Group Theory

A **group** is a set G equipped with a binary operation $\cdot : G \times G \to G$ satisfying:

1. Closure: $a \cdot b$ must lie in G for all $a, b \in G$
2. Associativity: For all $a, b, c \in G$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. Existence of Identity Element: $\exists e \in G : \forall a \in G$, $a \cdot e = e \cdot a = a$.
4. Existence of Inverse Elements: $\forall a \in G \ \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = e$.

A group is called **abelian** if the operation is also commutative, i.e., $a \cdot b = b \cdot a$ for all $a, b \in G$.

Notable groups

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ are abelian groups
- The Symmetric Group S_n of permutations on n letters is a non-abelian group for $n \geq 3$
- The Dihedral Group D_{2n}, the group of symmetries of a regular n-gon (non-abelian)
- The General Linear Group $GL_n(\mathbb{R})$ of invertible $n \times n$ matrices with real entries (non-abelian)

Cosets and Lagrange's Theorem

Subset H of a group G is a **subgroup** ($H \leq G$) if it is a group under operation inherited from G.

Cosets. Let $H \leq G$. A **left coset** of H in G with respect to an element $g \in G$ is the set $gH = \{gh \mid h \in H\}$. Similarly, a **right coset** is $Hg = \{hg \mid h \in H\}$. The number of distinct left (or right) cosets of H in G is the **index** of H in G, denoted $[G : H]$.

Lagrange's Theorem. If G is a finite group and H is a subgroup of G, then the order of H divides the order of G. That is, $|H| \mid |G|$. Moreover, $|G| = |H| \cdot [G : H]$.
Proof Sketch. The left cosets of H partition G. Each coset gH has the same cardinality as H, namely $|H|$. If there are $k = [G : H]$ distinct cosets, then $|G| = k \cdot |H|$.

Homomorphisms and Normal Subgroups

A map $\phi : G \to G'$ between two groups is a **homomorphism** if it preserves the group operation: $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.

The **kernel** of a homomorphism $\phi : G \to G'$ is the set $\ker(\phi) = \{g \in G \mid \phi(g) = e' \in G'\}$.
A subgroup $N \leq G$ is **normal** (denoted $N \trianglelefteq G$) if for all $g \in G$ and $n \in N$, the conjugate gng^{-1} is in N. Equivalently, $gN = Ng$ for all $g \in G$.
The kernel of any group homomorphism is always a normal subgroup of the domain.

Isomorphism Theorems

First Isomorphism Theorem. If $\phi : G \to G'$ is a homomorphism, then $G/\ker(\phi) \cong \mathrm{Im}(\phi)$.

Second (Diamond) Isomorphism Theorem. Let G be a group, $S \leq G$ be a subgroup, and $N \trianglelefteq G$ be a normal subgroup. Then $(SN)/N \cong S/(S \cap N)$.

Third Isomorphism Theorem. Let G be a group, and let H, K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$, and $(G/H)/(K/H) \cong G/K$.

Fourth (Lattice) Isomorphism Theorem. Let $N \trianglelefteq G$. There is a bijection between the set of subgroups of G containing N and the set of subgroups of G/N.

Cyclic Groups and Permutation Groups

Cyclic Group. A group G is **cyclic** if it can be generated by a single element, i.e., there exists an element $g \in G$ such that $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Every subgroup of a cyclic group is cyclic. For any finite cyclic group $G = \langle g \rangle$ of order n, there is a unique subgroup of order d for every divisor d of n.

Cayley's Theorem. Every group G is isomorphic to a subgroup of some symmetric group. If $|G| = n$, then G is isomorphic to a subgroup of S_n.

Cycle Decomposition. Every permutation in S_n can be written uniquely (up to ordering) as a product of disjoint cycles.

Group Actions and The Class Equation

Group Action. A (left) **group action** of a group G on a set X is a map $G \times X \to X$, denoted by $(g, x) \mapsto g \cdot x$, such that for all $x \in X$ and $g_1, g_2 \in G$:

1. $e \cdot x = x$ (where e is the identity in G).
2. $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

For an element $x \in X$, its **orbit** is the set $\mathrm{Orb}(x) = \{g \cdot x \mid g \in G\}$.
The **stabiliser** of x is the subgroup $\mathrm{Stab}(x) = \{g \in G \mid g \cdot x = x\}$.

Orbit-Stabiliser Theorem. For any $x \in X$, there is a bijection between the left cosets of $\mathrm{Stab}(x)$ in G and the elements of $\mathrm{Orb}(x)$. Consequently, $|G| = |\mathrm{Orb}(x)| \cdot |\mathrm{Stab}(x)|$.

Conjugacy and Centraliser. A group G acts on itself by **conjugation**: $g \cdot x = gxg^{-1}$.

