\overline{H}_1 \cdots \overline{H}_{k-1}) = \{1\}$ and then apply the isomorphism to obtain (3). ∎

Remark. In view of Theorem 6.7.(4), we can omit the terms "internal" and "external" and simply write direct product when the context is clear. However, we need to be careful when dealing with some properties that are not stated in the discussion above. For example, let $G = HK = HL$ be two internal direct products. Then

$$G/H \cong HK/H \cong K/(H \cap K) \cong K$$

by the Second Isomorphism Theorem. Similarly, we obtain $G/H \cong L$. Hence we get $H \cong L$. This result is not true for external direct product. When we view the set of real numbers $\mathbb{R}$ as an additive group, we have

$$\mathbb{R} \oplus \{0\} \cong \mathbb{R} \cong \mathbb{R} \oplus \mathbb{R}.$$

This provides a counterexample. Note that $\mathbb{R} \cong \mathbb{R} \oplus \mathbb{R}$ is a vector space isomorphism. It can be established by looking at the dimension of both vector spaces over $\mathbb{Q}$.

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*

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

Proof. Note that $|H_1 \cap H_2|$ divides both $|H_1|$ and $|H_2|$. So, we have $H_1 \cap H_2 = \{1\}$ because $|H_1 \cap H_2| = \gcd(|H_1|, |H_2|) = 1$. Therefore $|H_1 H_2| = |H_1| \cdot |H_2| / |H_1 \cap H_2| = |H_1| \cdot |H_2|$. Suppose that $|H_1 \cdots H_k| = |H_1| \cdots |H_k|$ for some $1 \leq k < n$. Then we see that

$$\begin{aligned} |H_1 \cdots H_k \cap H_{k+1}| &= \gcd(|H_1 \cdots H_k|, |H_{k+1}|) \\ &= \gcd(|H_1| \cdots |H_k|, |H_{k+1}|) \\ &= 1. \end{aligned}$$

This implies that

$$H_1 \cdots H_k \cap H_{k+1} = \{1\}$$

for all $1 \leq k \leq n-1$. This satisfies Theorem 6.7.(2). Therefore $H_1 \cdots H_n$ is isomorphic to the direct product by Theorem 6.7.(4). ∎

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

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

Proof. Write $Z_i = Z(H_i)$. If $i \neq j$, then H_i and H_j commute elementwise by Lemma 6.6. Let k be fixed. Then we see that $H_i \subseteq C_G(H_k) \subseteq C_G(Z_k)$ for all $i \neq k$. Clearly $H_k \subseteq C_G(Z_k)$. Thus $G = H_1 H_2 \cdots H_n \subseteq C_G(Z_k)$ and so $Z_k \subseteq Z(G)$ for each k. Thus $Z_1 Z_2 \cdots Z_n \subseteq Z(G)$.

Now let $z \in Z(G)$ and write $z = z_1 z_2 \cdots z_n$ with $z_i \in H_i$ for all i. Let $g \in G$, then

$$z = gzg^{-1} = (gz_1g^{-1})(gz_2g^{-1}) \cdots (gz_ng^{-1}).$$

Since $H_i \lhd G$, we have $gz_ig^{-1} \in H_i$ for all i. By Theorem 6.7.(1), we get $z_i = gz_ig^{-1}$ for all i, and thus $z_i \in Z(G)$. In particular, $z_i \in Z_i$. Therefore $z \in Z_1Z_2 \cdots Z_n$ and we have $Z(G) = Z_1Z_2 \cdots Z_n$. This product is direct because uniqueness is inherited from the fact that $G = \prod H_i$. ■

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 $N = N_1N_2 \ldots N_n$. 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.,

$$N_1N_2 \cdots N_n \cong N_1 \times N_2 \times \cdots \times N_n.$$

(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.,

$$\frac{H_1 \times H_2 \times \cdots \times H_n}{N_1N_2 \cdots N_n} \cong H_1/N_1 \times H_2/N_2 \times \cdots \times H_n/N_n.$$

Proof. (i) If $i \neq j$, then H_i and H_j commute elementwise by Lemma 6.6. Thus N_k commutes elementwise with H_i for $i \neq k$. Hence $N_G(N_k)$ contains all H_i and so $N_G(N_k) = H_1H_2 \cdots H_n = G$. Therefore we have $N_i \lhd G$.

(ii) It follows from $N_k \cap (N_1 \cdots N_{k-1}) = \{1\}$ for each $k = 2, \ldots, n$ and Theorem 6.7.

(iii) Let the function $\psi : G \to H_1/N_1 \times H_2/N_2 \times \cdots \times H_n/N_n$ be defined by

$$\psi(g) = (x_1N_1, \ldots, x_nN_n)$$

where $g = x_1 \cdots x_n$ and $x_i \in H_i$ for all i. Then ψ is a surjective homomorphism. Clearly $\ker \psi = N$. ■

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 ($\lambda \in \Lambda$).

Remark. If we only mention direct product, it means the restricted direct product. If $\Lambda = \{1, \dots, n\}$, then $\prod^w_{\lambda\in\Lambda} H_\lambda = H_1 \times \cdots \times H_n$.

Theorem 6.13. *Let $\prod_{\lambda\in\Lambda} H_\lambda$ be the unrestricted direct product of the groups H_λ ($\lambda \in \Lambda$). Then $\left(\prod_{\lambda\in\Lambda} H_\lambda, \{\pi_\lambda \mid \lambda \in \Lambda\}\right)$ 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.*

Proof. Let $(G, \{\varphi_\lambda : G \to H_\lambda\})$ be a pair of a group and homomorphisms. Then verify that the function

$$\begin{aligned} \varphi : G &\to \prod_{\lambda\in\Lambda} H_i \\ g &\mapsto (\varphi_\lambda(g))_{\lambda\in\Lambda} \end{aligned}$$

is a unique homomorphism such that $\pi_\lambda \circ \varphi = \varphi_\lambda$ for all $\lambda \in \Lambda$. ■

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 $\{\lambda_1, \dots, \lambda_n\}$ 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.

Proof. Routine. ■

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 non-identity 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 $G \cong \prod_{\lambda \in \Lambda}^{w} H_i$ such that the subgroup H_λ of G corresponds to the subgroup $\overline{H}_\lambda$ of the direct product.

Proof. (1) $\Rightarrow$ (2) We first show that for all finite subset $\{\lambda_1, \ldots, \lambda_k\}$ ($k \geq 2$), if $n_{\lambda_1} n_{\lambda_2} \cdots n_{\lambda_k} = 1$ where $n_{\lambda_i} \in H_i$, then $n_{\lambda_i} = 1$ for all i. Assume that $n_{\lambda_1} \neq 1$. Then some $n_{\lambda_i} \neq 1$. But the expression $n_{\lambda_1} = n_{\lambda_k}^{-1} \cdots n_{\lambda_2}^{-1}$ is not unique.

Fix λ and suppose $g \in H_\lambda \cap \langle H_\mu \mid \mu \neq \lambda \rangle$. Since $g \in \langle H_\mu \mid \mu \neq \lambda \rangle$, we can write $g = x_\lambda = x_{\mu_1} x_{\mu_2} \cdots x_{\mu_n}$ where $x_\lambda \in H_\lambda$ and $x_{\mu_i} \in H_{\mu_i}$ for all i. So $1 = x_\lambda^{-1} x_{\mu_1} x_{\mu_2} \cdots x_{\mu_n}$. The first paragraph implies that $g = x_\lambda = 1$.

(2) $\Rightarrow$ (1) The first assertion follows from Lemma 6.6. Since $G = \langle H_\lambda \mid \lambda \in \Lambda \rangle$, we can write any element x of G as $x_{\lambda_1} x_{\lambda_2} \cdots x_{\lambda_n}$ where $\{\lambda_1, \ldots, \lambda_n\}$ is a finite subset of Λ and $x_{\lambda_i} \in H_i \setminus \{1\}$ for all i. Let $x_{\mu_1} x_{\mu_2} \cdots x_{\mu_\ell}$ be another expression for x. If $x_{\mu_i} \notin \{\lambda_1, \ldots, \lambda_n\}$, then we apply the first assertion to obtain

$$x_{\mu_i} = (x_{\mu_2} \cdots x_{\mu_\ell})^{-1} x_{\lambda_1} x_{\lambda_2} \cdots x_{\lambda_n} \in H_{\mu_i} \cap \langle H_\lambda \mid \lambda \neq \mu_i \rangle = \{1\}.$$

Hence we have $\{\lambda_1, \ldots, \lambda_n\} = \{\mu_1, \ldots, \mu_\ell\}$. The first assertion allows us to reindex μ_i so that $x_{\lambda_i}, x_{\mu_i} \in H_{\lambda_i}$ for all i. Then we can use the same argument as in the proof of Theorem 6.7 to get (1).

(1) $\Rightarrow$ (3) Let g be an element of G. We can write the element g uniquely as $g = x_{\lambda_1} x_{\lambda_2} \cdots x_{\lambda_n}$, where $x_i \in H_{\lambda_i} \setminus \{1\}$ for all i. Let the function $\psi : G \to \prod_{\lambda \in \Lambda} H_\lambda$ be defined by $\psi(g) = \psi_g$, where

$$\psi_g(\lambda) = \begin{cases} x_i & \text{if } \lambda = \lambda_i, \\ 1 & \text{otherwise.} \end{cases}$$

Then we can check that ψ is a bijective homomorphism.

(3) $\Rightarrow$ (2) We can verify that $\overline{H}_\lambda \cap \langle \overline{H}_\mu \mid \mu \neq \lambda \rangle = \{1\}$ and then apply the isomorphism to obtain (2). ∎

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 $n_i \in \mathbb{Z}$,

$$n_1 x_1 + n_2 x_2 + \cdots + n_k x_k = 0 \implies n_i = 0 \text{ for every } i.$$

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

Remark. Depend on the context, the trivial group is considered as a free abelian group on the empty set.

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 $\bigoplus_{i \in I} \mathbb{Z}$, where*

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

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

Proof. Routine. ■

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.

Proof. (1) $\Rightarrow$ (2) Let $X = \{x_i \mid i \in I\}$ be a basis of F. Then for each $x \in X$, $nx = 0$ if and only if $n = 0$. Hence the subgroup generated by x_i is infinite cyclic. We show that

$$F = \bigoplus_{i \in I} \langle x_i \rangle.$$

Clearly $F = \sum_{i \in I} \langle x_i \rangle$. If there exists $x_i \in X$ such that

$$\langle x_i \rangle \cap \sum_{\substack{j \in I \\ j \neq i}} \langle x_j \rangle \neq \{0\},$$

then for some nonzero $n_i \in \mathbb{Z}$ and $n_1, \ldots, n_k \in \mathbb{Z}$ not all of which are zero such that $nx_i = n_1 x_{i_1} + \cdots + n_k x_{i_k}$ where $x_{i_1}, \ldots, x_{i_k}$ are distinct elements of X. This contradicts the fact that X is a basis.

(2) $\Rightarrow$ (3) Clearly each infinite cyclic group is isomorphic to $\mathbb{Z}$.

(3) $\Rightarrow$ (1) Suppose $F \cong \bigoplus_{i \in I} \mathbb{Z}$ where the copies of $\mathbb{Z}$ are indexed by a set I. By Lemma 7.2, $\{\theta_i \,|\, i \in I\}$ is a basis of $\bigoplus_{i \in I} \mathbb{Z}$. Then we use the isomorphism $F \cong \bigoplus_{i \in I} \mathbb{Z}$ to obtain a basis of F.

(1) $\Rightarrow$ (4) Let X be a basis of F and let $\iota : X \to F$ be the inclusion map. Suppose we are given a map $f : X \to G$. If $u \in F = \langle X \rangle$, then

$$u = n_1 x_1 + \cdots + n_k x_k$$

where $n_i \in \mathbb{Z}$ and $x_i \in X$. If

$$u = m_1 x_1 + \cdots + m_k x_k$$

where $m_i \in \mathbb{Z}$, then

$$\sum_{i=1}^{k} (n_i - m_i) x_i = 0$$

Since X is a basis, $n_i = m_i$ for all i. Consequently the map

$$\bar{f} : F \to G; \quad \sum_{i=1}^{k} n_i x_i \mapsto \sum_{i=1}^{k} n_i f(x_i)$$

is a well-defined function such that $\bar{f} \circ \iota = f$. In fact, $\bar{f}$ is a group homomorphism. For the uniqueness, if $g : F \to G$ is a homomorphism such that $g\iota = f$, then for any $x \in X$,

$$g(x) = g(\iota(x)) = f(x) = \bar{f}(x),$$

whence $g(u) = \bar{f}(u)$ for all $u \in F$. Therefore F is a free object on the set X in the category of abelian groups.

(4) $\Rightarrow$ (3) Suppose that F is free on X. Construct the direct sum $\bigoplus_{x \in X} \mathbb{Z}$ with the copies of $\mathbb{Z}$ indexed by X. Lemma 7.2 shows that $\bigoplus_{x \in X} \mathbb{Z}$ is a free object on the set $Y = \{\theta_x \,|\, x \in X\}$. Since we have $|X| = |Y|$, it follows that $F \cong \bigoplus_{x \in X} \mathbb{Z}$ by

Proposition 0.3. ■

Remark. From the categorical point of view, one should define a free abelian group using (4).

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

Proof. First suppose F has a basis X of finite cardinality n. By Proposition 7.3, we get

$$F \cong \bigoplus_{i=1}^{n} \mathbb{Z}.$$

Let p be a prime. For any additive group G, the set $pG = \{pg \,|\, g \in G\}$ is a subgroup of G. Clearly

$$pF \cong \bigoplus_{i=1}^{n} p\mathbb{Z}.$$

By Proposition 6.11, we have

$$F/pF \cong \bigoplus_{i=1}^{n} \mathbb{Z}/p\mathbb{Z} \cong \bigoplus_{i=1}^{n} \mathbb{Z}_p.$$

Therefore $|F/pF| = p^n$. Let Y be another basis of F containing at least r elements, then a similar argument shows that F/pF contains a subgroup isomorphic to $\bigoplus_{i=1}^{r} \mathbb{Z}_p$. Hence we have $|F/pF| \geq p^r$, whence $p^r \leq p^n$ and $r \leq n$. It follows that Y contains at most n elements. Let $|Y| = m \leq n$. Then $|F/pF| = p^m$. Therefore $p^m = p^n$ and $|X| = n = m = |Y|$.

By the previous paragraph, the existence of a finite basis would imply every basis is finite. So if one basis of F is infinite, then all bases are infinite. Let X be an infinite basis of F. It suffices to show that $|X| = |F|$. Clearly $|X| \leq |F|$. Let $\mathcal{P}_0(X)$ be the set of all finite subsets of X. For each $S = \{x_1, \ldots, x_n\} \in \mathcal{P}_0(X)$, let G_S be the subgroup of F generated by $x_1, \ldots, x_n$. Every element in F can be expressed as a linear combination of a finite subset of the basis X, and hence belongs to some G_S. So

$$F = \bigcup_{S \in \mathcal{P}_0(X)} G_S.$$

Also, we have

$$G_S \cong \langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle$$

for each $S = \{x_1, \ldots, x_n\}$. Therefore

$$|G_S| = |\langle x_1 \rangle \oplus \cdots \oplus \langle x_n \rangle| = \left| \bigoplus_{i=1}^{n} \mathbb{Z} \right| = |\mathbb{Z}|^n = |\mathbb{Z}| = \aleph_0$$

by Theorem 0.17.(ii). Hence we obtain

$$|F| = \left| \bigcup_{S \in \mathcal{P}_0(X)} G_S \right| \leq |\mathcal{P}_0(X)| \aleph_0.$$

by Theorem 0.15. By Theorem 0.11, we have $|\mathcal{P}_0(X)| = |X|$. By Theorems 0.14 and 0.16.(iii), we get

$$|F| \leq \max\{|X|, \aleph_0\} = |X|.$$

Therefore $|F| = |X|$ by Theorem 0.9. ■

Remark. The proof was adapted from Hungerford's Algebra. I feel that S in the original proof is a bit redundant. Prove me wrawwwwwng.

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,* $\operatorname{rank} G \leq \operatorname{rank} F$.

Proof using Zorn's Lemma. Let $\{x_i\}_{i \in I}$ be a basis for F. Consider the set $\mathcal{S}$ of all linearly independent sets Y_J in G, where J is a subset of the index set I, and the subgroup generated by Y_J is equal to $G \cap F(Y_J)$, where $F(Y_J)$ is the subgroup of F generated by those x_i's that appear in the expansions of the y_j's.

Consider the partial order on $\mathcal{S}$ by usual set inclusion. Every chain in $\mathcal{S}$ has an upper bound (given by the union of the sets in the chain). By Zorn's Lemma (Lemma 0.6), there exists a maximal element Y_{J_0}. We claim that Y_{J_0} is a basis for G. Since Y_{J_0} is linearly independent by definition, it suffices to show that $G = \langle Y_{J_0} \rangle$.

Suppose on the contrary that $G \neq \langle Y_{J_0} \rangle$. This means $\langle Y_{J_0} \rangle$ is a proper subgroup of G. Let $z \in G \setminus \langle Y_{J_0} \rangle$. The expansion of z in terms of the basis $\{x_i\}_{i \in I}$ must have some elements x_k's such that they not involved in the expansions of the y_j's. For convenience, we call such x_k a "new" element in z. For each element $z \in G \setminus \langle Y_{J_0} \rangle$, there is a non-empty set of new x_k's. We can choose an element z that involves the smallest number of new x_k's. Let these new elements be $x_{k_1}, \ldots, x_{k_\ell}$. The set of all

integers $n \in \mathbb{Z}$ such that there exists $y \in F(Y_{J_0} \cup \{x_{k_2}, \dots, x_{k_\ell}\})$ for which

$$nx_{k_1} + y \in G$$

is a nonzero ideal of $\mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain, we can find a generator α for this ideal. Hence we pick an element z so that the coefficient of x_{k_1} is α. More precisely, we write

$$z = \alpha x_{k_1} + d_2 x_{k_2} + \cdots + d_\ell x_{k_\ell} + y$$

for some $d_2, \dots, d_\ell \in \mathbb{Z}$ and $y \in F(Y_{J_0})$.

