MA2202S Notes

Lou Yi

Last Edited by: December 17, 2024

Contents

1 Groups and Subgroups

1.1 Basics of a Group

Definition: A binary operation $\times$ of a set G is a function from $G \times G$ to G, such that $(a, b) \mapsto a \times b$. We often write $a \times b = ab = a \cdot b$ to simplify the notations.
Definition: A binary operation is called associative if for any $a, b, c \in G$, we have $a(bc) = (ab)c$. Definition: A binary operation is called commutative if for any $a, b \in G$, we have $ab = ba$.

Lemma 1.1 *Let $\times$ be an associative binary operation on G. Then the product $a_1a_2 \cdots a_n$ is independent of how the expression is bracketed.*

Definition: a group is a set G with a binary operation $\times$ on G satisfying the following conditions:

- $a(bc) = (ab)c$ for any $a, b, c \in G$, i.e., multiplication is associative;
- there exists an identity element e such that $ae = ea = a$ for any $a \in G$;
- for any $a \in G$, there exists an element a^{-1}, called the inverse of a, such that $a^{-1}a = aa^{-1} = e$.

If it is further known that multiplication is commutative, we say G is commutative or abelian. In this case, we usually use $+$ for the group operation.
Definition: the order of G is the cardinality of the set G, often denoted by $|G|$. We say G is a finite group if $|G|$ is finite.
Definition: let G be a group and $x \in G$. The order of x, denoted by $|x|$ or $\mathrm{ord}(x)$, is the smallest positive integer such that $x^n = e$. We write $\mathrm{ord}(x) = \infty$ if such positive integer does not exist.

Lemma 1.2 *Let G be a group, then the following are true:*

- *The identity element in G is unique.*
- *For any $a \in G$, the inverse of a is unique. b is the inverse of a if and only if $ab = e$.*
- $(a^{-1})^{-1} = a$ *for any* $a \in G$.
- $(ab)^{-1} = b^{-1}a^{-1}$ *for any* $a, b \in G$.
- *For any $a, x, y \in G$, if $ax = ay$, then $x = y$.*
- *For any $a, x, y \in G$, if $xa = ya$, then $x = y$.*

Proposition 1.3 *Let G be a set with a binary operation $\times$. Then G is a group if and only if*

- *the binary operation is associative;*
- *there exists an element $e \in G$ such that $ea = a$ for any $a \in G$;*
- *for any $a \in G$, $\exists b \in G$, s.t., $ba = e$.*

Definition: Let R be a set with two binary operations $+$ and $\times$. Then $(R, +, \times)$ is called a ring if

1. $(R, +)$ is an abelian group;
2. $(R, \times)$ is associative;
3. We have $a \times (b + c) = a \times b + a \times c$ for any $a, b, c \in \mathbb{R}$;
4. We have $(b + c) \times a = b \times a + c \times a$ for any $a, b, c \in \mathbb{R}$.
5. (optional) there exists an element $0 \neq 1 \in R$ such that $1 \times a = a \times 1 = a$ for any $a \in R$.

Definition: a ring R is called a field, if $(R - \{0\}, \times)$ is an abelian group.

Definition: let $G = \{g_1, g_2, \cdots, g_n\}$ be a finite group with $g_1 = 1$. The multiplication table or group table of G is the $n \times n$ matrix whose i, j entry is the group element $g_i g_j$.

1.2 Subgroups

Definition: let G be a group. A non-empty subset $H \subset G$ is called a subgroup of G, denoted by $H \leq G$, if H is closed under multiplication and H is a group with respect to the same multiplication map.

Lemma 1.4 *Let G be a group with a subgroup H.*

1. *Then $e_H = e_G$;*
2. *$\forall a \in H$, $(a^{-1})_H = (a^{-1})_G$.*

Proposition 1.5 *The arbitrary intersection of subgroups of G is still a subgroup of G.*

Definition: let $A \subset G$ be a subset of G. We define the subgroup generated by A as the intersection of all subgroups containing A, denoted by $\langle A \rangle$.

Proposition 1.6 $\langle A \rangle = \{a_1^{r_1} a_2^{r_2} \cdots a_n^{r_n} \,|\, n \in \mathbb{Z}, n \geq 0 \text{ and } a_i \in A,\ r_i = \pm 1\}$.