- The orbit of x is its **conjugacy class**, $C(x) = \{gxg^{-1} \mid g \in G\}$.
- The stabiliser of x is its **centraliser**, $C_G(x) = \{g \in G \mid gx = xg\}$.
- Elements fixed by the action for all $g \in G$ form the **center** of the group, $Z(G) = \{x \in G \mid gx = xg \text{ for all } g \in G\}$.

The Class Equation. Let G be a finite group and let $x_1, \ldots, x_r$ be representatives of the distinct conjugacy classes that are not in the center $Z(G)$. Then

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

where $[G : C_G(x_i)]$ is the size of the conjugacy class of x_i.
Proof. The conjugacy classes partition G. The classes of size 1 are precisely the elements of the center $Z(G)$. The sum of the sizes of all conjugacy classes is $|G|$.

Important Theorems and Consequences

The center of a finite p-group is nontrivial. That is, if $|G| = p^n$ for a prime p and $n \geq 1$, then $|Z(G)| > 1$.
Proof. Consider the class equation $|G| = |Z(G)| + \sum[G : C_G(x_i)]$. Each term $[G : C_G(x_i)] = |G|/|C_G(x_i)|$ must be a power of p greater than 1. The order of the group, $|G|$, is divisible by p. Each term in the sum is also divisible by p. Therefore, $|Z(G)| = |G| - \sum[G : C_G(x_i)]$ must also be divisible by p. Since $e \in Z(G)$, we have $|Z(G)| \geq 1$. Thus, $|Z(G)|$ must be at least p.

Any subgroup $H \leq G$ with prime index $[G : H] = p$, where p is the smallest prime dividing $|G|$, is normal.
Proof. Let G act on the set of left cosets of H, $X = \{gH \mid g \in G\}$, by left multiplication. This action induces a homomorphism $\phi : G \to S_X \cong S_p$. The kernel $K = \ker(\phi)$ is a normal subgroup of G. By construction, K is the largest normal subgroup of G contained in H, so $K \leq H$. By the First Isomorphism Theorem, G/K is isomorphic to a subgroup of S_p. Thus, $|G/K| = [G : K]$ must divide $|S_p| = p!$. We also know that $[G : K] = [G : H][H : K] = p[H : K]$. So $p[H : K]$ divides $p!$. This implies $[H : K]$ divides $(p-1)!$. By Lagrange's Theorem, $[H : K]$ must also divide $|G|$. But by assumption, every prime divisor of $[H : K]$ is greater than or equal to p. Since all prime factors of $(p-1)!$ are strictly less than p, the only possibility is $[H : K] = 1$. Therefore $H = K$, which means H is a normal subgroup of G.

If the quotient group $G/Z(G)$ is cyclic, then G is abelian.
Proof. Let $G/Z(G)$ be cyclic, generated by the coset $gZ(G)$ for some $g \in G$. Then any element of $G/Z(G)$ is of the form $(gZ(G))^k = g^k Z(G)$ for some integer k. This means that for any $x \in G$, the coset $xZ(G)$ is equal to $g^k Z(G)$ for some k. This implies $x \in g^k Z(G)$, so $x = g^k z$ for some $z \in Z(G)$. Now, let a, b be two arbitrary elements in G. Then $a = g^i z_1$ and $b = g^j z_2$ for some integers i, j and $z_1, z_2 \in Z(G)$. We check for commutativity: $ab = (g^i z_1)(g^j z_2) = g^i g^j z_1 z_2 = g^{i+j} z_1 z_2$. $ba = (g^j z_2)(g^i z_1) = g^j g^i z_2 z_1 = g^{j+i} z_2 z_1$. Since powers of g commute with each other and elements of the center $Z(G)$ commute with all elements, $z_1 z_2 = z_2 z_1$. Thus, $ab = ba$, and G is abelian.

Any group of order p^2, where p is prime, is abelian.
Proof. Let $|G| = p^2$. We know $|Z(G)| > 1$, so $|Z(G)|$ can be p or p^2. If $|Z(G)| = p^2$, then $G = Z(G)$ and G is abelian. If $|Z(G)| = p$, then the quotient group $G/Z(G)$ has order $|G|/|Z(G)| = p^2/p = p$. Any group of prime order is cyclic. Thus $G/Z(G)$ is cyclic, which implies G is abelian.