Let $Y' = Y_{J_0} \cup \{z\}$. Now we show that Y' would contradicts the maximality of Y_{J_0}. First we show that Y' is linearly independent. Suppose that

$$\sum_{j=1}^{k} n_j y_j + nz = 0.$$

where $y_1, \dots, y_k$ are distinct elements in Y_{J_0} and $n_1, \dots, n_k \in \mathbb{Z}$. Remark that the case where linear combinations of elements without z is trivial, and so we omit the argument. If $n \neq 0$, then we have $nz \in \langle Y_{J_0} \rangle$. Note that the coefficient of x_{k_1} in the expansion of nz is $n\alpha$. Since nz is an element of $\langle Y_{J_0} \rangle$. By definition of new elements, the coefficient of x_{k_1} must be zero. Thus we get $n\alpha = 0$, a contradiction since α is also nonzero. This implies $n = 0$. Then $\sum_{j \in J_0} n_j y_j = 0$. Since Y_{J_0} is independent, $n_j = 0$ for all j.

Clearly $\langle Y' \rangle \subseteq G \cap F(Y')$. For the reverse direction, let $w \in G \cap F(Y')$. Then

$$w = c_1 x_{k_1} + \cdots + c_\ell x_{k_\ell} + y'$$

for some $c_1, \dots, c_\ell \in \mathbb{Z}$ and $y' \in F(Y_{J_0})$. By definition of α, we get $c_1 = \lambda\alpha$ for some λ. Therefore we have

$$w - \lambda z = (c_2 - \lambda d_2)x_{k_2} + \cdots + (c_\ell - \lambda d_\ell)x_{k_\ell} + y' - \lambda y.$$

The coefficient of x_{k_1} in $w - \lambda z$ is zero. So the number of new elements in $w - \lambda z$ is strictly less than that in z. Since z has the smallest number of new elements, it follows that $w - \lambda z$ contains no new element, and so $w - \lambda z \in \langle Y_{J_0} \rangle$. This implies that $w \in \langle Y_{J_0} \cup \{z\} \rangle = \langle Y' \rangle$. Clearly $Y' \supset Y_{J_0}$, which arrives at a contradiction. Hence $G = \langle Y_{J_0} \rangle$. Therefore G is a free abelian group.

By the argument above, we have found a basis of G indexed by the subset J_0 of the index set I. Hence $\operatorname{rank} G = |J_0| \leq |I| \leq \operatorname{rank} F$. This completes the proof. ■

Proof using Well-Ordering Theorem. Let $\{x_i\}_{i\in I}$ be a basis of F. In view of Well Ordering Theorem (Theorem 0.20), we may assume that I is well-ordered. Let g be any nonzero element in F. Then g has a unique expression of the form

$$g = c_1 x_{\alpha_1} + c_2 x_{\alpha_2} + \cdots + c_r x_{\alpha_r}$$

where $c_1, \ldots, c_r \in \mathbb{Z}$ and $\alpha_1, \ldots, \alpha_r$ are members of I. Note that $\{\alpha_1, \ldots, \alpha_r\}$ is a finite set, and thus contains a largest element according to the ordering of I. We call this largest element the **index** of g.

We proceed to the proof that G is free. For each $\beta \in I$, let $\mathbb{Z}_\beta$ be the subset of $\mathbb{Z}$ consisting of 0 and all coefficients of x_β that occur in elements of index β in G. We claim that $\mathbb{Z}_\beta$ is a subgroup of $\mathbb{Z}$. If $m, n \in \mathbb{Z}_\beta$, then we have

$$\begin{aligned} g_1 &= m x_\beta + \cdots, \\ g_2 &= n x_\beta + \cdots \end{aligned}$$

for suitable elements g_1, g_2 in G. If $m = n$, then $m - n = 0 \in \mathbb{Z}_\beta$. For $m \neq n$, the equation

$$g_1 - g_2 = (m-n) u_\beta + \cdots$$

proves that $m - n \in \mathbb{Z}_\beta$, because the remaining terms only involve elements x_γ with $\gamma < \beta$ (this is where we use the definition of index elements). This proves our claim.

Note that $\mathbb{Z}_\beta$ is cyclic. If $\mathbb{Z}_\beta = \{0\}$, we can ignore the index β. If $\mathbb{Z}_\beta \neq 0$, then we pick a generator c_β. By the definition of $\mathbb{Z}_\beta$, there exists an element y_β of index β in G such that the coefficient of x_β in y_β is the integer c_β.

Finally, we claim that $Y = \{y_\beta \in G \,|\, \mathbb{Z}_\beta \neq 0\}$ is a basis of G. Suppose that

$$\sum_{i=1}^{k} n_i y_{\alpha_i} = 0$$

where $y_{\alpha_1}, \ldots, y_{\alpha_k} \in Y$ and $n_1, \ldots, n_k \in \mathbb{Z}$. Without loss of generality, assume that $\alpha_1 < \alpha_2 < \cdots < \alpha_k$. By the construction of Y, we see that y_{α_i} and y_{α_j} have different index whenever $i \neq j$. We express each y_{α_i} in terms of x_i's. Then the coefficient of x_{α_k} in the equation above is $n_k c_{\alpha_k}$. Since x_i's are linearly independent, we get $n c_{\alpha_k} = 0$ and thus $n_k = 0$. Now the equation becomes $\sum_{i=1}^{k-1} n_i y_{\alpha_i} = 0$. Repeating this argument, we obtain $n_i = 0$ for all i. Hence Y is linearly independent. Suppose that $\langle Y \rangle \neq G$. Among all the elements of G that are not in $\langle Y \rangle$ we can pick one of minimal index (since I is well-ordered), let say g is that element and that γ is its

index. Write

$$g = dx_\gamma + \cdots .$$

Now d is an element of Z_γ and therefore is a multiple of the generator c_γ of Z_γ. Let

$$g' = g - \frac{d}{c_\gamma} y_\gamma .$$

Since $y_\gamma \in \langle Y \rangle$ and $g \notin \langle Y \rangle$, we have $g' \notin \langle Y \rangle$. The coefficient of x_γ in the right hand side is 0, and thus the index of g' is smaller than γ, a contradiction. Hence G is a free abelian group.

The second assertion follows immediately since the basis Y constructed above is indexed by a subset of I. ■

Proof using Transfinite Induction. Let $X = \{x_\alpha \,|\, \alpha < \beta\}$ be a basis of F where the index set is assumed to be well-ordered and order-isomorphic to β according to Counting Theorem (Theorem 0.27). Thus $F = \bigoplus_{\gamma<\beta} \langle x_\gamma \rangle$. Let G be a given subgroup. For each ordinal α, define

$$F_\alpha = \begin{cases} \bigoplus_{\gamma<\alpha} \langle x_\gamma \rangle & \text{if } \alpha < \beta, \\ F & \text{otherwise.} \end{cases}$$

$$G_\alpha = G \cap F_\alpha .$$

We use transfinite induction (Theorem 0.28) to show that G_α is free for all ordinals α. With this result, we can take an ordinal $\alpha \geq \beta$ to obtain that $G = G_\alpha$ is free.

For $\alpha = 0$, the set $\{\gamma \,|\, \gamma < \alpha\}$ is empty. The direct sum over an empty set is the trivial group. So $G_0 = \{0\}$ is a free abelian group. (Let's assume in this case the trivial group is free, see the remark below Definition 7.1).

Assume that the result holds for a given ordinal α. The case $\alpha \geq \beta$ is trivial since $G_{\alpha+1} = G \cap F_{\alpha+1} = G \cap F = G \cap F_\alpha = G_\alpha$. Suppose that $\alpha < \beta$. Clearly, $G_\alpha = G_{\alpha+1} \cap F_\alpha$. By the Second Isomorphism Theorem, we have

$$\frac{G_{\alpha+1}}{G_\alpha} = \frac{G_{\alpha+1}}{G_{\alpha+1} \cap F_\alpha} \cong \frac{G_{\alpha+1} + F_\alpha}{F_\alpha} .$$

The last quotient group is a subgroup of $F_{\alpha+1}/F_\alpha \cong \langle x_\alpha \rangle$, thus either $G_{\alpha+1} = G_\alpha$ or $G_{\alpha+1}/G_\alpha$ is an infinite cyclic group (which is free). If $G_{\alpha+1} = G_\alpha$, then we are done. If $G_{\alpha+1}/G_\alpha$ is free, then we conclude from Lemma 7.12 that $G_{\alpha+1} = G_\alpha \oplus \langle g_\alpha \rangle$ for some nonzero $g_\alpha \in G_{\alpha+1}$. By inductive hypothesis, G_α is free. So the union of a basis of G_α and $\{g_\alpha\}$ is a basis of $G_{\alpha+1}$. Hence $G_{\alpha+1}$ is free.

Suppose the result holds all $\alpha < \lambda$, where λ is a nonzero limit ordinal. Note that

$$F_\lambda = \bigcup_{\alpha<\lambda} F_\alpha.$$

Thus

$$G_\lambda = G \cap F_\lambda = G \cap \bigcup_{\alpha<\lambda} F_\alpha = \bigcup_{\alpha<\lambda} G_\alpha.$$

For each $\alpha < \lambda$, let Y_α be the basis for G_α constructed in the successor step, i.e., $Y_\alpha = \{g_\gamma \mid \gamma < \alpha,\, g_\gamma \neq 0\}$. Let $Y = \bigcup_{\alpha<\lambda} Y_\alpha$. We claim Y is a basis for G_λ. Clearly $G_\lambda = \langle Y \rangle$ since every g in G_λ belongs in some G_α, so g is a finite linear combination of elements in Y_α. Suppose that $\sum_{i=1}^{k} n_i y_i = 0$ where $y_i \in Y$ are distinct elements and $n_i \in \mathbb{Z}$. By the assumption on Y_α, each y_i can be identified as g_{α_i} for some index $\alpha_i < \lambda$ (Note that α_i is a successor ordinal because g_μ does not make sense in the construction above). Assume that $\alpha_1 < \cdots < \alpha_k$. Then the elements $y_1, \ldots, y_k$ belong to Y_{α_k}. Since Y_{α_k} is a basis, we get $n_i = 0$ for all i. Therefore G_λ is a free abelian group.

In the successor step, we construct the basis for G_α by at most adding one new basis element g_α corresponding to the basis element x_α of F. In the limit ordinal step, we do not add new basis element. Hence $\operatorname{rank} G_\alpha \leq \operatorname{rank} F$ for all ordinals α. ■

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.*

Proof. Let $\alpha : F_1 \to F_2$ be an isomorphism. Then $\alpha(X_1)$ is a basis of F_2. By Theorem 7.4, we have $|X_1| = |\alpha(X_1)| = |X_2|$. The converse follows from Proposition 0.3. ■

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.*

Proof. Let F be the free abelian group on the set X. Then F is of rank $|X|$. The inclusion map $f : X \to G$ induces a homomorphism $\bar{f}\colon F \to G$ such that $\bar{f} \circ \iota = f$. In particular, $\bar{f}(x) = f(x) = x$ for all $x \in X$, whence $X \subseteq \operatorname{im} \bar{f}$. Since X generates G we must have $\operatorname{im} \bar{f} = G$. ■

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

Proof. Let G be finitely generated by n elements. By Corollary 7.8, we can find a free abelian group F on n generators and a surjective homomorphism $\varphi : F \to G$.

Let H be a subgroup of G. The subgroup $\varphi^{-1}(H)$ of F is finitely generated by Theorem 7.6. Hence H itself 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.*

Proof. Assume G is not a trivial group. Since G is finitely generated, there exists a finite subset S of G for which $G = \langle S \rangle$. Let $X = \{x_1, \ldots, x_n\}$ be a maximal subset of S having the property that X is linearly independent. Note that $n \geq 1$ since $G \neq 0$. Let F be the subgroup generated by $x_1, \ldots, x_n$. Then F is free. Given $y \in G$ there exist integers $m_1, \ldots, m_n, m$ not all zero such that

$$my + m_1 x_1 + \cdots + m_n x_n = 0,$$

by the assumption of maximality on X. Furthermore, $m \neq 0$; otherwise all $m_i = 0$. Hence my lies in F. This is true for every $y \in S$, whence there exists an integer $m \neq 0$ such that $mG = m\langle S \rangle \subseteq F$ (by considering the least common multiple). The map $x \mapsto mx$ of G into itself is a homomorphism, having trivial kernel since G is torsion free. Hence it is an isomorphism of G onto mG. Since mG is a subgroup of F, it follows from Theorem 7.6 that mG is a free abelian group of finite rank. This completes the proof. ■

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*

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

Proof. Let $\{x_i'\}_{i \in I}$ be a basis of F, and for each $i \in I$, let x_i be an element of G such that $\varphi(x_i) = x_i'$. Let H be the subgroup of G generated by all elements $x_i, i \in I$, i.e.,

$$H = \langle x_i \,|\, i \in I \rangle.$$

We claim that $\{x_i\}_{i\in I}$ is a basis of H. Suppose that

$$\sum_{i\in I} n_i x_i = 0$$

with $n_i \in \mathbb{Z}$ and $n_i = 0$ for almost all i. Applying φ yields

$$0 = \sum_{i\in I} n_i \varphi(x_i) = \sum_{i\in I} n_i x_i'.$$

Since $\{x_i'\}_{i\in I}$ is a basis for F, we get $n_i = 0$ for all i. Hence $\{x_i\}_{i\in I}$ is a basis of H.

Now we show that G is an internal direct sum of $\ker\varphi$ and H. Let $z \in \ker\varphi \cap H$. Then $z = \sum_{i\in I} n_i x_i$ and $\varphi(z) = 0$ for some appropriate $n_i \in \mathbb{Z}$. Similar argument as above shows that $\ker\varphi \cap H = 0$. Let $x \in G$. Since $\varphi(x) \in F$ we can find some appropriate integers n_i such that

$$\varphi(x) = \sum_{i\in I} n_i x_i'.$$

From this, we obtain

$$0 = \varphi(x) - \sum_{i\in I} n_i x_i' = \varphi(x) - \sum_{i\in I} n_i \varphi(x_i) = \varphi\left(x - \sum_{i\in I} n_i x_i\right).$$

Hence $x - \sum_{i\in I} n_i x_i \in \ker\varphi$, whence

$$x = x - \sum_{i\in I} n_i x_i + \sum_{i\in I} n_i x_i \in \ker\varphi + H.$$

So the lemma follows. ■

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 $F \cong G/G_t$.*

Proof. By Corollary 7.9, the subgroup G_t is finitely generated, and thus finite because each element of G_t has finite order.

Next, we prove that G/G_t is torsion free. Let $x + G_t$ be an element of G/G_t such that $m(x + G_t) = 0$ for some integer $m \neq 0$. Then $mx \in G_t$, whence $qmx = 0$ for some integer $q \neq 0$. Then $x \in G_t$, so $x + G_t = G_t$, and G/G_t is torsion free. By Lemma 7.11, G/G_t is free and has finite rank. By applying Lemma 7.12 to the canonical projection $\pi : G \to G/G_t$, we obtain $G = G_t \oplus F$ where F is a subgroup of G such that $F \cong G/G_t$. By Corollary 7.7, F has finite rank. ■

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,*

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

Proof. Clearly $G_r + G_s \subseteq G_{rs}$. For the reverse direction, there exist integers u, v such that $ur + vs = 1$. Let $x \in G_{rs}$. Then $x = urx + vsx$, and $urx \in G_s$ while $vsx \in G_r$, and $G_{rs} = G_r + G_s$.

Let $x \in G_r \cap G_s$. Then $rx = 0 = sx$. So $dx = 0$ where $d = \gcd(r, s)$. Since $\gcd(r, s) = 1$, we get $x = 0$. This proves the assertion. ■

Remark. Let m and n be coprime positive integers. If we choose $G = \mathbb{Z}_{mn}$, then $G_{mn} = \mathbb{Z}_{mn}$. To show that $G_m \cong \mathbb{Z}_m$, we note that G_m can be generated by the element n in $\mathbb{Z}_{mn}$, which is of order m. Similarly we obtain $G_n \cong \mathbb{Z}_n$ and thus

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n.$$

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., $G(p) = \{x \in G \,|\, |x| = p^n \text{ for some } n \geq 0\}$.*

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

Proof. (i) Trivial.

(ii) We have a homomorphism

$$\begin{aligned} \varphi : \bigoplus_p G(p) &\to G \\ (x_p) &\mapsto \sum_p x_p. \end{aligned}$$

We prove that this homomorphism is bijective. Let $x = (x_p) \in \ker \varphi$. Then $\sum_p x_p = 0$. Let q be a prime. Then

$$x_q = \sum_{p \neq q} (-x_p).$$

Let m be the least common multiple of the orders of elements x_p on the right-hand side. Then $mx_q = 0$. By definition of $G(q)$, we also have $q^r x_q = 0$ for some integer $r \geq 0$. Let d be the greatest common divisor of m and q^r. Then $dx_q = 0$. But q

does not divide m, so $d = 1$ and thus $x_q = 0$. Hence $x_q = 0$ for every prime q, which means that the kernel is trivial, and φ is injective.

As for the surjectivity, for each positive integer $m \geq 2$, we let $m = p_1^{\ell_1} \cdots p_k^{\ell_k}$ be the prime factorization of m. Repeating Lemma 7.14 inductively, we conclude that every element in G_m can be expressed as a sum of elements in $G_{p_i^{\ell_i}}$ (which is a subgroup of $G(p_i)$), i.e.,

$$G_m = G_{p_1^{\ell_1}} \oplus \cdots \oplus G_{p_k^{\ell_k}} = \bigoplus_{i=1}^{k} G_{p_i^{\ell_i}}.$$

Since $G = \bigcup_{m \geq 1} G_m$, the map φ is surjective.

