Notes on PMATH-336:
Introduction to Group Theory

Unversity of Waterloo

David Duan

Last Updated: August 20, 2021 (draft)

Contents

Chapter 1

Introduction

Section 1. Preliminaries

1.1. Theorem (First Principle of Induction): *Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then also $n+1 \in S$. Then S contains every integer greater than or equal to a.*

1.2. Theorem (Second Principle of Induction): *Let S be a set of integers containing a. Suppose S has the property that the integer n belongs to S whenever each integer m with $a \leq m < n$ belongs to S. Then S contains every integer greater than or equal to a.*

Section 2. Equivalence Relations

2.1. Definition: An **equivalence relation** on a set S is a subset $R \subseteq S \times S$ satisfying the following properties:

(1). **reflexive**: $\forall a \in S : (a, a) \in R$;

(2). **symmetric**: $(a, b) \in R \implies (b, a) \in R$;

(3). **transitive**: $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$.

For each $a \in S$, the set $[a] = \{x \in S \mid (a, x) \in R\}$ is called the **equivalence class** of a.

2.2. Definition: A **partition** of a set S is a collection of non-empty disjoint subsets of S whose union is S.

2.3. Theorem: *The equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation whose equivalence classes are the elements of P.*

Section 3. Functions

3.1. Definition: A **function** φ from a set A to a set B is a rule that assigns to each element a of A exactly one element of B.

3.2. Definition: A function $\varphi : A \to B$ is called

- **injective** or **one-to-one** or **1-1** if $\varphi(a_1) = \varphi(a_2) \Longrightarrow a_1 = a_2$.
- **surjective** or **onto** if for every $b \in B$, there exists $a \in A$ with $\varphi(a) = b$.

3.3. Definition: Suppose A, B and C are sets and $\varphi : A \to B$ and $\psi : B \to C$ are functions. We define the **composition** of φ and ψ as

$$\psi\varphi(a) = \psi(\varphi(a)) \quad (a \in A)$$

3.4. Proposition: *Suppose A, B, C, D are sets and $\alpha : A \to B, \beta : B \to C, \gamma : C \to D$ are functions. Then the following hold:*

(1). (associativity): $\gamma(\alpha\beta) = (\gamma\alpha)\beta$;

(2). If α and β are one-to-one, then so is $\beta\alpha$;

(3). If α and β are onto, then so is $\beta\alpha$;

(4). If α is one-to-one and onto, then there exists a function $\alpha^{-1} : B \to A$ such that

$$\forall a \in A : \alpha^{-1}\alpha(a) = a$$
$$\forall b \in B : \alpha\alpha^{-1}(b) = b$$

3.5. Remark: Hence, given a set A, we can consider the set

$$\{\alpha : A \to A \mid \alpha \text{ is one-to-one and onto}\}$$

which has a product on it given by composition of functions. This is an important example that we will return to when we consider permutation groups.

Section 4. Basic Number Theory

4.1. Axiom (Well-Ordering Principle): *Every non-empty set of positive integers contains a smallest member.*

4.2. Definition: Let $m, n \in \mathbb{Z}$. We say that m **divides** n, denoted $m|n$, if there exists $k \in \mathbb{Z}$ such that $n = km$. The integer m is called a **divisor** of n.

4.3. Lemma: *Let $a, b, c \in \mathbb{Z}$.*

(1). If $a|b$ and $b|c$, then $a|c$.

(2). If $a|b$ and $a|c$, then $a|(bx + cy)$ for all $x, y \in \mathbb{Z}$.

(3). If $a|b$ and $b \neq 0$, then $|a| \leq |b|$.

Proof. Trivial. □

4.4. Theorem (Division Algorithm): *If $a, b \in \mathbb{Z}$ with $b > 0$, then there exist unique integers $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$. The integers q and r are called the* ***quotient*** *and the* ***remainder****, respectively.*

Proof. (Existence) Consider the set $S := \{a - bk \mid k \in \mathbb{Z}, a - bk \geq 0\}$. If $0 \in S$, then $b|a$ and we have $q = a/b$ and $r = 0$. Now assume $0 \notin S$. We claim that $S \neq \varnothing$. Indeed, if $a > 0$, then $a - b \cdot 0 \in S$; if $a < 0$, then $a - b(2a) = a(1 - 2b) \in S$; $a \neq 0$ since $0 \notin S$. Thus, we may apply the WOP to conclude that S has a smallest member, say $r = a - bq$. Then $a = bq + r$ and $r \geq 0$.

It remains to show that $r < b$. Suppose $r \geq b$. Then $a - b(q + 1) = a - bq - b = r - b \geq 0$ so $a - b(q + 1) \in S$. But $a - b(q + 1) < a - bq$, contradicts the assumption that $a - bq$ is the smallest member of S. Thus, $r < b$. This concludes the existence part.

(Uniqueness) Suppose there are integers q', r' such that $a = bq + r = bq' + r'$ with $0 \leq r, r' < b$. WLOG, assume $r' \geq r$. Then $b(q - q') = r' - r$ so b divides $r' - r$ and $0 \leq r' - r \leq r' < b$. It follows that $r' - r = 0$ and thus $r' = r$ and $q = q'$. □

4.5. Definition: The **greatest common divisor** of two non-zero integers a and b, denoted $\gcd(a, b)$, is the largest of all common divisors of a and b. If $\gcd(a, b) = 1$, we say a and b are **relatively prime**.

4.6. Theorem (Bezout): *For any non-zero integers a and b, there exist integers s and t such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.*

Proof. Consider the set $S = \{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\}$. Since S is obviously non-empty, WOP asserts that S has a smallest member, say, $d = as + bt$. We claim that $d = \gcd(a, b)$. By the division algorithm, write $a = bq + r$ where $0 \leq r < d$. If $r > 0$, then

$$r = a - dq = a - (as + bt)q = a - asq - btq = a(1 - sq) + b(-tq) \in S,$$

contradicting the fact that d is the smallest member of S. So $r = 0$ and $d|a$. By symmetry, $d|b$. This proves that d is a common divisor of a and b. Now suppose d' is another common divisor of a and b and write $a = d'h$ and $b = d'k$. Then

$$d = as + bt = (d'h)s + (d'k)t = d'(hs + kt) \implies d'|d.$$

Thus, among all common divisors of a and b, d is the greatest. □

4.7. Corollary: *If a and b are relatively prime, there exist integers s and t such that $as + bt = 1$.*

Proof. By definition, a and b are relatively prime means $\gcd(a, b) = 1$. Now apply Bezout's Identity above. □

4.8. Corollary (Euclid): *If p is a prime that divides ab, then p divides a or p divides b.*

Proof. If $p \nmid a$, then $\gcd(a, p) = 1$. Then by Corollary 4.7, there exist $s, t \in \mathbb{Z}$ such that $at + ps = 1$. Multiplying both sides by b, we get $bat + bps = b$. As p divides both terms on the LHS, it divides the sum, and thus $p|b$. □

4.9. Theorem (Fundamental Theorem of Arithmetic): *Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which factors appear.*

Proof. Later. □

Section 5. Modular Arithmetic

5.1. Definition: Let $n \in \mathbb{Z}_+$. If $a, b \in \mathbb{Z}$, we say a is **congruent to** b **modulo** n and write $a \equiv b \bmod n$ if $n|(a-b)$.

5.2. Theorem: *Let $n \in \mathbb{Z}_+$ and $R = \{(a,b) \mid a \equiv b \bmod n\}$. Then R is an equivalence relation.*

Proof. Check definition. □

5.3. Definition: Let $n \in \mathbb{Z}_+$. The **congruent class modulo** n of the integer a is the set $[a] := \{x \in \mathbb{Z} \mid x \equiv a \bmod n\}$.

5.4. Definition: Let $n \in \mathbb{Z}_+$. The **integers modulo** n, denoted by $\mathbb{Z}_n$, is the set of n congruence classes $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$.

5.5. Theorem: *Define two operations on $\mathbb{Z}_n$, addition and multiplication, as follows:*

$$[a] + [b] = [a+b]$$
$$[a] \cdot [b] = [a \cdot b]$$

Then for $[a], [b], [c] \in \mathbb{Z}_n$, we have

- $[a] + [b] = [b] + [a], [a][b] = [b][a]$ *(commutativity);*
- $([a] + [b]) + [c] = [a] + ([b] + [c]), ([a][b])[c] = [a]([b][c])$ *(associativity);*
- $[a]([b] + [c]) = [a][b] + [a][c]$ *(distributivity);*
- $[a] + [0] = [a] = [0] + [a]$ *(additive identity);*
- $[a][1] = [1][a] = [a]$ *(multiplicative identity);*
- $[a] + [-a] = [-a] + [a] = 0$ *(additive inverse).*

5.6. Theorem: *Let $n \in \mathbb{Z}_+$ and $[a] \in \mathbb{Z}_n$. Then $[a]$ has a multiplicative inverse iff* $\gcd(a,n) = 1$.

Proof. Suppose there exists $[s] \in \mathbb{Z}_n$ such that $[a][s] = [1]$. This means that $as \equiv 1 \bmod n \implies 1 = as + nt$ for some $t \in \mathbb{Z}$. By Bezout's identity, this means that $\gcd(a,n) = 1$. Conversely, suppose that $\gcd(a,n) = 1$. By Bezout's identity, there exists $s, t \in \mathbb{Z}$ such that $1 = ns + nt$. Hence $as \equiv 1 \bmod n$ and $[s]$ is a multiplicative inverse of $[a]$. □

Chapter 2

Groups

Section 1. Basic Definitions

1.1. Definition: A set G together with a binary operation

$$\begin{aligned} \cdot : G \times G &\to G, \\ (a,b) &\mapsto ab \end{aligned}$$

on G is called a **group** if the following hold:

- **Associativity**: $(ab)c = a(bc)$ for all $a, b, c \in G$.
- Existence of **identity**: There is an element $e \in G$ such that $ae = ea = a$ for all $a \in G$.
- Existence of **inverse**: For each $a \in G$, there is an element $b \in G$ such that $ab = ba = e$.

In addition, if $ab = ba$ for all $a, b \in G$, we say G is **Abelian** or **commutative**. Otherwise, we say G is **non-Abelian**.

1.2. Example: Elementary examples of groups concerning scalars:

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ are all Abelian groups under usual addition.
- $(\mathbb{Q}_+, \times)$ is an Abelian group under usual multiplication; the inverse of $a \in \mathbb{Q}_+$ is $1/a \in \mathbb{Q}_+$.
- $(\{1, -1, i, -i\}, \times) \subseteq \mathbb{C}$ is an Abelian group, where $(-1)(-1) = 1$ and $(i)(-i) = 1$.
- $(\mathbb{Z}_n := \{0, 1, \ldots, n-1\}, + \bmod n)$ is Abelian and known as the **group of integers modulo** n.
- $(\mathbb{R}^* := \mathbb{R} \setminus \{0\}, \times)$ is an Abelian group with identity 1 and inverse $1/a$ for $a \in \mathbb{R}^*$.

1.3. Example: Elementary examples of groups concerning matrices:

- $(M_n(\mathbb{R}), +)$, the set of $n \times n$ matrices with real entries is a group under addition.
- $\mathrm{GL}(n, \mathbb{R})$, the set of $n \times n$ matrices with non-zero determinant is a non-Abelian (for $n > 1$) group under matrix multiplication. It is called the **general linear group** of degree n.
- $\mathrm{SL}(n, \mathbb{R})$, the set of $n \times n$ matrices with determinant 1 is a non-Abelian (for $n > 1$) group under matrix multiplication. It is called the **special linear group** of degree n. Note that $\mathrm{SL}(n, \mathbb{R}) \subset \mathrm{GL}(n, \mathbb{R})$.

1.4. Example: Elementary examples of non-groups:

- $(\mathbb{Z}, \times)$ is not a group: the element 2 does not have an integer inverse.
- $(\mathbb{Z}, -)$ is not a group: the operation is not associative.
- $(\{x \mid x \in \mathbb{R}_+ \setminus \mathbb{Q}_+\} \cup \{1\}, \times)$ satisfies the three properties given in the definition but is not a group, as the set is not closed under multiplication: $\sqrt{2} \times \sqrt{2} = 2 \in \mathbb{Q}_+$.
- $(M_n(\mathbb{R}), \times)$ is not a group: inverses do not exist for matrices with 0 determinant.
- $\{0, 1, 2, 3\}$ is not a group under multiplication modulo 4. Although 1 and 3 have inverses, the elements 0 and 2 do not.

1.5. Proposition: *Let $n \in \mathbb{N}$. The set of integers that are smaller than n and relatively prime with n, $U(n) := \{m \in \mathbb{N} \mid m < n, \gcd(m,n) = 1\}$ is a group under multiplication modulo n.*

Proof. We first show that $U(n)$ is closed under multiplication modulo n, that is, $m_1, m_2 \in U(n)$, then $(m_1 m_2) \bmod n \in U(n)$. Let $i \in \{1,2\}$. Since $\gcd(m_i, n) = 1$, by Bezout's Lemma, there exists x_i, y_i such that $m_i x_i + n y_i = 1$ for $i = 1, 2$. Thus, $m_i x_i \equiv 1 \bmod n$ for $i \in \{1,2\}$ and hence $m_1 m_2 (x_1 x_2) \equiv 1 \bmod n$. It follows that $\gcd(m_1, m_2, n) = 1$ and $(m_1 m_2) \bmod n \in U(n)$.

We now check the three properties given in the definition:

- Associativity is inherited from multiplication modulo n;
- $1 \in U(n)$ is the identity element;
- Existence of inverse follows from Theorem 5.6, which states that $a \in \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ has a multiplicative inverse iff $\gcd(a,n) = 1$, which is satisfied by all $a \in U(n)$.

□

1.6. Corollary: $\{1, 2, \ldots, n-1\}$ *is a group under multiplication under modulo n iff n is prime.*

Proof. By Proposition 1.5, $\{1, 2, \ldots, n-1\}$ is a group under multiplication modulo n iff n is relatively prime to every $m \in \{1, 2, \ldots, n-1\}$ iff n is prime. □

Section 2. Elementary Properties of Groups

We start with three elementary properties:

- *Uniqueness of identity.*
- *Cancellation property.*
- *Uniqueness of inverse element.*

2.1. Theorem: *There exists a unique element $e \in G$ such that $ae = ea = a$ for every $a \in G$.*

Proof. The existence of an element e is guaranteed by the definiton of a group. Suppose e and f are both identity elements. Then $e = ef = f$. □

2.2. Theorem: *Let $a, b, c \in G$. Then $ba = ca \implies b = c$ and $ab = ac \implies b = c$.*

Proof. Suppose $ba = ca$. Then multiplying both sides on the right by an inverse of a gives $b = c$, so we have right cancellation. The other side follows similarly. □

2.3. Theorem: *For each $a \in G$, there exists a unique element $b \in G$ such that $ab = ba = e$.*

Proof. Suppose there exist $b, c \in G$ such that $ab = ba = e$ and $ac = ca = e$. Then $c = ce = c(ab) = (ca)b = eb = b$. □

2.4. Remark: Let G be a group.

- By uniqueness of inverses, we denote the inverse of an element $a \in G$ as $a^{-1} \in G$.
- The associative property means that we can unambiguously write the product

$$\underbrace{a \times \cdots \times a}_{n \text{ times}}$$

as a^n for $n \in \mathbb{N}$. For $n < 0$, we take a^n to be the $(-n)$-fold product of a^{-1} and $a^0 := e$.

In general, it is not true in a non-Abelian group G that $(ab)^n = a^n b^n$ for $a, b \in G$ and $n \in \mathbb{Z}$. Howver, we have the following result that expresses the inverse of a product as a reversed product of inverses.

2.5. Theorem: *Let G be a group and $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof. $(ab)b^{-1}a^{-1} = e = b^{-1}a^{-1}ab$. □

Chapter 3

Subgroups

Section 1. Subgroups

1.1. Definition: A subset H of a group G which is itself a group under the operation of G is called a **subgroup** of G. This is denoted by $H \leq G$.

1.2. Note:

- If $H \leq G$ and $H \neq G$, then H is called a **proper subgroup** of G, denoted $H < G$.
- The subgroup $\{e\}$ is called the **trivial subgroup** of G; others are said to be **non-trivial**.

1.3. Example:

- $(\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$: easy.
- $(\mathbb{Z}_n, + \bmod n) \not\leq (\mathbb{Z},+)$ because they have different operations.

Section 2. Subgroup Tests

If a subset of a group is closed under the group operation as well as the inverse operation, then it is a subgroup.

2.1. Theorem (One-Step Subgroup Test): *Let G be a group and H be a non-empty subset of G. If $ab^{-1} \in H$ for all $a, b \in H$, then H is a subgroup of G.*

Proof. We check the definition of groups:

(1). The operation of G defines a binary operation on H, that is, H is closed under the operation. Let $x, y \in H$. Then $xy = x(y^{-1})^{-1} \in H$ by the hypothesis.

(2). The associativity of the operation is inherited from G.

(3). As $H \neq \varnothing$, there exists some $a \in H$, so $e = aa^{-1} \in H$.

(4). Let $a \in H$. Then $a^{-1} = ea^{-1} \in H$ by the hypothesis.

Hence, H is a group in its own right and thus a subgroup of G. □

2.2. Corollary (Two-Step Subgroup Test): *Let G be a group and H be a non-empty subset of G. If $ab \in H$ for all $a, b \in H$ and $a^{-1} \in H$ for all $a \in H$, then H is a subgroup of G.*

Proof. Trivial. □

2.3. Note: Let G be a subgroup and $H \subseteq G$. To show that H is a subgroup of G:

(1). Show that H is non-empty.

(2). Let $a, b \in H$, show that $ab^{-1} \in H$ (or show $ab \in H$ and $a^{-1} \in H$ separately).

2.4. Example: Let G be an Abelian group. We use one-step subgroup test to show the following subsets are subgroups of G:

- $\{x \in G \mid x^2 = e\}$: Since $e^2 = e$, $H \neq \varnothing$. Let $a, b \in G$. Since G is Abelian, we have
$$(ab^{-1})(ab^{-1}) = a^2(b^{-1})^2 = ee = e \implies ab^{-1} \in H.$$
- $\{x^2 \mid x \in G\}$: Since $G \neq \varnothing$, $H \neq \varnothing$. Let $a, b \in H$ with $a = x^2$ and $b = y^2$ for $x, y \in G$. Then
$$ab^{-1} = x^2y^{-2} = (xy^{-1})^2 \in H.$$
- $HK = \{hk \mid h \in H \subseteq G, k \in K \subseteq G\}$: Since $e \in H$ and $e \in K$, $e = e^2 \in HK \Rightarrow HK \neq \varnothing$. Let $a, b \in HK$ so $a = h_k k_1$ and $b = h_2k_2$ with $h_i \in H$ and $k_i \in K$. Since G is Abelian,
$$ab^{-1} = h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = (h_1h_2^{-1})(k_1k_2^{-1}) \in HK.$$

2.5. Note: To prove a subset of a group is *not* a subgroup:

- Show that the identity is not in the set.
- Exhibit an element of the set whose inverse is not in the set.
- Exhibit two elements of the set whose product is not in the set.

2.6. Example: Let $G = \mathbb{R}^*$ with multiplication and H be the set of non-zero irrational numbers. Since $\sqrt{2} \in H$ but $\sqrt{2} \cdot \sqrt{2} = 2 \neq H$, we conclude that H is not a subgroup of G.

If the subset is finite, then all we need is its closure under the group operation.

2.7. Theorem (Subgroup Test for Finite Subsets): *Let H be a non-empty finite subset of a group G. If H is closed under the group operation of G, then H is a subgroup of G.*

Proof. As $ab \in H$ for all $a, b \in H$, it suffices to show that for each $a \in H$, its inverse in G, a^{-1} also belongs to H. The finiteness of H plays a key role here. Let $a \neq 0$. As H is closed under the operation of G, $\{a, a^2, \dots, \} \subseteq H$. As H is finite, we must have $a^i = a^j$ for some $i < j$. Hence, $a^{j-i} = e$ for some $j - i > 1$. Rewriting, we have $a(a^{j-i-1}) = e = (a^{j-i-1})a$ which implies that $a^{j-i-1} \in H$ is the inverse of a. □

What can we say about the union and intersection of subgroups?

2.8. Proposition: *Let H and K be subgroups of G. Then*

(1). $H \cap K$ is a subgroup of G.

(2). $H \cup K$ is a subgroup of G iff $H \subset K$ or $K \subset H$.

Proof. (1) Since $e \in H \cap K$, $H \cap K$ is non-empty. Let $x, y \in H \cap K$. Then $xy^{-1} \in H \cap K$.
(2) Suppose $H \subset K$ or $K \subset H$. Then $H \cup K = K$ or $H \cup K = H$. This direction is trivial. Conversely, suppose for a contradiction that $H \cup K$ is a subgroup but $H \not\subset K$ and $K \not\subset H$. Then there exists $h \in H \setminus K$ and $k \in K \setminus H$. Then as h and k are in $H \cup K$, so is their product hk. But this means either $k = h^{-1}(hk) \in H$ or $h = (hk)k^{-1} \in K$, both of which are impossible. Hence, we must have that one subgroup is included in the other. □

2.9. Corollary:

(1). An arbitrary intersection of subgroups is a subgroup.

(2). An arbitrary union of nested subgroups is a subgroup.

Proof. Omitted. □

Section 3. Cyclic Groups

In this section, we introduce the notion of cyclic groups as an example of subgroups and to demonstrate how our subgroup tests work. We will revisit cyclic groups in the next chapter.

3.1. Theorem: *Let G be any group and $a \in G$. Then $\langle a \rangle := \{a^m \mid m \in \mathbb{Z}\}$ is a subgroup of G.*

Proof. For $a^m, a^n \in \langle a \rangle$, we have $a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$. □

3.2. Definition: Let G be a group and $a \in G$.

- The set $\langle a \rangle := \{a^m \mid m \in \mathbb{Z}\}$ is called the **cyclic subgroup of G generated** by a.
- If $\langle a \rangle = G$, then G is said to be **cyclic** and a is called a **generator** of G.

3.3. Remark:

- In general, generators are not unique since if a is a generator of G, then so is a^{-1}.
- Although the list $\{\ldots, a^{-2}, a^{-1}, e, a^1, a^2, \ldots\}$ has infinitely many entries, the set $\{a^n \mid n \in \mathbb{Z}\}$ might have only finitely elements.
- Every cyclic group is Abelian since $a^i a^j = a^{i+j} = a^{j+i} = a^j a^i$.
- When the group operation is addition, a^n means na.

3.4. Example: Some basic examples:

- In $(\mathbb{Z}, +)$, $\mathbb{Z} = \langle 1 \rangle$.
- In $(\mathbb{Z}_{10}, + \bmod 10)$, $\langle 2 \rangle = \{2, 4, 6, 8, 0\}$.
- In $(\mathbb{Z}_n, + \bmod n)$, $\mathbb{Z}_n = \langle 1 \rangle = \langle n-1 \rangle$. (Think: $n = 10$.)

3.5. Example: Fix $n \in \mathbb{N}$ and define $G = \{z \in \mathbb{C} \mid z^n = 1\}$. From MATH-145, we know that $G = \{e^{2k\pi i/n} : k \in \mathbb{Z}\}$. Thus, $G = \left\langle e^{2\pi i/n} \right\rangle$ and hence is a cyclic group, known as the **group of nth root of unity**.

3.6. Example: Recall the group $U(10) = \{1, 3, 7, 9\}$ with multiplication mod 10. Consider the cyclic (sub)groups generated by the element 3, 7, and 9.

- $\langle 3 \rangle = \{3, 9, 7, 1\} = U(10)$ as $3^2 \bmod 10 = 9$, $3^3 \bmod 10 = 7$, and $3^4 \bmod 10 = 1$.
- $\langle 7 \rangle = \{7, 9, 3, 1\} = U(10)$;
- $\langle 9 \rangle = \{9, 1\}$, which is a proper subgroup of $U(10)$.

A cyclic group by definition is a subgroup generated by a single element of the group G. We can generalize this notion to a subgroup generated by any subset S of G.

3.7. Definition: Let S be a non-empty subset of group G. The subgroup **generated** by S, denoted $\langle S\rangle$, is the smallest subgroup of G containing S. More concretely, it is the subgroup of G containing all finite products of elements of S and their inverses.

3.8. Lemma: *If $S \subseteq G$ is a subgroup, then $\langle S\rangle = S$.*

Proof. Trivial. □

Different subsets can generate the same subgroup.

3.9. Example: Let $G = \mathbb{Z}_{12}$ with addition mod 12. Then $\langle\{2, 8\}\rangle = \{0, 2, 4, 6, 8, 10\} = \langle 2\rangle$.

Section 4. Center of a Group and Centralizer of an Element

We now discuss two more examples of subgroups.