Corollary 1.6.1 *Suppose $H \leq G$, then $\langle H \rangle = H$.*

Lemma 1.7 *Let $x \in G$, we have $\langle x \rangle = \{x^n \,|\, n \in \mathbb{Z}\}$ and $|\langle x \rangle| = \mathrm{ord}(x) = |x|$*

Lemma 1.8 *Let H and K be subgroups of G. Then $H \cup K$ is a subgroup of G iff one of them is contained in the other.*

Remark 1.8.1 *A group can't be the union of two of its proper subgroups, however, a group can be the union of three of its proper subgroups.*

Proof: To prove this one direction is easy. For the other direction, suppose $H \cup K$ is a group and none of them is a subset of the other. Then $\exists x, y$ s.t., $x \in H$ but $x \notin K$ and $y \in K$ but $y \notin H$. Notice $x, y \in H \cup K$, so $xy \in H \cup K$. Then either $xy \in H$ or $xy \in K$. However, this will leads to a contradiction, as it would either mean $y \in H$ or $x \in K$. $\square$

Definition: a proper subgroup M of G is called maximal if $M \leq G$ and the only subgroups of G which contain M are M and G.

Lemma 1.9 *Every non-trivial finitely generated group possesses a maximal subgroup.*

Proof: Zorn's Lemma. □

Remark: finitely generated is essential. Suppose G do not need to be finitely generated, then $(\mathbb{Q}, +)$ has no maximal subgroup.

Definition: A nontrivial abelian group A (written multiplicatively) is called divisible if for each element $a \in A$, and each nonzero integer k there is an element $x \in A$ such that $x^k = a$.
Example: $(\mathbb{Q}, +)$ is divisible.

1.3 Cosets

Definition: let N be a subgroup of G. For any $g \in G$, we respectively define the left coset and right coset as

$$gN = \{gn \in G \,|\, n \in N\}, \;\; Ng = \{ng \in G \,:\, n \in \mathbb{N}\}.$$

The set of left cosets or right cosets of N is denoted by G/N or $N \setminus G$ respectively.

Lemma 1.10 *Suppose $N \leq G$, $a, b \in G$, then $aN = bN$ if and only if $a^{-1}b \in N$ or $b^{-1}a \in N$.*

Lemma 1.11 *Let N be a subgroup of G. We denote a relation on G by $g \sim h$ if and only if $g = hn$ for some $n \in N$. Then $\sim$ defines an equivalence relation on G with equivalence classes G/N, i.e., the set of equivalence class partition the group G.*

Corollary 1.11.1 (Lagrange's Theorem) *Let G be a finite group and $H \leq G$ be a subgroup of G. Then the order of H divides the order of G and the number of left cosets of H in G equals $|G|/|H|$. So $|G/H|||G|$.*

Corollary 1.11.2 *The order of any element $x \in G$ divides the order of the group. If G is a group with prime order, then $G \cong Z_p$ and the group is generated by any non-identity element.*

Lemma 1.12 *If H and K are finite subgroups of a group, then*

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

Proof: Note $HK = \bigcup\{hK \,;\, h \in H\}$ and every coset of K have the same element and different cosets of K are disjoint, hence we just need to find out how many cosets there are. We know $h_1K = h_2K$ iff $h_1^{-1}h_2 \in K$, that is $h_1^{-1}h_2 \in H \cap K$. Note $H \cap K$ again partitions H, and if h_1, h_2 are in the same coset $H \cap K$, then $h_1K = h_2K$. Thus we conclude there are $|H|/|H \cap K|$ many cosets of K, and our desired formula hence follows. □

Definition: let G be a (potentially infinite) group with a subgroup H. The number of left cosets of H in G is called the index of H in G and is denoted by $|G : H|$.

Theorem 1.13 (Cauchy's Theorem) *If G is a finite group and p is a prime dividing $|G|$, then $|G|$ has an element of order p.*

Proof: Consider the following steps:

1. Define $S = \{(x_1, x_2, \cdots, x_p) \,|\, x_i \in G,\, x_1 x_2 \cdots x_p = 1\}$.
2. Show S has $|G|^{p-1}$ elements, hence has order divisible by p.
3. Define a relation $\sim$ on elements of S, such that $a \sim b$ if a is a cyclic permutation of b.
4. Show the cyclic permutation of an element of S is again an element of S.
5. An equivalence class contains only one element if and only if it is of the form $(x, \cdots, x)$, $x^p = 1$.
6. Show that every equivalence class is of order 1 or p.
7. Note $(1, \cdots, 1)$ is an equivalence class of size 1, then there must also be at least one other equivalence class of size 1.