If G is finitely generated, then G is finite by Theorem 7.13. Hence G must be a direct sum of a finitely many groups $G(p)$. ∎

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 $p^{k+\ell}$.*

Proof. From $p^\ell p^k g$, we have $|g| \leq p^{k+\ell}$.

Now let $|g| = p^n$ for some integer $n \geq 1$. Then $p^k g \neq 0$ implies that $k < n$. So $n - k > 0$. Since

$$p^{n-k} p^k b = 0,$$

we have $p^\ell \leq p^{n-k}$. Hence $|g| = p^n \geq p^{k+\ell}$. Therefore $|g| = p^{k+\ell}$. ∎

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.*

Proof. Let g be any representative of $\bar{g}$. Assume that the order of x is p^ℓ. Then $p^r g + \langle x \rangle = \langle x \rangle$ and so $p^r g \in \langle x \rangle$. So

$$p^r g = nx$$

for some integer $0 \leq n < p^\ell$. Note that the order of $\bar{g}$ is at most the order of g. If $n = 0$, then g has order p^r and we are done. Otherwise write $n = p^k m$ where m is coprime to p and $k \geq 0$. Then mx is also a generator of $\langle x \rangle$, and hence has order $|x| = p^\ell$. Now we have $k < \ell$ since $n < p^\ell$. Then $p^k mx$ has order $p^{\ell - k}$ (recall that $|\langle a^m \rangle| = |a| / \gcd(|a|, m)$). By Lemma 7.16, the element g has order $p^{r+\ell-k}$. Since x has maximal order we have $|x| \geq |g|$, whence $r + \ell - k \leq \ell$ and $r \leq k$. Let $g' = p^{k-r} mx$. Then $g' \in \langle x \rangle$ and $p^r g = p^r g'$. Let $g'' = g - g'$. Then $g'' + \langle x \rangle = g + \langle x \rangle = \bar{g}$ because

$g'' - g = -g' \in \langle x \rangle$. It follows that

$$|g''| \geq |g'' + \langle x \rangle| = |\bar{g}| = p^r.$$

Since $|g''| \leq p^r$ by $p^r g'' = 0$, we conclude that g'' 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*

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

Proof. Note that p^m has order p^{n-m}. So we have $p^m \mathbb{Z}_{p^n} = \langle p^m \rangle \cong \mathbb{Z}_{p^{n-m}}$. ■

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*

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

Proof. There is an isomorphism $\varphi : G \to \bigoplus_{i \in I} G_i$. Let $\psi : mG \to \bigoplus_{i \in I} G_i$ be defined by $\psi(x) = \varphi(x)$. Clearly $\ker \psi = \{0\}$ and $\operatorname{im} \psi = \bigoplus_{i \in I} mG_i$. ■

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.

Proof. We prove by induction on order of G. If G is cyclic, then we are done. Assume that G is not cyclic. Let $x_1 \in G$ be an element of maximal order. Let G_1 be the cyclic subgroup generated by x_1, of order p^{r_1}.

By inductive hypothesis, the quotient group G/G_1 is an internal direct sum of cyclic subgroups $\overline{G}_2, \ldots, \overline{G}_k$ of orders $p^{n_2}, \ldots, p^{n_k}$ respectively with $n_2 \geq \cdots \geq n_k$. More precisely,

$$G/G_1 = \overline{G}_2 \oplus \cdots \oplus \overline{G}_k \cong \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_k}}.$$

Let $\bar{x}_i$ be a generator of $\overline{G}_i$ for $i = 2, \ldots, k$. Since $\bar{x}_i \in G/G_1$, Lemma 7.17 guarantees that we can choose a representative x_i in G such that $|x_i| = |\bar{x}_i|$. Let G_i be the cyclic subgroup generated by x_i. We claim that $G = G_1 \oplus G_2 \oplus \cdots \oplus G_k$.

Given $x \in G$, let $\bar{x} = x + G_1 \in G/G_1$. There exist integers $m_2, \ldots, m_k$ such that

$$\bar{x} = m_2 \bar{x}_2 + \cdots + m_k \bar{x}_k.$$

Hence

$$x - m_2x_2 - \cdots - m_kx_k \in G_1.$$

So there exists an integer m_1 such that

$$x = m_1x_1 + m_2x_2 + \cdots + m_kx_k.$$

Hence $G_1 + \cdots + G_k = G$.

To verify the sum is an internal direct sum, it suffices to show that $x_1, \ldots, x_k$ are linearly independent, because it would imply that

$$(G_1 + \cdots + G_i) \cap G_{i+1} = 0$$

for each $i = 1, \ldots, k-1$. Suppose that

$$m_1x_1 + \cdots + m_kx_k = 0$$

where $m_1, \ldots, m_k$ are integers. Then we have

$$m_2\bar{x}_2 + \cdots + m_k\bar{x}_k = G_1.$$

Since G/G_1 is a direct sum of $\overline{G}_2, \ldots, \overline{G}_k$, we conclude from Theorem 6.7 that each $m_i = 0$ for $i = 2, \ldots, k$. Hence $m_1x_1 = 0$ and so $m_1 = 0$. Therefore G is the direct sum of $G_1, \ldots, G_k$.

We prove uniqueness by induction. Suppose that G is written in two ways as a direct sum of cyclic groups, say of type

$$(p^{n_1}, \ldots, p^{n_k}) \quad \text{and} \quad (p^{m_1}, \ldots, p^{m_s})$$

with $r_1 \geq \cdots \geq r_k \geq 1$ and $m_1 \geq \cdots \geq m_s \geq 1$. In view of Lemmas 7.18 and 7.19, the subgroup pG is of type

$$(p^{r_1-1}, \ldots, p^{r_k-1}) \quad \text{and} \quad (p^{m_1-1}, \ldots, p^{m_s-1}).$$

By induction, the subsequence of

$$(r_1 - 1, \ldots, r_k - 1)$$

consisting of those integers at least 1 is uniquely determined (those with 0 correspond

to the trivial subgroup), and is the same as the corresponding subsequence of

$$(m_1 - 1, \ldots, m_s - 1).$$

In other words, there exists an integer $\ell \geq 1$ such that $r_i - 1 = m_i - 1 \geq 1$ for all $i = 1, \ldots, \ell$. Hence $r_i = m_i$ for all $i = 1, \ldots, \ell$, and the two sequences

$$(p^{r_1}, \ldots, p^{r_k}) \quad \text{and} \quad (p^{m_1}, \ldots, p^{m_s})$$

can differ only in their last components which can be equal to p. Hence G is of type

$$(p^{r_1}, \ldots, p^{r_\ell}, \underbrace{p, \ldots, p}_{k-\ell \text{ times}}) \quad \text{and} \quad (p^{r_1}, \ldots, p^{r_\ell}, \underbrace{p, \ldots, p}_{s-\ell \text{ times}}).$$

Thus the order of G is equal to

$$p^{r_1 + \cdots + r_\ell} p^{k-\ell} = p^{r_1 + \cdots + r_\ell} p^{s-\ell},$$

whence $k = s$, and our theorem is proved. ■

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 $i = 1, \ldots, k$.

Remark. To emphasize the ordering of powers of primes, we can express G as

$$\bigoplus_{j=1}^{\ell} \bigoplus_{i=1}^{k_j} \mathbb{Z}_{p_j^{n_{ij}}}$$

where $p_1, p_2, \ldots, p_\ell$ are distinct primes and $n_{1j} \geq n_{2j} \geq \cdots \geq n_{k_j j} \geq 1$ for all j.

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 $i = 1, \ldots, r$.

Proof. We arrange the elementary divisors of G and insert $p_i^0 = 1$ as follows.

$$\begin{array}{cccc} p_1^{n_{11}} & p_2^{n_{12}} & \cdots & p_\ell^{n_{1\ell}} \\ p_1^{n_{21}} & p_2^{n_{22}} & \cdots & p_\ell^{n_{2\ell}} \\ \vdots & \vdots & & \vdots \\ p_1^{n_{k1}} & p_2^{n_{k2}} & \cdots & p_\ell^{n_{k\ell}} \end{array}$$

where $p_1, \ldots, p_r$ are distinct primes, $0 \leq n_{1j} \leq n_{2j} \leq \cdots \leq n_{tj}$ for each $j = 1, 2, \ldots, \ell$ and $n_{1j} \neq 0$ for some j (the last condition is to ensure that we do not insert excessive p_i^0). By Theorem 7.21, we get (after adding trivial groups in the decomposition)

$$G \cong \bigoplus_{j=1}^{\ell} \bigoplus_{i=1}^{k} \mathbb{Z}_{p_j^{n_{ij}}} \oplus F$$

where F is a free abelian group of finite rank. For each $i = 1, 2, \ldots, k$, let m_i be the product of elements in the ith row in the array above, i.e.,

$$m_i = p_1^{n_{i1}} p_2^{n_{i2}} \ldots p_\ell^{n_{i\ell}}.$$

Since some $n_{1j} \neq 0$ for some j, we have $m_1 > 1$. Clearly $m_1 | m_2 | \ldots | m_t$. Since

$p_1, \ldots, p_\ell$ are distinct primes, by Lemma 7.14, we have

$$\bigoplus_{j=1}^{\ell} \mathbb{Z}_{p_j^{n_{ij}}} \cong \mathbb{Z}_{m_i}$$

for each $i = 1, \ldots, k$. Hence we have

$$G \cong \bigoplus_{j=1}^{\ell} \bigoplus_{i=1}^{k} \mathbb{Z}_{p_j^{n_{ij}}} \oplus F \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{\ell} \mathbb{Z}_{p_j^{n_{ij}}} \oplus F \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{m_i} \oplus F.$$

Now we show the uniqueness. Suppose that

$$G \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{m_i} \oplus F_1 \cong \bigoplus_{i=1}^{t} \mathbb{Z}_{r_i} \oplus F_2$$

where F_1 and F_2 are free abelian, m_i, r_i are integers such that $m_1, r_1 > 1$, $m_1 | m_2 | \cdots | m_k$ and $r_1 | r_2 | \cdots | r_t$. Clearly $F_1 \cong F_2$. Now we write

$$\begin{aligned} m_i &= p_1^{c_{i1}} p_2^{c_{i2}} \ldots p_\ell^{c_{i\ell}} \quad \text{for } i = 1, \ldots, k, \\ r_i &= p_1^{d_{i1}} p_2^{d_{i2}} \ldots p_\ell^{d_{i\ell}} \quad \text{for } i = 1, \ldots, t \end{aligned}$$

where $p_1, \ldots, p_\ell$ are distinct primes and $c_{1j} \neq 0$ for some j and $d_{1j'} \neq 0$ for some j' since $m_1, r_1 > 1$. Also, we have $0 \leq c_{1j} \leq c_{2j} \leq \cdots \leq c_{kj}$ and $0 \leq d_{1j} \leq d_{2j} \leq \cdots \leq d_{tj}$ for all j. Note that the direct sums of cyclic groups are isomorphic to G_t. By Lemma 7.14, we get

$$\bigoplus_{i=1}^{k} \bigoplus_{j=1}^{\ell} \mathbb{Z}_{p_j^{c_{ij}}} \cong \bigoplus_{i=1}^{k} \mathbb{Z}_{m_i} \cong G_t \cong \bigoplus_{i=1}^{t} \mathbb{Z}_{r_i} \cong \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{\ell} \mathbb{Z}_{p_j^{d_{ij}}}.$$

By Theorem 7.21, both direct sums must have same number of nonzero summands (elementary divisors), so $k = t$ and $c_{ij} = d_{ij}$ for all i, j. Therefore $m_i = r_i$ for all $i = 1, \ldots, k$. ■

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).*

Proof. The result follows from the uniqueness. ■

Remark. To count the number of nonisomorphic abelian groups of order n, it suffices to count the number of nonisomorphic abelian groups of order the highest prime power p^k appeared in the prime factorization of n. It is the number of partitions of k, denoted $a(k)$. If $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$, then the number of nonisomorphic abelian groups is given by $\prod_{i=1}^{\ell} a(k_i)$. There is no explicit formula for $a(k)$, making it difficult to count the groups of large order.

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 $x, y \in G$,*

$$\begin{aligned} (uv)^x &= u^x v^x, \\ u^{xy} &= (u^x)^y, \\ u^1 &= u \end{aligned}$$

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.

Proof. Let $g, u, x \in H$ and $h, v, y \in G$ (The symbols are so misleading!). Then,

$$\begin{aligned} [(g,h)(u,v)](x,y) &= (gu^{h^{-1}}, hv)(x,y) \\ &= (gu^{h^{-1}} x^{(hv)^{-1}}, hvy) \\ &= (gu^{h^{-1}} x^{v^{-1}h^{-1}}, hvy) \\ &= (g(ux^{v^{-1}})^{h^{-1}}, hvy) \end{aligned}$$

$$= (g,h)(ux^{v^{-1}}, vy)$$
$$= (g,h)[(u,v)(x,y)].$$

This proves the associative law. Clearly $1 = (1,1)$ is the identity and the inverse of (h,g) is given by $((h^{-1})^g, g^{-1})$. So L forms a group with respect to the operation defined above. ■

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 $H \rtimes_\varphi G$.

Remark. If there is no confusion, we simply write $H \rtimes G$. It is important to note that semidirect products with respect to different actions might not isomorphic.

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 $(1,g)^{-1}(h,1)(1,g) = (h^g, 1)$.

Proof. Routine. ■

Remark. We may consider G and H as subgroups of $H \rtimes G$ by identifying G and H with $\overline{G}$ and $\overline{H}$ respectively.

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

Proof. By Proposition 8.5.(iii) & (iv). ■

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.

Proof. Let $\psi_{X,G} : X \to G$ and $\psi_{Y,H} : Y \to H$ be isomorphisms. Let $\theta(x)$ be the automorphism of Y defined by

$$y^x = \psi_{Y,H}^{-1}(\psi_{Y,H}(y)^{\psi_{X,G}(x)}).$$

Then θ is an action of X on Y. Now let $\phi : Y \rtimes_\theta X \to H \rtimes_\varphi G$ be defined by

$$\phi(y, x) = (\psi_{Y,H}(y), \psi_{X,G}(x)).$$

Now we show that ϕ is a homomorphism. Let $y_1, y_2 \in Y$ and $x_1, x_2 \in X$. Then

$$\begin{aligned}
\phi[(y_1, x_1)(y_2, x_2)] &= \phi(y_1 y_2^{x_1^{-1}}, x_1 x_2) \\
&= \phi\left(y_1 \psi_{Y,H}^{-1}(\psi_{Y,H}(y_2)^{\psi_{X,G}(x_1^{-1})}), x_1 x_2\right) \\
&= \left(\psi_{Y,H}(y_1)\psi_{Y,H}(y_2)^{\psi_{X,G}(x_1^{-1})}, \psi_{X,G}(x_1)\psi_{X,G}(x_2)\right), \\
\phi(y_1, x_1)\phi(y_2, x_2) &= (\psi_{Y,H}(y_1), \psi_{X,G}(x_1))(\psi_{Y,H}(y_2), \psi_{X,G}(x_2)) \\
&= \left(\psi_{Y,H}(y_1)\psi_{Y,H}(y_2)^{\psi_{X,G}(x_1)^{-1}}, \psi_{X,G}(x_1)\psi_{X,G}(x_2)\right) \\
&= \left(\psi_{Y,H}(y_1)\psi_{Y,H}(y_2)^{\psi_{X,G}(x_1^{-1})}, \psi_{X,G}(x_1)\psi_{X,G}(x_2)\right).
\end{aligned}$$

So $\phi[(y_1, x_1)(y_2, x_2)] = \phi(y_1, x_1)\phi(y_2, x_2)$ for all $y_1, y_2 \in Y$ and $x_1, x_2 \in X$ and ϕ is a homomorphism. Clearly ϕ is bijective. This completes the proof. ∎

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 $H \rtimes K \cong G$.

Proof. It can be checked that φ is an action of K on H. Let $f : H \rtimes K \to G$ be the function defined by

$$f(h,k) = hk.$$

By assumption, $G = HK = KH$. So the function f is surjective. Now we show that f is a homomorphism. For any $h, v \in H$ and $k, u \in K$, we have

$$f[(h,k)(u,v)] = f(hu^{k^{-1}}, kv) = hu^{k^{-1}}kv = hkuk^{-1}kv = hkuv = f(h,k)f(u,v).$$

Hence the function f is a homomorphism. Let $(k,h) \in \ker f$. Then we have $kh = 1$, or $k = h^{-1} \in K \cap H = \{1\}$. Thus the kernel of f is $\{1\}$. Therefore f is an isomorphism. ■

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 $H \rtimes G$.

Proof. (1) $\Rightarrow$ (2) Let $\mathrm{Id} : H \rtimes G \to H \times G$ be the identity map. Let $h_1, h_2 \in H$ and $g_1, g_2 \in G$. Then we have

$$\begin{aligned}(h_1 h_2^{g_1^{-1}}, g_1 g_2) &= \mathrm{Id}(h_1 h_2^{g_1^{-1}}, g_1 g_2) \\ &= \mathrm{Id}[(h_1, g_1)(h_2, g_2)] \\ &= (h_1, g_1)(h_2, g_2) \\ &= (h_1 h_2, g_1 g_2).\end{aligned}$$

So we obtain $h_2^{g_1^{-1}} = h_2$ for all $h_2 \in H$ and $g_1 \in G$, i.e., G acts trivially on H.

(2) $\Rightarrow$ (1) The operation in the semidirect product is then the same as that in the direct product.

(1) $\Rightarrow$ (3) Trivial.

(3) $\Rightarrow$ (2) Let $h \in H$ and $g \in G$. We have $[(h,1),(1,g)] \in H \cap G = \{1\}$. Thus $(1,g)^{-1}(h,1)(1,g) = (h,1)$. By Proposition 8.5.(vi), we have $(h^g,1) = (h,1)$. So $h^g = h$ for all $h \in H$ and $g \in G$. ■

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 $\varphi : K \to \mathrm{Aut}\, H$ 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

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

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 $\mathrm{im}\,\varphi_1$ and $\mathrm{im}\,\varphi_2$ 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 $H \rtimes_{\varphi_1} C \cong H \rtimes_{\varphi_2} C$.