- *The center of a group G, $Z(G) \leq G$, which contains the set of elements in G that commutes with every element $g \in G$;*
- *The centralizer of an element $a \in G$, $C(a) \leq G$, which contains the set of elements in G that commutes with a.*

4.1. Definition: The **center** $Z(G)$ of a group G is the subset of elements of G that commute with every element of G, i.e., $Z(G) = \{a \in G \mid \forall x \in G : ax = xa\}$.

4.2. Theorem: *The center of a group, $Z(G)$, is an Abelian subgroup of G.*

Proof. Let e be the identity of G. Then $e \in Z(G)$ so $Z(G) \neq \varnothing$. We show that $ab \in Z(G)$ and $a^{-1} \in Z(G)$ for all $a, b \in Z(G)$. First, let $a, b \in Z(G)$. Then

$$\forall x \in G : (ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab) \implies ab \in Z(G).$$

Next, for $a \in Z(G)$, we have

$$\forall x \in G : ax = xa \implies \cancel{a^{-1}}axa^{-1} = a^{-1}x\cancel{aa^{-1}} \implies xa^{-1} = a^{-1}x \implies z^{-1} \in Z(G).$$

Clearly, $Z(G)$ is an Abelian group. □

4.3. Definition: Let $a \in G$. The **centralizer** $C(a)$ of a in G is the set of all elements of G that commute with a, i.e., $C(a) = \{g \in G \mid ag = ga\}$.

4.4. Theorem: *For each $g \in G$, $C(a)$ is a subgroup of G.*

Proof. Clearly, $Z(G) \subseteq C(a)$ for each $a \in G$, so $C(a)$ is non-empty. We show that $cd \in C(a)$ and $c^{-1} \in C(a)$ for all $c, d \in C(a)$. First, let $c, d \in C(a)$, which means that $ca = ac$ and $da = ad$. Then

$$\forall x \in G : (cd)a = c(da) = c(ad) = (ca)d = (ac)d = a(cd) \implies cd \in C(a).$$

Next, for $c \in C(a)$, we have

$$\forall x \in G : ca = ac \implies \cancel{c^{-1}}cac^{-1} = c^{-1}a\cancel{cc^{-1}} \implies ac^{-1} = c^{-1}a \implies c^{-1} \in C(a).$$

□

There exists a nice relationship between the center and centralizers.

4.5. Lemma: $Z(G) = \bigcap_{a \in G} C(a)$.

Proof. $x \in Z(G)$ iff x commutes with every $a \in G$ iff $x \in C(a)$ for every $a \in G$ iff $x \in \bigcap_{a \in G} C(a)$. □

4.6. Lemma: *G is Abelian iff $C(a) = G$ for every $a \in G$.*

Proof. G is Abelian iff $ab = ba$ for every $a \in G$ iff $C(a) = G$ for every $a \in G$. □

Two important examples.

4.7. Example (Quaternion Group): The **quaternion group** Q is given by the set $\{1, -1, i, -i, j, -j, k, -k\}$ with multiplication table given as follows:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

- $Z(Q) = \{1, -1\}$ (note that $ij \neq ji$ and $kj \neq jk$);
- $C(i) = \{1, -1, i, -i\}$.

4.8. Example (Hisenberg Group): The set of matrices

$$H = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \middle| \; a, b, c \in \mathbb{R} \right\}$$

is a group with matrix multiplication. We will show that

$$Z(H) = \left\{ \begin{bmatrix} 1 & 0 & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \middle| \; y \in \mathbb{R} \right\}.$$

For an element $A \in H$ to be in the center of H, we must have

$$A = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}$$

such that

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

for $a, b, c \in \mathbb{R}$. With some computation, we see this implies that y can be arbitrary while $az = xs$ for all $ac \in \mathbb{R}$. Hence, $x = z = 0$ and A has the claimed form.

Section 5. Order of a Group and of an Element

As we will see, finite groups have interesting arithmetic properties.

5.1. Definition: The **order** of a group G, denoted by $|G|$, is the number of elements in G.

5.2. Definition: The **order** of an element $g \in G$, denoted by $|g|$, is the smallest positive integer n such that $g^n = e$. If not such n exists, the element g is said to have **infinite order**.

5.3. Example:

- Let $G = U(10) = \{1, 3, 7, 9\}$ with multiplication mod 10. Then $|U(10)| = 4$. Moreover, $|1| = 1$, $|3| = |7| = 4$, and $|9| = 2$.
- Let $G = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with addition mod 6. Then $|\mathbb{Z}_6| = 6$ and $|0| = 1, |1| = 6, |2| = 3, |3| = 2, |4| = 3, |5| = 6$.
- Let $G = \mathbb{Z}$ with addition. Then $\mathbb{Z}$ has infinite order and so does each of its non-zero elements.

Suppose G is a group and $a \in G$. We will soon show that the order of the element a is equal to the order of the cyclic group $\langle a \rangle$ generated by a. Thus, overloading "order" makes sense.

Chapter 4

Cyclic Groups

Section 1. Properties of Cyclic Groups

1.1. Definition: A group G is said to be **cyclic** if there exists an element $a \in G$ such that $G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$. Such an element a is called a **generator** of G.

1.2. Example: The group $(\mathbb{Z}, +)$ is cyclic with generators 1 and -1. Indeed, any positive integer can be written as $1 + \cdots + 1$ (n times) and negative integer $-n$ as $(-1 - \cdots - 1)$ (n times). By definition, a^0 here is the identity 0.

1.3. Example: The group $\mathbb{Z}_n$ with addition modulo n for $n \in \mathbb{N}$ is cyclic with generators 1 and $(n-1) \equiv (-1) \bmod n$. In some cases, $\mathbb{Z}_n$ may have other generators. For example, $\mathbb{Z}_7 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 6 \rangle$. We will formalize what generators $\mathbb{Z}_n$ has in Corollary 1.14.

1.4. Example: We have seen that $U(10) = \langle 3 \rangle = \langle 7 \rangle$. On the other hand, $U(8)$ is not cyclic. Indeed, $U(8) = \{1, 3, 5, 7\}$ while $\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{3, 1\}$, $\langle 5, \rangle = \{5, 1\}$, and $\langle 7 \rangle = \{7, 1\}$.

The following theorem says that the order of a cyclic subgroup generated by an element is equal to the order of the element itself, as there are precisely $|a|$ elements in $\langle a \rangle$, both when $|a|$ is finite and infinite. This also explains why we use the same terminology for the order of both a group and an element of a group.

1.5. Theorem: *Let G be a group and $a \in G$.*

- *If $|a| = \infty$, then $\langle a \rangle = \{e, a, a^2, \ldots\}$ and $a^i = a^j \iff i = j$.*
- *If $|a| = n < \infty$, then $\langle a \rangle = \{e, a, \ldots, a^{n-1}\}$ and $a^i = a^j \iff n \mid (j - i)$.*

Proof. Suppose $|a| = \infty$ and $a^i = a^j$. Then $a^{j-i} = e$. But $|a| = \infty$, so

$$a^{j-i} = e \iff j - i = 0 \iff j = i.$$

This also proves that $\langle a \rangle = \{e, a, a^2, \ldots\}$ as no two elements in the set are equal.

Next, suppose a has finite order equal to n, then $a^n = e$. It is clear that $\{e, a, \ldots, a^{n-1}\} \subseteq \langle a \rangle$. We need to show the other direction. Suppose $a^k \in \langle a \rangle$. By the division algorithm, there exist unique $q, r \in \mathbb{Z}$ such that $k = qn + r$ with $0 \leq r < n$. Hence, $a^k = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r$, so $a^k \in \{e, a, \ldots, a^{n-1}\}$.

We are left to show that if $|a| = n$, then $a^i = a^j$ iff $n \mid (j - i)$. Suppose $a^i = a^j$, then $a^{j-i} = e$. By the division algorithm, there exist $q, r \in \mathbb{Z}$ with $) \leq r < n$ such that $j - i = qn + r$. Hence, $e = a^{j-i} = (a^n)^q a^r = e^q a^r = a^r$. But by the definition of order of an element, n is the *least* positive integer such that $a^n = e$. Thus, we must have $r = 0$ and hence $j - i = qn$. It follows that $n \mid (j - i)$. Conversely, suppose $n \mid (j - i)$. Then there exists $q \in \mathbb{Z}$ such that $j - i = nq$. Hence $a^{j-i} = (a^n)^q = e$, so that $a^j = a^i$. □

1.6. Corollary: *Let G be a group and $a \in G$. Then $|a| = |\langle a \rangle|$.*

Proof. The case where $|a| < \infty$ is trivial. Now suppose $|a| = \infty$. Then $a^j \neq a^i$ for $i \neq j$. Hence, the group $\langle a \rangle = \{e, a, a^2, \ldots\}$ is of infinite order. □

1.7. Corollary: *Let G be a group and $a \in G$ be such that $a^k = e$. Then $|a|$ divides k.*

Proof. Let $|a| = n$. As $a^k = e = a^0$, by Theorem 1.5, n divides $k - 0 = k$. □

1.8. Intuition: Here's the key intuition for the theorem. In a cyclic group of order n, multiplication of powers of a corresponds to the addition of the powers mod n. Indeed, if $a^n = e$, then $a^{n+1} = a$, $a^{n+2} = a^2$, ..., and $a^i a^j = a^{(i+j) \bmod n}$ for $i, j \in \mathbb{Z}$. Hence, *a cyclic group of order n behaves exactly like $\mathbb{Z}_n$ with addition modulo n.* Similarly, *a cyclic group of order ∞ behaves just like $\mathbb{Z}$ with addition*, as products of powers of the generator a correspond to adding the powers of a in $\mathbb{Z}$. We formalize what we mean by "behaving like" when we talk about group homomorphisms.

If we know the order of an element $a \in G$, we can compute the order of a^k for any $k \in \mathbb{N}$.

1.9. Theorem: *Let $a \in G$ with $|a| = n \in \mathbb{Z}_+$ and let $k \in \mathbb{Z}_+$. Then*

$$\left\langle a^k \right\rangle = \left\langle a^{\gcd(n,k)} \right\rangle, \qquad \textit{and} \qquad \left| a^k \right| = \frac{n}{\gcd(n,k)}.$$

Proof. Let $d = \gcd(n,k)$. Then $k = dq$ for some $q \in \mathbb{Z}_+$ and $a^k = (a^d)^q$, so that $\langle a^k \rangle \subseteq \langle a^d \rangle$. To show the other inclusion, recall that there exists $s, t \in \mathbb{Z}$ such that $d = ns + kt$. Hence $a^d = a^{ns+kt} = (a^n)^s (a^k)^t = e(a^k)^t = (a^k)^t \in \langle a^k \rangle$, so $\langle a^d \rangle \subseteq \langle a^k \rangle$. Thus, $\langle a^d \rangle = \langle a^k \rangle$.

Next, let b be any divisor of n. Then $(a^b)^{n/b} = a^n = e$, so that $|a^b| \leq n/b$. But if $i < n/b$, then $(a^b)^i \neq e$ as $bi < n$. Hence, $|a^b| = n/b$ for any divisor b of n. In particular, for $d = \gcd(n,k)$, $|a^d| = n/d$. Altogether, along with Corollary 1.6, we get

$$\left| a^k \right| = \left| \left\langle a^k \right\rangle \right| = \left| \left\langle a^d \right\rangle \right| = \left| a^d \right| = \frac{n}{d} = \frac{n}{\gcd(n,k)}.$$

□

The advantage of Theorem 1.9 is that it allows us to replace one generator of a cyclic subgroup with a more convenient one, as shown in the following example.

1.10. Example: If $|a| = 30$, we have $\langle a^{26} \rangle = \langle a^2 \rangle, \langle a^{23} \rangle = \langle a \rangle, \langle a^{22} \rangle = \langle a^2 \rangle, \langle a^{21} \rangle = \langle a^3 \rangle$. From this we can easily see that $\left| a^{23} \right| = |a| = 30$ and $|a^{22}| = |a^2| = 15$. Moreover, if one wants to list the elements of, say, $\langle a^{21} \rangle$, it is easier to list the elements of $\langle a^3 \rangle$ instead.

Theorem 1.9 establishes an important relationship between the order of an element in a finite cyclic group and the order of the group. We now show that the order of an element in a finite cyclic group must divide the order of the group and look at the criterion for $\langle a^i \rangle = \langle a^j \rangle$, or equivalently, $|a^i| = |a^j|$.

1.11. Corollary: *In a finite cyclic group, the order of an element divides the order of the group.*

Proof. Let $G = \langle a \rangle$ and $a^k \in G$ for some $k \in \mathbb{Z}$, and let $|G| = |a| = n$. By Theorem 1.9,

$$|a^k| = \frac{n}{\gcd(n,k)},$$

so the order of a^k divides the order of G. □

1.12. Corollary: *Let G be a group and $a \in G$ with $|a| = n$. Then for all $i, j \in \mathbb{Z}$,*

$$\left\langle a^i \right\rangle = \left\langle a^j \right\rangle \iff \gcd(n,i) = \gcd(n,j) \iff |a^i| = |a^j|.$$

Proof. Suppose $\gcd(n,i) = \gcd(n,j)$. Then by Theorem 1.9,

$$\left\langle a^i \right\rangle = \left\langle a^{\gcd(n,i)} \right\rangle = \left\langle a^{\gcd(n,j)} \right\rangle = \left\langle a^j \right\rangle.$$

Conversely, suppose $\left\langle a^i \right\rangle = \left\langle a^j \right\rangle$, then $|a^i| = |a^j|$, whhich implies by the second part of Theorem 1.9 that

$$\frac{n}{\gcd(n,i)} = \frac{n}{\gcd(n,j)} \implies \gcd(n,i) = \gcd(n,j).$$

The second iff follows by using $|a_i| = n/\gcd(n,i)$. □

The next two corollaries are important special cases of the preceding corollary.

1.13. Corollary: *Let $|a| = n$. Then $\langle a \rangle = \left\langle a^j \right\rangle \iff \gcd(n,j) = 1 \iff |a| = |a^j|$.*

Proof. Substitute $i = 1$ in Corollary 1.12. □

1.14. Corollary: *An integer j in $\mathbb{Z}_n$ is a generator of $\mathbb{Z}_n$ iff $\gcd(n,j) = 1$.*

Proof. We have $\mathbb{Z}_n = \langle 1 \rangle$. By Corollary 1.12, $\langle j \rangle = \langle 1 \rangle = \mathbb{Z}_n$ iff $\gcd(n,j) = 1$. □

1.15. Example: Consider $U(10) = \{1,3,7,9\}$ with order 4. We know that $\langle 3 \rangle = U(10)$. By Corollary 1.13, $\left\langle 3^j \bmod 10 \right\rangle = \langle 3 \rangle \iff \gcd(4,j) = 1$, so $j \in \{1,3\}$, giving us that $3 = 3^1 \bmod 10$ and $7 = 3^3 \bmod 10$ are the generators of $U(10)$.

Section 2. Classification of Subgroups of Cyclic Groups

Suppose $G = \langle a \rangle$ with $|G| = |a| = 30$. The following theorem says that if H is any subgroup of G, then H has the form $\langle a^{30/k} \rangle$ for some k that is a divisor of 30. Moreover, G has one subgroup of each of the orders $1, 2, 3, 5, 6, 10, 15$ and 30, and no others.

2.1. Theorem: *Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n. For each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k, namely $\langle a^{n/k} \rangle$.*

Proof. Let $G = \langle a \rangle$ and $H \leq G$. If $H = \{e\}$, it is of course cyclic with generator e. Suppose H is a proper non-trivial subgroup. We first show there exists $t \in \mathbb{Z}_+$ such that $a^t \in H$. Indeed, we must have $a^t \in H$ for some $t \in \mathbb{Z} \setminus \{0\}$, so a^{-t} is also in H as H is a subgroup, and one of t and $-t$ is in $\mathbb{Z}_+$. Now let m be the smallest positive integer such that $a^m \in H$. We will prove that $\langle a^m \rangle = H$.

Suppose $a^k \in H$ for some $k \in \mathbb{Z}$. We will show that k must be a multiple of m. By the division algorithm, there exists $q, r \in \mathbb{Z}$ with $0 \leq r < m$ such that $k = qm + r$. Hence $a^k = a^{qm}a^r$ so that $a^r = a^k(a^m)^{-q} \in H$ as both a^k and a^m are in H. Since m is the *least* positive integer such that $a^m \in H$ and $0 \leq r < m$, so $r = 0$. Therefore, k is a multiple of m, which implies that $a^k \in \langle a^m \rangle$ and $H = \langle a^m \rangle$ is a cyclic subgroup.

Suppose now that G has finite order and $|G| = |a| = n$. The order of H is given by

$$|\langle a^m \rangle| = |a^m| = \frac{n}{\gcd(n, m)},$$

so the order of H divides n. We also note that $a^n = e \in H = \langle a^m \rangle$, so m divides n. Finally, let k be any positive divisor of n. Then $\langle a^{n/k} \rangle$ has order given by

$$\frac{n}{\gcd(n, n/k)} = \frac{n}{n/k} = k.$$

On the other hand, we will show that any subgroup of order k of $\langle a \rangle$ must be equal to $\langle a^{n/k} \rangle$. By the first part of the theorem, the subgroup must be of the form $\langle a^m \rangle$ for some $m \in \mathbb{N}$ where $m|n$. As $m = \gcd(m, n)$,

$$k = |\langle a^m \rangle| = \frac{n}{\gcd(m, n)} = \frac{n}{m}.$$

Hence, $m = n/k$ and $H = \langle a^{n/k} \rangle$. □

2.2. Corollary: *For each $n \in \mathbb{N}$ and positive divisor k of n, the cyclic subgroup $\langle n/k \rangle$ is the unique subgroup of $\mathbb{Z}_n$ of order k. Moreover, these are the only subgroups of $\mathbb{Z}_n$.*

Proof. Take the group in Theorem 2.1 to be $\mathbb{Z}_n$ and $a = 1$. □

Theorems 1.9 and 2.1 together provide a simple way to find all the generators of the subgroups of a finite cyclic group.

2.3. Example: Consider the cyclic group $\langle a\rangle$ with $|a| = 30$. By Theorem 2.1, we conclude that the subgroups of $\langle a\rangle$ are precisely those of the form $\langle a^m\rangle$ where $m|30$. Moreover, if k is a divisor of 30, then the subgroup of order k is $\left\langle a^{30/k}\right\rangle$ Thus, we can explicitly list out the subgroups of $\langle a\rangle$:

$$\begin{aligned}
\langle a\rangle &= \left\{e, a, a^2, \ldots, a^{29}\right\} && \text{order } 30,\\
\left\langle a^2\right\rangle &= \left\{e, a^2, a^4, \ldots, a^{28}\right\} && \text{order } 15,\\
\left\langle a^3\right\rangle &= \left\{e, a^3, a^6, \ldots, a^{27}\right\} && \text{order } 10,\\
\left\langle a^5\right\rangle &= \left\{e, a^5, a^{10}, a^{15}, a^{20}, a^{25}\right\} && \text{order } 6,\\
\left\langle a^6\right\rangle &= \left\{e, a^6, a^{12}, a^{18}, a^{24}\right\} && \text{order } 5,\\
\left\langle a^{10}\right\rangle &= \left\{e, a^{10}, a^{20}\right\} && \text{order } 3,\\
\left\langle a^{15}\right\rangle &= \left\{e, a^{15}\right\} && \text{order } 2,\\
\left\langle a^{30}\right\rangle &= \{e\} && \text{order } 1.
\end{aligned}$$

2.4. Example: The list of subgroups of $\mathbb{Z}_{30}$ is

$$\begin{aligned}
\langle 1\rangle &= \{0, 1, 2, \ldots, 29\} && \text{order } 30\ ,\\
\langle 2\rangle &= \{0, 2, 4, \ldots, 28\} && \text{order } 15,\\
\langle 3\rangle &= \{0, 3, 6, \ldots, 27\} && \text{order } 10,\\
\langle 5\rangle &= \{0, 5, 10, 15, 20, 25\} && \text{order } 6,\\
\langle 6\rangle &= \{0, 6, 12, 18, 24\} && \text{order } 5,\\
\langle 10\rangle &= \{0, 10, 20\} && \text{order } 3,\\
\langle 15\rangle &= \{0, 15\} && \text{order } 2,\\
\langle 30\rangle &= \{0\} && \text{order } 1.
\end{aligned}$$

2.5. Example: To find the generators of the subgroup of order 9 in $\mathbb{Z}_{36}$, we observe that $36/9 = 4$ is one generator. To find the others, we recall from Corollary 1.13 that $|a| = |a^j| \iff \gcd(n, j = 1)$. Thus, other generators are all elements of $\mathbb{Z}_{36}$ of the form $4j$ (operation is addition here, so power is translated to multiplication), where $\gcd(9, j) = 1$. Thus,

$$\langle 4\cdot 1\rangle = \langle 4\cdot 2\rangle = \langle 4\cdot 4\rangle = \langle 4\cdot 5\rangle = \langle 4\cdot 7\rangle = \langle 4\cdot 8\rangle.$$

In the generic case, to find all the subgroups of $\langle a\rangle$ of order 9 where $|a| = 36$, we have

$$\left\langle \left(a^4\right)^1\right\rangle = \left\langle \left(a^4\right)^2\right\rangle = \left\langle \left(a^4\right)^4\right\rangle = \left\langle \left(a^4\right)^5\right\rangle = \left\langle \left(a^4\right)^7\right\rangle = \left\langle \left(a^4\right)^8\right\rangle.$$

In particular, note that once you have the generator $a^{n/d}$ for the subgroup of order d where d is a divisor of $|a| = n$, all the generators of $\left\langle a^d\right\rangle$ have the form $\left(a^d\right)^j$ where $j \in U(d)$.

By combining Theorems 1.9 and 2.1, we can easily count the number of elements of each order in a finite cyclic group. For convenience, we introduce an important number-theoretic function called the ***Euler*** φ ***function****.*

2.6. Definition: Define the Euler **totient function** by

$$\begin{aligned}\varphi &: \mathbb{Z}_+ \to \mathbb{Z}_+\\ \varphi(1) &= 1\\ \varphi(n) &= \text{number of positive integers less than } n \text{ and relative prime to } n\end{aligned}$$

2.7. Example:

n	1	2	3	4	5	6	7	8	9	10	11	12	$\cdots$
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	$\cdots$

By definition, $|U(n)| = \varphi(n)$ *for each* $n \geq 2$*. We now show that* $\varphi(d)$ *gives the number of elements of order* d *in a cyclic group whose order is a multiple of* d*.*

2.8. Theorem: *If* d *is a positive divisor of* n*, then the number of elements of order* d *in a cyclic group of order* n *is* $\varphi(d)$*.*

Proof. Let $G = \langle b \rangle$ with $|G| = |b| = n$ and H be a unique subgroup of order d given by $\langle b^{n/d} \rangle$. For simplicity, write $a := bn/d$ and note that $|a| = d$. By Corollary 1.12, any element of order d also generates $\langle a \rangle$. Then by Corollary 1.13, an element a^k generates the subgroup $\langle a \rangle$ of order d iff $\gcd(k, d) = 1$. Hence, the number of elements of order d in G is equal to $\varphi(d)$. □

2.9. Remark: Note that for a finite cyclic group of order n, the number of elements of order d for any divisor d of n depends only on d! Thus, $\mathbb{Z}_8$, $\mathbb{Z}_{640}$, and $\mathbb{Z}_{80000}$ each has $\varphi(8) = 4$ elements of order 8, despite they have different orders.

2.10. Corollary: *In a finite group, the number of elements of order* d *is a multiple of* $\varphi(d)$*.*

Proof. If G has no elements of order d, the statement is true as $\varphi(d)$ divides 0. Suppose there exists $a \in G$ with $|a| = d$. Then $\langle a \rangle$ has $\varphi(d)$ elements of order d by Theorem 2.8. Suppose there exists $b \in G$ of order d such that $b \notin \langle a \rangle$. Then $\langle b \rangle$ has $\varphi(d)$ elements of order d. If there exists some c of order d such that $c \in \langle a \rangle \cap \langle b \rangle$, then $\langle a \rangle = \langle c \rangle = \langle b \rangle$, contradicting the fact that $b \notin \langle a \rangle$. Thus, $\langle a \rangle$ and $\langle b \rangle$ together have $2\varphi(d)$ elements. We continue enumerating in this way for each element of order d in G which is not contained in the previously enumerated cyclic subgroups. As G is finite, this process comes to an end to give us that there exists a multiple of $\varphi(d)$ elements of order d. □

The following properties of the φ function make computing $\varphi(n)$ simple. In particular, it is easily computed for powers of prime numbers and for products of relatively prime integers.