$\square$

Lemma 1.14 *Let $H \le K \le G$, then $|G : H| = |G : K| \cdot |K : H|$.*

Proof: Construct explicit bijections using complete representation. $\square$

Definition: let H and K be subgroups of G, then we define the HK double coset of x in G to be the set

$$HxK = \{hxk \,|\, h \in H,\, k \in K\}.$$

The set of all HK double coset is denoted $H\backslash G/K$. Note HxK is the union of left cosets of K, or it is the union of right cosets of H.

Lemma 1.15 *HxK and HyK are either the same or disjoint $\forall x, y \in G$. So the set of double cosets partition G. Furthermore, we have*

1. $|HxK| = |K| \cdot |H : H \cap xKx^{-1}|$;
2. $|HxK| = |H| \cdot |K : K \cap xHx^{-1}|$.

Proposition 1.16 *Let H and K be subgroups of a group G, then the intersection $xH \cap yK$ of two cosets of H and K is either empty or else is a coset of the subgroup $H \cap K$.*

Proof: Suppose $xH \cap yK \neq \emptyset$, then $\exists a$ in this inteserction. Then $a = xh = yk$ for some $h \in H$ and $k \in K$, so $h = x^{-1}a$, $k = y^{-1}b$. Then $aH = xH$ and $aK = yK$. Hence $xH \cap yK = aH \cap aK = a(H \cap K)$. $\square$

Proposition 1.17 *Suppose H and K are two subgroups of a group G with finite index, then $H \cap K$ is a subgroup of G with finite index.*

Proof: Establish a surjection between $G/H \times G/K$ and $G/H \cap K$. $\square$

Lemma 1.18 *Let S be a non-empty subset of a group G, then S is a subgroup of G if and only if $SS = S$, $S = S^{-1}$, and $e \in S$.*

Proof: Clear. $\square$

Corollary 1.18.1 *Let H and K be subgroups of a group G, then HK is a subgroup of G if and only if $HK = KH$.*

Proof: If HK is a subgroup, then

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH.$$

Conversely, if $HK = KH$, then

$$(HK)^{-1} = K^{-1}H^{-1} = KH = HK;$$

$$(HK)(HK) = H(KH)K = H(HK)K = HK$$

It is also clear that $e \in HK$ and $HK \neq \emptyset$. Hence HK is a subgroup of G. $\square$

1.4 Normal subgroups and Quotient Groups

Definition: let $g, n \in G$, then gng^{-1} is called the conjugate of n by g. If $N \leq G$, then gNg^{-1} is known as the conjugate of N by g.

Definition: let N be a subgroup of G. Then N is called a normal subgroup of G denoted by $N \trianglelefteq G$, if for any $g \in G$, we have $gN = Ng$ or $gNg^{-1} = N$.

Lemma 1.19 *Let A be a subset of a group G, then $gAg^{-1} \subset A \forall g \in G$ if and only if $gAg^{-1} = A \forall g \in G$. Hence N is normal in G, if it is a subgroup of G and $\forall g \in G$, $gNg^{-1} \subset G$.*

Lemma 1.20 *The arbitrary intersection of normal subgroups of G is still a normal group of G.*

Lemma 1.21 *If $N \trianglelefteq G$, then $N_G(N) = G$. In particular, if $N_G(N) = H$, then H is the largest subgroup of G which N is normal in.*

Lemma 1.22 *Suppose $N \trianglelefteq G$, and H is any subgroup of G, then $N \cap H \trianglelefteq H$.*

Proposition 1.23 *Suppose $|G| = p^n$, $n \geq 1$. Let $m \in \mathbb{Z}$, s.t., $0 \leq m \leq n$, then G has a normal subgroup of order p^m*

Proof: Induction using the center of $|G|$. $\square$

Lemma 1.24 *Let N be a subgroup of G. Then the naive multiplication map on G/N is well-defined if and only if N is a normal subgroup of G.*

Theorem 1.25 *Let N be a normal subgroup of G. Then G/N is a group with the naive multiplication map. Moreover, the projection map $\pi : G \to G/N$, $g \mapsto gN$ is a group homomorphism.*

Definition: the group G/N is called the quotient group of G with respect to N.