Proof. There is an automorphism $\sigma \in \mathrm{Aut}(H)$ such that $\sigma^{-1}\,\mathrm{im}\,\varphi_1\sigma = \mathrm{im}\,\varphi_2$. Let x be a generator for C. Then there is some $k \in \mathbb{Z}$ such that $\sigma^{-1}\varphi_1(x)\sigma = \varphi_2(x^k)$. For every $x^\ell \in C$, we see that $\sigma^{-1}\varphi_1(x^\ell)\sigma = \varphi_2(x^{\ell k})$. Hence $\sigma^{-1}\varphi_1(y)\sigma = \varphi_2(y)^k$ for all $y \in C$. Hence we obtain

$$\begin{aligned} \mathrm{im}\,\varphi_2 &= \sigma^{-1}\,\mathrm{im}\,\varphi_1\sigma \\ &= \langle \sigma^{-1}\varphi_1(x)\sigma \rangle \\ &= \langle \varphi_2(x)^k \rangle. \end{aligned} \tag{$*$}$$

Let $\psi : H \rtimes_{\varphi_1} C \to H \rtimes_{\varphi_2} C$ be defined by

$$\psi(h, y) = (\sigma(h), y^k).$$

Let $h_1, h_2 \in H$ and $y_1, y_2 \in C$. Then

$$\begin{aligned}
\psi[(h_1, y_1)(h_2, y_2)] &= \psi(h_1\varphi_1(y_1^{-1})(h_2), y_1 y_2) \\
&= \left(\sigma(h_1)(\varphi_1(y_1^{-1})\sigma)(h_2), y_1^k y_2^k\right), \\
\psi(h_1, y_1)\psi(h_2, y_2) &= \left(\sigma(h_1), y_1^k\right)\left(\sigma(h_2), y_2^k\right) \\
&= \left(\sigma(h_1)\varphi_2(y_1^{-k})(\sigma(h_2)), y_1^k y_2^k\right) \\
&= \left(\sigma(h_1)(\sigma\varphi_2(y_1^{-k}))(h_2), y_1^k y_2^k\right) \\
&= \left(\sigma(h_1)(\varphi_1(y_1^{-1})\sigma)(h_2), y_1^k y_2^k\right).
\end{aligned}$$

Hence ψ is a homomorphism. To show that it is bijective, we consider two cases:

(i) If C is of order n, then we have $|\varphi_1(x)| = |\operatorname{im}\varphi_1| = |\operatorname{im}\varphi_2| = |\varphi_2(x)|$. Write $m = |\varphi_2(x)|$. Hence k is coprime to m, because $|\varphi_2(x)^k| = |\sigma^{-1}\varphi_1(x)\sigma| = |\varphi_1(x)| = |\varphi_2(x)| = m$. If k is not coprime to n, we let $k' = k + am$, where a is the product of all primes dividing n but not k. Then for every prime p dividing n, $p \nmid k'$. Therefore $\gcd(k', n) = 1$. Note that $\varphi_2(x)^{k'} = \varphi_2(x)^k$. So we can without loss of generality assume that $\gcd(k, n) = 1$. Then there are integers r, s for which $rk + sn = 1$. Then ψ is bijective because we have a two-sided inverse

$$\psi^{-1}(h, y) = (\sigma^{-1}(h), y^r).$$

(ii) Since C is infinite cyclic and φ_2 is injective, the image $\operatorname{im}\varphi_2$ is infinite cyclic. By $(*)$, $\varphi_2(x)^k$ is also a generator for $\operatorname{im}\varphi_2$. Thus we must have $k = \pm 1$. Hence we have a two-sided inverse

$$\psi^{-1}(h, y) = (\sigma^{-1}(h), y^k).$$ ∎

Remark. In the case of finite cyclic groups, if $\operatorname{im}\varphi_1 = \operatorname{im}\varphi_2$, then the resulting semidirect products are isomorphic.

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 $P \in \operatorname{Syl}_p(G)$ and $Q \in \operatorname{Syl}_q(G)$. 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 $\operatorname{Aut}(P) \cong \mathbb{Z}_{p-1}$ 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 $\operatorname{Aut}(P)$ 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 $\operatorname{Aut}(P)$ is cyclic it contains a unique subgroup of order q, say $\langle \gamma \rangle$. Hence any homomorphism $\varphi : Q \to \operatorname{Aut}(P)$ 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* $\ker \varphi_1 \cong \ker \varphi_2$.

Proof. Let $\theta : P \rtimes_{\varphi_1} Q \to P \rtimes_{\varphi_2} Q$ be an isomorphism. Let $G_1 = P \rtimes_{\varphi_1} Q$ and $G_2 = P \rtimes_{\varphi_2} Q$. Note that P in normal in G_1 and G_2, and hence unique in both semidirect products. The uniqueness implies that $\theta(P) = P$. Since θ is an isomorphism, we have $C_{G_1}(P) \cong C_{G_2}(\theta(P)) = C_{G_2}(P)$. Now we verify that $C_{G_1}(P) = P \ker \varphi_1$ and $C_{G_2}(P) = P \ker \varphi_2$. Clearly $P \ker \varphi_i \subseteq C_{G_1}(P)$. Let $g \in C_{G_i}(P)$. Since $g \in G_i = P \rtimes_{\varphi_1} Q$, it can be written uniquely as $g = pq$ where $p \in P$ and $q \in Q$. Hence $(pq)^{-1} x pq = x$ for all $x \in P$. Since P is abelian, we get $q^{-1} x q = x$. Since $x^q = q^{-1} x q$, we obtain $x^q = x$ for all $x \in P$, and thus $q \in \ker \varphi_i$. This proves our claim. Note that $P \cap \ker \varphi_i = \{1\}$ for $i = 1, 2$. Hence we have

$$P \times \ker \varphi_1 \cong C_{G_1}(P) \cong C_{G_2}(P) \cong P \times \ker \varphi_2.$$

Since $\ker \varphi_i$ is normal Sylow q-subgroup in $P \times \ker \varphi_i$, it is unique. Let $\psi : P \times \ker \varphi_1 \to P \times \ker \varphi_2$ be an isomorphism. Then the restriction of ψ to $\ker \varphi_1$ induces an isomorphism $\ker \varphi_1 \cong \ker \varphi_2$. ∎

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 $\varphi : Q \to \mathrm{Aut}\, P$ and identify which isomorphic types the corresponding semidirect products belong to. By the First Isomorphism Theorem, we have $Q/\ker \varphi \cong \mathrm{im}\, \varphi$. Since $\mathrm{Aut}\, P \cong \mathbb{Z}_6$ 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) $\mathbb{Z}_7 \rtimes_\varphi D_4$, $\ker\varphi \cong \langle r \,|\, r^4 = 1\rangle$;
  (11) $\mathbb{Z}_7 \rtimes_\varphi D_4$, $\ker\varphi \cong \langle r^2, s \,|\, r^4 = s^2 = 1,\ s^{-1}rs = r^{-1}\rangle$;
  (12) $\mathbb{Z}_7 \rtimes_\varphi Q_8$, $\ker\varphi \cong \langle i \,|\, i^4 = 1\rangle$;

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 3.9), $|O_P(y)| = |P| = 7$. 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 $\operatorname{im}\varphi$ and $\operatorname{im}\theta$ are of order 7, whence they are Sylow 7-subgroup of $\operatorname{Aut} Q$. 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 $(Uh)^x = Uh^x$.

Proof. (i) Trivial.

(ii) First we show that the action is well defined. If $Uh_1 = Uh_2$, then $h_1 h_2^{-1} \in U$. Since U is Q-invariant,

$$(h_1 h_2^{-1})^x = h_1^x (h_2^{-1})^x = h_1^x (h_2^x)^{-1} \in U,$$

and we have $Uh_1^x = Uh_2^x$. The rest is trivial. ∎

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

Proof. Note that for any $x \in Q$, we have

$$\begin{aligned} \varphi(x)U = U &\iff u^x \in U \text{ for all } u \in U \\ &\iff x^{-1}ux \in U \text{ for all } u \in U \\ &\iff x \in N_L(U) \end{aligned}$$

which is the desired conclusion. ■

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

Proof. We want to show that for all $q \in Q$, $N_H(U)^q = N_H(U)$. Let $x \in N_H(U)$. Then $x^{-1}Ux = U$. We write $x = (x^{q^{-1}})^q$. To prove that $x \in N_H(U)^q$, it suffices to show that $x^{q^{-1}} \in N_H(U)$. Since U is Q-invariant, we have $U^{q^{-1}} = U$. From $x^{-1}Ux = U$, we have

$$(x^{-1})^{q^{-1}} U^{q^{-1}} x^{q^{-1}} = U^{q^{-1}}.$$

Since $U^{q^{-1}} = U$ and $(x^{-1})^{q^{-1}} = (x^{q^{-1}})^{-1}$, we get

$$(x^{q^{-1}})^{-1} U x^{q^{-1}} = U.$$

Hence $x^{q^{-1}} \in N_H(U)$ and $N_H(U) \subseteq N_H(U)^q$.

Now let $x \in N_H(U)^q$. Then we have $x = y^q$ for some $y \in N_H(U)$. Since $U^q = U$, it follows that

$$x^{-1}Ux = (y^q)^{-1}U^q y^q = (y^{-1})^q U^q y^q = (y^{-1}Uy)^q = U^q = U.$$

So $N_H(U)^q \subseteq N_H(U)$. This completes the proof. ■

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 $G = N_G(S)H$.*

Proof. Let $g \in G$. Consider the conjugate $g^{-1}Sg$ by g. Since $S \subseteq H$ and $H \lhd G$, we have $g^{-1}Sg \leq g^{-1}Hg = H$. So $g^{-1}Sg$ is contained in H and $g^{-1}Sg$ is a Sylow p-subgroup of H. By the Second Sylow's Theorem (Theorem 4.9), $g^{-1}Sg$ is conjugate to S in H. Therefore there is an element h of G such that $g^{-1}Sg = h^{-1}Sh$. Let $n = gh^{-1}$. Then $n \in N_G(S)$. Since $g = nh$, we get $g \in N_G(S)H$. So 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.*

Proof. Suppose on the contrary that P is not a Sylow p-subgroup of G. By the First Sylow Theorem (Theorem 4.8), there is a Sylow p-subgroup S of G which would contain P as a proper subgroup. Hence p divides $[S : P]$. By Proposition 4.6.(ii), we have $N_S(P) \neq P$. Since $N_S(P)$ is a p-subgroup of $N_G(P)$ with order larger than $|P|$, this contradicts to the fact that P is a Sylow p-subgroup of $N_G(P)$. ■

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*

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

Proof. Since $H \cap K = \{1\}$, we can use a commutator to show that K and $N_G(K) \cap H$ commute elementwise. So, $N_G(K) \cap H \subseteq C_H(K)$. Clearly we have $C_H(K) \subseteq N_G(K) \cap H$, so the first formula holds.

By Dedekind Law (Lemma 5.17), we get

$$N_G(K) = G \cap N_G(K) = HK \cap N_G(K) = K(H \cap N_G(K)).$$

So the first formula implies the second. ■

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 $x^{-1}Hx = k^{-1}Hk$.*

Proof. Since $G = HK$, the element x of G can be written as a product $x = hk$ with $h \in H$ and $k \in K$. So we have $x^{-1}Hx = k^{-1}h^{-1}Hhk = k^{-1}Hk$. ■

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 $C_H(Q)$.

Proof. We note that, under the assumptions, the group Q is a Sylow q-subgroup of L. Assume that $|Q| = q^k$.

(i) Let S be a Sylow p-subgroup of H. Since $H \lhd L$, it follows from Lemma 8.24 that $L = N_L(S)H$. By the Second Isomorphism Theorem, we have

$$\frac{L}{H} = \frac{N_L(S)H}{H} \cong \frac{N_L(S)}{N_L(S) \cap H} = \frac{N_L(S)}{N_H(S)}$$

and so $[N_L(S) : N_H(S)] = [L : H]$. Since q does not divide $|H|$, it follows that q^k must divides $[L : H]$ and hence divides $|N_L(S)|$. By the First Sylow Theorem (Theorem 4.8), the subgroup $N_L(S)$ contains a Sylow q-subgroup Q_1 of L. By the Second Sylow Theorem (Theorem 4.9), we can find an element $x \in L$ such that $Q = x^{-1}Q_1x$. Then

$$Q = x^{-1}Q_1x \subseteq x^{-1}N_L(S)x = N_L(x^{-1}Sx).$$

By Lemma 8.22, $x^{-1}Sx$ is Q-invariant. Note that $x^{-1}Sx \subseteq x^{-1}Hx \subseteq H$ since $H \lhd L$. So $x^{-1}Sx$ is our desired Sylow p-subgroup of H.

(ii) Let P be a p-subgroup of H which is maximal among Q-invariant p-subgroups of H. We want to show that P is Sylow p-subgroup of H. By definition, the subgroup P is Q-invariant. So $N_H(P)$ is Q-invariant by Lemma 8.23. Hence Q acts on $N_H(P)/P$ by Proposition 8.21. By (i), $N_H(P)/P$ contains a Q-invariant Sylow p-subgroup $\bar{S}$. In view of the Correspondence Theorem, we let S be the subgroup of $N_H(P)$ corresponding to $\bar{S}$. Then, for any $s \in S$ and $x \in Q$, we have $\bar{s}^x \in \bar{S}^x = \bar{S}$, whence $s^x \in S$. Hence S is a Q-invariant p-subgroup of H which contains P. By the maximality, we get $P = S$. This means that P is a Sylow p-subgroup of $N_H(P)$. By Lemma 8.25, P is a Sylow p-subgroup of H.

(iii) Let S_1 and S_2 be two Q-invariant S_p-subgroups of H. By the Second Sylow Theorem (Theorem 4.9), there exists an element x of H such that $S_2 = x^{-1}S_1x$. Since both S_1 and S_2 are Q-invariant, we have $Q \subseteq N_L(S_i)$ for $i = 1, 2$ by Lemma 8.22. Since

$$x^{-1}Qx \subseteq x^{-1}N_L(S_1)x = N_L(x^{-1}S_1x) = N_L(S_2),$$

both Q and $x^{-1}Qx$ are S_q-subgroups of $N_L(S_2)$. On the other hand, $L = QH$ and Dedekind Law (Lemma 5.17) imply that

$$N_L(S_2) = L \cap N_L(S_2) = QH \cap N_L(S_2) = Q(H \cap N_L(S_2)).$$

By Lemma 8.27, there is an element y in $H \cap N_L(S_2)$ such that $Q = y^{-1}x^{-1}Qxy$. Let $z = xy$. We verify that z is an element of $C_H(Q)$. Since z normalizes Q and $x, y \in H$, we obtain $z \in N_L(Q) \cap H$. Since $N_L(Q) \cap H = C_H(Q)$ by Lemma 8.26, we

have $z \in C_H(Q)$. Therefore we get

$$z^{-1}S_1 z = y^{-1}x^{-1}S_1 xy = y^{-1}S_2 y = S_2.$$

Thus S_1 and S_2 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. 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.

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

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

$$\vartheta(\omega^g) = \vartheta(\omega)^{\chi(g)} \quad \text{for all } \omega \in \Omega, g \in G.$$

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

$$\begin{array}{ccc}
\Omega & \xrightarrow{\ g\ } & \Omega \\
{\scriptstyle\vartheta}\downarrow & & \downarrow{\scriptstyle\vartheta} \\
\Delta & \xrightarrow[\chi(g)]{} & \Delta
\end{array}$$

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.*

Proof. It is easy to see that the G-action on Δ is well defined and is permutationally isomorphic to the G-action on Ω. ■

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 $\varphi(G_\omega) = H_\delta$.

Proof. (1) $\Rightarrow$ (2) Let $(\vartheta : \Omega \to \Delta, \varphi : G \to H)$ be a permutational isomorphism. Let $\omega \in \Omega$ and $g \in G_\omega$. Then $\vartheta(\omega)^{\varphi(g)} = \vartheta(\omega^g) = \vartheta(\omega)$, and so $\varphi(g) \in H_{\vartheta(\omega)}$. Therefore $\varphi(G_\omega) \leq H_{\vartheta(\omega)}$.

On the other hand if $g_2 \in H_{\vartheta(\omega)}$ then there is some $g_1 \in G$ such that $\varphi(g_1) = g_2$. Then $\vartheta(\omega) = \vartheta(\omega)^{g_2} = \vartheta(\omega)^{\varphi(g_1)} = \vartheta(\omega^{g_1})$. Applying ϑ^{-1} we obtain $\omega = \omega^{g_1}$. Therefore $g_1 \in G_\omega$, and hence $g_2 = \varphi(g_1) \in \varphi(G_\omega)$. This shows that $\varphi(G_\omega) = H_{\vartheta(\omega)}$.

(2) $\Rightarrow$ (3) Since both G and H are transitive, $\{G_{\omega'} \mid \omega' \in \Omega\}$ and $\{H_{\delta'} \mid \delta' \in \Delta\}$ are conjugacy classes in G and H, respectively, by Proposition 3.7.(ii). Let $\varphi : G \to H$ be an isomorphism, and $\omega \in \Omega, \delta \in \Delta$ such that $\varphi(G_\omega) = H_\delta$, and let $\omega' \in \Omega$ and $\delta' \in \Delta$. Then there are $\sigma_1 \in \operatorname{Inn} G$ and $\sigma_2 \in \operatorname{Inn} H$ such that $\sigma_1(G_{\omega'}) = G_\omega$ and $\sigma_2(H_\delta) = H_{\delta'}$. If $\phi = \sigma_1 \varphi \sigma_2$ then clearly $\phi(G_{\omega'}) = H_{\delta'}$.