2.11. Theorem:

- *For a prime p and $n \in \mathbb{Z}_+$, $\varphi(p^n) = p^n - p^{n-1}$.*
- *Suppose $m, n \in \mathbb{Z}_+$ and $\gcd(m,n) = 1$. Then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. Part 1. We want to enumerate the number of positive integers less than or equal to p^n that are relatively prime to p^n. There are p^n positive integers less than or equal to p^n. Let m be a positive integer less than or equal to p^n. To have $\gcd(p,m) > 1, p$ must be a divisor of m, so m can be one of $p, 2p, \ldots, p^{n-1}p$. There are p^{n-1} such possibilities. Hence $\gcd(p^n, m) = 1$ for $p^n - p^{n-1}$ positive integers m less than p^n, hence $\varphi(p^n) = p^n - p^{n-1}$.

Part 2. We want to enumerate the number of positive integers less than mn that are relatively prime to mn. We list the integers between 1 and mn out as follows:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \ldots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \ldots & (n-1)m+2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ m & m+m & 2m+m & \ldots & (n-1)m+m = mn. \end{array}$$

For each $r \in \{1, \ldots, m\}$, the r-th row contains the elements $km + r$, for $k \in \{0, \ldots, n-1\}$. Now, clearly $\gcd(km + r, m) = \gcd(r, m)$, so that all entries of the r-th row are relatively prime to m if and only if $\gcd(r, m) = 1$. If an integer r is not relatively prime to m, it is not relatively prime to mn, hence to compute $\varphi(mn)$ we can ignore all rows numbered by r where $\gcd(r, m) > 1$. Hence we only consider $\varphi(m)$ rows.

Now, within each of these $\varphi(m)$ rows, we only need those elements that are relatively prime to mn. As $\gcd(m, n) = 1$, the set $\{[0(m) + r], [1(m) + r], \ldots, [(n-1)m + r]\}$ consists of all the possible congruence classes under congruence $\bmod n$, for each r that is relatively prime to m. Out of these, we only need to consider those integers that are relatively prime to n, so there are $\varphi(n)$ such integers. By being in this row, they are also relatively prime to m, hence they are relatively prime to mn.

Thus in total, there are $\varphi(m)$ rows with $\varphi(n)$ elements each that are relatively prime to mn. Hence $\varphi(mn) = \varphi(m)\varphi(n)$. □

Chapter 5

Permutation Groups

Section 1. Definition and Notations

1.1. Definition: Let A be a non-empty set.

- A **permutation** of A is a bijective function from A to A.
- A **permutation group** of a set A is a set of permutations of A that form a group under function composition.

1.2. Remark: We focus on the case where A is finite, of the form $\{1, 2, \dots, n\}$ for some $n \in \mathbb{Z}_+$.

1.3. Notation: Let $A = \{1, 2, 3, 4\}$. Define $\alpha : A \to A$ as

$$\alpha(1) = 2, \quad \alpha(2) = 3, \quad \alpha(3) = 1, \quad \alpha(4) = 4.$$

This can also be written compactly in array form as

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix},$$

where $\alpha(j)$ is placed directly below j for each $j \in A$.

1.4. (Cont'd): Composition of permutations expressed in array notation is carried out from right to left by going from top to bottom, then again from top to bottom. For example, given two permutations

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}, \quad \gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix},$$

we have $(\gamma\sigma)(1) = \gamma(\sigma(1)) = \gamma(2) = 4$:

$$\gamma\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ & \downarrow & & & \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & & & & \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

We note that the product given by function composition is not commutative.

1.5. Example: Consider two permutations $\alpha, \beta : A \to A$ defined by

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}, \quad \beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

Observe that

$$\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}, \quad \beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{bmatrix}.$$

We now give an example of a permutation group.

1.6. Example: Let S_3 denote the set of all bijective functions from $\{1,2,3\}$ to itself. It's easy to see that $|S_3| = 3! = 6$ as there are 6 permutations on a set of size 3. We list the elements out explicitly:

$$S_3 = \left\{ \varepsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right.$$
$$\left. \beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} \right\}$$

Here, ε denotes the identity permutation. Note that $\alpha^3 = \varepsilon = \beta^2$ and $\beta\alpha = \alpha^2 = \beta$.

*This permutation group S_3 is called the **symmetric group** of degree 3.*

1.7. Definition: Let $A = \{1, 2, \ldots, n\}$ and S_n denote the group of all permutations of A, equipped with function composition. Elements of S_n have the following array form:

$$\alpha = \begin{bmatrix} 1 & 2 & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n) \end{bmatrix}$$

S_n is called the **symmetric group of degree** n. It is clear that $|S_n| = n!$.

Permutation groups on A are non-Abelian for if there are at least three elements in A.

1.8. Lemma: *Let $n \geq 3$. Then the center $Z(S_n)$ of S_n is trivial.*

Proof. Let $\varepsilon \neq \pi \in S_n$ be a permutation such that $\pi(i) = j$ for $i \neq j \in A$. Since permutations are injective, $\pi(j) \neq j$. Since $n \geq 3$, we can find $k \notin \{j, \pi(j)\}$ and $\rho \in S_n$ which interchanges j and k and fixes everything else. Let $\pi(j) = m$. Then $m \neq j$ and $m \neq k$, so ρ fixes m, which implies that $\rho(\pi(j)) = \rho(m) = m = \pi(j)$. Now $k = \rho(j)$ by definition of ρ, so $\pi(k) = \pi\rho(j)$. But $\pi(j) \neq \pi(k)$ since permutations are injective. Thus, $\rho\pi(j) \neq \pi\rho(j)$. Therefore, $\pi \neq \varepsilon$ is not in $Z(S_n)$ since there exists a $\rho \in S_n$ such that π does not commute with ρ. Since π was chosen arbitrarily, we conclude that only $\varepsilon \in Z(S_n)$ and hence $Z(S_n)$ is trivial. □

1.9. Proposition: *For $n \geq 3$, S_n is non-Abelian.*

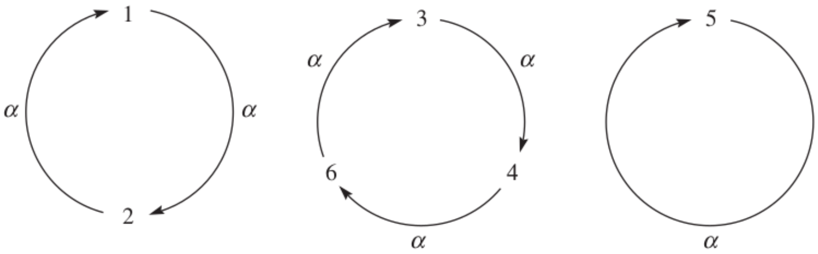
Proof. Recall that a group G is Abelian iff $C(a) = G$ for every $a \in G$. In the Lemma above, we see that for any $\varepsilon \neq \pi \in S_n$, we have a group $\rho \in S_n$ such that $\pi\rho \neq \rho\pi$. It follows that S_n is non-Abelian. □

Section 2. Properties of Permutations

Another common notation for specifying permutations is the ***cycle notation****.*

2.1. Definition: An expression of the form $(a_1, a_2, \ldots, a_m)$ is called a **cycle of length** m or an m**-cycle**.

2.2. Example:



$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix} \iff (1,2)(3,4,6)(5)$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix} \iff (1,5,2,3)(4,6)$$

Often, a cycle with a single entry is omitted and it is understood that the point in question is fixed. For example, the cycle $(4,6)$ can be thought of as representing the permutation $(1)(2)(3)(4,6)(5)$. The identity permutation is often denoted by $\varepsilon = (1)$.

We first show that each permutation can be represented by a product of disjoint cycles.

2.3. Theorem: *Every permutation of a finite set can be written as a product of disjoint cycles.*

Proof. Let α be a permutation on $A = \{1, 2, \ldots, n\}$. Choose $a_1 \in A$, $a_2 = \alpha(a_1)$, $a_3 = \alpha(a_2) = \alpha^2(a_1)$, ..., until we arrive at $a_1 = \alpha^m(a_1)$ for some m. Since A is finite, $m < \infty$. To be precise, we must have $i < j \in \mathbb{N}_0$ such that $\alpha^i(a_1) = \alpha^j(a_1)$, so that $a_1 = \alpha^{j-i}(a_1)$.[1] We express this relationship among $a_1, \ldots, a_m$ as the cycle $(a_1, \ldots, a_m)$ and write $\alpha = (a_1, \ldots, a_m)\cdots$. If $A = \{a_1, \ldots, a_m\}$, we are done. Otherwise, choose $b_1 \in A\backslash\{a_1, \ldots, a_m\}$ and repeat the same process to get a cycle $(b_1, \ldots, b_k)$. We claim that these two cycles are disjoint. Indeed, if $\alpha^i(a_1) = \alpha^j(b_1)$ for some $i, j \in \mathbb{N}_0$, then $\alpha^{i-j}(a_1) = b_1$, which contradicts the criterion for choosing b_1. Continuing in this manner until we find enough disjoint cycles that contain all elements of the finite set A. □

[1] Consider $A = \{1, 2, 3\}$ with
$$\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}.$$
Choose $1 \in A$, $2 = \alpha(1)$, $3 = \alpha(2) = \alpha^2(1)$. We then arrive that $\alpha(3) = \alpha^3(1) = 1$. Here, $m = 3$. To be precisely, $\alpha^0(1) = 1 = \alpha^3(1)$, which gives us $a_1 = \alpha^{3-0}(a_1)$ as desired.

Next, disjoint cycles commute.

2.4. Theorem: *If the pair of cycles $\alpha = (a_1, \ldots, a_m)$ and $\beta = (b_1, \ldots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.*

Proof. Suppose α and β are permutations of $S = \{a_1, \ldots, a_m, b_1, \ldots, b_n, c_1, \ldots, c_s\}$, where the c_i's are left fixed by α and β (not required to exist). We show that $\alpha\beta(x) = \beta\alpha(x)$ for all $x \in S$. The case for $x = c_i$ is trivial. Next, since $a_i \notin \beta$, we know $\beta(a_i) = a_i$ for all i's. Thus, for $x = a_i$,

$$\alpha\beta(a_i) = \alpha(a_i) = a_{i+1} = \beta(a_{i+1}) = \beta\alpha(a_i),$$

with the understanding that $a_{m+1} = a_1$. Similarly, $b_i \notin \alpha \implies \alpha(b_i) = b_i$ for all i's, so

$$\alpha\beta(b_i) = \alpha(b_{i+1}) = b_{i+1} = \beta(b_i) = \beta\alpha(b_i),$$

with the understanding that $b_{n+1} = b_1$. □

We now look at the order of a permutation.

2.5. Lemma: *A cycle of length n has order n; that is, for $\sigma \in S_m$ of length n, $|\langle\sigma\rangle| = n$.*

Proof. By definition, the order of a permutation σ is the smallest positive integer n such that $\sigma^n = \varepsilon$. Suppose we have an n-cycle $\sigma = (a_0, a_1, \ldots, a_{n-1})$. Its order cannot be less than n, because if $0 < k < n$, then $\sigma^k(a_0) = a_k$ and it's implicit in the concept of a cycle that $a_0 \neq a_k$.

On the other hand, σ^n is certainly the identity permutation, because it acts on each element of the cycle by moving it around the entire cycle once. Formally, one can prove by induction that $\sigma^k(a_j) = a_{(j+k) \bmod n}$ and since $n \equiv 0 \bmod n$, we have $(j + n) \bmod n = j$ whenever $0 \leq j < n$.

Finally, elements that are not in the cycle are fixed by σ and therefore also by σ^n. Since $\sigma^n = e$ and $\sigma^k = e$ when $0 < k < n$, we conclude that $|\sigma| = n$. □

2.6. Theorem: *The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.*

Proof. Let us call the elements $c_1, \ldots, c_s$ that appear in a permutation $\gamma = (c_1, \ldots, c_s)$ **symbols**. Suppose that α and β are disjoint cycle of length m and n, and let $k = \text{lcm}(m, n)$. By the Lemma above, $|\alpha| = |\beta| = k$, so $\alpha^k = \varepsilon = \beta^k$. Now $(\alpha\beta)^k = \alpha^k\beta^k$ as α and β commute by Theorem 2.4.

Let t be the order of $\alpha\beta$. Since $(\alpha\beta)^k = \varepsilon$, t divides k. Now $(\alpha\beta)^t = \alpha^t\beta^t = \varepsilon$, so $\alpha^t = \beta^{-t}$. As α and β are disjoint cycles, they have no common symbol. The same holds for α^t and β^{-t} as raising a cycle to a power does not introduce any new symbols. Hence, the equality of α^t and β^{-t} means that we must have $\alpha^t = \varepsilon = \beta^{-t}$, so that m and n both divide t (again since $\alpha^m = \varepsilon = \beta^n$). Hence, the least common multiple k of m and n also divides t. Combined with above, we conclude that $k = t$. That is, $|\alpha\beta| = \text{lcm}(m, n)$. This argument can now be extended to any finite product of disjoint cycles. □

The Theorem above is a powerful tool for calculating the order of permutations and the number of permutations of a particular order.

2.7. Example: Let us find the number of elements of S_7 of order 3. By the Theorem above, we need only count the number of permutations of the form (a_1, a_2, a_3) and $(a_1, a_2, a_3)(a_4, a_5, a_6)$.

- First form: ${}_7P_3 = 70$.
- Second form: $({}_7P_3) \cdot ({}_4P_3) \cdot \frac{1}{2} = 280$. [a]

Thus, there are in total 350 elements of S_7 of order 3.

[a] We need $\frac{1}{2}$ since $(a_1, a_2, a_3)(a_4, a_5, a_6) = (a_4, a_5, a_6)(a_1, a_2, a_3)$ for fixed $\{a_1, \ldots, a_6\}$.

2*-cycles, which are also called* ***transpositions****, are of particular importance.*

2.8. Theorem: *Every permutation in S_n for $n \geq 2$ is a product of 2-cycles.*

Proof. First, write the identity as $\varepsilon = (1,2)(2,1)$. We know that every permutation can be written as a product of disjoint cycles:

$$(a_1, \ldots, a_m)\,(b_1, \ldots, b_n) \cdots (c_1, \ldots, c_s)\,.$$

It is easily verified that this can be written as

$$(a_1, a_m)\,(a_1, a_{m-1}) \cdots (a_1, a_2)\,(b_1, b_n)\,(b_1, b_{n-1}) \cdots (b_1, b_2) \cdots (c_1, c_s)\,(c_1, c_{s-1}) \cdots (c_1 c_2)$$

□

2.9. Example: We claim that $\beta = (1,2,3,4,5) \equiv (1,5)(1,4)(1,3)(1,2)$. By definition, we have

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix}.$$

Observe that

$$\begin{aligned}
&((1,5)(1,4)(1,3)(1,2))(1) = ((1,5)(1,4)(1,3))(2) = 2 \\
&((1,5)(1,4)(1,3)(1,2))(2) = ((1,5)(1,4)(1,3))(1) = ((1,5)(1,4)(1,3))(3) = 3 \\
&((1,5)(1,4)(1,3)(1,2))(3) = ((1,5)(1,4)(1,3))(3) = ((1,5)(1,4))(1) = 4 \\
&((1,5)(1,4)(1,3)(1,2))(4) = ((1,5)(1,4))(4) = ((1,5))(1) = 5 \\
&((1,5)(1,4)(1,3)(1,2))(5) = ((1,5))(5) = 1
\end{aligned}$$

2.10. Remark: It is worth noting that this decomposition into 2-cycles is not unique. For example, the cycle $(1,2,3,4,5)$ can also be expressed as $(5,4)(5,2)(2,1)(2,5)(2,3)(1,3)$.

2.11. Lemma: *If $\varepsilon = \beta_1\beta_2\cdots\beta_r$ where β_i's are 2-cycles, then r is even.*

Proof. Clearly, $r \neq 1$ as a 2-cycle cannot be the identity ε. If $r = 2$, we are done. Now suppose $r > 2$ and that the result is true for all $s < r$. Suppose the rightmost 2-cycle is (a, b). Since $(i, j) = (j, i)$, the product $\beta_{r-1}\beta_r$ can be expressed in one of the following forms for some symbols c, d in the set on which the permutation is considered. The expression on the right in each case can be written as a product of cycles so that a does not occur in the right cycle on the LHS:

$$\begin{aligned}\varepsilon &= (a,b)(a,b)\\ (a,b)(b,c) &= (a,c)(a,b)\\ (a,c)(c,b) &= (b,c)(a,b)\\ (a,b)(c,d) &= (c,d)(a,b)\end{aligned}$$

If the first case occurs, we may delete $\beta_{r-1}\beta_r$ from the original product to obtain $\varepsilon = \beta_1\beta_2\cdots\beta_{r-2}$. By IH, $r-2$ is even, r is even. In the other three cases, we replace the form of $\beta_{r-1}\beta_r$ on the right by its counterpart on the left to obtain a new product of r 2-cycles that is still the identity, but where the rightmost occurrence of the integer a is in the second-from-the-rightmost 2-cycle of the product instead of the rightmost 2-cycle. We now repeat the procedure just described with $\beta_{r-2}\beta_{r-1}$, and, as before, we obtain a product of $(r-2)$ 2-cycles equal to the identity or a new product of r 2-cycles, where the rightmost occurrence of a is in the third 2-cycle from the right. Continuing this process, we must obtain a product of $(r-2)$ 2-cycles equal to the identity, because otherwise we have a product equal to the identity in which the only occurrence of the integer a is in the leftmost 2-cycle, and such a product does not fix a, whereas the identity does. Hence, by IH, $r-2$ is even, and r is even as well. □

All 2-cycle-decompositions of the same permutation have the same parity.

2.12. Theorem: *If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even (respectively, odd) number of 2-cycles.*

Proof. Suppose $\alpha = \beta_1\cdots\beta_r = \gamma_1\cdots\gamma_s$ for $r, s \in \mathbb{N}$. Then $\varepsilon = \gamma_1\cdots\gamma_s\beta_r^{-1}\cdots\beta_1^{-1} = \gamma_1\cdots\gamma_s\beta_r\cdots\beta_1$. Note that we used above that the inverse of a 2-cycle is itself. By the Lemma above, $s+r$ is even, so s, r are both odd or both even. □

The above theorem allows us to make the following definition.

2.13. Definition: A permutation that can be expressed as a product of an even (odd) number of 2-cycles is called an **even** (respectively, **odd**) **permutation**.

2.14. Theorem: *The set of even permutations in S_n forms a subgroup of S_n.*

Proof. First, $\varepsilon \in A_n$. It is clear that a 2-cycle is its own inverse. Hence the inverse of an even permutation is also even. Finally, clearly the product of two even permutations is even. □

2.15. Definition: The group of even permutations in S_n, denoted by A_n, is called the **alternating group** of degree n.

2.16. Theorem: *For $n \geq 2, |A_n| = n!/2$.*

Proof. For each odd permutation α, the permutation $(1,2)\alpha$ is even and $(1,2)\alpha \neq (1,2)\beta$ when $\alpha \neq \beta$. Thus the number of even permutations is greater than or equal to the number of odd permutations. Similarly if α is even, the permutation $(1,2)\alpha$ is odd and $(1,2)\alpha \neq (1,2)\beta$ if $\alpha \neq \beta$. Hence the number of odd permutations is greater than or equal to the number of even permutations. So, indeed, these numbers must be equal and each is equal to $\frac{|S_n|}{2}$. So $|A_n| = \frac{n!}{2}$. □

Section 3. Dihedral Groups

3.1. Motivation: We look at a particular type of permutation groups called **dihedral groups**. We are interested in the so-called **symmetries** of the regular polygon with $n \geq 3$ sides. These are bijections from the polygon onto itself such that the orientation is preserved.They consist of **rotational** and **refection** symmetries.

3.2. Consider an equilateral triangle. In its resting state, the vertices a, b, c are in the positions $1, 2, 3$, respectively. On applying one of our symmetries, the resulting figure must look the same, and only the labels may change. It is clear then that the rotational symmetries are given by rotating (counterclockwise) by 0, $\frac{2\pi}{3}$, and $\frac{4\pi}{3}$. For example, rotating by $\frac{2\pi}{3}$ sends the vertex a to position 2, vertex b to position 3, and vertex c to position 1.

3.3. Let us formalize this using array form and cycle form. First, rotation by $\frac{2\pi}{3}$:

$$r_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} = (1, 2, 3).$$

Next, reflection about the bisector passing through the vertex in the first position:

$$s_0 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = (2, 3).$$

In general, we have

$$\{r_0 = (1), r_1 = (1, 2, 3), r_2 = (1, 3, 2), s_0 = (2, 3), s_1 = (1, 2), s_2 = (1, 3)\},$$

Note there are $6 = 2 \cdot 3$ such symmetries. We are now ready to define dihedral groups.

3.4. For $n \geq 3$, consider the regular n -polygon in $\mathbb{R}^2$. It has $2n$ symmetries, namely n rotations r_k (counter-clockwise) by $\frac{2\pi k}{n}$ for $k = 0, 2, \ldots, n-1$, and n reflections s_l about the axis passing through $\frac{\pi l}{n}$ for $l = 0, \ldots, n-1$. There are $2n$ such symmetries in total. The key point is that the set $\{r_0, \ldots, r_{n-1}, s_0, \ldots, s_{n-1}\}$ forms a group under the product given by composition of maps.

Let us form the multiplication table for the symmetries of the regular 3 -gon, that is, the equilateral triangle considered above.

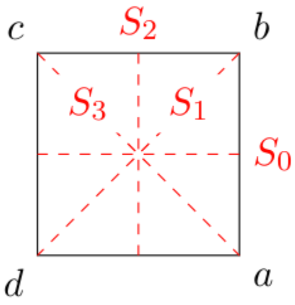
	r_0	r_1	r_2	s_0	s_1	s_2
r_0	r_0	r_1	r_2	s_0	s_1	s_2
r_1	r_1	r_2	r_0	s_1	s_2	s_0
r_2	r_2	r_0	r_1	s_2	s_0	s_1
s_0	s_0	s_2	s_1	r_0	r_2	r_1
s_1	s_1	s_0	s_2	r_1	r_0	r_2
s_2	s_2	s_1	s_0	r_2	r_1	r_0

We now define the dihedral group D_n of order $2n$ abstractly as follows.

3.5. Definition: The dihedral group D_n of order $2n$ is defined by

$$\begin{aligned} r_i r_j &= r_{(i+j) \bmod n} \\ r_i s_j &= s_{(i+j) \bmod n} \\ s_i r_j &= s_{(i-j) \bmod n} \\ s_i s_j &= r_{(i-j) \bmod n} \end{aligned}$$

3.6. Example: Consider the symmetries of a square. $D_4 = \{r_0, r_1, r_2, r_3, s_0, s_1, s_2, s_3\}$, where r_i denotes the (counterclockwise) rotation by $\frac{2\pi i}{4}$ and s_i denote the reflection about the axis passing through $\frac{\pi i}{4}$. The corresponding axes are marked on the figure as S_i:



Let us write the elements of D_4 in array form:

$$\begin{aligned}
r_0 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} = (1) = \varepsilon \\
r_1 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} = (1,2,3,4) \\
r_2 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} = (1,3)(2,4) \\
r_3 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix} = (1,4,3,2) \\
s_0 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} = (1,2)(3,4) \\
s_1 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix} = (1,3) \\
s_2 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} = (1,4)(2,3) \\
s_3 &= \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix} = (2,4)
\end{aligned}$$

Chapter 6

Isomorphisms

Section 1. Definition and Examples

1.1. Definition: A **homomorphism** φ from a group G equipped with a product to another group $\overline{G}$ with product $\star$ is a mapping that preserves the group operation, i.e.,

$$\forall a, b \in G : \varphi(a \cdot b) = \varphi(a) \star \varphi(b).$$

We often omit the product symbol and write $\varphi(ab) = \varphi(a)\varphi(b)$, where it is understood that the product of a and b on the LHS is in G and the product of $\varphi(a)$ and $\varphi(b)$ on the RHS is in $\overline{G}$.

1.2. Definition: An **isomorphism** from a group G to a group $\overline{G}$ is a homomorphism which is *one-to-one* and *onto*. In this case, we say that the groups are **isomorphic** and write $G \cong \overline{G}$.

Implicitly, the existence of a bijective between G and $\overline{G}$ implies that they have the same order. To prove that two groups are isomorphic, we need to show the existence of a well-defined function between the two sets, which is bijective and preserves the group structure.

1.3. Example: Let $G = (\mathbb{R}, +)$ and $\overline{G} = (\mathbb{R}, \times)$. Then G and $\overline{G}$ are isomorphic under the mapping $\varphi(x) = 2^x$. To show this,

- $\varphi(x + y) = 2^{x+y} = 2^x 2^y = \varphi(x)\varphi(y)$.
- Suppose $2^x = 2^y$, then $\log_2 2^x = \log_2 2^y$ so that $x = y$. This φ is injective.
- For every $y \in \mathbb{R}_+$, $x = \log_2(y)$ is the pre-image of y under φ, so it is surjective.