Lemma 1.26 *A subgroup of G is normal if and only if it is the kernel of some homomorphism.*

Definition: let R be a subset of a group G. We define the normal closure of R in G as the intersection of all normal subgroups of G which contains R, denoted by $\langle R^G \rangle$.

Lemma 1.27 $\langle R^G \rangle = \langle \bigcup_{g \in G} gRg^{-1} \rangle$.

Lemma 1.28 *Suppose $N = \langle S \rangle$, then $N \trianglelefteq G$ if and only if $gSg^{-1} \subseteq N$ for all $g \in G$.*

Lemma 1.29 *If H and K are normal groups of G and $H \cap K = 1$, then $xy = yx$ for any $x \in H, y \in K$, and further we have $HK \cong H \times K$.*

Proposition 1.30 *Let P be a partition of a group G with the property that for any pair of element A, B of the partition, the product set AB is contained entirely within another element C of the partition. Let N be the element of P that contains the identity, then N is a normal subgroup of G and P is the set of its cosets.*

Proof: Firstly, we show N is a subgroup of G. It is given the e is in N. For any $g \in G$, let $[g]$ denote the equivalence class of g induced by this partition. So suppose $g, h \in N$, then $[g][h] = NN \subset N$, as $e \in N$, and the partitions are disjoint, so $gh \in N$. Next, suppose $g \in N$, then $[g][g^{-1}] = N[g^{-1}]$. $g^{-1} \in N[g^{-1}]$, so $N[g^{-1}] \subset [g^{-1}]$ and $e \in N[g^{-1}]$, so $N[g^{-1}] \subset N$. Hence $g^{-1} \in N$, and we conclude that N is a group.

Next, we show for all $g \in G$, $gN = Ng$. $[g]N \subset [g]$, but as $e \in N$, then $[g]N \supset [g]$, so $[g]N = gN$. Similarly, we can show $N[g] = Ng$. I.e., P is the set of cosets of N. I.e., $[g] = gN$. Then as $g \in gN$ and $g \in Ng$, we must have $gN = [g] = Ng$ for any $g \in G$, hence N is normal. $\square$

1.5 Product Groups

Definition: let G and H be groups. The direct product $G \times H$ of G and H is defined as follows:

- $G \times H = \{(g, h) \mid g \in G,\, h \in H\}$ as a set;
- We define $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

We can further define the product of multiple groups $G_1 \times G_2 \times \cdots \times G_n$ and the infinite product of groups in a similar way.

Lemma 1.31 *Suppose $G_1, G_2, \cdots, G_n$ are groups and $\sigma \in \mathrm{Perm}(n)$, then*

$$G_1 \times \cdots \times G_n \cong G_{\sigma(1)} \times \cdots \times G_{\sigma(n)}.$$

Proposition 1.32 *If $G_1, \cdots, G_n$ are groups, let $G = G_1 \times \cdots \times G_n$ be their direct product, then:*

1. *G is a group of order $|G_1||G_2| \cdots |G_n|$.*

2. *For each fixed i, the set of elements of G which have the identity of G_j in the jth position for all $j \neq i$ and arbitrary elements of G_i in the position i is a subgroup of G isomorphic to G_i:*

$$G_i \cong \{(1, \cdots, g_i, \cdots, 1) \,|\, g_i \in G_i\}.$$

If we identify G_i with this subgroup, then $G_i \trianglelefteq G$ and

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

3. *For each fixed i, the kernel of the canonical projection onto the ith coordinate is isomorphic to*

$$G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

4. *Let I be a proper, nonempty subset of $\{1, \cdots, n\}$, and let $J = \{1, \cdots, n\} \setminus I$. Define G_i to be the set of elements of G that have the identity of G_j in position j for all $j \in J$.*

   - *G_I is isomorphic to the direct product of the groups G_i, $i \in I$.*
   - *G_I is a normal subgroup of G and $G/G_I \cong G_J$.*
   - *$G \cong G_I \times G_J$.*
   - *If $K \subset J$, and $x \in G_I$, $y \in G_K$, then $xy = yx$.*

5. *$Z(G) = Z(G_1) \times Z(G_2) \times \cdots \times Z(G_n)$.*

Remark: the proposition can be generalized to infinite products.