Cauchy's and Sylow's Theorems

Cauchy's Theorem. If G is a finite group and p is a prime that divides the order of G, then G has an element of order p.
Proof by Induction on $|G|$. The statement is true for $|G| = p$. Assume it is true for all groups of order less than $|G|$.
Case 1: G is abelian. Pick any non-identity element $x \in G$ of order m. If $p \mid m$, then $x^{m/p}$ is an element of order p. If $p \nmid m$, consider the quotient group $\bar{G} = G/\langle x \rangle$. Since $|\bar{G}| < |G|$ and $p \mid |\bar{G}|$, by the induction hypothesis there exists an element $\bar{y} \in \bar{G}$ of order p. Let y be a representative of $\bar{y}$ in G. Then the order of y in G is a multiple of p. We are now in the first subcase, so we can find an element of order p.
Case 2: G is not abelian. Consider the class equation: $|G| = |Z(G)| + \sum_i [G : C_G(x_i)]$. If p divides $|C_G(x_i)|$ for some $x_i \notin Z(G)$, then since $|C_G(x_i)| < |G|$, by the induction hypothesis $C_G(x_i)$ contains an element of order p, and thus G does. If p does not divide $|C_G(x_i)|$ for any $x_i \notin Z(G)$, then since $p \mid |G| = |C_G(x_i)|[G : C_G(x_i)]$, it must be that $p \mid [G : C_G(x_i)]$ for all i. The class equation implies p must also divide $|Z(G)|$. Since $Z(G)$ is a finite abelian group, by Case 1, $Z(G)$ contains an element of order p.

Sylow's Theorems. Let $|G| = p^n m$, where p is a prime and $p \nmid m$. A subgroup of order p^n is called a **Sylow p-subgroup**.

1. **(Existence)** G contains at least one Sylow p-subgroup.
2. **(Relationship)** All Sylow p-subgroups are conjugate to one another.
3. **(Number)** Let number of Sylow p-subgroups $= n_p$. Then $n_p \equiv 1 \pmod{p}$ and n_p divides m.

Structure Theorems

Direct Product. The **external direct product** $G_1 \times G_2$ is the set of ordered pairs (g_1, g_2) with $g_1 \in G_1, g_2 \in G_2$ and component-wise operation.

Fundamental Theorem of Finitely Generated Abelian Groups. Every finitely generated abelian group G is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s}$$

where $r \geq 0$ and n_i are integers such that $n_1 | n_2 | \ldots | n_s$. This decomposition is unique.

Series of Groups

Filtration and Composition Series. A **filtration** or subnormal series of a group G is a sequence of subgroups

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

The factor groups are G_i/G_{i-1}. A **composition series** is a filtration where each factor group G_i/G_{i-1} is a simple group.

Jordan-Hölder Theorem. Any two composition series for a finite group G have the same length, and their factor groups are isomorphic up to a permutation.

Miscellaneous Results and Examples

If every element g in a group G satisfies $g^2 = e$, then G is abelian.
Proof. For any $g \in G$, $g^2 = e$ implies $g = g^{-1}$. Let $a, b \in G$. Then $(ab)^2 = e$, so $abab = e$. Multiplying on the right by b gives $aba = b$. Multiplying on the right by a gives $ab = ba$.

Counterexamples.

- A group of order p^3 is not necessarily abelian. For $p = 2$, the Dihedral group D_8 and the Quaternion group Q_8 are non-abelian groups of order $8 = 2^3$.
- The Symmetric Group S_3 is the smallest non-abelian group and serves as an excellent source of counterexamples. For instance, not all subgroups are normal (e.g., $\langle(12)\rangle$). It also shows that the converse of Lagrange's Theorem is false; a common counterexample is the alternating group A_4 which has order 12 but no subgroup of order 6.

Ring Theory

Rings are sets of elements R with two operations $+$ and $\cdot$ satisfying:

- $(R, +)$ is an abelian group.
- $(R, \cdot)$ is a closed and associative set. (Commutativity is often not assumed).
- $\cdot$ distributes over $+$.

A Ring with multiplicative identity and inverses for all non-zero elements is a **Field**. R is a ring; its identity is 1_R; the characteristic is the order of 1_R under addition. $R[x]$ is the ring of all polynomials with coefficients in ring R. A Subring S of R is a subset of R which is a ring under the same operations.

Ring homomorphism: A map $\phi : R \to S$ such that:

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \\ \phi(a \cdot b) &= \phi(a) \cdot \phi(b) \\ \phi(1_R) &= 1_S \quad \text{(if } R, S \text{ have identity)} \end{aligned}$$

An ideal I of R is a subset $I \subseteq R$ such that:

- $(I, +)$ is a subgroup of $(R, +)$.
- For all $r \in R$ and $s \in I$, both $rs \in I$ and $sr \in I$ (absorption property).

Ideals are basically subrings that absorb multiplication by elements of R. The ideal generated by $\{a_1, a_2, \ldots, a_n\}$ is denoted $(a_1, a_2, \ldots, a_n)$.

First Isomorphism Theorem: If $\phi : R \to S$ is a surjective ring homomorphism with kernel $I = \ker(\phi)$, then $R/I \cong S$. **Third Isomorphism Theorem**: If I is an ideal of R and K is an ideal of R containing I ($I \subset K \leq R$), then K/I is an ideal of R/I, and $(R/I)/(K/I) \cong R/K$.