1.4. Example: A cyclic group of infinite order is isomorphic to $\mathbb{Z}$. Let $G = \langle a \rangle$. Define $\varphi : G \to \mathbb{Z}$ by $\varphi(a^k) = k$. Then φ is well-defined and is an isomorphism:

- $\varphi(a^k a^l) = \varphi(a^{k+l}) = k + l = \varphi(a^k) + \varphi(a^l)$, so φ is a homomorphism.
- $\varphi(a^k) = \varphi(a^l) \implies k = l \implies a^k = a^l$, so φ is injective.
- For each $k \in \mathbb{Z}$, the element $a^k \in G$ is mapped to k under φ, so φ is surjective.

1.5. Example: A finite cyclic group $\langle a \rangle$ of order n is isomorphic to $\mathbb{Z}_n$ under the mapping $\varphi(a^k) = k \bmod n$. The mapping φ is well-defined because $a^k = a^l$ in a cyclic group of order n implies that n divides $k - l$. It is an isomorphism as the following hold:

- $\varphi(a^k a^l) = \varphi(a^{k+l}) = (k + l)(\mathrm{mod} n) = k(\mathrm{mod} n) + l(\mathrm{mod} n) = \varphi(a^k) + \varphi(a^l)$, so φ is a homomorphism.
- $\varphi(a^k) = \varphi(a^l) \implies k \bmod n = \ell \bmod n \implies n|(k - l)$, so $a^k = a^l$. Hence, φ is injective.
- For each $k \in \mathbb{Z}_n$, the element $a^k \in G$ is mapped to k under φ, so φ is surjective.

1.6. Example: $U(10)$ and $U(5)$ are both isomorphic to $\mathbb{Z}_4$. Recall that $U(10) = \{1, 3, 7, 9\} = \langle 3 \rangle$ and $U(5) = \{1, 2, 3, 4\} = \langle 3 \rangle$, so both groups are cyclic of order 4 and hence isomorphism to $\mathbb{Z}_4$.

1.7. Example: Let $G = \mathrm{SL}(2, \mathbb{R})$, the simple linear group of 2×2 real matrices with determinant equal to 1. Let $M \in \mathrm{SL}(2, \mathbb{R})$ and define φ_M from G to itself by $\varphi_M(A) = MAM^{-1}$ for $A \in G$. As the determinant is multiplicative, MAM^{-1} does indeed belong to G for each $A \in G$. We will show that φ_M is indeed an isomorphism of G into itself.

- $\varphi_M(AB) = MABM^{-1} = MAM^{-1}MBM^{-1} = \varphi_M(A)\varphi_M(B)$ so φ_M is a group homomorphism.
- Suppose $\varphi_M(A) = \varphi_M(B)$. Then $MAM^{-1} = MBM^{-1}$, so $A = B$ follows by left and right cancellation and thus φ_M is one-to-one.
- Let $B \in G$. Then $A = M^{-1}BM \in G$ and $\varphi_M(A) = MM^{-1}BMM^{-1} = B$, so φ is onto.

This mapping φ_M is called **conjugation** by M.

1.8. Example: We now look at some non-examples.

- The mapping from $\mathbb{R}$ with addition to itself given by $\varphi(x) = x^3$ is not an isomorphism. φ is one-to-one and onto but not a group homomorphism as it is not true that $(x+y)^3 = x^3 + y^3$ for all $x, y \in \mathbb{R}$.
- Two groups of the same order need not be isomorphic. For example, consider $U(10) = \{1, 3, 7, 9\}$ and $U(12) = \{1, 5, 7, 11\}$ both of which are of order 4. Note that $U(10)$ is cyclic with generators 3 and 7, but $U(12)$ is not cyclic. In fact, for each $x \in U(12)$, $x^2 = 1$. Suppose that φ is a group homomorphism from $U(10)$ onto $U(12)$. Then
$$\varphi(9) = \varphi(3 \cdot 3) = \varphi(3)\varphi(3) = 1 = \varphi(1)\varphi(1) = \varphi(1 \cdot 1) = \varphi(1).$$
This means that φ cannot be injective and $U(10) \ncong U(12)$. As we will see later, if two groups are isomorphic and one is cyclic, then the other must also be cyclic.
- $(\mathbb{Q}, +)$ and $(\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}, \times)$ are not isomorphic. If φ were a group isomorphism from $\mathbb{Q}$ onto $\mathbb{Q}^*$ there would exist some rational number a such that $\varphi(a) = -1$. Then
$$-1 = \varphi(a) = \varphi\left(\frac{a}{2} + \frac{a}{2}\right) = \varphi\left(\frac{a}{2}\right)\varphi\left(\frac{a}{2}\right) = \varphi^2\left(\frac{a}{2}\right).$$
However, the square of a rational number cannot be equal to -1.

Section 2. Cayley's Theorem

2.1. Theorem (Cayley): *Every group is isomorphic to a group of permutations.*

Proof. Let G be a group. For $g \in G$, define $L_g : G \to G$ by

$$\forall x \in G : L_g(x) = gx.$$

That is, for each $g \in G$, L_g is the function of left multiplication by g on G. Then L_g is a permutation on G, as it is one-to-one and onto from G to itself.

Let $\overline{G} = \{L_g \mid g \in G\}$. We will define an operation on $\overline{G}$ that makes it a group. As $\overline{G}$ is a set consisting of functions, the obvious operation to define on it is the function composition. We will now show that $\overline{G}$ is indeed a group with this this operation.

- For $g, h \in G$, $L_g L_h(x) = (gh)x = L_{gh}(x) \in \overline{G}$, so $\overline{G}$ is closed under function composition.
- Associativity follows by associativity of function composition.
- L_e is the identity element of $\overline{G}$, where e is the identity of G.
- For each $g \in G$, $L_{g^{-1}}$ is the inverse of L_g.

It remains to show that there exists an isomorphism $\varphi : G \to \overline{G}$. Define $\varphi(g) = L_g$ for $g \in G$. We have already shown that $L_{gh} = L_g L_h$, so that $\varphi(gh) = \varphi(g)\varphi(h)$. Now suppose $L_g = L_h$. Then in particular, $L_g(e) = L_h(e)$, so $ge = he$ and thus $g = h$. Hence, φ is one-to-one. By the definition of $\overline{G}$, it is clear that φ is onto. We have shown that G is isomorphic to the group $\overline{G}$ of permutations of left multipliers on G. Note that $\overline{G}$ is called the **left regular representation** of G. □

Section 3. Properties of Isomorphisms

3.1. Theorem: *Suppose that φ is an isomorphism from a group G onto a group $\overline{G}$ with identity elements denoted by e_G and $e_{\overline{G}}$, respectively. Then the following properties hold:*

(1). φ carries the identity of G to $\overline{G}$, that is, $\varphi(e_G) = e_{\overline{G}}$.

(2). For each $n \in \mathbb{Z}$ and $a \in G$, $\varphi(a^n) = \varphi^n(a)$. In particular, $\varphi(a^{-1}) = \varphi^{-1}(a)$.

(3). For $a, b \in G$, $ab = ba \iff \varphi(a)\varphi(b) = \varphi(b) = \varphi(a)$.

(4). $G = \langle a \rangle \iff \overline{G} = \langle \varphi(a) \rangle$.

(5). $|a| = |\varphi(a)|$ for all $a \in G$.

(6). For $k \in \mathbb{Z}$ and $b \in G$, the equation $x^k = b$ has the same number of solutions in G as does the equation $y^k = \varphi(b)$ in $\overline{G}$.

(7). If $|G|$ is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

Proof.

(1). $e_{\overline{G}}\varphi(e_G) = \varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G)\varphi(e_G)$. By cancellation, $\varphi(e_G) = e_{\overline{G}}$.

(2). For positive integers $n \in \mathbb{N}$, we show that $\varphi(a^n) = \varphi^n(a)$ by induction. The base case $n = 1, 2$ are trivial. Suppose it is true for $k \in \mathbb{N}$, that is, $\varphi(a^k) = \varphi^k(a)$. Then

$$\varphi(a^{k+1}) = \varphi(a^k a) = \varphi(a^k)\varphi(a) = \varphi^k(a)\varphi(a) = \varphi^{k+1}(a).$$

For $n = 0$, we already have the equality $\varphi(e_G) = e_{\overline{G}}$. The $n < 0$ case is identical.

(3). $ab = ba \Leftrightarrow \varphi(ab) = \varphi(ba) \Leftrightarrow \varphi(a)\varphi(b) = \varphi(b)\varphi(a)$ by injectivity and multiplicativity of φ.

(4). Suppose $G = \langle a \rangle$, then certainly $\langle \varphi(a) \rangle \leq \overline{G}$. On the other hand, for any $\overline{g} \in \overline{G}$, there exists $g \in G = \langle a \rangle$ such that $\varphi(g) = \overline{g}$. The element g must be of the form a^k for some $k \in \mathbb{Z}$, hence $\overline{g} = \varphi(a^k) = \varphi^k(a) \in \langle \varphi(a) \rangle$.

(5). If $\varphi^m(a) = e_{\overline{G}}$ for some $m \in \mathbb{N}$ and m is the smallest such positive integer, then $\varphi(a^m) = e_{\overline{G}} = \varphi(e_G)$ so that $a^m = e_G$ by injectivity of φ. Suppose $a^k = e_G$ for some smaller positive integer than m. Then $\varphi^k(a) = e_{\overline{G}}$, a contradiction. Hence, $|a| = |\varphi(a)|$.

(6). Suppose $g^k = b$ for some $g \in G$, then $\varphi(g)^k = \varphi(g^k) = \varphi(b)$, so that $\varphi(g)$ is a solution of the equation $y^k = \varphi(b)$ in $\overline{G}$. Conversely, if $\overline{g}^k = \varphi(b)$ and let $g \in G$ be the unique pre-image of $\overline{g}$ under φ. Then $\varphi(g^k) = \varphi^k(g) = \overline{g}^k = \varphi(b)$, so that $g^k = b$ by injectivity.

(7). Follows from the fact that $|a| = |\varphi(a)|$ for all $a \in G$.

□

3.2. The failure of any one of the above properties can be used to show that certain groups are not isomorphic.

3.3. Theorem: *Suppose that φ is an isomorphism from a group G onto a group $\overline{G}$. Then*

(1). φ^{-1} is an isomorphism from $\overline{G}$ onto G.

(2). G is Abelian iff $\overline{G}$ is Abelian.

(3). G is cyclic iff $\overline{G}$ is cyclic.

(4). If $K \leq G$, then $\varphi(K) = \{\varphi(k) \mid k \in K\} \leq \overline{G}$.

(5). If $\overline{K} \leq \overline{G}$, then $\varphi^{-1}(\overline{K}) = \{g \in G \mid \varphi(g) \in \overline{K}\}$ is a subgroup of G.

(6). $\varphi(Z(G)) = Z(\overline{G})$.

Proof.

(1). We show that φ^{-1} is a group homomorphism. Let $x, y \in \overline{G}$. Then there exists $a, b \in G$ such that $x = \varphi(a)$ and $y = \varphi(b)$. Hence, $\varphi^{-1}(xy) = \varphi^{-1}(\varphi(a)\varphi(b)) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(x)\varphi^{-1}(y)$. Finally, φ^{-1} is bijective as φ is bijective.

(2). Follows from Theorem 3.1(3).

(3). Follows from Theorem 3.1(4).

(4). Clearly, $e_{\overline{G}} = \varphi(e_G) \in \varphi(K)$ so $\varphi(K)$ is non-empty. Suppose $\varphi(k_1), \varphi(k_2) \in \varphi(K)$. Then $\varphi(k_1)\varphi(k_2)^{-1} = \varphi(k_1 k_2^{-1}) \in \varphi(K)$ as $k_1 k_2^{-1} \in K$. Hence, $\varphi(K)$ is a subgroup.

(5). Follows from (1) and (4).

(6). Follows from Theorem 3.1(3).

□

Section 4. Automorphisms

4.1. Definition: An **automorphism** is an isomorphism from a group G onto itself. The set of automorphisms of a group G is denoted by $\mathrm{Aut}(G)$.

4.2. Example: The function $\varphi : \mathbb{C} \to \mathbb{C}, \varphi(a + bi) = a - b_i$ is an automorphism on $(\mathbb{C}, +)$.

4.3. Definition: Let G be a group and $a \in G$. The function φ_a defined on G by $\varphi_a(g) = aga^{-1}$ for all $g \in G$ is called the **inner automorphism** of G induced by a. The set of all inner automorphisms of G is denoted by $\mathrm{Inn}(G)$.

4.4. Example: Consider φ_{r_1} induced by r_1 on D_4. Recall that $r_1^{-1} = r_3$. Thus,

x	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1xr_1^{-1}$
r_0	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1r_0r_1^{-1} = r_1r_0r_3 = r_0$
r_1	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1r_1r_1^{-1} = r_1$
r_2	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1r_2r_1^{-1} = r_1r_2r_3 = r_2$
r_3	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1r_3r_1^{-1} = r_1r_3r_3 = r_3$
s_0	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1s_0r_1^{-1} = r_1s_0r_3 = s_2$
s_1	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1s_1r_1^{-1} = r_1s_1r_3 = s_3$
s_2	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1s_2r_1^{-1} = r_1s_2r_3 = s_0$
s_3	$\overset{\varphi_{r_1}}{\mapsto}$	$r_1s_3r_1^{-1} = r_1s_3r_3 = s_1$

4.5. Theorem: *For a group G, $\mathrm{Aut}(G)$ and $\mathrm{Inn}(G)$ are groups under function composition.*

Proof. The proof for $\mathrm{Aut}(G)$ is trivial. Now suppose φ_a, φ_b are inner automorphisms induced by $a, b \in G$. Then $\varphi_a\varphi_b(x) = \varphi_a(bxb^{-1}) = a(bxb^{-1})a^{-1} = (ab)x(ab)^{-1} = \varphi_{ab}(x)$. Associativity follows from function composition. Clearly, φ_e is the identity and $(\varphi_a)^{-1} = \varphi_{a^{-1}}$. □

4.6. Example: Let us compute $\mathrm{Inn}(D_4)$, the set of all inner automorphisms on the group D_4. First, for any $y \in Z(G)$, $\varphi_y = \varphi_{r_0}$ which is the identity automorphism:

$$y \in Z(G) \implies \forall x \in G : yxy^{-1} = xyy^{-1} = x \implies \varphi_y = \varphi_{r_0}.$$

From the table, $r_0, r_2 \in Z(D_4)$, so $\varphi_{r_2} = \varphi_{r_0}$. Next,

$$\varphi_{r_3}(x) = r_3xr_3^{-1} = r_1r_2xr_2^{-1}r_1^{-1} = r_1xr_1^{-1} = \varphi_{r_1}(x).$$

Similarly, as $s_0 = r_2s_2$ and $s_1 = r_2s_3$, we have $\varphi_{s_0} = \varphi_{s_2}$ and $\varphi_{s_1} = \varphi_{s_3}$, so we are now left with only $\varphi_{r_0}, \varphi_{r_1}, \varphi_{s_0}, \varphi_{s_1}$. These are the distinct inner automorphisms (details omitted).

4.7. Example: We now show how to compute $\text{Aut}(\mathbb{Z}_{10})$. Let $\alpha \in \text{Aut}(\mathbb{Z}_{10})$. Then by the group automorphism property, α is completely determined by its value at the identity, 1, as $\alpha(l) = \alpha(l(1)) = l\alpha(1)$. As 1 is an element of order 10, by Theorem 3.1 (v), for α to be an isomorphism, $\alpha(1)$ must also be an element of order 10. By Corollary 1.13 applied to $\mathbb{Z}_{10}$, we have $|k| = |1| = 10$ iff $\gcd(10, k) = 1$, hence $k \in \{1, 3, 7, 9\}$. Hence, we can choose $\alpha(1)$ to be one of these four possible values. Depending on our choice, let us denote the corresponding mappings by $\alpha_1, \alpha_3, \alpha_7, \alpha_9$. We will now show that each of these mappings is indeed an automorphism.

As $\alpha_1(k) = k\alpha_1(1) = k$, α_1 is the identity automorphism. For each remaining α_k, $x \bmod 10 \equiv y \bmod 10 \iff kx \bmod 10 \equiv ky \bmod 10$ as $\gcd(k, 10) = 1$. Thus, each α_k is well-defined. It is clearly a group homomorphism as $\alpha_k(a + b) = k(a + b) \bmod 10 = (ka + kb) \bmod 10 = (\alpha_k(a) + \alpha_k(b)) \bmod 10$. As k is a generator of $\mathbb{Z}_{10}$ for each k with $\gcd(k, 10) = 1$, each α_k is onto. To see it's one-to-one, suppose $\alpha_k(a) = \alpha_k(b)$, then $ka \equiv kb \bmod 10$ which implies that $10|k(b - a)$. But then $\gcd(k, 10) = 1 \implies 10(b - a)$ so $a \equiv b \bmod 10$.

	α_1	α_3	α_7	α_9
α_1	α_1	α_3	α_7	α_9
α_3	α_3	α_9	α_1	α_7
α_7	α_7	α_1	α_9	α_3
α_9	α_9	α_7	α_3	α_1

We now have the following multiplication table for $\text{Aut}(\mathbb{Z}_{10})$. It is parallel to the multiplication table of $U(10)$, which is not a coincidence.

4.8. Theorem: *For each $n \in \mathbb{N}$, $\text{Aut}(\mathbb{Z}_n)$ is isomorphic to $U(n)$.*

Proof. Any automorphism α is determined by the value of $\alpha(1)$. As $\alpha(1)$ must have order equal to the order of 1 which is n, it can take values in $U(n)$ by Corollary 1.13. Define the map $T : \text{Aut}(\mathbb{Z}_n) \to U(n)$ by $T(\alpha) = \alpha(1)$. As α is uniquely determined by $\alpha(1)$, T is a one-to-one mapping. To show T is onto, let $k \in U(n)$ and $\alpha_k \in \text{Aut}(\mathbb{Z}_n)$ be the map such that $\alpha_k(1) = k$. Then of course $T(\alpha_k) = k$. It remains to show that T is a group homomorphism. Let $\alpha, \beta \in \text{Aut}(\mathbb{Z}_n)$. Then

$$T(\alpha\beta) = \alpha\beta(1) = \alpha\underbrace{(1 + \cdots + 1)}_{\beta(1) \text{ times}} = \underbrace{\alpha(1) + \cdots + \alpha(1)}_{\beta(1) \text{ times}} = \alpha(1)\beta(1) = T(\alpha)T(\beta).$$

□

Chapter 7

Cosets and Lagrange's Theorem

Section 1. Cosets

1.1. Definition: Let G be a group and H be a non-empty subset of G. For any $a \in G$, define

$$\begin{aligned} aH &= \{ah \mid h \in H\} \\ Ha &= \{ha \mid h \in H\} \\ aHa^{-1} &= \{aha^{-1} \mid h \in G\} \end{aligned}$$

If $H \leq G$, aH is called the **left coset of H in G containing** a and Ha is called the **right coset of H in G containing** a. The element a is called the **coset representative** of aH (or Ha).

1.2. Example: Consider the following elementary examples:

- Let $G = S_3$, $H = \{(1), (1,3)\}$. The left cosets of H in S_3 are:

$$\begin{aligned} (1)H &= H \\ (1,2)H &= \{(1,2)(1), (1,2)(1,3)\} = \{(1,2), (1,3,2)\} \\ (1,3,2)H &= \{(1,3,2), (1,3,2)(1,3)\} = \{(1,3,2), (1,2)\} \\ (1,3)H &= \{(1,3), (1,3)(1,3)\} = \{(1,3), (1)\} = H \\ (2,3)H &= \{(2,3), (2,3)(1,3)\} = \{(2,3), (1,2,3)\} \\ (1,2,3)H &= \{(1,2,3), (1,2,3)(1,3)\} = \{(1,2,3), (2,3)\} \end{aligned}$$

- Let $G = \mathbb{Z}_9$, $H = \{0, 3, 6\}$. The cosets of H in $\mathbb{Z}_9$ are:

$$\begin{aligned} 0 + H = \{0,3,6\} = 3 + H = 6 + H \\ 1 + H = \{1,4,7\} = 4 + H = 7 + H \\ 2 + H = \{2,5,8\} = 5 + H = 8 + H \end{aligned}$$

- Let $G = D_4$, $H = \{r_0, r_2\}$. The cosets of H in D_4 are

$$\begin{aligned} r_0H &= \{r_0, r_2\} = H \\ r_1H &= \{r_1, r_1r_2\} = \{r_1, r_3\} \\ r_2H &= \{r_2, r_2r_2\} = \{r_2, r_0\} = H \\ r_3H &= \{r_3, r_3r_2\} = \{r_3, r_1\} \\ s_0H &= \{s_0, s_0r_2\} = \{s_0, s_2\} \\ s_1H &= \{s_1, s_1r_2\} = \{s_1, s_3\} \\ s_2H &= \{s_2, s_2r_2\} = \{s_2, s_0\} \\ s_3H &= \{s_3, s_3r_2\} = \{s_3, s_1\} \end{aligned}$$

We have some observations:

- Cosets need not be subgroups.
- Cosets of a subgroup H corresponding to different elements $a, b \in G$ can be the same.
- The left coset does not need to equal to the right coset, i.e., aH need not be the same as Ha.

These examples and observations raise many questions:

- *When does $aH = bH$? (See Lemma 1.3 (4), (6).)*
- *Do aH and bH have any elements in common? (See Lemma 1.3 (5).)*
- *When does $aH = Ha$? (See Lemma 1.3 (8).)*
- *Which cosets are subgroups? (See Lemma 1.3 (9).)*

1.3. Lemma: *Let $H \leq G$ and $a, b \in G$. Then*

(1). $a \in aH$.

(2). $aH = H \iff a \in H$.

(3). $(ab)H = a(bH)$ *and* $H(ab) = (Ha)b$.

(4). $aH = bH \iff a \in bH$.

(5). Either $aH = bH$ *or* $aH \cap bH = \varnothing$.

(6). $aH = bH \iff a^{-1}b \in H$.

(7). $|aH| = |bH|$.

(8). $aH = Ha \iff H = aHa^{-1}$.

(9). $aH \leq G \iff a \in H$.

Proof. (1). $H \leq G \Rightarrow e \in H \Rightarrow a = ae \in aH$.

(2). $a \in H \Rightarrow \forall h \in H : ah \in H \Rightarrow aH \subseteq H$. On the other hand, $a \in H \Rightarrow a^{-1} \in H \Rightarrow h = a(a^{-1}h) \in aH \Rightarrow H \subseteq aH$. Conversely, suppose that $aH = H$. Then $a = ae \in aH = H$.

(3). By associativity, $(ab)h = a(bh)$ and $h(ab) = (ha)b$ for all $h \in H$.

(4). $aH = bH \Rightarrow a = ae \in aH = bH$. Conversely, $a \in bH \Rightarrow \exists h_1 \in H : a = bh_1 \Rightarrow aH = (bh_1)H = b(h_1)H = bH$ by (2) and (3).

(5). $c \in aH \cap bH \Rightarrow aH = cH = bH$ by (4).

(6). $aH = bH \Leftrightarrow H = a^{-1}bH \Leftrightarrow a^{-1}b \in H$ by (4).

(7). The map $ah \to bh$ from aH to bH is bijective, so they have the same size.

(8). $aH = Ha \Leftrightarrow aHa^{-1} = Haa^{-1} = H$.

(9). $a \in H \Rightarrow aH = H \leq G$ by (2). Conversely, $aH \leq G \Rightarrow e \in aH \Rightarrow eH \cap aH \neq \varnothing$. By (5), $aH = eH = H$ so $a \in H$ by (2).

□

1.4. Remark: Note that (1), (5), and (7) imply that a group G can be partitioned into distinct cosets of equal cardinality, and indeed the relation $a \sim b$ iff $aH = bH$ is an equivalence relation that partitions G into equivalence classes given by distinct cosets. The subgroup H is often thus chosen in such a way as to partition the group in some desirable way. For example, consider $H = \mathrm{SL}(2, \mathbb{R}) \leq G = \mathrm{GL}(2, \mathbb{R})$ and its cosets. For any matrix $A \in \mathrm{GL}(2, \mathbb{R})$, the coset AH consists of all matrices with the same determinant as A.