(3) $\Rightarrow$ (2) Let $\omega \in \Omega, \delta \in \Delta$, and $\varphi : G \to H$ be an isomorphism such that $\varphi(G_\omega) = H_\delta$. Then define $\vartheta : \Omega \to \Delta$ by $\vartheta(\omega^g) = \delta^{\varphi(g)}$ for $g \in G$. We show that ϑ is well defined. Since G is transitive, we have $\Omega = \{\omega^g \mid g \in G\}$. If $\omega^{g_1} = \omega^{g_2}$ for some $g_1, g_2 \in G$, then, $g_1 g_2^{-1} \in G_\omega$, and so $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} \in H_\delta$. Hence $\delta^{\varphi(g_1)} = \delta^{\varphi(g_2)}$, and so ϑ is well defined. Since $H = \varphi(G)$ is transitive, ϑ is surjective. For injectivity, suppose that $\vartheta(\omega^{g_1}) = \vartheta(\omega^{g_2})$ for some $g_1, g_2 \in G$, then, by the definition of ϑ, we have $\delta^{\varphi(g_1)} = \delta^{\varphi(g_2)}$ and so $\varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1 g_2^{-1}) \in H_\delta$. Thus $g_1 g_2^{-1} \in G_\omega$, and so $\omega^{g_1} = \omega^{g_2}$. Therefore ϑ is injective, and hence ϑ is a bijection.

If $\omega \in \Omega$ and $g \in G$ then there is a $g_1 \in G$ such that $\omega = \omega^{g_1}$. Then

$$\vartheta(\omega^g) = \vartheta((\omega^{g_1})^g) = \delta^{\varphi(g_1 g)} = \delta^{\varphi(g_1)\varphi(g)} = \vartheta(\omega^{g_1})^{\varphi(g)} = \vartheta(\omega)^{\varphi(g)}.$$

Thus (ϑ, φ) is a permutational isomorphism. ■

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 $g \in G_1$.*

Proof. Assume that G_1 and G_2 are permutationally isomorphic, and let $(\vartheta : \Omega \to \Omega, \varphi : G_1 \to G_2)$ be a permutational isomorphism. Then we have $\vartheta(\omega^g) = \vartheta(\omega)^{\varphi(g)}$ for all $g \in G_1$ and $\omega \in \Omega$, i.e., $\omega^g = \vartheta^{-1}(\vartheta(\omega)^{\varphi(g)})$. This shows that $\vartheta^{-1}g\vartheta = \varphi(g)$, and so G_1 is conjugate to $\varphi(G_1) = G_2$.

Suppose conversely that $\vartheta \in \operatorname{Sym}\Omega$ such that $\vartheta^{-1}G_1\vartheta = G_2$ and let $\varphi : G_1 \to G_2$ be the isomorphism defined by $\varphi(g) = \vartheta^{-1}g\vartheta$. Then $\vartheta(\omega)^{\varphi(g)} = \vartheta(\omega)^{\vartheta^{-1}g\vartheta} = \vartheta((\vartheta^{-1}(\vartheta(\omega)))^g) = \vartheta(\omega^g)$ for $g \in G$ and $\omega \in \Omega$. Hence (ϑ, φ) is a permutational isomorphism. ■

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 3.28, 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}.*

Proof. Since G is transitive, we have $\omega^G = \Omega$. Let $\vartheta : \Omega \to \Gamma_{G_\omega}$ be the bijective function as defined in Lemma 3.8.(ii). Then $\vartheta((\omega^g)^h) = \vartheta(\omega^{gh}) = G_\omega gh = (G_\omega g)^h = \vartheta(\omega^g)^h$. This shows that $(\vartheta, \mathrm{Id}_G)$ is a permutational isomorphism. ■

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 $G = G_\omega H$.*

Proof. ($\Rightarrow$) Since H is transitive, for every $g \in G$, there exists $h \in H$ such that $\omega^g = \omega^h$. By Proposition 9.5, we get $G_\omega g = G_\omega h$. Hence we can write $gh^{-1} = g' \in G$ and thus $g = g'h \in G_\omega H$.

($\Leftarrow$) Reverse the argument in the previous paragraph. ■

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**.

Definition 9.8. 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.

Proposition 9.9. *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) Let Σ be a system of imprimitivity and let $\Delta \in \Sigma$. Then $\Sigma = \{\Delta^g \mid g \in G\}$. In particular, $|\Delta^g| = |\Delta|$.

(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.

Proof. ■

Definition 9.10. 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 9.11. *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.

Proof. ■

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.*

Proof. Let Δ be a block containing $\omega \in \Omega$, and consider the set $H_\Delta = \{g \in G \mid \omega^g \in \Delta\}$. We claim that H_Δ is a subgroup of G. Clearly, $e \in H_\Delta$. Let $g, g' \in H_\Delta$. Since ω and ω^g both lie in Δ, we see that $\Delta^g \cap \Delta \neq \emptyset$ and hence that $\Delta^g = \Delta$. Now we have $\omega^{gg'} = (\omega^g)^{g'} \in \Delta^{g'} = \Delta$ and hence $gg' \in H_\Delta$. Also, for $g \in H_\Delta$ we have $\omega^g \in \Delta$. Since ω is also in Δ, this means $\Delta \cap \Delta^g \neq \emptyset$, which implies $\Delta^g = \Delta$. Acting on both sides by g^{-1}, we get $\Delta^{g^{-1}} = (\Delta^g)^{g^{-1}} = \Delta$. Since $\omega \in \Delta$, it follows that $\omega^{g^{-1}} \in \Delta^{g^{-1}} = \Delta$, and hence $g^{-1} \in H_\Delta$. Therefore H_Δ is a subgroup of G.

Observe that $G_\omega \leq H_\Delta$ since for any $s \in G_\omega$, we have $\omega^s = \omega \in \Delta$. Let Σ be the set of blocks of Ω containing ω and let $\mathcal{H}$ be the set of subgroups containing G_ω. Let $\theta : \Sigma \to \mathcal{H}$ be the function defined by $\theta(\Delta) = H_\Delta$. We claim that θ is bijective.

Let Δ and Δ' be distinct blocks in Σ. Without loss of generality assume that $\Delta' \not\subseteq \Delta$. Then there exists some $\delta \in \Delta'$ with $\delta \notin \Delta$. Since G acts transitively on Ω, there exists some $g \in G$ such that $\omega^g = \delta$. So $g \in H_{\Delta'}$. Since $\delta \notin \Delta$, we have $g \notin H_\Delta$, and hence $H_\Delta \neq H_{\Delta'}$. This shows that θ is injective.

Let $H \in \mathcal{H}$. Consider the subset $C = \{\omega^h \mid h \in H\}$ of Ω. We show that C is a block. Clearly C is non-empty and $C^g = C$ for each $g \in H$. Let $g \in G$ be such that $C^g \cap C \neq \emptyset$. Then there exist $h_1, h_2 \in H$ such that $(\omega^{h_1})^g = \omega^{h_2}$. This gives $\omega^{h_1 g} = \omega^{h_2}$, so $\omega^{h_1 g h_2^{-1}} = \omega$. Hence $h_1 g h_2^{-1} \in G_\omega \leq H$, and thus $g \in H$. Consequently $C^g = C$. Therefore C is a block. Note that $\theta(C) = H_C = \{g \in G \mid \omega^g \in C\}$. Clearly $H \leq H_C$. Let $g \in H_C$. Then $\omega^g = \omega^h$ for some $h \in H$. Hence $\omega^{gh^{-1}} = \omega$ and thus $gh^{-1} \in G_\omega \leq H$, giving $g \in H$. So $\theta(C) = H$, which shows that θ is surjective. ■

Remark. This correspondence is order-preserving, i.e., if Δ_1, Δ_2 are blocks of Ω containing ω, then $\Delta_1 \subseteq \Delta_2$ if and only if $\theta(\Delta_1) \subseteq \theta(\Delta_2)$. Indeed $\Delta_1 \subseteq \Delta_2$ implies that $\omega^g \in \Delta_1 \subseteq \Delta_2$ for all $g \in H_{\Delta_1}$. Conversely, suppose that $H_{\Delta_1} \leq H_{\Delta_2}$. Let $\delta \in \Delta_1$. So there exists $g \in G$ such that $\delta = \omega^g$. This implies $g \in H_{\Delta_1} \subseteq H_{\Delta_2}$. So $\delta = \omega^g \in \Delta_2$. This shows that θ is order-preserving.

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

Proof. Suppose G is primitive on Ω. Let $\omega \in \Omega$. Since G is primitive, there are two blocks containing ω, namely $\{\omega\}$ and Ω. By Proposition 9.13, there are only two subgroups of G containing G_ω, namely G_ω and G. So there is no proper subgroup of G which properly contains G_ω. Therefore G_ω is maximal in G.

Conversely, suppose that every stabilizer is a maximal subgroup. Fix $\omega \in \Omega$. Then there are only two subgroups of G containing G_ω, namely G_ω and G. By Proposition 9.13, we only have two such blocks $\{\omega\}$ and Ω. Consequently, Ω can have no other blocks besides itself and its singletons, and so Ω is primitive. ■

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 $\operatorname{Sym} \Gamma_H$.

Proof. ■

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 $C = 1$.

Proof. ■

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 $\beta \in \Omega$.*

Proof. Let $\sigma \in \operatorname{im} \Psi$, so $\sigma = \Psi(x)$ for some $x \in N$. Then $(G_\alpha)^\sigma = x^{-1} G_\alpha x = G_\beta$ where $\beta = \alpha^x$. Conversely, suppose that $(G_\alpha)^\sigma = G_\beta$ for some $\beta \in \Omega$. Then the two transitive permutation representations of G into $\operatorname{Sym} \Omega$ given by $x \mapsto x$ and $x \mapsto x^\sigma$ are equivalent because G_β is a point stabilizer for each of them. This means that for some $t \in \operatorname{Sym} \Omega$ we have $xt = tx^\sigma$ for all $x \in G$. Clearly $t \in N$. Hence $\sigma = \Psi(t) \in \operatorname{im} \Psi$ as required. ■

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 $\operatorname{Hol} G$.*

Proof. Since G is regular, therefore $G_\alpha = 1$, and so $\operatorname{im}\Psi = \operatorname{Aut} G$ by theorem xxx. The centralizer C of G in $\operatorname{Sym}(\Omega)$ is regular and isomorphic to G by Theorem 4.2A, and therefore $N = CN_\alpha$ with $C \triangleleft N$ and $C \cap N_\alpha = 1$. Hence $\operatorname{Aut} G = \operatorname{im}\Psi \cong N/\ker\Psi = N/C \cong N_\alpha$. Finally, because G is regular and normal in N, therefore $G \cap N_\alpha = 1$ and $N = GN_\alpha \cong G \rtimes \operatorname{Aut} G$. ■

Main References. [PS18; DM96; Cam99]

10 Wreath Products

We will always consider right actions in this section. This is probably influenced by FAR-RIGHT mathematicians.

10.1 Construction and Basic Properties

Let G be an arbitrary group and let H be a group acting on a set Δ. Let G^Δ be the group of all functions from Δ into G with pointwise multiplication. In other words, G^Δ is isomorphic to a direct product of copies of G indexed by Δ. Now we define an action of H on G^Δ by

$$f^h(\delta) = f(\delta^{h^{-1}}).$$

Definition 10.1. The semidirect product $W = G^\Delta \rtimes H$ with respect to the action defined above is called the **(complete) wreath product** of G by H. This W will be denoted by $G \operatorname{Wr}_\Delta H$. We can define the **restricted wreath product** $G \operatorname{wr}_\Delta H$ of G by H, by using the same setting, but with $f \in G^{(\Delta)}$, where $G^{(\Delta)}$ is the set of all functions such that $f(y) = e$ for all but finitely many $y \in \Delta$. The wreath product is said to be **trivial** if either G or H is the trivial group. In $G \operatorname{Wr}_\Delta H$ (resp. $G \operatorname{wr}_\Delta H$), the subgroup G^Δ (resp. $G^{(\Delta)}$) is called the **base group**, G is called the **bottom group** and H is called the **top group**.

Remark. Let us restrict to the case where Δ is a finite set. If $\Delta = \{1, \ldots, n\}$, then we can think of the base group as

$$G^\Delta = \underbrace{G \times \cdots \times G}_{n \text{ times}}.$$

So the elements of the base group are just an n-tuples of elements in G. Now the action of H on the base group corresponds to permuting coordinates of elements in G as follows.

$$(g_1, g_2, \ldots, g_n)^h = (g_{1^{h^{-1}}}, g_{2^{h^{-1}}}, \ldots, g_{n^{h^{-1}}}).$$

Note that it is necessary to introduce h^{-1} rather than h since we are considering right action.

Definition 10.2. The **standard wreath product** $G \operatorname{Wr} H$ (or $G \operatorname{wr} H$) of G by H is the wreath product $G \operatorname{Wr}_H H$ (or $G \operatorname{wr}_H H$) where G and H act on themselves by right translation.

10.2 Imprimitive Action

Proposition 10.3. *Let (G, Ω) and (H, Δ) be permutation groups. Then $G \operatorname{Wr}_\Delta H$ (resp. $G \operatorname{wr}_\Delta H$) acts on $\Omega \times \Delta$ via*

$$(\omega, \delta)^{(f,h)} = (\omega^{f(\delta)}, \delta^h).$$

Proof. Let $(\omega, \delta) \in \Omega \times \Delta$. Clearly $(\omega, \delta)^{(1,1)} = (\omega^{1(\delta)}, \delta^1) = (\omega^1, \delta) = (\omega, \delta)$. Let $f_1, f_2 \in G^\Delta$ and $h_1, h_2 \in H$. Then

$$\begin{aligned}
((\omega, \delta)^{(f_1,h_1)})^{(f_2,h_2)} &= (\omega^{f_1(\delta)}, \delta^{h_1})^{(f_2,h_2)} \\
&= ((\omega^{f_1(\delta)})^{f_2(\delta^{h_1})}, (\delta^{h_1})^{h_2}) \\
&= (\omega^{f_1(\delta) f_2(\delta^{h_1})}, \delta^{h_1 h_2}), \\
(\omega, \delta)^{(f_1,h_1)(f_2,h_2)} &= (\omega, \delta)^{(f_1 f_2^{h_1^{-1}}, h_1 h_2)} \\
&= (\omega^{(f_1 f_2^{h_1^{-1}})(\delta)}, \delta^{h_1 h_2}) \\
&= (\omega^{f_1(\delta) f_2^{h_1^{-1}}(\delta)}, \delta^{h_1 h_2}) \\
&= (\omega^{f_1(\delta) f_2(\delta^{h_1})}, \delta^{h_1 h_2}).
\end{aligned}$$

So $((\omega, \delta)^{(f_1,h_1)})^{(f_2,h_2)} = (\omega, \delta)^{(f_1,h_1)(f_2,h_2)}$. This shows that $G \operatorname{Wr}_\Delta H$ acts on $\Omega \times \Delta$ with respect to this action. ■

Definition 10.4. The action defined in Proposition 10.3 is called the **imprimitive action** of $G \operatorname{Wr}_\Delta H$.

Proposition 10.5. *Let G and H act on Ω and Δ respectively.*

(i) The set $\Omega \times \Delta$ is a transitive $G \operatorname{Wr}_\Delta H$-set if and only if both X and Δ are transitive sets.

(ii) $G \operatorname{Wr}_\Delta H$ acts faithfully on $\Omega \times \Delta$ if and only if both actions are faithful.

(iii) If $|\Omega|, |\Delta| \geq 2$, then the action of $G \operatorname{Wr}_\Delta H$ on $\Omega \times \Delta$ is imprimitive.

(iv) In this form the wreath product is associative in the sense that, if K acts on Γ, then the action of $(G \operatorname{Wr}_\Delta H) \operatorname{Wr}_\Gamma K$ on $\Omega \times \Delta \times \Gamma$ is permutationally isomorphic to the action of $G \operatorname{Wr}_{\Delta \times \Gamma} (H \operatorname{Wr}_\Gamma K)$ on $\Omega \times \Delta \times \Gamma$.

Proof. ■

Theorem 10.6 (Embedding Theorem)**.** *Let G act transitively on Ω. Let $\mathcal{B} = \{\Omega_\lambda \mid \lambda \in \Lambda\}$ be a system of imprimitivity of Ω. Fix a block $\Omega_\iota \in \mathcal{B}$ and let $\phi : G \to \operatorname{Sym}\mathcal{B}$ be the induced representation of G on $\mathcal{B}$. Then (G, Ω) is permutationally embedded into $(G_{\Omega_\iota} \operatorname{Wr}_{\mathcal{B}} \phi(G), \Omega_\iota \times \mathcal{B})$.*

Proof. Since G acts transitively on $\mathcal{B}$, for each $\Omega_\lambda \in \mathcal{B}$ we choose an element $g_\lambda \in G$ such that $\Omega_\lambda = \Omega_\iota^{g_\lambda}$. Define $\vartheta : \Omega \to \Omega_\iota \times \mathcal{B}$ by

$$\vartheta(\omega) = (\omega^{g_\lambda^{-1}}, \Omega_\lambda)$$

where $\omega \in \Omega_\lambda$. Clearly ϑ is well-defined. We claim that ϑ is a bijection. Suppose that $\vartheta(\omega_1) = \vartheta(\omega_2)$ for some $\omega_1, \omega_2 \in \Omega$. Then $\omega_1, \omega_2 \in \Omega_\lambda$ for some $\Omega_\lambda \in \mathcal{B}$ and $\omega_1^{g_\lambda^{-1}} = \omega_2^{g_\lambda^{-1}}$. Thus we get $\omega_1 = \omega_2$ and ϑ is injective. Let $(\omega, \Omega_\lambda) \in \Omega_\iota \times \mathcal{B}$. Take the unique element $\delta \in \Omega$ such that $\delta = \omega^{g_\lambda}$. Then, by definition, ϑ is surjective.