An ideal $P \neq R$ of R is a **prime ideal** if:

$$ab \in P \implies a \in P \text{ or } b \in P$$

P is a prime ideal $\iff R/P$ is an **integral domain**.

An ideal $M \neq R$ of R is a **maximal ideal** if:

$$M \subseteq I \subseteq R \implies I = M \text{ or } I = R$$

M is a maximal ideal $\iff R/M$ is a **field**.

Zorn's Lemma implies every commutative ring R with identity has at least one maximal ideal. A **Domain** R is a commutative ring with identity and no zero divisors.

$$\text{In a domain } R : a \cdot b = 0 \implies a = 0 \text{ or } b = 0$$

Any subring of a field is an integral domain.

S is a **multiplicatively closed (m.c.) set** iff:

- $0 \notin S$ and $1 \in S$.
- For all $s, t \in S$, $s \cdot t \in S$.

Localisation (Rings of Fractions) The set of fractions $R \times S/\sim$ where $(r, s) \sim (r', s')$ if $rs' = r's$, forms the ring of fractions, $S^{-1}R$. The equivalence class is denoted $[r/s]$ or $\frac{r}{s}$.
Examples of multiplicatively closed sets:

1. $S = R \setminus \{0\}$ (gives the field of fractions $\mathrm{Frac}(R)$ if R is a domain).
2. $S = R \setminus P$, where P is a prime ideal in R (gives the localisation R_P).
3. $S = \{1, f, f^2, f^3, \ldots\}$, where $0 \neq f \in R$.

I, J are ideals in R:

- Sum: $I + J = \{i + j \mid i \in I, j \in J\}$
- I and J are **comaximal** iff $I + J = R$.

I and J are comaximal $\implies$ $I \cap J = I \cdot J$ and $R/(I \cap J) \cong R/I \times R/J$ (**Chinese Remainder Theorem**).

Polynomial Ring K[x]

Elements are $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ where $a_i \in K$. The degree of f, $\deg(f)$, is the largest integer n such that $a_n \neq 0$.

For all $f, g \neq 0$ in $K[x]$, $\deg(fg) = \deg(f) + \deg(g)$.
Division Algorithm: For all $f(x) \neq 0, g(x) \in R[x]$, there exist unique $q(x), r(x) \in R[x]$ such that $g = f \cdot q + r$, where $r(x) = 0$ or $\deg(r) < \deg(f)$.
All ideals in $K[x]$ are **principal ideals**: For all ideals I in $K[x]$, there exists a unique monic polynomial $f(x) \in I$ such that $I = (f(x))$.

$f(x)$ is a **prime element** iff:

- $f(x)$ is not a unit.
- $f(x) \mid g(x)h(x) \implies f(x) \mid g(x)$ or $f(x) \mid h(x)$.

$f(x)$ is a prime element $\iff$ the ideal $(f(x))$ is a **prime ideal**.
$f(x)$ is **irreducible** iff:

- $f(x)$ is not a unit.
- $f(x) = g(x)h(x) \implies g(x)$ is a unit or $h(x)$ is a unit.

$f(x)$ is irreducible $\iff$ the ideal $(f(x))$ is a **maximal ideal**.

Eisenstein Criterion (for irreducibility): Let R be a domain and P a prime ideal. If $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ is a monic polynomial such that:

- $a_i \in P$ for all $i = 0, \ldots, n-1$.
- $a_0 \notin P^2$.

Then $f(x)$ is irreducible over the field of fractions $\mathrm{Frac}(R)$.

Integral Domains

Principle Ideal Domain (PID) A domain R is a PID if every ideal in R is principal. Examples: $\mathbb{Z}$, $\mathbb{Z}[i]$ (Gaussian integers), $\mathbb{Z}[\omega]$ (Eisenstein integers). In a PID, prime elements are irreducible and vice-versa.
Euclidean Domain (ED) An ED is a domain R with a norm $N : R \setminus \{0\} \to \mathbb{N}_0$ satisfying the Division Algorithm. All Euclidean Domains are PIDs.
Unique Factorisation Domain (UFD) A domain R is a UFD if every non-zero, non-unit element has a unique (up to associates and order) factorisation into irreducible elements. If R is a UFD, then $R[x]$ is a UFD.
Gauss Lemma: Let R be a UFD and $K = \mathrm{Frac}(R)$. If a non-constant polynomial $f(x) \in R[x]$ factors in $K[x]$ as $f(x) = g(x)h(x)$, then there exist polynomials $g'(x), h'(x) \in R[x]$ such that $f(x) = g'(x)h'(x)$.

Further Topics

- Localisation
- Noetherian Rings
- Module Theory