Section 2. Lagrange's Theorem

2.1. Theorem: *If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$. The number of distinct left/right cosets of H in G is $|G|/|H|$.*

Proof. Let $a_1H, \dots, a_rH$ denote the distinct left cosets of H in G. Then for each $a \in G$, $aH = a_iH$ for some i. By Lemma 1.3(1), $a \in aH = a_iH$. Thus, each $a \in G$ belongs to some coset a_iH, i.e.,

$$G = a_1H \cup \cdots \cup a_rH.$$

This union is disjoint by Lemma 1.3(5), hence $|G| = |a_1H| + \cdots + |a_rH| = r|H|$ by Lemma 1.3(7). Hence, $|H|$ divides $|G|$ and $|G|/|H|$ is equal to the number of left cosets of H in G. □

Lagrange's Theorem is a subgroup candidate criterion, that is, it provides a list of candidates for the orders of subgroups of a group. For example, a group of order 12 may have subgroups of order 12, 6,4,3,2,1, but no others. However, the converse of Lagrange's Theorem is False! In other words, a group of order 12 need not have a subgroup of order 6. See below.

2.2. Example: The converse of Lagrange's theorem is false. Consider A_4, the alternating group of degree 4 (the set of even permutations of $\{1, 2, 3, 4\}$ under composition). Then

$$|A_4| = \frac{4!}{2} = 12,$$

but we claim that A_4 has no subgroups of order 6. To see this, observe that S_4 has 8 elements of order 3 as they are all 3-cycles; they are even permutations and belong to A_4. Now suppose that A_4 has a subgroup H of order 6. Let a be any element of order 3 in A_4 and suppose $a \notin H$. Then $A_4 = H \cup aH$ so that $a^2 \in H$ or $a^2 \in aH$. If $a^2 \in H$, then $a = a^4 \in H$, a contradiction. On the other hand, $a^2 \in aH$ implies that $a^2 = ah$ for some $h \in H$, so $a \in H$, a contradiction. Thus, it must be true that $a \in H$ for every a with order 3. But this implies that 8 elements belong to a subgroup of order 6, contradiction.

This counterexample shows that unlike in a cyclic group, a finite group of order n need not have a subgroup of order k if k divides n. (Compare with Theorem 2.1.)

Next, we give a special name and notation for the number of left/cosets of a subgroup in a group. Corollary 2.4 is an immediate consequence of the proof of Lagrange's Theorem.

2.3. Definition: The **index** of a subgroup H in G, denoted by $|G : H|$, is the number of distinct left cosets of H in G.

2.4. Corollary: *If G is a finite group and $H \leq G$, then $|G : H| = |G|/|H|$.*

Proof. Trivial. □

2.5. Corollary: *In a finite group, the order of each element of the group divides the order of the group.*

Proof. Let G be a finite group and $a \in G$. Then $\langle a \rangle \leq G$ and hence $|a| = | \langle a \rangle |$ divides $|G|$. □

2.6. Corollary: *A group of prime order is cyclic.*

Proof. Let G have prime order, say p, and let $e \neq a \in G$. By Lagrange, $| \langle a \rangle |$ divides $|G| = p$, so $| \langle a \rangle | = p$ or 1. As $a \neq e$, $\langle a \rangle = p$, which implies that $\langle a \rangle = G$. □

2.7. Corollary: *Let G be a finite group and $a \in G$. Then $a^{|G|} = e$.*

Proof. By Corollary 2.5, there exists $n \in \mathbb{N}$ such that $n|a| = |G|$. Hence $a^{|G|} = a^{n|a|} = e$. □

2.8. Corollary (Fermat's Little Theorem): *For every $a \in \mathbb{Z}$ and every prime p,*

$$a^p \bmod p = a \bmod p.$$

Proof. There exist $m, r \in \mathbb{Z}$ with $0 \leq r < p$ such that $a = pm + r$, that is, $a \bmod p \equiv r$. It remains to prove that $r^p \bmod p \equiv r$. If $r = 0$, the result holds. If $r \in \{1, 2, \ldots, p-1\} = U(p)$, then by Lemma 2.7, $r^{p-1} \bmod p \equiv 1$. Hence, $r^p \bmod p \equiv r$. □

2.9. Example: Consider $p = 2^{257} - 1$. If p is prime, then by Fermat's Little Theorem,

$$10^p \bmod p = 10 \bmod p \implies 10^{p+1} \bmod p = 100 \bmod p.$$

Using multiple precision and a simple loop, a computer was able to calculate

$$10^{p+1} \bmod p = 10^{2^{257}} \bmod p$$

in a few seconds. The result was not 100, so p is not prime.

The following places powerful limits on the existence of certain subgroups in finite groups.

2.10. Theorem: *For two finite subgroups H and K of a group, let $HK = \{hk \mid h \in H, k \in K\}$. Then*

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

Proof. The set HK has hk products, but they may not all be distinct. That is, we may have $hk = h'k$ with $h \neq h' \in H$ and $k \neq k' \in K$. To determine $|HK|$, we must find the extent to which this happens. For each $t \in H \cap K$, $hk = h(tt^{-1})k = (ht)(t^{-1}k) \in HK$ as $ht \in H$ and $t^{-1}k \in K$. Hence, each group element in HK is represented by at least $|H \cap K|$ products in HK. But $hk = h'k'$ implies $t := h^{-1}h' = kk'^{-1} \in H \cap K$, so that $h' = ht$ and $k' = t^{-1}k$. Thus, each element in HK is represented by exactly $|H \cap K|$ products. The result follows. □

2.11. Example: A group of order 75 can have at most one subgroup of order 25. Suppose for a contradiction that G has two subgroups of order 25, H and K. Since $|H \cap K|$ divides $|H| = 25$, we know that $|H \cap K| \in \{1, 5, 25\}$. By Theorem 2.10, we have

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{25 \cdot 25}{|H \cap K|} \in \{625, 125, 25\}.$$

But $HK \subseteq G$, so $|HK| \leq |G| = 75$. It follows that $|H \cap K| = 25$ and therefore $H = K$.

For any prime $p > 2$, we know that $\mathbb{Z}_{2p}$ and D_p are non-isomorphic groups of order $2p$. This naturally raises the question of whether there could be other possible groups of these orders.

2.12. Theorem (Classification of Groups of Order $2p$): *Let G be a group of order $2p$, where $p > 2$ is prime. Then G is isomorphic to $\mathbb{Z}_{2p}$ or D_p.*

Proof. If G has an element of order $2p$, then $G \cong \langle a \rangle$, i.e., G is a cyclic group of order $2p$ and is thus isomorphic to $\mathbb{Z}_{2p}$. Now suppose there is no element of order $2p$ in G. Then any non-identity element of G must have order 2 or p by Corollary 2.5. If every non-identity element of G has order 2, then G is Abelian. In this case, the set $\{e, a, b, ab\}$ is closed and contains all inverses, hence it is a subgroup of order 4 of G, contradicts to the fact that any subgroup of G must have order 2 or p by Lagrange's Theorem. Hence, some element $a \in G$ must have order p.

Let $b \in G \setminus \langle a \rangle$. Then $|b| \in \{2, p\}$. By another application of Lagrange's Theorem, $|\langle a \rangle \cap \langle b \rangle|$ divides $|\langle a \rangle| = p$ and $\langle a \rangle \neq \langle b \rangle \implies |\langle a \rangle \cap \langle b \rangle| = 1$. If $|b| = p$, then by Theorem 2.10,

$$|\langle a \rangle \langle b \rangle| = \frac{p^2}{1} = p^2 > 2p = |G|,$$

which is impossible, so it must hold that $|b| = 2$. Thus, altogether, we have shown that any element outside $\langle a \rangle$ must have order 2. Further, note that $e, a, a^2, \ldots, a^{p-1}$ and $b, ab, a^2b, \ldots, a^{p-1}b$ are all distinct elements of G. Since there are $2p = |G|$ such elements, they must be all the elements of G.

Consider the element ab. Since it does not belong to $\langle a \rangle$, it must have order 2. Hence, $ab = (ab)^{-1} = ba^{-1}$. This relation will determine the multiplication table of G.

Recall the dihedral group D_p of order $2p$ for $p \geq 3$. Choose a rotation of order p (e.g., r_1) and any reflection (e.g., s_2). Then every element of D_{2p} can be written as products of these two elements. The set $\{r_1, s_2\}$ is said to *generate* the group G. Further, $r_1 s_2 = s_3$ and $s_2 r_1^{-1} = s_2 r_{p-1} = s_{(2-p+1) \bmod p} = s_3$ so that $r_1 s_2 = s_2 r_1^{-1}$.

In G (and D_p), the multiplication table is completely determined by the relation $ab = ba^{-1}$ as we have the following:

$$a^k a^l = a^{k+l \bmod p} \quad , \quad a^k(a^l b) = a^{k+l \bmod p} b$$
$$(a^l b)a^k = ba^{-l}a^k = ba^{k-l \bmod p} = a^{l-k \bmod p} b \quad , \quad (a^k b)(a^l b) = a^k b^2 a^{-l} = a^{k-l \bmod p}$$

Hence $G \cong D_p$ via the isomorphism $\varphi(a^q b^r) = r_1^q s_2^r$ for $q = 0, 1, \ldots, p-1$ and $r = 0, 1$. □

2.13. Corollary: $S_3 \cong D_3$.

Proof. $|S_3| = 2(3) = 6$ and it is not cyclic. □

Section 3. An Application to Permutation Groups

3.1. Definition: Let G be a group of permutations of a set S. For each $i \in S$,

- the **stabilizer** of i in G is defined as $\mathrm{stab}_G(i) = \{\varphi \in G \mid \varphi(i) = i\} \subseteq G$.
- the **orbit** of i in G is defined as $\mathrm{orb}_G(i) = \{\varphi(i) \mid \varphi \in G\} \subseteq S$.

3.2. Lemma: *For all $i \in G$, $\mathrm{stab}_G(i) \leq G$.*

Proof. Trivial. □

3.3. Example: Let the group G be given by

$$G = \{(1), (1,3,2)(4,6,5)(7,8), (1,3,2)4,6,5), (1,2,3)(4,5,6), (1,2,3)(4,5,6)(7,8), (7,8)\}$$

Then

$$\begin{array}{rcl@{\qquad}rcl}
\mathrm{orb}_G(1) & = & \{1,3,2\} & \mathrm{stab}_G(1) & = & \{(1),(7,8)\} \\
\mathrm{orb}_G(2) & = & \{2,1,3\} & \mathrm{stab}_G(2) & = & \{(1),(7,8)\} \\
\mathrm{orb}_G(3) & = & \{3,2,1\} & \mathrm{stab}_G(3) & = & \{(1),(7,8)\} \\
\mathrm{orb}_G(4) & = & \{4,6,5\} & \mathrm{stab}_G(4) & = & \{(1),(7,8)\} \\
\mathrm{orb}_G(5) & = & \{5,4,6\} & \mathrm{stab}_G(5) & = & \{(1),(7,8)\} \\
\mathrm{orb}_G(6) & = & \{6,5,4\} & \mathrm{stab}_G(6) & = & \{(1),(7,8)\} \\
\mathrm{orb}_G(7) & = & \{7,8\} & \mathrm{stab}_G(7) & = & \{(1),(1,3,2)(4,6,5),(1,2,3)(4,5,6)\} \\
\mathrm{orb}_G(8) & = & \{8,7\} & \mathrm{stab}_G(8) & = & \{(1),(1,3,2)(4,6,5),(1,2,3)(4,5,6)\}
\end{array}$$

3.4. Theorem: *[Orbit Stabilizer] Let G be a finite group of permutations of a set S. Then*

$$\forall i \in S : |G| = |\mathrm{orb}_G(i)| \cdot |\mathrm{stab}_G(i)|.$$

Proof. By Lagrange's theorem, $\frac{|G|}{|\mathrm{stab}_G(i)|}$ gives the number of left cosets of $\mathrm{stab}_G(i)$ in G. We will give a one-to-one correspondence between the left-cosets of $\mathrm{stab}_G(i)$ and the elements in the orbit of i. Define $T(\varphi(\mathrm{stab}_G(i))) = \varphi(i)$. To see that T is well-defined, note that if

$$\alpha \cdot \mathrm{stab}_G(i) = \beta \cdot \mathrm{stab}_G(i),$$

then $\alpha^{-1}\beta \in \mathrm{stab}_G(i)$ which implies that $(\alpha^{-1}\beta)(i) = i$. This gives that $\alpha(i) = \beta(i)$ so T is well-defined. To see it's one-to-one, suppose that $\alpha(i) = \beta(i)$. Then $(\alpha^{-1}\beta)(i) = i$, so $\alpha^{-1}\beta \in \mathrm{stab}_G(i)$. This implies that $\alpha \cdot \mathrm{stab}_G(i) = \beta \cdot \mathrm{stab}_G(i)$, establishing that T is one-to-one. Finally, we show that T is onto. Let $j \in \mathrm{orb}_G(i)$, so $j = \alpha(i)$ for some $\alpha \in G$. Hence $j = \alpha(i) = T(\alpha \cdot \mathrm{stab}_G(i))$. Altogether, we have shown that there exists a bijection between the left cosets of $\mathrm{stab}_G(i)$ and the orbit of i, hence

$$\frac{|G|}{|\mathrm{stab}_G(i)|} = |\mathrm{orb}_G(i)|.$$

□

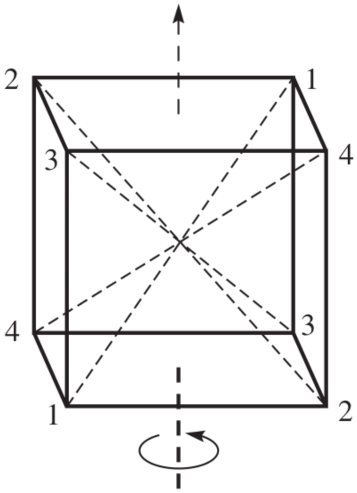
Section 4. Rotation Group of a Cube

Let G be the rotation group of a cube. What is $|G|$? Let us view G as a group of permutations on the set $\{1, 2, 3, 4, 5, 6\}$, as any rotation must carry a face of the cube to a face of the cube.

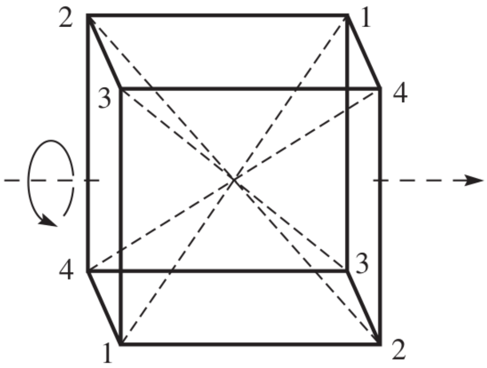
WLOG, let us fix the face corresponding to 1 and use the Orbit-Stabilizer theorem. There exists a rotation that carries face 1 to each of the faces 1, 2,3, 4, 5, 6, so $|\mathrm{orb}_G(i)| = 6$. The rotations that fix face 1 are given by rotations $0, \pi/2, \pi, 3\pi/2$ about the line perpendicular to face 1 passing through the center of the cube. Hence, $|\mathrm{stab}_G(i)| = 4$. Altogether,

$$|G| = |\mathrm{orb}_G(1)| \cdot |\mathrm{stab}_G(1)| = 6 \cdot 4 = 24.$$

4.1. Theorem: *The group of rotations of a cube is isomorphic to S_4.*



$\alpha = (1234)$



$\beta = (1423)$

Proof. We show that G maps to a subgroup of S_4, hence must be equal to S_4 as $|S_4| = 24$. To each rotation of the cube, we associate an element of S_4. In particular, a cube has 4 diagonals and the rotation group induces a group of permutations on the four diagonals. Labelling the diagonals a, b, c, d, we see that a $\pi/2$ rotation yields the permutation $\alpha = (1, 2, 3, 4)$ and another $\pi/2$ rotation yields $\beta = (1, 4, 2, 3)$. Hence, the group of permutations of the diagonals induced by the rotations of the cube contains the 8 element subgroup

$$\{\varepsilon, \alpha, \alpha^2, \alpha^3, \beta^2, \beta^2\alpha, \beta^2\alpha^2, \beta^2\alpha^3\},$$

and the element $\alpha\beta$ has order 3. Clearly, then, the rotations yield all 24 permutations, since the order of the rotation group must be divisible by both 8 and 3 (by Lagrange and Corollary 2.5). It follows that $G \cong S_4$. □

Chapter 8

Direct Products

Section 1. Definition

1.1. Definition: The **external direct product** of groups $G_1, \ldots, G_n$, written as $G_1 \oplus \cdots \oplus G_n$, is the set of all n-tuples in which the ith component is an element of G_i, and the operation is component-wise. That is,

$$G_1 \oplus \cdots \oplus G_n = \{(g_1, \ldots, g_n) \mid g_i \in G_i\}$$

with $(g_1, \ldots, g_n)(h_1, \ldots, h_n) = (g_1h_1, \ldots, g_nh_n)$.

It is implicit in the definition that the operation in each component i corresponds to the binary operation of G_i. It is easy to show that the external direct produt of groups is itself a group.

1.2. Example:

$$\begin{aligned} U(5) \oplus U(3) &= \{1,2,3,4\} \oplus \{1,2\} \\ &= \{(1,1),(1,2),(2,1),(2,2),(3,1),(3,2),(4,1),(4,2)\}. \end{aligned}$$

As an example $(2,2)(3,1) = (1,2)$ as $(2 \cdot 3) \bmod 5 = 1$ and $(2 \cdot 1) \bmod 3 = 2$.

1.3. Example:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}.$$

Note that this group is Abelian and of order 6, so it is isomorphic to $\mathbb{Z}_6$. To see this, we show that $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ is cyclic of order 6. Consider the element $(1,1)$ in the direct product. We have

$$\begin{array}{lll} 1(1,1) = (1,1) & 2(1,1) = (0,2) & 3(1,1) = (1,0) \\ 4(1,1) = (0,1) & 5(1,1) = (1,2) & 6(1,1) = (0,0) \end{array}$$

1.4. Example: Any group of order 4 is isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Let $G = \{e, a, b, ab\}$. If G is cyclic, it is isomorphic to $\mathbb{Z}_4$. If not, by Lagrange's theorem it holds that each non-identity element has order 2, that is, $|a| = |b| = |ab| = 2$. Define the mapping $\varphi : G \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$ by $\varphi(e) = (0,0)$, $\varphi(a) = (1,0)$, $\varphi(b) = (0,1)$, and $\varphi(ab) = (1,1)$. Then it is easily verified that φ is an isomorphism.

Combining this example with Theorem 2.12 gives a complete classification of all groups of order $2p$ for p prime.

Section 2. Properties of External Direct Products

2.1. Theorem: *The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. That is,*

$$|(g_1, g_2, \ldots, g_n)| = \operatorname{lcm}(|g_1|, |g_2|, \ldots, |g_n|).$$

Proof. Let e_i denote the identity of G_i for $i = 1, \ldots, n$. Define $s = \operatorname{lcm}(|g_1|, \ldots, |g_n|)$ an $t = |(g_1, \ldots, g_n)|$. Then $(g_1, \ldots, g_n)^s = (g_1^s, \ldots, g_n^s) = (e_1, \ldots, e_n)$, so that t divides s by Corollary 1.7. On the other hand, as $(g_1^t, \ldots, g_n^t) = (g_1, \ldots, g_n)^t = (e_1, \ldots, e_n)$, we have $g_i^t = e_i$ for each i. Again by Corollary 1.7, we have $|g_i|$ divides t for each i. Hence, the least common multiple of all the $|g_i|$'s, s, divides t. □

2.2. Example: We determine the number of elements in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ of order 5. By Theorem 2.1, we must count those elements $(a, b) \in \mathbb{Z}_{25} \oplus \mathbb{Z}_5$ such that $5 = \operatorname{lcm}(|a|, |b|)$. This tells us that we either have $|a| = 5$ and $|b| \in \{1, 5\}$, or $|a| = 1$ and $|b| = 5$.

- In the first case, $a \in \{5, 10, 14, 20\}$ (by Corollary 1.13); $b \in \{0, 1, 2, 3, 4\}$ (order either 1 or 5). Hence, there are 4 choices for a and 5 choices for b, with a total of 20 choices.
- In the second case, $a = 0$ and $b \in \{1, 2, 3, 4\}$. This case gives 4 elements of order 5.

Altogether, there are $20 + 4 = 24$ elements of order 5 in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$.

2.3. Example: We determine the number of cyclic subgroups in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$ of order 10. Let us enumerate the number of elements of order 10. By Theorem 2.1, we have two cases: $|a| = 10 \wedge |b| \in \{1, 5\}$, or $|a| = 2 \wedge |b| = 5$.

- In the first case, we have $a \in \{10, 30, 70, 90\}$ and $b \in \{1, 5, 10, 15, 20\}$.
- In the second case, we have $a = 1$ and $b \in \{5, 10, 15, 20\}$.

Hence, we get a total of 24 elements of order 10. However, as each subgroup of order 10 has 4 generators, there are in total 6 cyclic subgroups of order 10.

2.4. Theorem: *Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic iff $|G|$ and $|H|$ are relatively prime.*

Proof. Suppose $G \oplus H$ is cyclic and $m = |G|, n = |H|$. Let $d = \gcd(m, n)$. Then $|G \oplus H| = |G||H| = mn$. Suppose (a, b) is a generator of $G \oplus H$. Then

$$(a, b)^{mn/d} = ((a^m)^{n/d}, (b^n)^{m/d}) = (e_G, e_H)$$

as $a^m = e_G$ and $b^n = e_H$. Hence $mn = |(a, b)|$ divides mn/d which forces that $d = 1$.

On the other hand, suppose $\gcd(m, n) = 1$ and a, b are generators of G, H, respectively. Then

$$|(a, b)| = \operatorname{lcm}(m, n) = mn = |G \oplus H|$$

as $\gcd(m, n) = 1$, so that (a, b) must be a generator of $G \oplus H$. □

2.5. Corollary: *An external direct product $G_1 \oplus \cdots \oplus G_n$ of finite cyclic groups is cyclic iff $|G_i|$ and $|G_j|$ are relatively prime for all $i \neq j$.*

Proof. Induction on Theorem 2.4. □

2.6. Corollary: *Let $m = n_1 \cdots n_k$. Then $\mathbb{Z}_m$ is isomorphic to $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ iff $\gcd(n_i, n_j) = 1$ for all $i \neq j$.*

Proof. $|Z_{n_i}| = |n_i|$. Now apply Theorem 2.4. □

2.7. Remark: This result can be used to express the same group up to isomorphism in different forms. For example,

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{15} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$$

We also have

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{10}$$

Section 3. Internal Direct Products

So far, we have been looking at the external direct product, where we start with a finite number of groups and use them to arrive at a larger group in such a way that properties of the larger group can be derived from them:

- *If $G = H \oplus K$, then $|G| = |H||K|$.*
- *Every element of G has the form (h, k) with $h \in H$ and $k \in K$.*
- *If $|h|$ and $|k|$ are finite, then $|(h, k)| = \operatorname{lcm}(|h|, |k|)$.*
- *If H and K are Abelian, then so is $G = H \oplus K$.*
- *If H and K are cyclic and $\gcd(|H|, |K|) = 1$, then $G = H \oplus K$ is also cyclic.*

*We would now like to reverse this process, that is, to start with a group G and break it down into a product of subgroups so that properties of G can be obtained from properties of the subgroups. It is possible to do this if the subgroups are **normal**.*

3.1. Definition: A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all $a \in G$. This is denoted by $H \trianglelefteq G$.

3.2. Proposition: *Let H be a normal subgroup of a group G and K be any subgroup of G. Then HK is a subgroup of G.*

Proof. The identity $e = ee \in HK$, so HK is non-empty. Let $a = h_1k_1, b = h_2k_2 \in HK$. Then $ab^{-1} = (h_1k_1)\left(k_2^{-1}h_2^{-1}\right) = h_1\left(k_1k_2^{-1}\right)h_2 = h_1h'\left(k_1k_2^{-1}\right)$ for some $h' \in H$ as H is normal. Hence $ab^{-1} = (h_1h')\left(k_1k_2^{-1}\right) \in HK$ so that HK is a subgroup. □

3.3. Definition: A group G is said to be the internal direct product of H and K and we write $G = H \times K$ if H and K are normal subgroups of G, $G = HK$, and $H \cap K = \{e\}$.

3.4. Example: Let $G = D_6 = \{r_0, \ldots, r_5, s_0, \ldots, s_5\}$ be the dihedral group of order 12. Let $H = \{r_0, r_2, r_4, s_0, r_2s_0, r_4s_0\}$ and $K = \{r_0, r_3\}$. Then H and K are normal subgroups of G, $H \cap K = \{r_0\}$, and $HK = G$.

3.5. Definition: Let $H_1, \ldots, H_n$ be a finite collection of normal subgroups of G. We say that G is the internal direct product of $H_1, \ldots, H_n$ and write $G = H_1 \times \cdots \times H_n$ if

- $G = H_1 \cdots H_n$;
- $(H_1 \cdots H_i) \cap H_{i+1} = \{e\}$ for $i = 1, \ldots, n-1$.

3.6. Theorem: *If a group G is the internal direct product of a finite number of subgroups*

$H_1, \ldots, H_n$, then G is isomorphic to the external direct product of $H_1, \ldots, H_n$.