Let $\psi : G \to G_{\Omega_\iota} \operatorname{Wr}_{\mathcal{B}} \phi(G)$ be defined by

$$\psi(x) = (f_x, \phi(x))$$

where f_x is a function from $\mathcal{B}$ into G_{Ω_ι} with $f_x(\Omega_\lambda) = g_\lambda x g_{\lambda^x}^{-1}$ where g_{λ^x} is the element corresponding to Ω_λ^x It can be checked that $\Omega_\iota^{g_\lambda x g_{\lambda^x}^{-1}} = \Omega_\iota$ and so $g_\lambda x g_{\lambda^x}^{-1} \in G_{\Omega_\iota}$. We claim that ψ is a monomorphism. Clearly ψ is injective, because $x \in \ker\psi$ implies that $x = g_\iota^{-1} 1 g_{\iota^x} = g_\iota^{-1} 1 g_\iota = 1$. Now we show that ψ is a homomorphism. Let $x, y \in G$. Then $\psi(x)\psi(y) = (f_x, x)(f_y, y) = (f_x f_y^{x^{-1}}, xy)$. Note that for all $\Omega_\lambda \in \mathcal{B}$,

$$\begin{aligned}
(f_x f_y^{x^{-1}})(\Omega_\lambda) &= f_x(\Omega_\lambda) f_y^{x^{-1}}(\Omega_\lambda) \\
&= f_x(\Omega_\lambda) f_y(\Omega_\lambda^x) \\
&= g_\lambda x g_{\lambda^x}^{-1} g_{\lambda^x} y g_{(\lambda^x)^y}^{-1} \\
&= g_\lambda x y g_{\lambda^{xy}}^{-1} \\
&= f_{xy}(\Omega_\lambda).
\end{aligned}$$

So $\psi(x)\psi(y) = \psi(xy)$. Next, we want to prove

$$\vartheta(\omega^x) = \vartheta(\omega)^{\psi(x)}$$

for all $\omega \in \Omega$ and $x \in G$.

$$\begin{aligned}
\vartheta(\omega)^{\psi(x)} &= (\omega^{g_\lambda^{-1}}, \Omega_\lambda)^{(f_x, x)} \\
&= ((\omega^{g_\lambda^{-1}})^{f_x(\Omega_\lambda)}, \Omega_\lambda^x)
\end{aligned}$$

$$
\begin{aligned}
&= ((\omega^{g_\lambda^{-1}})^{g_\lambda x g_{\lambda^x}^{-1}}, \Omega_\lambda^x) \\
&= ((\omega^x)^{g_{\lambda^x}^{-1}}, \Omega_\lambda^x) \\
&= \vartheta(\omega^x).
\end{aligned}
$$

This shows that (ϑ, ψ) is a permutational embedding. ■

Corollary 10.7 (Kaluzhnin–Krasner Embedding Theorem)**.** *Let G be a group and let N be a subgroup of G. Let H be the permutation group induced by G on the set of right cosets. Then G is embedded into $N \operatorname{Wr} H$. If N is normal in G, then G is embedded into $N \operatorname{Wr} G/N$.*

Proof. Apply Theorem 10.6 using the right regular action. ■

10.3 Product Action

Proposition 10.8. *Let (G, Ω) and (H, Δ) be permutation groups. Then $G \operatorname{Wr}_\Delta H$ (resp. $G \operatorname{wr}_\Delta H$) acts on Δ^Ω via*

$$
\varphi^{(f,h)}(\delta) = \varphi(\delta^{h^{-1}})^{f(\delta^{h^{-1}})}.
$$

Proof. Let $\varphi \in \Delta^\Omega$ and let $\delta \in \Delta$. Clearly $\varphi^{(1,1)}(\delta) = \varphi(\delta^1)^{1(\delta^1)} = \varphi(\delta)^1 = \varphi(\delta)$. Let $f_1, f_2 \in G^\Delta$ and $h_1, h_2 \in H$. Then

$$
\begin{aligned}
(\varphi^{(f_1,h_1)})^{(f_2,h_2)}(\delta) &= \varphi^{(f_1,h_1)}(\delta^{h_2^{-1}})^{f_2(\delta^{h_2^{-1}})} \\
&= \big(\varphi\big((\delta^{h_2^{-1}})^{h_1^{-1}}\big)^{f_1((\delta^{h_2^{-1}})^{h_1^{-1}})}\big)^{f_2(\delta^{h_2^{-1}})} \\
&= \big(\varphi\big(\delta^{(h_1h_2)^{-1}}\big)^{f_1(\delta^{(h_1h_2)^{-1}})}\big)^{f_2(\delta^{h_2^{-1}})} \\
&= \varphi\big(\delta^{(h_1h_2)^{-1}}\big)^{f_1(\delta^{(h_1h_2)^{-1}})f_2(\delta^{h_2^{-1}})}, \\
\varphi^{(f_1,h_1)(f_2,h_2)}(\delta) &= \varphi^{(f_1 f_2^{h_1^{-1}}, h_1h_2)}(\delta) \\
&= \varphi\big(\delta^{(h_1h_2)^{-1}}\big)^{(f_1 f_2^{h_1^{-1}})(\delta^{(h_1h_2)^{-1}})} \\
&= \varphi\big(\delta^{(h_1h_2)^{-1}}\big)^{f_1(\delta^{(h_1h_2)^{-1}})f_2^{h_1^{-1}}(\delta^{(h_1h_2)^{-1}})} \\
&= \varphi\big(\delta^{(h_1h_2)^{-1}}\big)^{f_1(\delta^{(h_1h_2)^{-1}})f_2((\delta^{(h_1h_2)^{-1}})^{h_1})} \\
&= \varphi\big(\delta^{(h_1h_2)^{-1}}\big)^{f_1(\delta^{(h_1h_2)^{-1}})f_2((\delta^{h_2^{-1}})}.
\end{aligned}
$$

So $(\varphi^{(f_1,h_1)})^{(f_2,h_2)} = \varphi^{(f_1,h_1)(f_2,h_2)}$. This shows that $G \operatorname{Wr}_\Delta H$ acts on Δ^Ω with respect to this action. ■

Definition 10.9. The action defined in Proposition 10.8 is called the **product action** of $G \operatorname{Wr}_\Delta H$.

Main References. [Mel95; PS18; DM96]

11 O'Nan-Scott Theorem: The Classification of Maximal Subgroups of Symmetric Groups

11.1 Classes of Groups

11.1.1 Intransitive Groups

11.1.2 Transitive Imprimitive Groups

11.1.3 Primitive Wreath Products

11.1.4 Affine Groups

11.1.5 Diagonal Groups

11.1.6 Almost Simple Groups

11.2 Main Result

Theorem 11.1 (O'Nan-Scott Theorem)**.** *If H is any proper subgroup of S_n other than A_n, then H is a subgroup of one or more of the following subgroups:*

(i) an intransitive group $S_k \times S_m$, where $n = k + m$;

(ii) a transitive imprimitive group $S_k \operatorname{wr} S_m$, where $n = km$;

(iii) a primitive wreath product, $S_k \operatorname{wr} S_m$, where $n = k^m$;

(iv) an affine group $AGL_d(p) \cong p^d : GL_d(p)$, where $n = p^d$;

(v) a group of shape $T^m.(Out(T) \times S_m)$, where T is a non-abelian simple group, acting on the cosets of a subgroup $Aut(T) \times S_m$, where $n = |T|^{m-1}$;

(vi) an almost simple group acting on the cosets of a maximal subgroup of index n.

Main References. [Wil09; Cam99; Smi18; LPS88; AS85]

12 Solvable and Nilpotent Groups

12.1 Solvable Groups

Definition 12.1. A group G is said to be **solvable** if there exists a normal series

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

such that G_{i+1}/G_i is abelian for $0 \leq i < n$.

We give a characterization of solvability is in terms of the "derived series".

Recall that the commutator subgroup $[G, G]$ of G is the subgroup generated by all commutators $[x, y] = xyx^{-1}y^{-1}$ for $x, y \in G$. It is the unique smallest normal subgroup of G such that the corresponding quotient group is abelian.

Let $G^{(0)} = G$ and general, $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$ for $n > 0$. Clearly $G^{(i)} \geq G^{(i+1)}$ and we can use induction to show that $G^{(i)} \lhd G$ for all i. Hence $G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \cdots$ constitutes the **derived series** of G.

Theorem 12.2. *A group G is solvable if and only if $G^{(n)} = \{e\}$ for some integer n.*

Proof. If $G^{(n)} = \{e\}$ for some integer n, then the derived series

$$\{e\} = G^{(n)} \leq G^{(n-1)} \leq \cdots \leq G^{(1)} \leq G^{(0)} = G$$

shows that G is solvable.

Conversely, suppose G is solvable. Then we have subgroups $G_i \lhd G$ with

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

and such that G_{i+1}/G_i is abelian for $0 \leq i < n$. Thus $[G_{i+1}, G_{i+1}] \subseteq G_i$ for all i by the definition of commutator subgroups. In particular, $G^{(1)} = [G_n, G_n] \subseteq G_{n-1}$. Inductively, we obtain $G^{(i)} \subseteq G_{n-i}$ for $0 \leq i \leq n$. Consequently, $G^{(n)} \subseteq G_0 = \{e\}$. ∎

Corollary 12.3. *Subgroups and quotient groups of solvable groups are solvable.*

Proof. Let G be a solvable group. Then for some n we have $G^{(n)} = \{e\}$.

Let H be a subgroup of G. Then we have $H^{(k)} \subseteq G^{(k)}$ for all k (using induction), and hence H is solvable.

If $N \lhd G$, then the canonical projection $\rho : G \to G/N$ yields that $(G/N)^{(k)} = \varphi(G^{(k)})$ for all k, and so $(G/N)^{(n)} = \varphi(G^n) = \{e\}$. ∎

Proposition 12.4. *If G and H are solvable groups, then $G \rtimes H$ is solvable.*

Proof. BRUH ■

Theorem 12.5. *Let*

$$\{e\} = H_0 < H_1 < \cdots < H_n = G$$

be a composition series for G. Then G is solvable if and only if each composition factor H_{i+1}/H_i has prime order.

Proof. Assume that G is solvable. Then each composition factor H_{i+1}/H_i is solvable by Corollary 12.3. Since these factors are simple, it suffices to show that a solvable simple group must have prime order. If G is a solvable simple group, then $[G, G] = \{e\}$ (we cannot have $[G, G] = G$ by Theorem 12.2) and G is abelian. It follows from Proposition 5.4 that simple abelian groups have prime order.

Conversely, assume that the composition factors have prime order. These factors H_{i+1}/H_i are abelian since every group of prime order is cyclic. Therefore $G^{(i)} \subseteq H_{n-i}$ for all i by induction. It follows that $G^{(n)} = \{e\}$ and G is solvable. ■

Definition 12.6. Let G be a solvable group. The **derived length** $\mathrm{dl}(G)$ of G is the smallest integer n such that $G^{(n)} = \{e\}$.

Corollary 12.7. *Let N be a normal subgroup of a group G. Then G is solvable if and only if both N and G/N are solvable. Moreover,*

$$dl(G) \leq dl(N) + dl(G/N).$$

Proof. The group G is solvable implies that N and G/N are solvable by Corollary 12.3.

Conversely, assume that both N and G/N are solvable. Let $\mathrm{dl}(N) = n$ and $\mathrm{dl}(G/N) = m$. Let $\rho : G \to G/N$ be the canonical projection. Since $\rho(G^{(m)}) = (G/N)^{(m)} = \{e\}$, we get $G^{(m)} \subseteq \ker \rho = N$. Thus $G^{(m+n)} = (G^{(m)})^{(n)} \subseteq N^{(n)} = 1$, and the result follows. ■

12.2 Nilpotent Groups

Definition 12.8. A group G is said to be **nilpotent** if there exists a normal series

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

such that

$$G_{i+1}/G_i \subseteq Z(G/G_i)$$

for $0 \leq i < n$.

The series above is also called a **central series** for a group G. In general, how can we generate a central series for G? One way to do this is by using some of the existing tools:

(1) The center of a group is always a normal subgroup of the group, and hence we can always find a quotient group.

(2) The Correspondence Theorem helps us to find a normal subgroup of a group corresponding to a subgroup of its quotient group.

Let G be a group. The center $Z_1(G) = Z(G)$ of G is a normal subgroup. Let $Z_2(G)$ be the subgroup of G corresponding to $Z(G/Z_1(G))$, i.e., $Z_2(G)/Z_1(G) = Z(G/Z(G))$. The Correspondence Theorem shows that $Z_1(G) \lhd Z_2(G) \lhd G$. Continue this process by defining inductively: $Z_i(G)$ is the subgroup of G corresponding to $Z(G/Z_{i-1}(G))$, i.e., $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$. This leads to the following definition.

Definition 12.9. The **ascending central series** of a group G is a sequence of normal subgroups of G given by

$$\langle e \rangle \leq Z_1(G) \leq Z_2(G) \leq \cdots .$$

Clearly if $Z_n(G) = G$ for some integer n, then G is nilpotent. The converse of this statement is also true. Before proving the converse, we shall introduce the descending central series. Let $G^0 = G$ and $G^i = [G^{i-1}, G]$ for $i \geq 1$. Note that G_i is a subgroup of G_{i-1}. This is proved by using the fact that if $H \subseteq K \subseteq G$, then $[H, G] \subseteq [K, G]$. Also, we can induction to show that $G^i \lhd G$ for all i. It remains to show that $G_{i-1}/G_i \subseteq Z(G/G^i)$ for all i. We show it by using a lemma below.

Lemma 12.10. *Let G be a group. Let X be a subgroup of G and let Y be a normal subgroup of G. Then $[X, G] \subseteq Y$ if and only if $XY/Y \subseteq Z(G/Y)$.*

Proof. Consider the canonical projection $G \to G/Y$. ■

Set $X = G^{i-1}$ and $Y = G^i$. Then we are done. So the following definition makes sense.

Definition 12.11. The **descending central series** of a group G is a sequence of normal subgroups of G given by

$$G = G^0 \geq G^1 \geq G^2 \geq \cdots .$$

Theorem 12.12. *Let G be a group. Then G is nilpotent if and only if $Z_n(G) = G$ for some integer n.*

Proof. If $Z_n(G) = G$, then G is nilpotent.

Conversely, suppose that G is nilpotent. Let $\{e\} = N_0 \leq \cdots \leq N_k = G$ be a central series for G. We write $Z_i = Z_i(G)$ and show that $N_i \subseteq Z_i$ for all i. This certainly holds for $i = 0$. We prove by induction. Assume that $N_i \subseteq Z_i$ for some $i \geq 0$. Since $N_{i+1}/N_i \subseteq Z(G/N_i)$, by Lemma 12.10, we have $[N_{i+1}, G] \subseteq N_i \subseteq Z_i$. So applying Lemma 12.10 again gives

$$N_{i+1}Z_i/Z_i \subseteq Z(G/Z_i) = Z_{i+1}/Z_i.$$

Hence $N_{i+1} \subseteq Z_{i+1}$. It follows that $Z_k(G) = G$. ■

Corollary 12.13. *Let G be any group and suppose $n \geq 1$. Then $G^n = \{e\}$ if and only if $Z_n(G) = G$.*

Proof. Suppose that $G^n = \{e\}$. Let $G = G^0 \geq G^1 \geq \cdots \geq G^{n-1} \geq G^n = \{e\}$ be the descending central series of G. If we let $N_i = G^{n-i}$ in the proof of Theorem 12.12, then we see that $G^{n-i} \subseteq Z_i(G)$ for all i. In particular, $G = G^0 = Z_n(G)$.

Suppose that $Z_n(G) = G$. Let $\{e\} = Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_n(G) = G$ be the ascending central series for G. Write $Z_i = Z_i(G)$. Since $Z_{i+1}/Z_i = Z(G/Z_i)$, it follows from Lemma 12.10 that $[Z_{i+1}, G] \subseteq Z_i$ for all i. Note that $G^i \subseteq Z_{k-i}$ and so $G^n = Z_0 = \{e\}$. ■

Corollary 12.14. *Subgroups and quotient groups of nilpotent groups are nilpotent.*

Proof. Since G is nilpotent, we have $G^n = \{e\}$ for some integer n by Theorem 12.12 and Corollary 12.13.

If $H \subseteq G$, then $H^n \subseteq G^n$and so $H^n = \{e\}$.

To prove the result for quotient groups, let $N \lhd G$ and let $\rho : G \to G/N$ be the canonical projection. Then $\rho(G^n) = (G/N)^n$. Therefore we have $(G/N)^n = \rho(\{e\}) = \{e\}$. ■

Lemma 12.15. *Let G be a group. Then $G^{(k)} \subseteq G^k$ for all $k \geq 1$.*

Proof. Use induction and note that $G^{(k+1)} = [G^{(k)}, G^{(k)}] \subseteq [G^{(k)}, G] = G^{k+1}$. ■

This immediately yields the following consequence.

Proposition 12.16. *Every nilpotent group is solvable.*

Proof. Trivial. ■

Definition 12.17. Let G be a nilpotent group. The smallest integer n such that $Z_n(G) = G$ is called the **class** of G.

Proposition 12.18. *Let G be a nilpotent group of class n. Then the following propositions holds.*

(i) We have $G^n = \{e\}$. If $n \neq 0$, then $G^{n-1} \neq \{e\}$.

(ii) Any central series of G has at least $n+1$ terms, and there is a central series with exactly $n+1$ terms.

(iii) The quotient group $G/Z(G)$ is a nilpotent group of class $n-1$. The converse is also true.

Remark. We can remember the proposition above using the following diagram:

$$\begin{array}{ccccccccccc}
G & = & Z_n(G) & \geq & Z_{n-1} & \geq & \cdots & \geq & Z_0(G) & = & \{e\} \\
 & & \| & & \cup & & & & \| & & \\
G & = & G_n & \geq & G_{n-1} & \geq & \cdots & \geq & G_0 & = & \{e\} \\
 & & \| & & \cup & & & & \| & & \\
G & = & G^0 & \geq & G^1 & \geq & \cdots & \geq & G^n & = & \{e\}
\end{array}$$

Proposition 12.19. *Let H be a nilpotent group of class c, and let K be nilpotent of class d. Then the direct product $H \times K$ is a nilpotent group of class e, where $e = \max\{c, d\}$.*

Proof. If any one of the groups is $\{e\}$, then it is trivial. So we may assume that $H \neq \{e\}$, $K \neq \{e\}$, and $c \geq d > 0$.