Proof. We first show that $h_i \in H_i$ and $h_j \in H_j$ commute for $i \neq j$. Observe that

$$(h_i h_j h_i^{-1}) h_j^{-1} \in H_j h_j^{-1} = H_j$$

as H_j is normal. Similarly,

$$h_i (h_j h_i^{-1} h_j^{-1}) \in h_i H_i = H_i$$

as H_i is normal. Hence, $h_i h_j h_i^{-1} h_j^{-1} \in H_i \cap H_j = \{e\}$, so $h_i h_j = h_j h_i$.

Next, we show that each element of G has a unique representation in the form $h_1 \cdots h_n$ with $h_i \in H_i$. Indeed, suppose $h_1 \cdots h_n = h_1' \cdots h_n'$ with $h_i, h_i' \in H_i$ for each i. Then $h_n' h_n^{-1} = \left(h_{n-1}'\right)^{-1} \cdots (h_1')^{-1} h_1 \cdots h_{n-1}$. By the fact that h_i and h_j commute for $i \neq j$, we get $h_n' h_n^{-1} = (h_1')^{-1} h_1 (h_2')^{-1} h_2 \cdots \left(h_{n-1}'\right)^{-1} h_{n-1}$, so that $h_n' h_n^{-1} \in H_n \cap H_1 H_2 \cdots H_{n-1} = \{e\}$ and $h_n' = h_n$. We can now cancel h_n and h_n' from the two sides of $h_1 \cdots h_n = h_1' \cdots h_n'$ and repeat the same process until we arrive at $h_i = h_i'$ for all i.

Now that we have established the uniqueness of the representation of an element g in G as a product of elements of H_i we can define the following map $\varphi : G \to H_1 \oplus H_2 \oplus \cdots \oplus H_n$ without ambiguity:

$$\varphi \left(h_1 h_2 \cdots h_n\right) = (h_1, h_2, \cdots, h_n)$$

Then φ is an isomorphism (verify this!). □

Chapter 9

Normal Subgroups

Section 1. Definitions and Examples

We have seen that for $H \leq G$, it is not always true that $aH = Ha$. When this special property holds, we say that H is a ***normal*** *subgroup of G and write $H \trianglelefteq G$.*

1.1. Definition: A subgroup H of a group G is called a **normal subgroup** of G, denoted $H \trianglelefteq G$, if $aH = Ha$ for all $a \in G$.

1.2. Intuition: In a normal subgroup H of G, you can switch the order of a product of an element a from the group G and an element h from the normal subgroup H, but you must "fudge" a bit on the element from the normal subgroup H by using some h' from H rather than h. That is, there is an element h' in H such that $ah = h'a$. Likewise, there is some h'' in H such that $ha = ah''$. (It is possible that $h' = h$ and $h'' = h$, but we may not assume this.)

The following result is known as the ***normal subgroup test****.*

1.3. Theorem: *A subgroup H of G is normal iff $xHx^{-1} \subseteq H$ for all $x \in G$.*

Proof. If H is normal, then for each $x \in G$ and $h \in H$, $xh = h'x$ for some $h' \in H$. Hence $xhx^{-1} = h' \in H$ and $xHx^{-1} \subseteq H$. Now suppose $xHx^{-1} \subseteq H$ for all $x \in G$. Then for each $h \in H$, there exists $h' \in H$ such that $xhx^{-1} = h'$, which implies that $xh = h'x$ and $xH \subseteq Hx$. On the other hand, since $x^{-1} \in G$, there exists $h'' \in H$ such that $x^{-1}hx = h''$ for each $h \in H$, so that $hx = xh''$ and $Hx \subseteq xH$. □

1.4. Lemma: *Every subgroup of an Abelian group is normal.*

Proof. Let G be Abelian and $H \leq G$. Then $\forall g \in G : gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg$. □

1.5. Lemma: *The center $Z(G)$ of a group is normal.*

Proof. Recall that the center $Z(G)$ is an Abelian subgroup, i.e., $\forall a \in G, \forall h \in Z(G) : ah = ha$. □

1.6. Lemma: *H is a normal subgroup of its normalizer $N(H) := \{x \in G \mid xHx^{-1} = H\}$.*

Proof. We first show that $H \leq N(H)$. For $x \in H$, we have $xH = H$. Also, $x^{-1} \in H$ by group axiom, so $Hx^{-1} = H$. Together, we see that $xHx^{-1} = H$ and $x \in N(H)$. This tells us that $H \subseteq N(H)$. Now H is itself a group so it is a subgroup of $N(H)$, i.e., $H \leq N(H)$.

It remains to show that H is normal in $N(H)$. Let $a \in H$ and $b \in N(H)$. By the definition of normalizer, $bab^{-1} \in H$. It follows that H is normal in $N(H)$. □

1.7. Lemma: *The alternating group A_n is a normal subgroup of S_n for each n.*

Proof. Later. □

1.8. Lemma: *Every subgroup of D_n consisting only of rotations is normal.*

Proof. For any rotation R and any reflection F, we have $FR = R^{-1}F$. Moreover, any two rotations commute. □

1.9. Lemma: *Let H be a normal subgroup of a group G and K be any subgroup of G. Then HK is a subgroup of G.*

Proof. Note that $e = ee$ is in HK. Then for any $a = h_1k_1$ and $b = h_2k_2$ where $h_1, h_2 \in H$ and $k_1, k_2 \in K$, there is an element $h' \in H$ such that

$$ab^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1(k_1k_2^{-1})h_2^{-1} = (h_1h')(k_1k_2^{-1}).$$

Thus, $ab^{-1} \in HK$. As a warning, you should not assume that this result holds for arbitrary subgroups H and K of G. □

1.10. Lemma: *If a group G has a unique subgroup H of some finite order, then $H \trianglelefteq G$.*

Proof. For any $g \in G$, $gHg^{-1} \leq G$ and $|gHg^{-1}| = |H|$. □

1.11. Lemma: $\mathrm{SL}(2, \mathbb{R}) \trianglelefteq \mathrm{GL}(2, \mathbb{R})$.

Proof. Let $x \in \mathrm{GL}(2, \mathbb{R}) = G$ and $h \in \mathrm{SL}(2, \mathbb{R}) = H$. Note that $\det(xhx^{-1}) = \det(x) \cdot \det(h) \cdot (\det(x))^{-1} = \det(x) \cdot (\det(x))^{-1} = 1$. Thus, $xhx^{-1} \in H$ and $xHx^{-1} \subseteq H$. □

Section 2. Quotient Groups

*The reason why normal subgroups are of special significance is that when $H \trianglelefteq G$ is normal, then the set of left/right cosets of H in G is itself a group, called the **factor group** or **quotient group** of G by H. We can often obtain information about a group by studying one of its factor groups.*

2.1. Theorem: *Let G be group and $H \trianglelefteq G$. The set $G/H = \{aH \mid a \in G\}$ is a group under the operation $(aH)(bH) = abH$.*

Proof. We first show that the operation is well-defined. Suppose $aH = a'H$ and $bH = b'H$. Then there exists $h_1, h_2 \in H$ such that $a' = ah_1$ and $b' = bh_2$, so that

$$\begin{aligned} a'b'H = ah_1bh_2H &= ah_1bH \\ &= ah_1Hb && H \text{ is normal} \\ &= aHb \\ &= abH && H \text{ is normal} \end{aligned}$$

Clearly, eH is the identity and $a^{-1}H$ is the inverse of aH for each $a \in G$. Finally, associativity follows because for $a, b, c \in G$,

$$(aHbH)cH = (abH)(cH) = (ab)cH = a(bc)H = aH(bcH) = aH(bHcH).$$

□

2.2. Remark: For the above group operation to be well-defined, H must be a normal subgroup of G. To see this, for any $h \in H$, $hH = eH = H$. Hence for $a \in G$, $eHaH = eaH = aH$ is the same as $hHaH = haH$, so that $aH = haH$ for every $h \in H$. This tells us that $a^{-1}ha \in H$ and $a^{-1}Ha \subseteq H$ for every $a \in G$. By definition, H is normal.

2.3. Definition: Let $H \trianglelefteq G$. Then the group G/H is called the **quotient group** of G by H.

2.4. Remark: Clearly, the order of the quotient group G/H is the number of left cosets of H in G, which is the index of H in G, given by $|G : H|$. If $|G| < \infty$ and H is normal,

$$|G/H| = \frac{|G|}{|H|}.$$

2.5. Remark: Note that for a normal subgroup H of G and $g \in G$, $|gH|$ can denote both the order of the coset gH in the quotient group G/H and the cardinality of the coset gH, and these two numbers need not be equal. It will generally be clear from the context what we mean.

2.6. Example: Let $4\mathbb{Z} = \{0, \pm 4, \pm 8, \ldots\}$. Then $\mathbb{Z}/4\mathbb{Z}$ consists of the left cosets of $4\mathbb{Z}$ in $\mathbb{Z}$, which are $0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}$. The "multiplication table" of $\mathbb{Z}/4\mathbb{Z}$ (with addition) is given by

	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

It follows then that $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$ with order 4. It is not hard to show that for any $n \in \mathbb{N}$, taking $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$, we have $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

2.7. Example: Consider the subgroup $K = \{r_0, r_2\}$ of the dihedral group D_4. We have seen that $r_0K = r_2K$, $r_1K = r_3K$, $s_0K = s_2K$, and $s_1K = s_3K$. Thus, $K \trianglelefteq D_4$ and the quotient group $D_4/K = \{K, r_1K, s_0K, s_2K\}$ has multiplication table

	K	r_1K	s_0K	s_1K
K	K	r_1K	s_0K	s_1K
r_1K	r_1K	K	s_1K	s_0K
s_0K	s_0K	s_1K	K	r_1K
s_1K	s_1K	s_0K	r_1K	K

$=$

	r_0	r_2	r_1	r_3	s_0	s_2	s_1	s_3
r_0	r_0	r_2	r_1	r_3	s_0	s_2	s_1	s_3
r_2	r_2	r_0	r_3	r_1	s_2	s_0	s_3	s_1
r_1	r_1	r_3	r_2	r_0	s_1	s_3	s_2	s_0
r_3	r_3	r_1	r_0	r_3	s_3	s_1	s_0	s_2
s_0	s_0	s_2	s_3	s_1	r_0	r_2	r_3	r_1
s_2	s_2	s_0	s_1	s_3	r_2	r_0	r_1	r_3
s_1	s_1	s_3	s_0	s_2	r_1	r_3	r_0	r_2
s_3	s_3	s_1	s_2	s_0	r_3	r_1	r_2	r_0

The above table is simply the multiplication table of D_4 but arranged in a way that corresponds to the multiplication table of D_4/K. We see that the formation of a quotient group causes a systematic collapse of the elements of G, i.e., all the elements in the coset of H containing a reduce to a single element aH in G/H.

Section 3. Applications of Quotient Groups

3.1. Example: We prove that the alternating group A_4 has no subgroups of order 6 using quotient groups. Suppose $H \leq A_4$ with $|H| = 6$. We claim that H is a normal subgroup. In fact, we show that for any group G, a subgruop H with index 2 must be normal.

To see this, let $a \in G$. If $a \in H$, then of course $aH = H = Ha$. Otherwise, if $a \notin H$, then aH and Ha are both the sets of elements of G that do not belong to H, hence they are equal to each other. It follows that H is normal.

We can thus consider the quotient group A_4/H which must have order 2. Hence, for every $\alpha \in A_4$, $\alpha^2 H = (\alpha H)^2 = H$ so that $\alpha^2 \in H$ for every $\alpha \in A_4$. But it can be verified that A_4 has 9 distinct elements of the form α^2, whereas H was assumed to have order 6. Contradiction.

3.2. Theorem: *Let G be a group and $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, then G is Abelian.*

Proof. Recall that G is Abelian iff $G = Z(G)$. We will show that $G/Z(G) = \{Z(G)\}$ which implies that $G = Z(G)$. Since $G/Z(G)$ is cyclic, $G/Z(G) = \langle gZ(G)\rangle$ for some $g \in G$.

Let $a \in G$. Then $aZ(G) = (gZ(G))^i = g^i Z(G)$ for some $i \in \mathbb{Z}$. Thus, $a = g^i z$ for some $z \in Z(G)$. As $z, g \in C(g)$ where $C(g) \leq G$ is the centralizer of g ($z \in Z(G)$ so z commutes with g; g commutes with itself), we also have $a \in C(g)$ as the group $C(g)$ is closed under the group operation. This gives us $ag = ga$. Since a was chosen arbitrarily, g commutes with a for all $a \in G$. Thus, $g \in Z(G)$, $gZ(G) = Z(G)$, and $G/Z(G) = \{Z(G)\}$. □

3.3. Remark: Note that this proof shows that if G/H is cyclic for any subgroup H of $Z(G)$, then G is Abelian.

3.4. Remark: Taking the contrapositive, if G is not Abelian, then $G/Z(G)$ is not cyclic. In particular, suppose G has order pq where p and q are primes. Suppose $e \neq a \in Z(G)$. Then $|Z(G)|$ is either p or q by Lagrange's theorem. By another application of Lagrange's theorem, this shows that $|G/Z(G)|$ is either q or p, so that $G/Z(G)$ is cyclic (Corollary 2.6). Hence, G must be Abelian or $Z(G) = \{e\}$.

3.5. Theorem: *For any group G, $G/Z(G) \cong \mathrm{Inn}(G)$.*

Proof. For $g \in G$, define $T(gZ(G)) := \varphi_g$ where φ_g is the inner automorphism given by $\varphi_g(x) = gxg^{-1}$ for all $x \in G$. We will show that T is a well-defined isomorphism.

We have $gZ(G) = hZ(G)$ iff $h^{-1}g \in Z(G)$. Now for each $x \in G$, $\varphi_g(x) = \varphi_h(x)$ iff $gxg^{-1} = hxh^{-1} \iff h^{-1}gx = xh^{-1}g$ for each $x \in G$ iff $h^{-1}g = Z(G)$ iff $gZ(G) = hZ(G)$. Hence, φ is well-defined and one-to-one. T is clearly onto $\mathrm{Inn}(G)$ as every inner automorphism is of the form

φ_g for some $g \in G$.

Finally, we observe that $\varphi_g\varphi_h(x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \varphi_{gh}(x)$ for each $x \in G$. Hence, $T(gZ(G)hZ(G)) = T(ghZ(G)) = \varphi_{gh} = \varphi_g\varphi_h = T(gZ(G))T(hZ(G))$, so that T is a group homomorphism and indeed an isomorphism. □

3.6. Theorem (Cauchy's Theorem for Abelian Groups): *Let G be a finite Abelian group and p be a prime that divides the order of G. Then G has an element of order p.*

Proof. We do induction on $|G|$. If $|G| = 2$, then $G = \{e, a\}$ where $|a| = 2$.

Now suppose the result is true for all Abelian groups with order less than $|G|$. We claim that G has an element x of prime order. Let $x \in G$ with $|x| = m$. If m is prime, we are done. Otherwise, if $m = qn$ where q is prime, then $|x^n| = q$, which is prime.

WLOG, let $x \in G$ with $|x| = q$ where q is prime. If $q = p$, we are finished. Otherwise, since every subgroup of an Abelian group is normal, we may construct the quotient group $\overline{G} = G/\langle x\rangle$. Then $\overline{G}$ is Abelian and p divides $|\overline{G}|$ as $|\overline{G}| = |G|/q$. By induction, then, $\overline{G}$ has an element, call it $y\langle x\rangle$, of order p.

Then $(y\langle x\rangle)^p = y^p\langle x\rangle = \langle x\rangle$ and therefore $y^p \in \langle x\rangle$. If $y^p = e$, we are done. If not, then y^p has order q and y^q has order p. □

Section 4. Connection to Direct Products

Recall that the internal direct product of subgroups of a group is isomorphic to their external direct product. We now consider some consequences of this. One strength of the external direct product is that its order is simply the product of the orders of the constituent groups.

4.1. Theorem: *Every group of order p^2, where p is prime, is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \oplus \mathbb{Z}_p$.*

Proof. Let $|G| = p^2$. If G has an element of order p^2, then G is cyclic and hence isomorphic to $\mathbb{Z}_{p^2}$. If not, then every non-identity element of G must have order p. We claim that for each $a \in G \setminus \{e\}$, then subgroup $\langle a \rangle$ is normal. Suppose it is not normal, then there exists $b \in G$ with $bab^{-1} \notin \langle a \rangle$. Then $\langle a \rangle$ and $\left\langle bab^{-1} \right\rangle$ are distinct subgroups of order p^2. Since $\langle a \rangle \cap \left\langle bab^{-1} \right\rangle$ is a subgroup of both groups, it must be the trivial subgroup $\{e\}$. This gives us that the distinct left cosets of $\left\langle bab^{-1} \right\rangle$ in G are $\left\langle bab^{-1} \right\rangle, a\left\langle bab^{-1} \right\rangle, a^2\left\langle bab^{-1} \right\rangle, \ldots, a^{p-1}\left\langle bab^{-1} \right\rangle$. The element b^{-1} must belong to one of these cosets, that is, $b^{-1} = a^i(bab^{-1})^j = a^i ba^j b^{-1}$ for some integers i and j. But this implies that $a^i ba^j = e$ which gives that $b = a^{-i-j} \in \langle a \rangle$, a contradiction as $bab^{-1} \notin \langle a \rangle$. Hence, $\langle a \rangle$ is normal.

This means that for $x \neq y \in G$, both of order p, $\langle x \rangle \times \langle y \rangle$ is isomorphic to $\langle x \rangle \oplus \langle y \rangle$ and hence is a subgroup of G or order p^2. This means that $G = \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, as promised. □

4.2. Corollary: *If $|G| = p^2$ where p is a prime, then G is Abelian.*

Section 5. The Group of Units Modulo n as an External Direct Product

5.1. Definition: Let $n \in \mathbb{N}$ and k be a positive divisor of n. Define

$$U_k(n) = \{x \in U(n) \mid x \bmod k \equiv 1\}.$$

To be finished.

Chapter 10

Group Homomorphisms

Section 1. Definitions and Examples

1.1. Definition: A **homomorphism** φ from a group G to a group $\overline{G}$ is a mapping from G into φG such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.

Recall from linear algebra, the kernel of a linear mapping $L : V \to W$ is a subspace $\ker(L)$ of V consists of the vectors that get mapped to the zero vector 0_W of W. We generalize this notion here by defining the kernel of a homomorphism $\varphi : G \to \overline{G}$ as the set of elements that get mapped to the identity element $e_{\overline{G}}$ of $\overline{G}$.

1.2. Definition: The **kernel** of a homomorphism $\varphi : G \to \overline{G}$, denoted $\mathrm{Ker}(\varphi)$ is the set $\{x \in G \mid \varphi(x) = e_{\overline{G}}\}$.

1.3. Example:

- $\varphi : \mathrm{GL}(2,\mathbb{R}) \to \mathbb{R}^*$, $\varphi(A) = \det(A)$ is a group homomorphism with $\mathrm{Ker}(\varphi) = \mathrm{SL}(2,\mathbb{R})$.
  - The identity of $\mathbb{R}^*$ is 1.
  - The set of matrices in $\mathrm{SL}(2,\mathbb{R})$ has a determinant of 1.
- $\varphi : \mathbb{R}^* \to \mathbb{R}^*$, $\varphi(x) = |x|$ is a homomorphism with $\mathrm{Ker}(\varphi) = \{1, -1\}$.
  - ± 1 gets mapped to 1 by the absolute value function, which is the identity of $\mathbb{R}^*$.
- Let $\mathbb{R}[x]$ be the group of real polynomials in one variable with pointwise addition. Then $\varphi : \mathbb{R}[x] \to \mathbb{R}[x]$, $\varphi(f) = f'$ (the first derivative) is a group homomorphism with $\mathrm{Ker}(\varphi)$ given by the set of constant polynomials.
  - Differentiating a constant yields zero (the zero polynomial), which is the identity of $\mathbb{R}[x]$.
- $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(m) = m \bmod n$ is a group homomorphism with $\mathrm{Ker}(\varphi) = n\mathbb{Z} = \langle n \rangle$.
  - $m \equiv 0 \bmod n \iff m = kn$ for some $k \in \mathbb{Z}$.
- $\varphi : \mathbb{R}^* \to \mathbb{R}^*$, $\varphi(x) = x^2$ is a group homomorphism with $\mathrm{Ker}(\varphi) = \{1, -1\}$.
  - ± 1 gets mapped to 1 by the square function, which is the identity of $\mathbb{R}^*$.
- $\varphi : (\mathbb{R}, +) \to (\mathbb{R}, +)$, $\varphi(x) = x^2$ is not a homomorphism as $(x + y)^2 \neq x^2 + y^2$ in general.

Section 2. Properties of Homomorphisms

2.1. Theorem: *Let G and $\overline{G}$ be groups, $\varphi : G \to \overline{G}$ be a homomorphism, $g \in G$, e_G and $e_{\overline{G}}$ be the identity elements of G and $\overline{G}$, respectively. Then*

(1). $\varphi(e_G) = e_{\overline{G}}$.

(2). $\varphi(g^n) = [\varphi(g)]^n$ *for all* $n \in \mathbb{Z}$.

(3). If $|g| < \infty$, *then* $|\varphi(g)|$ *divides* $|g|$.

(4). $\mathrm{Ker}(\varphi)$ *is a subgroup of* G.

(5). $\varphi(a) = \varphi(b) \iff a\mathrm{Ker}(\varphi) = b\mathrm{Ker}(\varphi)$.

(6). $\varphi(g) = g' \implies \varphi^{-1}(g') = \{x \in G \mid \varphi(x) = g'\} = g\mathrm{Ker}(\varphi)$.

Proof. (1) is trivial; (2) is simply $\varphi(g^n) = \varphi(g) \cdots \varphi(g)$ for n times.

- For (3), note that if $g^n = e_G$ for $n \in \mathbb{Z}$, then $\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = e_{\overline{G}}$. In other words, $|g| = n$ must be a multiple of the order of $|\varphi(g)|$.
- For (4), $\mathrm{Ker}(\varphi) \neq \varnothing$ as $e_G \in \mathrm{Ker}(\varphi)$. Now for $x, y \in \mathrm{Ker}(\varphi)$, $\varphi(xy^{-1}) = \varphi(x)\varphi^{-1}(y) = e_{\overline{G}}$.
- For (5), $\varphi(a) = \varphi(b) \Leftrightarrow \varphi(a)^{-1}\varphi(b) = \varphi(a^{-1}b) = e_{\overline{G}} \Leftrightarrow a^{-1}b \in \mathrm{Ker}(\varphi) \Leftrightarrow a\mathrm{Ker}(\varphi) = b\mathrm{Ker}(\varphi)$.
- For (6), note that if $h \in g\mathrm{Ker}(\varphi)$, then $h = gk$ for some $k \in \mathrm{Ker}(\varphi)$, so that

$$\varphi(h) = \varphi(gk) = \varphi(g)\varphi(k) = g' \implies g\mathrm{Ker}(\varphi) \subseteq \varphi^{-1}(g').$$

Suppose $x \in \varphi^{-1}(g')$ so that $\varphi(x) = g' = \varphi(g)$. By (5), this implies that $x\mathrm{Ker}(\varphi) = g\mathrm{Ker}(\varphi)$, so that $x \in g\mathrm{Ker}(\varphi)$ and thus $\varphi^{-1}(g') \subseteq g\mathrm{Ker}\varphi$.

□

Group homomorphisms preserve the binary operation structure of the groups, hence they preserve certain properties of groups.

2.2. Theorem: *Let* $\varphi : G \to \overline{G}$ *be a homomorphism with* $H \leq G$. *Then*

(1). $\varphi(H) = \{\varphi(h) \mid h \in H\} \subseteq \overline{G}$.

(2). H *is cyclic* $\implies \varphi(H)$ *is cyclic.*

(3). H *is Abelian* $\implies \varphi(H)$ *is Abelian.*

(4). $H \trianglelefteq G \implies \varphi(H) \trianglelefteq \varphi(G)$.

(5). $|\mathrm{Ker}(\varphi)| = n \implies \varphi$ *is an* n*-to-*1 *mapping from* G *to* $\varphi(G)$.

(6). $|\varphi(H)|$ *divides* $|H|$.

(7). $\overline{K} \subseteq \overline{G} \implies \varphi^{-1}(\overline{K}) = \{k \in G \mid \varphi(k) \in \overline{K}\} \leq G$.

(8). $\overline{K}$ *is normal* $\implies \varphi^{-1}(\overline{K})$ *is normal.*

(9). If φ *is onto and* $\mathrm{Ker}(\varphi) = \{e_G\}$, *then* φ *is an isomorphism from* G *to* $\overline{G}$.

Proof. The proof for (1), (2), (3) are from Theorem 3.3.

- (4): If $\varphi(h) \in \varphi(H)$, $\varphi(g) \in \varphi(G)$, then $\varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(ghg^{-1}) \in \varphi(H)$ as H is normal.
- (5): For $g' = \varphi(g) \in \varphi(G)$, we have $\varphi^{-1}(g') = g\text{Ker}(\varphi)$ by Theorem 2.1 (6), and $|\varphi^{-1}(g')| = |g\text{Ker}(\varphi)| = |\text{Ker}(\varphi)| = n$.
- (6): Set $\varphi_H = \varphi|_H$, the restriction of φ to the subgroup H. Then $\varphi_H : H \to \varphi(H)$ is an onto homomorphism. Suppose $|\text{Ker}(\varphi_H)| = t$, then by (5), φ_H is a t-to-1 mapping. Hence $t \cdot |\varphi(H)| = |H|$, so $|\varphi(H)|$ divides $|H|$.
- (7): Since $e_G \in \varphi^{-1}(\overline{K})$, so it is non-empty. Suppose $x, y \in \varphi^{-1}(\overline{K})$. then $\varphi\left(xy^{-1}\right) = \varphi(x)\varphi(y)^{-1} \in \overline{K}$ as $\overline{K}$ is a subgroup. Hence $\varphi^{-1}(\overline{K})$ is a subgroup.
- (8): Let $k \in \varphi^{-1}(\overline{K})$ and $x \in G$. Then $\varphi\left(xkx^{-1}\right) = \varphi(x)\varphi(k)\varphi(x)^{-1} \in \overline{K}$ as $\overline{K}$ is normal and $\varphi(k) \in \overline{K}$. Hence $xkx^{-1} \in \varphi^{-1}(\overline{K})$.
- Finally, (9) clearly follows from part (5).

□

2.3. Corollary: *Let $\varphi : G \to \overline{G}$ be a group homomorphism. Then* $\text{Ker}(\varphi) \trianglelefteq G$.

Proof. Theorem 2.2 (6) and (7). □

2.4. Example:

- Let $\varphi : \mathbb{C}^* \to \mathbb{C}^*$ be given by $\varphi(x) = x^4$. Then $\text{Ker}(\varphi) = \{1, -1, i, -i\}$ and φ is a 4-to-1 mapping. Then by Theorem 2.1 (6), since $\varphi(\sqrt[4]{2}) = 2$, we get
$$\varphi^{-1}(2) = \sqrt[4]{2}\text{Ker}(\varphi) = \{\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i\}.$$
- Consider $\varphi : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ given by $\varphi(x) = 3x$. Then $\text{Ker}(\varphi) = \{0, 4, 8\}$. Since $2 \in \varphi^{-1}(6)$, we have $\varphi^{-1}(6) = 2 + \text{Ker}\,\varphi = \{2, 6, 10\}$. Also note that $|\varphi(2)| = |6| = 2$, which divides $6 = |2|$. Let $K = \{0, 6\}$. Then $\varphi^{-1}(K) = \{0, 2, 4, 6, 8, 10\}$ (which is a subgroup of $\mathbb{Z}_{12}$).
- We determine all homomorphisms from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{30}$. Any homomorphism is completely determined by its action on the generator $1 \in \mathbb{Z}_{12}$. To be precise, if $\varphi(1) = a$, then $\varphi(x) = xa$. Now $|a| = |\varphi(1)|$ divides $|1| = 12$. We also have that $|a|$ divides 30 . Hence $|a| = 1, 2, 3$ or 6. This gives that $a = 0$ (with order 1), 15 (with order 2), 10 or 20 (with order 3), or 5 or 25 (with order 6).

Section 3. First Isomorphism Theorem

The following theorem relates the structure of the kernel and the image of a homomorphism via a quotient group.

3.1. Theorem: *Let $\varphi : G \to \overline{G}$ be a group homomorphism. Then the mapping*

$$\begin{aligned}\psi : G/\mathrm{Ker}(\varphi) &\to \varphi(G)\\ g\mathrm{Ker}(\varphi) &\mapsto \varphi(g)\end{aligned}$$

That is,

$$G/\mathrm{Ker}(\varphi) \cong \varphi(G).$$

Proof. We will show that ψ is a well-defined isomorphism. By Theorem 2.1, $g\mathrm{Ker}(\varphi) = h\mathrm{Ker}(\varphi)$ iff $\varphi(g) = \varphi(h)$, so ψ is well-defined and injective. It is clearly onto $\varphi(G)$. It remains to show that ψ is multiplicative. This holds as

$$\psi((g\mathrm{Ker}\varphi)(h\mathrm{Ker}\varphi)) = \psi(gh\mathrm{Ker}\varphi) = \varphi(gh) = \varphi(g)\varphi(h) = \psi(g\mathrm{Ker}\varphi)\psi(h\mathrm{Ker}\varphi).$$

□

3.2. Remark:

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[dr, "\gamma"'] & \varphi(G) \\
& G/\mathrm{Ker}\,\varphi \arrow[u, "\psi"']
\end{tikzcd}$$

Here, the map $\gamma : G \to G/\mathrm{Ker}\varphi$ given by $\gamma(g) = g\mathrm{Ker}\varphi$ is called the **natural** or **canonical map** onto $G/\mathrm{Ker}\varphi$. The relationship between the three maps in the future is as follows:

$$\psi\gamma = \varphi.$$

The diagram is said to be *commutative* as taking the route from G to $\varphi(G)$ remains the same through the direct route (the right arrow φ) and the "longer route" (γ then ψ).

3.3. Corollary: *If $\varphi : G \to \overline{G}$ is a homomorphism and $|G|$ is finite, then $|\varphi(G)|$ divides $|G|$.*

Proof. Note that

$$\frac{|G|}{|\mathrm{Ker}\varphi|} = |G/\mathrm{Ker}\varphi| = |\varphi(G)|.$$

□

3.4. Example: Consider $\varphi : D_4 \to D_4$ given by

$$\begin{aligned}\varphi(r_0) &= \varphi(r_2) = r_0\\ \varphi(r_1) &= \varphi(r_3) = s_0\\ \varphi(s_0) &= \varphi(s_2) = r_2\\ \varphi(s_1) &= \varphi(s_3) = s_2\end{aligned}$$

Then φ is a homomorphism with $\text{Ker}\varphi = \{r_0, r_2\}$. Now

$$\begin{aligned}\psi : D_4/\text{Ker}\varphi &\to \varphi(D_4) = \{r_0, r_2, s_0, s_2\}\\ r_0\text{Ker}\varphi &\mapsto r_0\\ r_1\text{Ker}\varphi &\mapsto s_0\\ s_0\text{Ker}\varphi &\mapsto r_2\\ s_1\text{Ker}\varphi &\mapsto s_2\end{aligned}$$

is an isomorphism.

3.5. Example: Consider the map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ given by $\varphi(m) = m \bmod n$. We saw that $\text{Ker}\varphi = \langle n \rangle$. The map φ is clearly onto $\mathbb{Z}_n$. Thus, we have

$$\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n.$$

3.6. Example: Let $H \leq G$. Recall the **normalizer** $N(H) = \{x \in G \mid xHx^{-1} = H\}$ and the **centralizer** $C(H) = \{x \in G \mid \forall h \in H : xhx^{-1}x\}$ which are both groups. Also, $C(H) \leq N(H)$. Define $\chi : N(H) \to \text{Aut}(H)$ by $\chi(g) = \varphi_g$, the inner automorphism induced by g. Then χ is a homomorphism.

To verify this, first note that for all $h \in H$, $\varphi_g(h) = ghg^{-1} \in H$ as $g \in N(H)$. Further, we have already seen that $\varphi_{gh} = \varphi_g\varphi_h$, so χ is a homomorphism. To find the kernel of χ, note that $\varphi_g = \varphi_e \iff ghg^{-1} = ehe^{-1} = h$ for all $h \in H$. This is precisely the criterion for $g \in C(H)$, so $\text{Ker}\chi = C(H)$. Hence, we have

$$N(H)/C(H) \cong \text{Aut}(H).$$

This is sometimes called the N/C **theorem**.

The following is an application of the N/C theorem.

3.7. Example: Let G be a group of order 35. We show that G is cyclic. First, every non-identity element of G has order in $\{5, 7, 35\}$. Now, not all elements can have order 5, as elements of order 5 appear in groups of 4 (i.e., if x has order 5, so does x^2, x^3, x^4 and 4 does not divide $35 - 1 = 34$. Similarly, not all elements have order 7 as these elements appear in groups of 6, which also does not divide 34. Hence G has both elements of order 7 and 5.

Let $H \leq G$ be a subgroup of order 7. We claim that H is the only subgroup of order 7, for if

$K \leq G$ with $|K| = 7$ and $K \neq H$, then

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{7 \cdot 7}{1} = 49$$

which is impossible in a group of order 35. Note that $|H \cap K| = 1$ as it cannot have order 7. Hence, for all $a \in G$, $aHa^{-1} = H$, so that $N(H) = G$. Now as $|H| = 7$, H is cyclic and thus Abelian, so $H \leq C(H)$. This implies that 7 divides the order of $C(H)$ and as $|C(H)|$ divides 35, either $|C(H)| = 7$ or $|C(H)| = 35$. In the first case, $|N(H)/C(H)| = 35/7 = 5$. But this quotient group must be isomorphic to a subgroup of $\text{Aut}(\mathbb{Z}_7) \cong U(7)$ which has order 6, and of course, 5 does not divide 6. On the other hand, if $C(H) = G$, then taking $x = hk$ with h a non-identity element of H (and hence of order 7) and $k \in G$ with order 5 gives $|x| = |hk| = 35$ as h and k commute and h and k have orders 7 and 5, respectively.

The following statement gives the converse to "the kernel of a homomorphism is a normal subgroup".

3.8. Theorem: *Every normal subgroup N of G is the kernel of a homomorphism of G. Namely, $N = \text{Ker}\gamma$ for $\gamma : G \to G/N$ given by $\gamma(g) = gN$.*

Proof. Clearly, γ is well-defined. It is multiplicative as $\gamma(gh) = ghN = gNhN = \gamma(g)\gamma(h)$ for $g, h \in G$. The kernel of γ is given by $\{g \in G \mid gN = N\}$ which is precisely equal to $\{g \in G \mid g \in N\} = N$. □

Chapter 11

Fundamental Theorem of Finite Abelian Groups

0.9. Remark: The goal of this chapter is to establish the following result: *Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the direct product and the orders of the cyclic groups are uniquely determined by the group.* In other words, for any finite Abelian group G, we have

$$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}},$$

where the p_i's are not necessarily distinct and the prime-powers $p_1^{n_1}, \ldots, p_k^{n_k}$ are uniquely determined by G. Expressing G as such a direct product is known as **determining the isomorphism classes** of G.

We delay the proof and consider some applications first.

Section 1. The Isomorphism Classes of Abelian Groups

1.1. Note: We can use the fundamental theorem to construct Abelian groups of any order. Suppose the group has order p^k where p is a prime and $k \in \mathbb{Z}_+$ can be written as a sum of positive integers $k = n_1 + \cdots + n_t$. The set of positive integers $\{n_1, \ldots, n_t\}$ is called a partition of k; each partition gives rise to the following Abelian group of order p^k:

$$\mathbb{Z}_p^{n_1} \oplus \cdots \oplus \mathbb{Z}_p^{n_t}.$$

Further, the fundamental theorem gives that each partition yields a distinct isomorphism class of finite Abelian groups. Let us consider some concrete constructions for $k = 1, 2, 3$ and 4.

Order of G	k	Partitions of k	Possible direct products for G
p	1	1	$\mathbb{Z}_p$
p^2	2	2 $1+1$	$\mathbb{Z}_{p^2}$ $\mathbb{Z}_p \oplus \mathbb{Z}_p$
p^3	3	3 $2+1$ $1+1+1$	$\mathbb{Z}_{p^3}$ $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$ $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
p^4	4	4 $3+1$ $2+2$ $2+1+1$ $1+1+1+1$	$\mathbb{Z}_{p^4}$ $\mathbb{Z}_{p^3} \oplus \mathbb{Z}_p$ $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$ $\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$ $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

The fundamental theorem makes it easy to classify all Abelian groups of a given order.

1.2. Note: Now that we have described how to use partitions to construct Abelian groups of prime-power order, we move to the general case of any finite order, say n. We first write the prime-power decomposition of n, say

$$n = p_1^{n_1} \cdots p_k^{n_k}.$$

Now form all the Abelian groups of orders $p_1^{n_1}, \ldots, p_k^{n_k}$ as outlined above using partitions. Finally, we put them together to form all possible external direct products of these groups.

1.3. Example: Consider $|G| = 7938 = 2 \cdot 3^4 \cdot 7^2$. The prime-power 2 gives us $\mathbb{Z}_2$; 3^4 gives us one of $\mathbb{Z}_{81}, \mathbb{Z}_{27} \oplus \mathbb{Z}_3, \mathbb{Z}_9 \oplus \mathbb{Z}_9, \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, or $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$; 7^2 gives $\mathbb{Z}_{49}$ or $\mathbb{Z}_7 \oplus \mathbb{Z}_7$. Thus,

G must be isomorphic to one of the following:

$$\begin{gathered}
\mathbb{Z}_2 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_{49} \\
\mathbb{Z}_2 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \\
\mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49} \\
\mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \\
\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{49} \\
\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \\
\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49} \\
\mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7 \\
\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49} \\
\mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7
\end{gathered}$$

How do we know which of the options it is equal to? One could, for instance, compare the number of elements of given orders to narrow it down. For instance, if G has an element of order 49, it must be the first, third, fifth, seventh, or ninth option above. If we know that G has an element of order 81, then it must be isomorphic to the second option.

1.4. Note: How do we express a finite Abelian group G as an *internal* direct product? Suppose we have a group of order 2^n. Pick an element a_1 of maximum order, say 2^r. Then $\langle a_1 \rangle$ is one of the factors in the internal direct product. If $G \neq \langle a_1 \rangle$, choose an element of maximum order 2^s such that $s \leq n - r$ and none of $a_2, a_2^2, a_2^4, \ldots, a_2^{2^{s-1}}$ is in $\langle a_1 \rangle$. Then $\langle a_2 \rangle$ is another direct factor. If $G \neq \langle a_1 \rangle \times \langle a_2 \rangle = \{a_1^i a_2^j \mid 0 \leq i < 2^r, 0 \leq j < 2^s\}$, then choose a_3 of maximum order 2^t such that $t \leq n - r - s$ and none of $a_3, a_3^2, \ldots, a_3^{2^{t-1}}$ is in $\langle a_1 \rangle \times \langle a_2 \rangle$. Then $\langle a_3 \rangle$ is another direct factor. We continue in this manner until our direct product has the same order as G. If the order of G is $n = p_1^{n_1} \cdots p_k^{n_k}$, then we build the pieces for each prime and put them together as an internal direct product.

1.5. Example: Let $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ under multiplication modulo 65. G has order $16 = 2^4$, so it must be isomorphic to one of the following:

$$\begin{gathered}
\mathbb{Z}_{16} \\
\mathbb{Z}_8 \oplus \mathbb{Z}_2 \\
\mathbb{Z}_4 \oplus \mathbb{Z}_4 \\
\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\
\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2
\end{gathered}$$

To decide which of the five options G must be isomorphic to, we list the orders of its elements:

Element	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
order	1	4	4	2	4	4	4	4	4	4	4	4	2	4	4	2

As the only possible orders are 1, 2, and 4, we can rule out the first two and the last options. Next, $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has only 8 elements of order 4, whereas G has 12. Thus, G must be isomorphic by elimination to $\mathbb{Z}_4 \oplus \mathbb{Z}_4$. We now show how to express G as an internal direct product. Choose 8, say, which has the maximum order $4 = 2^2$, so $\langle 8 \rangle$ is one factor. Next, choose some element a which has maximal order $4 - 2 = 2$ and $a, a^2 \notin \langle 8 \rangle = \{8, 64, 57, 1\}$, say $a = 12$. Then $G = \langle 8 \rangle \times \langle 12 \rangle$.

1.6. Example: Let

$$G = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\},$$

under multiplication modulo 135.

As $|G| = 24 = 2^3 \times 3, G$ must be isomorphic to one of the following:

$$\begin{gathered} \mathbb{Z}_8 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{24} \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2 \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \end{gathered}$$

The element 8 has order 12 , so the last option is ruled out. The elements 109 and 134 both have order 2, so the group cannot be cyclic (as it has two subgroups of order 2). Hence G must be isomorphic to $\mathbb{Z}_{12} \oplus \mathbb{Z}_2$. So G can be expressed as $G = \langle 8 \rangle \times \langle 134 \rangle$.

To express G as an internal direct product using our algorithm, we see that as $G \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2$, the maximum order an element can have of power 2 is 4, say for instance, 28. Hence $\langle 28 \rangle$ is one factor, and we can choose an element of order 2 , say 134 which is not in $\{1, 28, 109, 82\}$. Then $\langle 28 \rangle \times \langle 134 \rangle$ takes care of the powers of 2 . The element 46 is of order 3 , so we get $G = \langle 28 \rangle \times \langle 134 \rangle \times \langle 46 \rangle$. This is isomorphic to the direct product we have already obtained.

The fundamental theorem gives us the following corollary, which is a converse of Lagrange's theorem for finite Abelian groups.

1.7. Corollary: *If m divides the order of a finite Abelian group G, then G has a subgroup of order m.*

1.8. Example: Suppose G is an Abelian group of order $72 = 2^3 \times 3^2$. We will find a subgroup of G of order 12 . By the fundamental theorem G must be isomorphic to one of the following six groups:

$$\begin{array}{ll} \mathbb{Z}_8 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{72} & \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{24} \oplus \mathbb{Z}_3 \\ \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{36} \oplus \mathbb{Z}_2 & \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \\ \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{18} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2 \end{array}$$

It is clear that one can find a subgroup of order 12 in the first four cases, since there is a cyclic group whose order is a multiple of 12 sitting in the direct product $(\mathbb{Z}_{72}, \mathbb{Z}_{24}, \mathbb{Z}_{36}, \mathbb{Z}_{12})$. Let us try to find subgroups in the last two cases which have order 12. Clearly, $\langle 6 \rangle \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a subgroup of order 12 in $\mathbb{Z}_{18} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ and $\mathbb{Z}_6 \oplus \{0\} \oplus \mathbb{Z}_2$ has order 12 in $\mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$.

Section 2. Proof of the Fundamental Theorem

We will prove the fundamental theorem via a series of lemmas.

2.1. Lemma: *Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m. Then $G = H \times K$, where $H = \left\{x \in G \mid x^{p^n} = e\right\}$ and $K = \{x \in G \mid x^m = e\}$. Moreover, $|H| = p^n$.*

Proof. Any set of the form $\{x \in G \mid x^l = e\}$ for some integer l is a subgroup, as $e^l = e$ and $x^l = y^l = e$ implies that $\left(xy^{-1}\right)^l = x^i y^{-l} = e$ as G is Abelian. Hence, H and K are subgroups. We will now prove that $G = HK$ and $H \cap K = \{e\}$. The latter follows easily as $x \in H \cap K$ implies that $x^{p^n} = e = x^m$, so that $|x|$ divides m and p^n. But as p is prime and does not divide m, it must hold that $|x| = 1$ and $x = e$.

Let $x \in G$. As $\gcd(m, p^n) = 1$, there exist $s, t \in \mathbb{Z}$ such that $sm + tp^n = 1$, so that $x = x^{sm+tp^n} = x^{sm}x^{tp^n}$. Now, $x^{sm} \in H$ as $(x^{sm})^{p^n} = x^{s|G|} = e$; similarly, $x^{tp^n} \in K$, so $x \in HK$. Finally, $p^n m = |HK| = |H||K|$. If p divides $|K|$, then K has an element of order p by Cauchy's Theorem (9.3.4). Hence p divides m, a contradiction. So it must hold that $|H| = p^n$. Repeated applications of Lemma 11.2.1 give the following. Let G be an Abelian group with $|G| = p_1^{n_1} \cdots p_k^{n_k}$, where the p_i -s are distinct primes. Then taking $G(p_i) = \{x \in G \mid x^{p_i^{n_i}} = e\}$,

$$G = G(p_1) \times \cdots \times G(p_k)$$

and $|G(p_i)| = p_i^{n_i}$. □

We will now further decompose each $G(p_i)$.

2.2. Lemma: *Let G be an Abelian group of prime-power order and let a be an element of maximum order in G. Then G can be written in the form $\langle a \rangle \times K$ for some subgroup K.*

Proof. Let $|G| = p^n$. We will prove the result by induction on n. If $n = 1$, then $|G| = p$ and $|a| = p$, so that $G = \langle a \rangle \times \langle e \rangle$. Next, suppose that the statement is true for all Abelian groups of order p^k, where $k < n$. Choose an element a of maximum order p^m. Then $x^{p^m} = e$ for all $x \in G$ (as the order of any element must be a power of p and p^m is the highest among such orders). If $G = \langle a \rangle$, we are done.

Otherwise, choose b of smallest order such that $b \notin \langle a \rangle$. We claim that $\langle a \rangle \cap \langle b \rangle = \{e\}$. Since $|b^p| = \frac{|b|}{p} < |b|$, we know that $b^p \in \langle a \rangle$. Suppose $b^p = a^i$, then $e = b^{p^m} = (b^p)^{p^{m-1}} = \left(a^i\right)^{p^m-1}$, so that $\left|a^i\right| \leq p^{m-1}$. Hence a^i is not a generator of $\langle a \rangle$, so that $\gcd(p^m, i) \neq 1$ This implies that p divides i, so that $i = pj$ for some integer j. Hence $b^p = a^i = a^{pj}$. Let $c = a^{-j}b$. Then $c \notin \langle a \rangle$, and $c^p = a^{-jp}b^p = e$. We have thus found an element c of order p with $c \notin \langle a \rangle$, so by the way we have chosen b, it must hold that $|b| = p$.

Now, suppose $x \in \langle a \rangle \cap \langle b \rangle$. If $x \neq e$, then x generates $\langle b \rangle$ so that $b \in \langle a \rangle$, a contradiction. Hence the intersection is $\{e\}$. Now, let $\bar{G} := G/\langle b \rangle$ and write any coset $x\langle b \rangle$ as $\bar{x}$. If $|\bar{a}| < |a| = p^m$, then

$\bar{a}^{p^{m-1}} = \bar{e}$ hence $a^{p^{m-1}} \in \langle a \rangle \cap \langle b \rangle = \{e\}$. This is a contradiction as $|a| = p^m$, hence $|\bar{a}| = p^m$. That is, $\bar{a}$ is an element of maximum order in $|G|$ As $|\bar{G}| < |G|$, we can use the induction hypothesis to get

$$\bar{G} = \langle \bar{a} \rangle \times \bar{K}$$

for some subgroup $\bar{K}$ of $\bar{G}$ Let $K = \{x \in G \mid \bar{x} \in \bar{K}\}$. We will show that $G = \langle a \rangle \times K$. Let $x \in \langle a \rangle \cap K$, then $\bar{x} \in \langle \bar{a} \rangle \cap \bar{K} = \{\bar{e}\} = \{\langle b \rangle\}$. Hence $x \in \langle b \rangle$, but as $x \in \langle a \rangle$, we have $x = e$. Now, $|\langle a \rangle K| = |\langle a \rangle||K| = |\bar{a}||\bar{K}|p = |\bar{G}|p = |G|$ so that indeed $G = \langle a \rangle \times K$. □

Lemma 11.2.2 and induction gives the following lemma.

2.3. Lemma: *A finite Abelian group of prime-power order is an internal direct product of cyclic groups.*

Hence altogether we have proved that

$$G = G(p_1) \times \cdots \times G(p_n)$$

and that each $G(p_i)$ is an internal direct product of cyclic groups. Hence G is an internal direct product of cyclic groups of prime-power order. We are left to show the uniqueness of the direct product obtained above.

The groups $G(p_i)$ are uniquely determined by G as they contain those elements of G whose orders are powers of p_i. We are left to prove that there is only one way (up to isomorphism) to write each $G(p_i)$ as an internal direct product of cyclic subgroups.

2.4. Lemma: *Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times \cdots \times H_m$ and $G = K_1 \times \cdots \times K_n$, where the $H_i - s$ and $K_i - s$ are nontrivial cyclic subgroups with $|H_1| \geq \cdots \geq |H_m|$ and $|K_1| \geq \cdots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for each i.*

Proof. The proof is by induction on $|G|$. If $|G| = p$, the result is true. Suppose the statement is true for all Abelian groups of order less than $|G|$.

Let $G^p = \{x^p \mid x \in G\}$. Then G^p is a subgroup of G (verify this). Further, if p divides the order of G, then G has an element of order p, say a. Hence $a \neq e, a^p = e$, so that the map $a \mapsto a^p$ is not injective, and G^p is a proper subgroup of G.