We prove by induction on c. If $c = 1$, then $Z(H) = Z_1(H) = H$. This implies that both H and K are abelian. So the direct product $H \times K$ is also abelian and hence is a nilpotent group of class 1. Suppose that $c > 1$. Let $G = H \times K$. By Corollary 6.10, we have $Z(G) = Z(H) \times Z(K)$. By Proposition 6.11, we obtain

$$G/Z(G) = (H/Z(H)) \times (K/Z(K)).$$

In view of Proposition 12.18.(iii), the class of the nilpotent group $H/Z(H)$ is $c-1$. By the inductive hypothesis, $G/Z(G)$ is a nilpotent group of class $c-1$. By Proposition 12.18.(iii), we conclude that G is a nilpotent group of class c. ■

Corollary 12.20. *The direct product of a finite number of nilpotent groups is nilpotent.*

12.3 Examples

12.3.1 Triangular Matrices

Example 12.21. Let $\mathrm{GL}(n, \mathbb{F})$ be the group of $n \times n$ invertible matrices over a field $\mathbb{F}$ under matrix multiplication. Consider the following subgroups of $\mathrm{GL}(n, \mathbb{F})$.

$$T = \{(a_{ij}) \in \mathrm{GL}(n, \mathbb{F}) \,|\, a_{ij} = 0 \text{ for } j - i < 0 \text{ and } a_{ii} \neq 0 \text{ for } 1 \leq i \leq n\},$$
$$U = \{(a_{ij}) \in T \,|\, a_{ii} \neq 0 \text{ for } 1 \leq i \leq n\}.$$

Then T is a solvable group, and U is a nilpotent group.

Example 12.22. Let V be an n-dimensional vector space over a field $\mathbb{F}$. Let

$$V = V_0 \geq V_1 \geq \cdots \geq V_n = \{0\}$$

be a chain of subspaces such that $\dim V_i/V_{i+1} = 1$ for $0 \leq i < n$. For convenience, if $m > n$, then we set $V_m = \{0\}$. Let $\mathrm{GL}(V)$ be the group of vector space automorphisms of V. For each integer $r \geq 1$, we define

$$U_r = \{x \in \mathrm{GL}(V) \,|\, (x - 1)(V_i) \subseteq V_{i+r} \text{ for all } i\}.$$

where $1 \in \mathrm{GL}(V)$ is the identity map. It can be checked that:

(i) each U_r is a subgroup;

(ii) $U_1 \geq U_2 \geq \cdots \geq U_n = \{1\}$;

(iii) U_r is closed under multiplication;

(iv) U_r is closed under inverses.

Let $x, y \in U_r$. Then

$$(xy - 1)(V_i) = ((x - 1)y)(V_i) + (y - 1)(V_i) \subseteq V_{i+r}$$

and so U_r is closed under multiplication. Assume that $x = 1 - X \in U_r$, where $X \in \mathrm{End}_{\mathbb{F}}(V)$ is an vector space endomorphism with $X^n = 0$. Then we have

$$x^{-1} = (1 - X)^{-1} = \sum_{k=0}^{n-1} X^k = 1 + X \sum_{k=1}^{n-1} X^{k-1} \in U_r,$$

which shows that U_r is closed under inverses.

Now we claim that for all r, s, we have $[U_r, U_s] \subseteq U_{r+s}$. Let $x = 1 - X \in U_r$ and $y = 1 - Y \in U_s$. Expanding $[x, y] = xyx^{-1}y^{-1}$ as in $\mathrm{End}_{\mathbb{F}}(V)$. To collect terms according to X and Y, we get

$$\begin{aligned}(1-X)(1-Y)(1-X)^{-1}(1-Y)^{-1} &= (1-X)(1-Y)\sum_{k=0}^{n-1} X^k \sum_{h=0}^{n-1} Y^h \\ &= c + p(X) + q(Y) + r(X, Y)\end{aligned}$$

where c is the constant term, $P(X)$ is a sum of terms containing X, $q(Y)$ is a sum of terms containing Y, and $r(X, Y)$ is a sum of terms containing X, Y. It can be verified that $c = 1$, $p(X) = q(Y) = 0$. Hence we have $r(X, Y) = [x, y] - 1$. Since $r(X, Y)$ have X and Y, such terms must map V_i to V_{i+r+s}. Therefore $[x, y] \in U_{r+s}$, and thus we have proved that $[U_r, U_s] \subseteq U_{r+s}$. As a corollary, we have $U_r \lhd U_s$ whenever $r \geq s$. To see this, note that $xyx^{-1} = [x, y]y \in U_r$ for all $x \in U_s$, $y \in U_r$.

Set $U = U^1 = U_1$ and $U^i = U_i$ for $2 \leq i \leq n$. It follows that $U_r \lhd U$ and $[U_r, U] \subseteq U_{r+1}$. Hence the series

$$U = U^1 \geq U^2 \geq \cdots \geq U^n = \{1\}$$

implies that U is a nilpotent group.

Let

$$T = \{x \in \mathrm{GL}(V) \mid x(V_i) \subseteq V_i \text{ for all } i\}.$$

We have a surjective group homomorphism

$$\begin{aligned}\Phi : T &\to \bigoplus_{i=0}^{n-1} \mathrm{GL}(V_i/V_{i+1}) \cong (\mathbb{F}^\times)^n, \\ x &\mapsto (x|_{V_i/V_{i+1}})_{i=0}^{n-1},\end{aligned}$$

where $x|_{V_i/V_{i+1}}$ is the induced automorphism on each quotient V_i/V_{i+1} defined by $x|_{V_i/V_{i+1}}(v+V_{i+1}) = x(v)+V_{i+1}$. We see that $\ker(\Phi) = U$, so $U \lhd T$ and $T/U \cong \mathrm{im}(\Phi)$ is abelian (recall that the direct product of abelian groups is abelian). Since T/U is abelian (and hence solvable) and U is solvable (by Proposition 12.16), it follows from Corollary 12.3 that T is solvable.

Take an ordered basis $\mathcal{B} = \{e_1, \ldots, e_n\}$ for V such that

$$V_i = \bigoplus_{j=1}^{n-i} \mathbb{F} e_j$$

and write elements of $\mathrm{GL}(V)$ as matrices with respect to $\mathcal{B}$. Then we recover Example 12.21, where each $x|_{V_i/V_{i+1}}$ is represented by the ith diagonal element.

12.3.2 p-groups

Proposition 12.23. *Let G be a p-group and let H be a nontrivial normal subgroup of G. Then $H \cap Z(G) \neq \{e\}$. In particular, $Z(G) \neq \{e\}$.*

Proof. Clearly H is a p-group. Since $H \lhd G$, the p-group G acts on H by conjugation. By Fixed point lemma (Lemma 4.3), H_G contains an element $x \in H$ other than e. By the definition of H_G, we have $x = g^{-1}xg$ for all $g \in G$. Thus $x \in Z(G)$ and so $H \cap Z(G) \neq \{e\}$. The last assertion is obtained by setting $G = H$. ■

Proposition 12.24. *Let p be a prime. Then any p-group is nilpotent.*

Proof. Any p-group G and all its nontrivial quotient groups are p-groups and thus have nontrivial centers by Proposition 12.23. If $G \neq Z_i(G)$, then $Z_i(G)$ is strictly contained in $Z_{i+1}(G)$. Since G is finite, $Z_m(G)$ must be G for some m. ■

12.3.3 Symmetric Groups

Proposition 12.25. *The symmetric group S_n is solvable for $n = 1, 2, 3, 4$.*

Proof. It is trivial for S_1.

The group S_2 is solvable because it is an abelian group.

The group S_3 is solvable because we have the following series

$$1 \lhd A_3 \lhd S_3.$$

Clearly $S_3/A_3 \cong \mathbb{Z}_2$ and $A_3/\{e\} \cong \mathbb{Z}_3$. Thus they are abelian.

The group S_4 is solvable because we have the following normal series

$$\{e\} \lhd V_4 \lhd A_4 \lhd S_4$$

where V_4 is the Klein 4-group.

`https://math.stackexchange.com/questions/120429/prove-that-s-3-and-s-4-a`

■

Proposition 12.26. *The symmetric group S_n is not solvable for $n \geq 5$.*

Proof. Note that A_n is a nonabelian and simple group. Hence $[A_n, A_n] = A_n$ and so A_n is not solvable by Theorem 12.2. Then we use Corollary 12.3 to obtain the conclusion. ■

12.4 Characterization of Finite Nilpotent Groups

Lemma 12.27. *Let S be a Sylow p-subgroup of a group G. If a subgroup H of G contains $N_G(S)$, then we have $H = N_G(H)$.*

Proof. By assumption, $S \subseteq N_G(S) \subseteq H$. Let $L = N_G(H)$. Then $H \lhd L$. By applying Lemma 8.24 to L, we get

$$N_G(H) = L = N_L(S)H \subseteq \langle N_G(S), H \rangle = H.$$

Clearly, $H \subseteq N_G(H)$, so we have $H = N_G(H)$. ■

The following theorem gives some of the main properties which characterize finite nilpotent groups. We include Theorem 12.12 and Corollary 12.13 for convenience.

Theorem 12.28. *Let G be a finite group. Then the following are equivalent.*

(1) There exists an integer n such that $Z_n(G) = G$.

(2) There is at least one central series of G.

(3) There exists an integer n such that $G^n = \{e\}$.

(4) The normalizer of any proper subgroup H is strictly larger than H, i.e., $N_G(H) \neq H$.

(5) Any maximal subgroup is normal.

(6) For any prime number p, every Sylow p-subgroup is normal.

(7) The group G is a direct product of Sylow subgroups.

(8) The group G is a direct product of groups of prime power order.

Proof. We have already established that (1), (2) and (3) are equivalent.

(2) $\Rightarrow$ (4) Let

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

be a central series for G. Let H be a proper subgroup of G. Let k be the integer such that $G_{k+1} \not\subseteq H$ and $G_k \subseteq H$. Such integer must exist since H contains G_0. Then

$$[G_{k+1}, H] \subseteq [G_{k+1}, G] \subseteq G_k \subseteq H.$$

So $G_{k+1} \subseteq N_G(H)$ and hence we have $N_G(H) \neq H$.

(4) $\Rightarrow$ (5) Let M be a maximal subgroup of G. Since M is proper subgroup, we have $M < N_G(M)$. By the definition of maximal subgroups, we get $N_G(M) = G$. Hence $M \lhd G$.

(5) $\Rightarrow$ (6) Suppose on the contrary that a Sylow p-subgroup P of G is not normal. Then $N_G(P) < G$. In view of Proposition 5.12, we can take a maximal subgroup M which contains $N_G(P)$. By Lemma 12.27, we have $N_G(M) = M$. Hence M is not normal, since $N_G(M) < G$. This is a contradiction.

(6) $\Rightarrow$ (7) By Corollary 6.9.

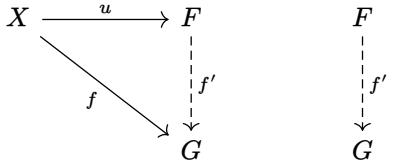
(7) $\Rightarrow$ (8) Trivial.

(8) $\Rightarrow$ (1) Any group of prime power order is nilpotent by Proposition 12.24. The result follows from Corollary 12.20. ■

13 Free Groups

13.1 Definition

Definition 13.1. Let X be a set and let F be a group. We call F a **free group** on X if F is a free object on X in the category of groups, i.e., there is a set function $u : X \to F$ such that the pair (F, u) satisfies the following universal property: for every group G and a set function $f : X \to G$, there is a unique group homomorphism $f' : F \to G$ such that $f' \circ u = f$, as shown in the following commutative diagram.



Proposition 13.2. *Let $u : X \to F$ be the function defined in Definition 13.1. Then the following propositions hold.*

(i) The elements $u(x)$ $(x \in X)$ generate F.

(ii) The function u is injective.

Proof. (i) Let G be the subgroup of F generated by the elements $u(x)$ $(x \in X)$. Let $f : X \to G$ be the function defined by $f(x) = u(x)$. Then there exists a unique group homomorphism $f' : F \to G$ such that $f' \circ u = f$. Let $\iota : G \to F$ be the inclusion mapping. Consider the function $\iota \circ f$. By the universal property, there exists a unique group homomorphism $\varphi : F \to F$ such that $f'' \circ u = \iota \circ f$. Note that left multiplication of ι on the equality $f' \circ u = f$ yields $(\iota \circ f') \circ u = \iota \circ f$. By the uniqueness, we obtain $f'' = \iota \circ f'$. On the other hand, we see that $1 \circ u = \iota \circ f$, where $1 : F \to F$ is the identity mapping. Hence we get $f'' = 1$. Thus $\iota \circ f' = 1$. So ι has a right inverse. This implies that ι is surjective (recall that surjectivity $\Leftrightarrow$ having right inverse), whence $F = \iota(G) = G = \langle u(x) \,|\, x \in X \rangle$.

(ii) Let $x, y \in X$ be distinct elements, i.e., $x \neq y$. Let $f : X \to \mathbb{Z}_2$ be defined by $f(x) = 0$, $f(z) = 1$ for all $z \in X \setminus \{x\}$. By the universal property, there is a unique $f' : F \to \mathbb{Z}_2$ such that $f' \circ u = f$. In particular, $f'(u(x)) = (f' \circ u)(x) = f(x) = 0$ and $f'(u(y)) = f(y) = 1$. Hence $f'(u(x)) \neq f'(u(y))$. Since f' is well-defined, we get $u(x) \neq u(y)$. Therefore u is injective. ∎

Remark. Since u is an injective function, we shall identify X as a subset of F. Simply speaking, one usually omits u and writes x for its image $u(x)$.

13.2 Three Ways of Constructing Free Groups

Theorem 13.3. *For any set X, there exists a unique (up to isomorphism) free group on X.*

The uniqueness follows from Proposition 0.3. Now we prove the existence in three different ways.

13.2.1 Groups of Words: a Beginner's Favourite

13.2.2 Construction from Equivalence Classes: a Logician's Favourite

Definition 13.4. Let X be a set. A **group-theoretic term** is a finite string of symbols from X using formal group operations $\cdot$, $^{-1}$ and e, where parentheses are introduced among the symbols.

This definition is actually motivated from the set of all group-theoretic terms, which makes something more precise.

Definition 13.5. The set of all **group-theoretic terms** in the elements of X under the formal group operations $\cdot$, ι, e is a set T satisfying the following: There are some functions

$$\mathrm{symb}_T : X \to T, \quad \cdot_T : T \times T \to T, \quad \iota_T : T \to T, \quad \text{and} \quad e_T : T^0 \to T,$$

where T^0 is a set of one distinguished element, such that

(i) each of these maps is one-to-one;

(ii) their images are disjoint and T is the union of those images;

(iii) T is generated by $\mathrm{symb}_T(X)$ under the operations $\cdot_T$, ι_T, and e_T;

(iv) T has no proper subset which contains $\mathrm{symb}_T(X)$ and is closed under those operations.

Now we construct a free group on a given set X. Let T be the set of all group-theoretic terms in the elements of X under $\cdot$, ι, e. Let $\sim$ be the **least** relation on T that satisfy: (Group Axioms)

$$(\forall p, q, r \in T) \quad (p \cdot q) \cdot r \sim p \cdot (q \cdot r), \tag{G1}$$

$$(\forall p \in T) \quad (p \cdot e \sim p) \wedge (e \cdot p \sim p), \tag{G2}$$

$$(\forall p \in T) \quad (p \cdot p^{-1} \sim e) \wedge (p^{-1} \cdot p \sim e). \tag{G3}$$

(Well-definedness)

$$(\forall p, p', q \in T) \quad (p \sim p') \implies ((p \cdot q \sim p' \cdot q) \wedge (q \cdot p \sim q \cdot p')) \tag{WD}$$

(Equivalence Relations)

$$(\forall p \in T) \quad p \sim p, \tag{R1}$$

$$(\forall p, q \in T) \quad (p \sim q) \implies (q \sim p), \tag{R2}$$

$$(\forall p, q, r \in T) \quad ((p \sim q) \wedge (q \sim r)) \implies (p \sim r). \tag{R3}$$

This least relation on T can be constructed by forming the set-theoretic intersection of all relations on T satisfying the conditions above. By (R1)–(R3), the relation $\sim$ is an equivalence relation. Let F be the equivalence classes of $\sim$, i.e.,

$$F = \frac{T}{\sim} = \{[p] \,|\, p \in T\}.$$

Let $u : X \to F$ be the function defined by

$$u(x) = [x].$$

Define operation $\cdot$, $^{-1}$ and e on F by

$$[p] \cdot [q] = [p \cdot q].$$

Then the operation is well-defined by (WD). It can be verified that $[e]$ is the identity and $[p]^{-1} = [p^{-1}]$ for all $p \in T$. It follows that F is a group by (G1)–(G3). Now we claim that (F, u) satisfies the universal property.

13.2.3 Crazy Construction from Direct Products: Only Serge Lang's Favourite

13.3 Group Presentations

13.4 Nielsen-Schreier Theorem

Theorem 13.6 (Nielsen-Schreier Theorem)**.** *If H is a subgroup of a free group G, then H is free.*

Main References. [Lan02; Ber15; RS10]

Part II
Ring Theory

14 Ideals

Part III
Miscellaneous

0 Zabalang

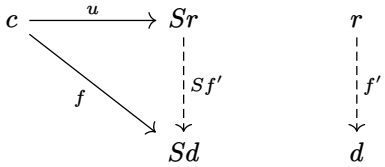
This is a collection of all results used in the previous section, but we have not yet learned them in any undergraduate studies.

0.1 Freeeee

Definition 0.1. Let $(\mathcal{C}, U)$ be a concrete category, where $U : \mathcal{C} \to \mathbf{Set}$ is a forgetful functor. If $\iota : X \to UF$ a function from a set X to the underlying set of an object F in $\mathcal{C}$, then F is called **free on** X if for every $A \in \mathrm{obj}\,\mathcal{C}$ and map $f : X \to UA$, there exists a unique morphism $f' : F \to A$ such that $Uf' \circ \iota = f$.