Now $G^p = H_1^p \times \cdots \times H_{m'}^p$ and $G^p = K_1^p \times \cdots \times K_{n'}^p$, where m' is the largest integer i such that $|H_i| > p$ and n' is the largest integer j such that $|K_j| > p$ (this is to ensure that the direct product decomposition of G^p does not have trivial factors). By the induction hypothesis, since $|G^p| < |G|$, we have $m' = n'$ and $|H_i^p| = |K_i^p|$ for all $i = 1, \ldots, m'$. Since $|H_i| = |H_i^p|p$, it follows that $|H_i| = |K_i|$ for all $i = 1, \ldots, m'$. For the remaining i, $|H_i| = p = |K_i|$.

Finally, since $|H_i| \cdots |H_m'| p^{m-m'} = |G| = |K_i| \cdots |K_n'| p^{n-n'}$, we have $m - m' = n - n'$, so that $m = n$. □

Chapter 12

Group Actions and Burnside's Lemma

Section 1. Group Actions

1.1. Definition: A **(left) group action** of a group G on a set X is a function $\varphi : G \times X \to X$ satisfy the following properties:

- **Compatibility**: $\varphi(gh, x) = \varphi(g, \varphi(h, x))$ for all $g, h \in G$ and $x \in X$.
- **Identity**: $\varphi(e, x) = x$ for all $x \in X$.

1.2. Intuition: The above definition simply states that for each $g \in G$, there exists a map $\varphi(g, \cdot) : X \to X$, which we will show shortly is actually a bijection or permutation of the set X. Further, we will show that the map $g \mapsto \varphi(g, \cdot)$ is a group homomorphism from G to a permutation group on the set X, and conversely, that any group homomorphism from G to a permutation group on the set X is obtained via a group action.

1.3. Example: Define $\varphi_1, \varphi_2 : \mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$ by $\varphi_1(a, (x, y)) = (x + a, y)$ and $\varphi_2(b, (x, y)) = (x, y + b)$. Then φ_1 and φ_2 are group actions. They are the actions of horizontal and vertical translations respectively on $\mathbb{R}^2$. We check that φ_1 is a group action:

- $\varphi_1(a_1 + a_2, (x, y)) = (x + a_1 + a_2, y) = \varphi_1(a_1, (x + a_2, y)) = \varphi(a_1, \varphi_1(a_2, (x, y))$ for all $a_1, a_2 \in \mathbb{R}$ and for all $(x, y) \in \mathbb{R}^2$
- $\varphi(0, (x, y)) = (x + 0, y) = (x, y)$ for all $(x, y) \in \mathbb{R}^2$. Note that here G is the Abelian group $\mathbb{R}$ with the operation of addition, and $X = \mathbb{R}^2$.

1.4. Example: Let $G = \{e, a\}$ and $X = \mathbb{C}$. Then G acts on X by $\varphi : G \times X \to X$ given by $\varphi(e, x + iy) = x + iy$ and $\varphi(a, x + iy) = x - iy$.

1.5. Example: Every subgroup H of a group G (including G itself) acts on G by left multiplication. That is, $\varphi(h, x) = hx$ for all $h \in H$ and for all $x \in G$ is a group action. To see this, observe that $\varphi(h_1h_2, x) = (h_1h_2)x = h_1(h_2x) = \varphi(h_1, h_2x) = \varphi(h_1, \varphi(h_2, x))$ and $\varphi(e, x) = x$ for all $h_1, h_2 \in H$ and $x \in G$. If $H = G$, we get for each $g \in G$ and $x \in G, \varphi(g, x) = gx = L_g(x)$, where L_g is the function of left multiplication on G. Recall from the proof of Cayley's theorem that L_g is a bijection or permutation of G for each $g \in G$ and the map $g \mapsto L_g$ is a group homomorphism.

1.6. Example: In A2, we defined for a group G, a subgruop $H \leq G$, and L, the set of cosets of H in G, the map $L_g : L \to L$ given by $L_g(xH) = gxH$. Then $\varphi : G \times L \to L$ given by $\varphi(g, xH) = L_g(xH) = gxH$ is a group action.

1.7. Example: A subgroup H of a group G actions on G by conjugation $\varphi(h, x) = hxh^{-1}$.

1.8. Example: Let $X = \{1, \ldots, n\}$ and $G = S_n$. Then G acts on X by $\varphi(\alpha, i) = \alpha(i)$.

1.9. Theorem: *Let G be a group acting on the set X.*

- *For every $g \in G$, the mapping $\varphi_g : X \to X$ defined by $\varphi_g(x) = \varphi(g,x)$ for all $x \in X$, is a permutation of X.*
- *The mapping $g \mapsto \varphi_g$ is a group homomorphism between G and a group of permutations of X.*

Proof.

- We will show that $\varphi_{g^{-1}}$ is the inverse of each φ_g, so that the latter (and the former!) is a bijection. $\varphi_{g^{-1}}\varphi_g(x) = \varphi\left(g^{-1}, \varphi(g,x)\right) = \varphi\left(g^{-1}g, x\right) = \varphi(e,x) = x$ for each $x \in X$. Similarly, $\varphi_g\varphi_{g^{-1}}(x) = x$ for all $x \in X$.
- Let $g, h \in G$ and $x \in X$. Then $\varphi_{gh}(x) = \varphi(gh,x) = \varphi(g,\varphi(h,x)) = \varphi\left(g, \varphi_h(x)\right) = \varphi_g\varphi_h(x)$, so that $\varphi_{gh} = \varphi_g\varphi_h$. This shows that $g \mapsto \varphi_g$ is a homomorphism.

□

The converse of the above theorem is also true.

1.10. Theorem: *Let G be a group, X be a set and $\mathcal{S}$ be a permutation group of X. If $\psi : G \to \mathcal{S}$ is a group homomorphism, then $\varphi : G \times X \to X$ given by $\varphi(g,x) = \psi(g)(x)$, for all $g \in G$ and $x \in X$, is a group action of G on X. The theorem gives in particular that $\psi(g) = \varphi_g$ for every $g \in G$.*

Proof. We check that the two conditions of a group action are satisfied:

- $\varphi(e,x) = \psi(e)x = x$ as ψ by virtue of being a homomorphism must take the identity of G to the identity permutation.
- $\varphi(gh,x) = \psi(gh)(x) = \psi(g)\psi(h)(x) = \psi(g)(\varphi(h,x)) = \varphi(g,\varphi(h,x))$ as ψ is a homomorphism.

□

1.11. Motivation: With the above two theorems, we have a one-to-one correspondence between homomorphisms from a group G to a permutation group of a set X, and group actions of G on X.

Section 2. Burnside's Lemma

We now prove an important result in counting applications using the machinery of group actions. This result is also known as the ***Cauchy-Frobenius Lemma****. We start by restating the definitions of the stabilizer and orbit in the context of group actions, then translate the Orbit-Stabilizer theorem that we encountered before.*

2.1. Definition: Let $\varphi : G \times X \to X$ be a group action. The **stabilizer** of an element $x \in X$ in G is defined as the following set:

$$\mathrm{stab}_G^{\varphi}(x) = \{g \in G \mid \varphi(g, x) = \varphi_g(x) = x\}$$

2.2. Definition: Definition 12.2.2. Let $\varphi : G \times X \to X$ be a group action. The orbit of an element $x \in X$ under G is defined as the following set:

$$\mathrm{orb}_G^{\varphi}(x) = \{\varphi_g(x) \mid g \in G\}.$$

2.3. Theorem (Orbit Stabilizer theorem for Group Actions): *Let G be a finite group, X a set, and $\varphi : G \times X \to X$ be a group action. Then for any $x \in X$, $|G| = \left|\mathrm{orb}_G^{\varphi}(x)\right| \left|\mathrm{stab}_G^{\varphi}(x)\right|$.*

Proof. See Theorem 3.4. □

2.4. Definition: Let $\varphi : G \times X \to X$ be a group action. For $g \in G$, let X^g denote the set of elements of X that are **fixed** by φ_g :

$$X^g = \{x \in X \mid \varphi_g(x) = \varphi(g, x) = x\}.$$

2.5. Remark:

- Let $\varphi : G \times X \to X$ be a group action. For an element $x \in X$, $\left|\mathrm{orb}_G^{\varphi}(x)\right| = 1$ if and only if $\mathrm{orb}_G^{\varphi}(x) = \{x\}$ if and only if $x \in X^g$ for all $g \in G$
- If a and b are in the same orbit, then the orbits of a and b are equal. This gives immediately that the relation $a \sim b$ if $a \in \mathrm{orb}_G^{\varphi}(b)$ is an equivalence relation.
- Further, by the orbit stabilizer theorem, if $a \sim b$, then the cardinalities of $\mathrm{stab}_G^{\varphi}(a)$ and $\mathrm{stab}_G^{\varphi}(b)$ are the same.

We are now ready to state and prove the main result of this subsection, which is essentially a theorem that gives us a way to count the number of orbits of a given group action.

2.6. Theorem (Burnside's lemma/Orbit Counting theorem/Cauchy-Frobenius lemma): *Let $\varphi : G \times X \to X$ be a group action, where G is a finite group and X is a set. Then the number of distinct orbits of elements of X is given by*

$$\frac{1}{|G|}\sum_{g\in G}|X^g|$$

Proof. Let n be equal to the number of pairs (g, x) where $\varphi_g(x) = \varphi(g, x) = x$. This can be counted in two ways. One is by fixing $g \in G$ first, and the other, by fixing $x \in X$ first.

For each $g \in G$, the number of pairs such that $\varphi_g(x) = x$ is equal to $|X^g|$, so that $n = \sum_{g\in G}|X^g|$. On the other hand, for each $x \in X$, the number of such pairs is equal to $|\operatorname{stab}_G^\varphi(x)|$, so that $n = \sum_{x\in X}\left|\operatorname{stab}_G^\varphi(x)\right|$.

For each $x \in X$, summing over orb $^\varphi_G(x)$ gives $\sum_{t\in\operatorname{orb}_G^\varphi(x)}\left|\operatorname{stab}_G^\varphi(t)\right| = \left|\operatorname{orb}_G^\varphi(s)\right|\left|\operatorname{stab}_G^\varphi(x)\right| = |G|$ by the orbit stabilizer theorem. That is, the sum of $\left|\operatorname{stab}_g^\varphi(t)\right|$ where t varies over a fixed orbit is $|G|$.

Hence, $\sum_{g\in G}|X^g| = \sum_{x\in X}\left|\operatorname{stab}_G^\varphi(x)\right| = |G| \times$ number of orbits. □

Section 3. Counting Applications

3.1. Example: Suppose we have a string of n beads where each bead can have t colours. There are t^n such configurations. As the string can be flipped over, we have certain repetitions. This can be explained using the tool of a group acting on a set. Let X be the set of all possible configurations. As the only symmetry possible is about the centre of the string (achieved by flipping the string over), the group we consider is $G = \mathbb{Z}_2$. Here 0 will act on X by doing nothing, and 1 acts by flipping the string.

Say, for example that $n = 5$ and $t = 3$, with colours say, green, yellow and blue. Some examples of configurations which are the same as each other (on flipping over) are

$$G\,Y\,Y\,B\,B \qquad \text{and} \qquad B\,B\,Y\,Y\,G$$

In the language of orbits, the two configurations above are equivalent via the relation of belonging to the same orbit.

We want to count the number of distinct configurations, or in other words, the number of distinct orbits. By Burnside's Lemma,

$$\text{Number of orbits } = \frac{1}{|\mathbb{Z}_2|} \sum_{g \in \mathbb{Z}_2} X^g$$

For $g = 0, X^g = X$ as every configuration is fixed by doing nothing. On the other hand, the number of fixed points of 1 (flipping the string over) are determined by one half of the string (as the other half must be the same by symmetry). This depends on whether n is even or odd. If n is even, then we have $t^{\frac{n}{2}}$ fixed points, and if n is odd, we have $t^{\frac{n+1}{2}}$ fixed points. So we get

$$\text{Number of orbits } = \frac{1}{2}\left(t^n + t^{\frac{n}{2}}\right)$$

if n is even and

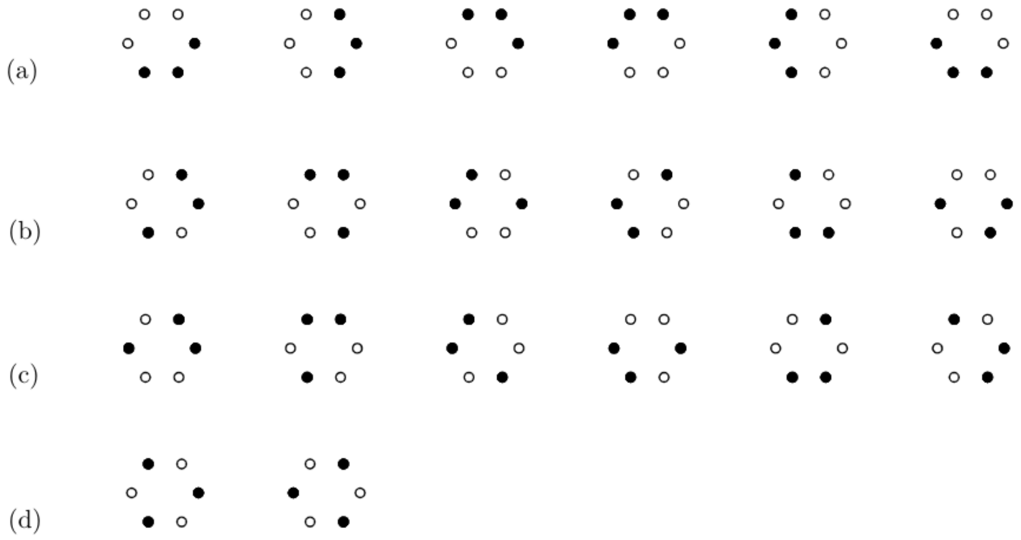
$$\text{Number of orbits } = \frac{1}{2}\left(t^n + t^{\frac{n+1}{2}}\right)$$

if n is odd.

In both cases, if $t = 1$, then for any n we get only one orbit. This is as expected since only one distinct string of n beads can be made if the beads are all of the same colour.

3.2. Example: Suppose we want to count the number of ways in which the six vertices of a hexagon can be coloured so that three are black and three are white. There are $\binom{6}{3} = 20$ ways to do this. However, if the hexagons were actually ceramic tiles, say, there would clearly be some repetitions as some of the patterns can be obtained from the remaining ones by rotation.

The 20 possibilities are given below, where the figures on each line can be obtained from the others on the same line by rotation.



We will now take X to be the set of all 20 possibilities given above and G to be the group of rotational symmetries of the hexagon $\{r_0, r_1, \ldots, r_5\}$ (with notation borrowed from the dihedral group D_6). Then G acts on X by rotating the diagrams, and the lines a, b, c and d of diagrams that can be obtained from each other by rotation describe precisely the distinct orbits of the group action. In other words, a diagram that can be obtained from another by a rotation is equivalent to it via the equivalence relation of belonging to the same orbit. We can now use Burnside's Lemma to verify that the number of orbits of this group action is indeed 4.

$$\text{Number of orbits } = \frac{1}{|G|}\sum_{g\in G}|X^g|$$

Here $|G| = 6$. We calculate X^g for each $g \in G$ below.

Element	$\lvert X^g\rvert$
r_0	20
r_1	0
r_2	2
r_3	0
r_4	2
r_5	0

Here, we see that r_2 and r_4 fix exactly the two elements on line (d), r_0 fixes all 20 elements and the remaining rotations do not fix any of the figures. Hence

$$\text{Number of orbits } = \frac{1}{6}(20 + 2 + 2) = 4$$

What happens if we consider these patterns not on a hexagonal ceramic tile, but instead on a necklace? In this case, all the figures on line (b) would be equivalent to those on line (c) as the necklace can also be turned over. So the number of distinct configurations would only be 3. To understand this in terms of orbits, we see that G in this case is all of D_6, as the necklaces remain unchanged on reflections as well. In this case we get

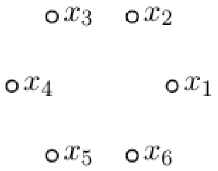
Element	$\lvert X^g \rvert$
r_0	20
r_1	0
r_2	2
r_3	0
r_4	2
r_5	0
s_0	4
s_1	0
s_2	4
s_3	0
s_4	4
s_5	0

and

$$\text{Number of orbits} = \frac{1}{12}(20+2+2+4+4+4) = 3.$$

3.3. Example: Now suppose that the necklace consists of 6 beads, where each bead can be one of t colours. How many distinct figures are possible?

Here again, as the necklace can be rotated and flipped, we will take $G = D_6$ and X to be the set of possible configurations. The number of configurations $|X| = t^6$. Let us now consider the number of fixed points for each element of D_6. We label the vertices $x_1, \ldots, x_6$, where each x_i can be one of t colours. Being a fixed point of each rotational/reflectional symmetry places certain conditions on the choice of x_i.



Then we get the following number of fixed points for each element of D_6. Each letter A, B, C, D denotes a distinct colour. Hence we get

$$\text{Number of orbits} \;= \frac{1}{12}\left(t^6 + 3t^4 + 4t^3 + 2t^2 + 2t\right)$$

If $t = 1$, we get

$$\frac{1}{12}(1+3+4+2+2) = 1$$

as expected, as there is only one necklace that can be made with six beads of the same colour.

Element	$\lvert X^g \rvert$	Pattern
r_0	t^6	All patterns
r_1	t	$AAAAAA$
r_2	t^2	$ABABAB$
r_3	t^3	$ABCABC$
r_4	t^2	$ABABAB$
r_5	t	$AAAAAA$
s_0	t^4	$ABCDCB$
s_1	t^3	$AABCCB$
s_2	t^4	$ABACDC$
s_3	t^3	$ABBACC$
s_4	t^4	$ABCBAD$
s_5	t^3	$ABCCBA$

Chapter 13

Sylow Theorems

Section 1. Definition and Notations

1.1. Definition: Let G be a group and $a, b \in G$. We say that a and b are **conjugate** in G if $xax^{-1} = b$ for some $x \in G$. The **conjugacy class** of a is the set $\operatorname{conj}(a) = \{xax^{-1} \mid x \in G\}$.

1.2. Example: For $G = D_4$, we have

- $\operatorname{conj}(r_0) = \{r_0\}$,
- $\operatorname{conj}(r_1) = \{r_1, r_3\} = \operatorname{conj}(r_3)$,
- $\operatorname{conj}(r_2) = \{r_2\}$,
- $\operatorname{conj}(s_0) = \{s_0, s_2\} = \operatorname{conj}(s_2)$,
- $\operatorname{conj}(s_1) = \{s_1, s_3\} = \operatorname{conj}(s_3)$.

1.3. Theorem: *Let G be a finite group, $a \in G$, and $C(a) = \{x \in G \mid xa = ax\}$ be the centralizer of a. Then $|\operatorname{conj}(a)| = |G : C(a)|$.*

Proof. Define the map T that sends the coset $xC(a)$ to the conjugate xax^{-1} of a. Now $xax^{-1} = yay^{-1}$ if and only if $x^{-1}ya = ax^{-1}y$ if and only if $x^{-1}y \in C(a)$, which in turn is true if and only if the cosets $xC(a)$ and $yC(a)$ are equal. Hence T is well-defined and one-to-one. It is clearly onto the conjugacy class of a. Hence the number of cosets of $C(a)$ in G given by the index $|G : C(a)|$ is equal to the number of conjugates of a, so that $|\operatorname{conj}(a)| = |G : C(a)|$. □

Recall that we showed in Assignment 1 that $|G| =| \operatorname{conj}(a||C(a) \mid$ for each $a \in G$. This follows from Theorem ?? and the fact that for the finite group $G, |G : C(a)| = \frac{|G|}{|C(a)|}$. We get the following corollary immediately.

1.4. Corollary: *If G is a finite group, then $|\operatorname{conj}(a)|$ divides $|G|$.*

Section 2. Sylow Theorems

2.1. Theorem (Sylow I): *Let G be a finite group and $p \in \mathbb{Z}$ be prime. If p^k divides $|G|$ for some $k \in \mathbb{N}$, then G has at least one subgroup of order p^k.*

Proof. We do induction on $|G|$. If G is trivial, the theorem trivially holds as no prime power divides 1. Now suppose the statement holds for all groups of order less than $|G|$.

If G as a proper subgroup H such that p^k divides $|H|$, then by IH, H has a subgroup of order p^k, and so does G too. Hence, we assume that G does not have a proper subgroup such that p^k divides its order.

Recall the following equation from a previous proof:

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} |G : C(a)|.$$

Now p^k divides $|G|$ but p^k does not divide $|C(a)|$ for each $a \notin Z(G)$ as $C(a)$ is a proper subgroup of G. As $|G| = |G : C(a)| \cdot |C(a)|$ and p is a prime, we must have that p divides $|G : C(a)|$ for each $a \notin Z(G)$. This gives in turn that p divides $Z(G)$. Now, $Z(G)$ is an Abelian group, hence by Cauchy's theorem (Theorem **??**), $Z(G)$ contains an element of order p, say x. As $\langle x \rangle$ is a normal subgroup of $G, G/\langle x \rangle$ is a quotient group. Further, p^{k-1} divides $|G/\langle x \rangle|$, so by the induction hypothesis $G/\langle x \rangle$ has a subgroup of order p^{k-1}. It is left as an exercise to prove that this subgroup is of the form $H/\langle x \rangle$ where H is some subgroup of G (Hint: Use Theorem 2.2 (vii)). Now $|H/\left\langle x \right\rangle| = p^{k-1}$ and $|\langle x \rangle| = p$, hence $|H| = p^k$ as required. □

2.2. Definition: Let G be a finite group and p be prime. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$ for some $k \in \mathbb{Z}_+$, then any subgroup of order p^k is called a **Sylow p-subgroup** of G.

2.3. Remark: Suppose $|G| = 2^3 \cdot 3^2 \cdot 5^4 \cdot 7$. Then Sylow's first theorem tells us that G has subgroups of orders $2, 4, 8, 3, 9, 5, 25, 125, 625$ and 7. Moreover, the Sylow 2-subgroup has order 8 , the Sylow 3 -subgroup has order 9, the Sylow 5 -subgroup has order 625 and the Sylow 7 -subgroup has order 7. In other words, a Sylow p -subgroup of G is a subgroup whose order is the largest power of p consistent with Lagrange's theorem.

As every subgroup of prime order must be cyclic, we get the following corollary as a generalization of Cauchy's theorem.

2.4. Corollary: *Let G be a group of finite order and suppose p is a prime that divides $|G|$. Then G has an element of order p.*

2.5. Definition: Let H and K be subgroups of a group G. We say that H and K are conjugate in G if there exists $g \in G$ such that $H = gKg^{-1}$.

2.6. Remark: Note that $H = gKg^{-1}$ implies that $|H| = |K|$.

2.7. Lemma: *Let K be a Sylow p-subgroup of a finite group G. Recall that $N(K) = \{g \in G \mid gKg^{-1} = K\}$ is the normalizer of K. If $x \in N(K)$ and $|x|$ is a power of p, then $x \in K$.*

Proof. K is a normal subgroup of $N(K)$ and $\langle x \rangle$ a subgroup of $N(K)$ so that their product $\langle x \rangle K$ is a subgroup of $N(K)$. Suppose $|x| = p^l$ and $|K| = p^k$, then by Theorem 2.10,

$$|\langle x \rangle K| = \frac{|\langle x \rangle||K|}{|\langle x \rangle \cap K|} = \frac{p^l p^k}{|\langle x \rangle \cap K|}.$$

Hence $|\langle x \rangle \cap K| \geq p^l$ as the subgroup $\langle x \rangle K$ is a subgroup whose order is a power of p, where the power cannot be greater than k. On the other hand $|\langle x \rangle \cap K| \leq p^l$, so that $\langle x \rangle \cap K = \langle x \rangle$ and $x \in K$. □

2.8. Lemma: *Let K be a subgroup of a finite group G and let $C = \{K_1, \ldots, K_n\}$ be the set of conjugates of K. Then $|C| = |G : N(K)|$.*

Proof. Later. □

2.9. Theorem (Sylow II): *If H is a subgroup of a finite group G and $|H|$ is a power of a prime p, then H is contained in some Sylow p-subgroup of G.*

Proof. Later. □

2.10. Theorem (Sylow III): *Let p be a prime and G be a finite group with $|G| = p^k m$ where p does not divide m. Then with n denoting the number of Sylow p-subgroups of G, we have $n \equiv 1 \bmod p$ and n divides m. Further, any two Sylow p-subgroups of G are conjugate.*

Proof. Later. □

2.11. Remark: Henceforth, we will denote the number of Sylow p-subgroups of a finite group G by n_p.

2.12. Corollary: *A Sylow p-subgroup of a finite group G is a normal subgroup iff it is the only Sylow p-subgroup of G.*