Remark. In fact, we call ι a **universal arrow** from X to U. Note that ι is often omitted when introducing a free object, but it must exist. In this case, we shall say the pair (F, ι) satisfies the **universal property**. We present the definition of this general concept below.

Definition 0.2. If $S : \mathcal{D} \to \mathcal{C}$ is a functor and c an object of $\mathcal{C}$, a **universal arrow** from c to S is a pair (r, u) consisting of an object r of $\mathcal{D}$ and an arrow $u : c \to Sr$ of $\mathcal{C}$, such that to every pair (d, f) with d an object of $\mathcal{C}$ and $f : c \to Sd$ an arrow of $\mathcal{C}$, there is a unique arrow $f' : r \to d$ of $\mathcal{D}$ with $Sf' \circ u = f$. In other words, every arrow f to S factors uniquely through the universal arrow u, as in the commutative diagram



Proposition 0.3. *Let $\mathbb{C}$ be a concrete category. If F and F' are free objects on sets X and X', respectively with $|X| = |X'|$, then $F \cong F'$.*

0.2 ZORN'S LEMMA!!!!

Definition 0.4. Let $(A, \leq)$ be a partially ordered set. An element $a \in A$ is **maximal** in A if for every $c \in A$ which is comparable to a, $c \leq a$; in other words, for all $c \in A$, $a \leq c \Rightarrow a = c$

Definition 0.5. An **upper bound** of a nonempty subset B of A is an element $d \in A$ such that $b \leq d$ for every $b \in B$. A nonempty subset B of A that is linearly ordered by $\leq$ is called a **chain** in A.

Remark. Note that if a is maximal, it need not be the case that $c \leq a$ for all $c \in A$ (there may exist $c \in A$ that are not comparable to a). Furthermore, a given set may have many maximal elements or none at all (for example, $\mathbb{Z}$ with its usual ordering).

Lemma 0.6 (Zorn's Lemma)**.** *If A is a nonempty partially ordered set such that every chain in A has an upper bound in A, then A contains a maximal element.*

0.3 BILA NAK COUNTABLE OR UNCOUNTABLE, PENANG LIH

0.3.1 How We Actually Define the "Size" of a Set

Definition 0.7. Let S and T be sets.

(i) Two sets S and T have the same **cardinality**, written

$$|S| = |T|$$

if there is a bijective function (a **one-to-one correspondence**) between the sets.

(ii) If S is in one-to-one correspondence with a **subset** of T, then we write

$$|S| \leq |T|.$$

(iii) If S is in one-to-one correspondence with a **proper subset** of T but **not all** of T, then we write

$$|S| < |T|.$$

The second condition is necessary, since, for instance, $\mathbb{N}$ is in one-to-one correspondence with a proper subset of $\mathbb{Z}$ and yet $\mathbb{N}$ is also in one-to-one correspondence with $\mathbb{Z}$ itself. Hence $|\mathbb{N}| = |\mathbb{Z}|$.

Definition 0.8. (i) A set is **finite** if it can be put in one-to-one correspondence with a set of the form $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, for some nonnegative integer n. A set that is not finite is **infinite**. The **cardinal number** (or **cardinality**) of a finite set is just the number of elements in the set.

(ii) The **cardinal number** of the set $\mathbb{N}$ of natural numbers is $\aleph_0$.

(iii) Any set with cardinality $\aleph_0$ is called a **countably infinite** set and any finite or countably infinite set is called a **countable** set. An infinite set that is not countable is said to be **uncountable**.

0.3.2 Tools to "Compare the Size"

Theorem 0.9 (Schröder–Bernstein theorem)**.** *For any sets S and T,*

$$|S| \leq |T| \text{ and } |T| \leq |S| \Rightarrow |S| = |T|.$$

Theorem 0.10 (Cantor's Theorem)**.** *If $\mathcal{P}(S)$ denotes the power set of S, then*

$$|S| < |\mathcal{P}(S)|.$$

Theorem 0.11. *If $\mathcal{P}_0(S)$ denotes the set of all finite subsets of S and if S is an infinite set, then*

$$|S| = |\mathcal{P}_0(S)|.$$

0.3.3 Cardinal Arithmetic Is Strange but Not Weirdo

Definition 0.12. Let κ and λ denote cardinal numbers. Let S and T be disjoint sets for which $|S| = \kappa$ and $|T| = \lambda$.

(i) The **sum** $\kappa + \lambda$ is the cardinal number of $S \cup T$.

(ii) The **product** $\kappa\lambda$ is the cardinal number of $S \times T$.

(iii) The **power** κ^λ is the cardinal number of S^T, where S^T is the set of all functions from T to S.

Theorem 0.13. *Let κ, λ and μ be cardinal numbers. Then the following properties hold.*

(i) (Associativity)

$$\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu,$$
$$\kappa(\lambda\mu) = (\kappa\lambda)\mu.$$

(ii) (Commutativity)

$$\kappa + \lambda = \lambda + \kappa,$$
$$\kappa\lambda = \lambda\kappa.$$

(iii) (Distributivity)

$$\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu.$$

(iv) (Properties of Exponents)

$$\begin{aligned} \kappa^{\lambda+\mu} &= \kappa^{\lambda}\kappa^{\mu}, \\ (\kappa^{\lambda})^{\mu} &= \kappa^{\lambda\mu}, \\ (\kappa\lambda)^{\mu} &= \kappa^{\mu}\lambda^{\mu}. \end{aligned}$$

Theorem 0.14. *Let κ and λ be cardinal numbers, at least one of which is infinite. Then*

$$\kappa + \lambda = \kappa\lambda = \max\{\kappa, \lambda\}.$$

Theorem 0.15. *Let $\{A_k \mid k \in K\}$ be a collection of sets, indexed by the set K, with $|K| = \kappa$. If $|A_k| \leq \lambda$ for all $k \in K$, then*

$$\left| \bigcup_{k \in K} A_k \right| \leq \lambda\kappa.$$

Theorem 0.16. *Let κ be any cardinal number.*

(i) If $|S| = \kappa$, then $|\mathcal{P}(S)| = 2^{\kappa}$.

(ii) $\kappa < 2^{\kappa}$.

(iii) If $\kappa < \aleph_0$, then κ is a natural number.

Remark. There is a reason why we use 2^{κ}. In fact $|\mathbb{R}|$, is equal to $2^{\aleph_0}$. This means we can use $\aleph_0$ for the size of countable sets and $2^{\aleph_0}$ for the size of uncountable sets.

Theorem 0.17. *The following results hold for $\aleph_0$.*

(i) Addition applied a countable number of times to the cardinal number $\aleph_0$ does not yield anything more than $\aleph_0$, i.e.,

$$\aleph_0 \cdot \aleph_0 = \aleph_0.$$

*(ii) Multiplication applied a **finite number** of times to the cardinal number $\aleph_0$ does not yield anything more than $\aleph_0$, i.e., for any positive integer $n \in \mathbb{N}$,*

$$\aleph_0^n = \aleph_0.$$

The result is not true when we apply a countable number of times. More precisely,

$$\aleph_0^{\aleph_0} = 2^{\aleph_0}.$$

(iii) Addition and multiplication applied a countable number of times to the cardinal number $2^{\aleph_0}$ does not yield more than $2^{\aleph_0}$, i.e.,

$$\aleph_0 \cdot 2^{\aleph_0} = 2^{\aleph_0},$$
$$(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0}.$$

0.3.4 All the Facts That Make You a Weirdo

The following results hold.

(1) $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = \aleph_0$.

(2) $|\mathbb{R}| = 2^{\aleph_0}$.

(3) We can "translate" everything from theorems above to some statements. The following are some examples.

- (i) The power set of a countable set is uncountable.
- (ii) The power set of an uncountable set is uncountable.
- (iii) The set of all finite subsets of a uncountable set is uncountable.
- (iv) A countable union of countable sets is countable.
- (v) The set of functions from a countable set to a countable set is uncountable.
- (vi) The set of functions from a countable set to a uncountable set is uncountable.

0.4 Ordinal was not invented by ordinary people

It wasn't ordinary people, and it wasn't OVALTINE.

0.4.1 How we actually "order" elements

Definition 0.18. A binary relation $<$ on a set P is a **partial ordering** of P if:

(i) $p \not< p$ for any $p \in P$;

(ii) if $p < q$ and $q < r$, then $p < r$.

$(P, <)$ is called a **partially ordered set**. A partial ordering $<$ of P is a **linear ordering** if moreover

(iii) $p < q$ or $p = q$ or $q < p$ for all $p, q \in P$.

0.4.2 Elements are always ordered nicely, not nicely, whatever

Definition 0.19. A linear ordering $<$ of a set P is a **well-ordering** if every nonempty subset of P has a least element.

Theorem 0.20 (Well-Ordering Theorem)**.** *Every set can be well-ordered.*

0.4.3 One, two, three, ... OMEGA!

Definition 0.21. A set T is **transitive** if every element of T is a subset of T.

Definition 0.22. A set is an **ordinal number** (an **ordinal**) if it is transitive and well-ordered by $\in$.

We shall denote ordinals by lowercase Greek letters $\alpha, \beta, \gamma, \ldots$. The class of all ordinals is denoted by Ord.

Proposition 0.23. *Define*

$$\alpha < \beta \quad \textit{if and only if} \quad \alpha \in \beta.$$

Then we have the following results.

(i) $<$ *is a linear ordering of the class* Ord.

(ii) For each α, $\alpha = \{\beta \mid \beta < \alpha\}$.

(iii) If C *is a nonempty class of ordinals, then* $\bigcap C$ *is an ordinal,* $\bigcap C \in C$ *and* $\bigcap C = \inf C$.

(iv) If X *is a nonempty set of ordinals, then* $\bigcup X$ *is an ordinal, and* $\bigcup X = \sup X$.

(v) For every α, $\alpha \cup \{\alpha\}$ *is an ordinal and* $\alpha \cup \{\alpha\} = \inf\{\beta \mid \beta > \alpha\}$.

We thus define $\alpha + 1 := \alpha \cup \{\alpha\}$ (the **successor** of α) and denote $\alpha + (n+1) := (\alpha + n) + 1$ for all $n \geq 1$.

Definition 0.24. Let α be an ordinal. If $\alpha = \beta + 1$ for some ordinal β, then α is a **successor ordinal**. If α is not a successor ordinal, then $\alpha = \sup\{\beta \mid \beta < \alpha\} = \bigcup \alpha$ is called a **limit ordinal**. We also consider 0 a limit ordinal and define $\sup \emptyset = 0$.

In this fashion, we can generate greater and greater "numbers": $\omega, \omega + 1, \omega + 2, \ldots, \omega + n, \ldots$ for all $n \in \mathbb{N}$. A number following all $\omega + n$ can again be conceived of as a set of all smaller numbers:

$$\omega 2 := \omega + \omega = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\}.$$

Then we can still generate greater numbers:

$$\begin{aligned}\omega 2+1 = \omega+\omega+1 &= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots,\omega+\omega\},\\ \omega 3 = \omega+\omega+\omega &\\ &= \{0,1,2,\ldots,\omega,\omega+1,\omega+2,\ldots,\omega+\omega,\omega+\omega+1,\ldots\},\\ \omega^2 := \omega\omega &= \{0,1,2,\ldots,\omega,\omega+1,\ldots,\omega 2,\omega\cdot 2+1,\ldots,\omega 3,\ldots,\omega 4,\ldots\}.\end{aligned}$$

After that the whole thing starts over again: $\omega^2+1, \omega^2+2, \ldots, \omega^2+\omega, \omega^2+\omega+1, \omega^2+\omega+2, \ldots, \omega^2+\omega 2, \omega^2+\omega 2+1, \ldots, \omega^2+\omega 3, \ldots, \omega^2+\omega 4, \ldots, \omega^2 2, \ldots, \omega^2 3, \ldots, \omega^3, \ldots, \omega^4, \ldots, \omega^\omega, \ldots, \omega^{\omega^\omega}, \ldots, \omega^{\omega^{(\omega^\omega)}}, \ldots$. The next one after all that is ε_0. Then come $\varepsilon_0+1, \varepsilon_0+2, \ldots, \varepsilon_0+\omega, \ldots, \varepsilon_0+\omega 2, \ldots, \varepsilon_0+\omega^2, \ldots, \varepsilon_0+\omega^\omega, \ldots, \varepsilon_0 2, \ldots, \varepsilon_0\omega, \ldots, \varepsilon_0\omega^\omega, \ldots, \varepsilon_0^2, \ldots$.

0.4.4 Each well ordered set has a unique order type

Definition 0.25. If $(P,<)$ and $(Q,<)$ are partially ordered sets and $f : P \to Q$, then f is **order-preserving** if $x < y$ implies $f(x) < f(y)$.

Definition 0.26. A bijective function $f : P \to Q$ is an **isomorphism** of P and Q if both f and f^{-1} are order-preserving. In other words, we say that $(P,<)$ is **isomorphic** to $(Q,<)$.

Theorem 0.27 (Counting Theorem)**.** *Every well-ordered set is isomorphic to a unique ordinal number.*

0.4.5 Playing Dominoes at The Edge of Universe

Theorem 0.28 (Transfinite Induction)**.** *Let $P(x)$ be a property. Assume that*

(i) $P(0)$ holds.

(ii) $P(\alpha)$ implies $P(\alpha+1)$ for all ordinals α.

(iii) For all limit ordinals $\alpha \neq 0$, if $P(\beta)$ holds for all $\beta < \alpha$, then $P(\alpha)$ holds.

Then $P(\alpha)$ holds for all ordinals α.

Main References. [Rom08; Hal74; Jec03; Osb00; Hun80]

References

[AB95] J. L. Alperin and Rowen B. Bell. *Groups and representations*. English. Vol. 162. Grad. Texts Math. New York, NY: Springer-Verlag, 1995.

[Art91] Michael Artin. *Algebra*. English. Englewood Cliffs, NJ: Prentice-Hall, 1991.

[AS85] M. Aschbacher and L. Scott. "Maximal subgroups of finite groups". English. In: *J. Algebra* 92 (1985), pp. 44–80.

[Ber15] George M. Bergman. *An invitation to general algebra and universal constructions*. English. 2nd ed. Universitext. Cham: Springer, 2015.

[Cam99] Peter J. Cameron. *Permutation groups*. English. Vol. 45. Lond. Math. Soc. Stud. Texts. Cambridge: Cambridge University Press, 1999.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. English. 3rd ed. Chichester: Wiley, 2004.

[DM96] John D. Dixon and Brian Mortimer. *Permutation groups*. English. Vol. 163. Grad. Texts Math. New York, NY: Springer-Verlag, 1996.

[Hal74] Paul R. Halmos. *Naive set theory*. English. Undergraduate Texts Math. Springer, Cham, 1974.

[Hun80] Thomas W. Hungerford. *Algebra*. English. Vol. 73. Grad. Texts Math. Springer, Cham, 1980.

[Isa09] I. Marin Isaacs. *Algebra. A graduate course*. English. Vol. 100. Grad. Stud. Math. Providence, RI: American Mathematical Society (AMS), 2009.

[Jec03] Thomas Jech. *Set theory*. English. The third millennium edition, revised and expanded. Springer Monogr. Math. Berlin: Springer, 2003.

[Kap54] Irving Kaplansky. *Infinite abelian groups*. English. Ann Arbor: University of Michigan Press, 1954.

[Kap77] Irving Kaplansky. *Set theory and metric spaces. 2nd ed.* English. New York: Chelsea Publishing Company, 1977.

[Lan02] Serge Lang. *Algebra*. English. 3rd revised ed. Vol. 211. Grad. Texts Math. New York, NY: Springer, 2002.

[Li25] Wen-Wei Li. *Methods of algebra: Volume 1 (in Chinese)*. 2025.

[LPS88] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl. "On the O'Nan-Scott theorem for finite primitive permutation groups". English. In: *J. Aust. Math. Soc., Ser. A* 44.3 (1988), pp. 389–396.

[Mel95] J. D. P. Meldrum. *Wreath products of groups and semigroups.* English. Vol. 74. Pitman Monogr. Surv. Pure Appl. Math. Harlow, Essex: Longman Group Ltd., 1995.

[Osb00] M. Scott Osborne. *Basic homological algebra.* English. Vol. 196. Grad. Texts Math. New York, NY: Springer, 2000.

[PS18] Cheryl E. Praeger and Csaba Schneider. *Permutation groups and Cartesian decompositions.* English. Vol. 449. Lond. Math. Soc. Lect. Note Ser. Cambridge: Cambridge University Press, 2018.

[Rob82] Derek J. S. Robinson. *A course in the theory of groups.* English. Vol. 80. Grad. Texts Math. Springer, Cham, 1982.

[Rom08] Steven Roman. *Advanced linear algebra.* English. 3rd ed. Vol. 135. Grad. Texts Math. New York, NY: Springer, 2008.

[Rot15] Joseph J. Rotman. *Advanced modern algebra. Part 1.* English. 3rd edition. Vol. 165. Grad. Stud. Math. Providence, RI: American Mathematical Society (AMS), 2015.

[Rot95] Joseph J. Rotman. *An introduction to the theory of groups.* English. 4th ed. Vol. 148. Grad. Texts Math. New York, NY: Springer-Verlag, 1995.

[RS10] Luis Ribes and Benjamin Steinberg. "A wreath product approach to classical subgroup theorems." English. In: *Enseign. Math. (2)* 56.1-2 (2010), pp. 49–72.

[Smi18] Stephen D. Smith. *Applying the classification of finite simple groups. A user's guide.* English. Vol. 230. Math. Surv. Monogr. Providence, RI: American Mathematical Society (AMS), 2018.

[Suz82] M. Suzuki. *Group Theory I.* Springer Berlin, Heidelberg, 1982.

[Wil09] Robert A. Wilson. *The Finite Simple Groups.* Springer London, 2009.