Proposition 1.33 *Let $K_1, K_2, \cdots, K_n$ be non-abelian simple groups and let $G = K_1 \times K_2 \times \cdots \times K_n$. Then every normal subgroup of G is of the form $K_{i_1} \times K_{i_2} \times \cdots \times K_{i_m}$ for some subset $I = \{i_1, i_2, \cdots, i_m\}$ of $\{1, 2, \cdots, n\}$.*

Proof: Suppose H is a non-trivial normal subgroup of G. We prove the following:
For each $i \in \{1, 2, \cdots, n\}$, either $K_i \leq H$, or every $h \in H$ can be written as $h = k_1 k_2 \cdots k_n$ with $k_j \in K_j$ and $k_i = 1$. WLOG, we show for the case $i = 1$.

Assume that there is some element $h = k_1 k_2 \cdots k_n$ with $k_1 \neq 1$. For any $g \in K_1$, by the normality of H, we know $ghg^{-1} = gk_1 \cdots k_n g^{-1} \in H$. So

$$[g, k_1] = gk_1 g^{-1} k_1^{-1} = ghg^{-1}h^{-1} \in H$$

since g commutes with $k_2, \cdots, k_n$. Hence the subgroup $[K_1, k_1]$ generated by $\{[g, k_1] : g \in K_1\}$ is a subgroup of $H \cap K_1$.

We show that $[K_1, k_1]$ is a normal subgroup of K_1. let $x \in K_1$, then

$$xgk_1 g^{-1} k_1^{-1} x^{-1} = (xg)k_1(xg)^{-1} k_1^{-1} (xk_1 x^{-1} k^{-1})^{-1} \in [K_1, k_1].$$

So $[K_1, k_1]$ is normal and clearly not equal to $\{e\}$ because there must be some g not commutative with k_1. Otherwise $\langle k_1 \rangle$ would be an abelian normal proper subgroup of K_1 (K_1 is not abelian), a contradiction. Thus $[K_1, k_1] = K_1$ so $K_1 \leq H$. We have thus proved the claim. $\square$

2 Homomorphism

2.1 Group Homomorphism

Definition: let G and H be two groups.

- A group homomorphism is a map $\phi : G \to H$, $g \mapsto \phi(g)$ such that $\phi(g \times_H h) = \phi(g) \times_H \phi(h)$ for any $g, h \in G$.
- A group homomorphism $\phi : G \to H$ is called invertible if there exists a group homomorphism $\psi : H \to G$ such that $\phi \circ \psi = id_H$ and $\psi \circ \phi = id_G$.
- We say G is isomorphic to H, denoted by $G \cong H$, if there is an invertible group homomorphism $\phi : G \to H$.
- Let $\phi : G \to H$ be a group homomorphism, then $\ker \phi^{-1}(e_H) = \{g \in G : \phi(g) = e\}$ is called the kernel of ϕ.

Lemma 2.1 *Let G and H be two groups. Let $\phi : G \to H$ be a group homomorphism, then*

- $\phi(e_G) = e_H$.
- $\phi(g^{-1}) = \phi(g)^{-1}$.
- *The image $\phi(G)$ is a subgroup of H. Suppose K is a subgroup of G, then $\phi(K)$ is also a subgroup of H. If ϕ is surjective, then the image of a normal subgroup in G is normal in H.*
- *Let K be a subgroup of H, then the preimage of K under ϕ is a subgroup of G. The preimage of a normal subgroup in H is a normal subgroup of G.*
- *Let $\psi : H \to K$ be another group homomorphism. Then the composition $\psi \circ \phi : G \to K$ is a group homomorphism. In particular, if ϕ is a homomorphism from G and H, and $K \leq G$, then $\phi|_K$ is a homomorphism from K to H.*
- *The map ϕ is an isomorphism if and only if it is a bijective group homomorphism.*
- $\ker \phi$ *is a normal subgroup of G, and ϕ is injective if and only if* $\ker \phi = \{e_G\}$.

2.2 Isomorphism Theorems

Theorem 2.2 (The First Isomorphism Theorem) *Let $\phi : G \to H$ be a group homomorphism. Then $G/\ker \phi \cong \phi(G)$.*

Lemma 2.3 *Recall H and K are subgroups of G, then HK is a group if and only if $HK = KH$. Then if $K \trianglelefteq G$, then HK is a group for any subgroup H of G.*

Theorem 2.4 (The Second Isomorphism Theorem) *Let G be a group. Let H and K be a subgroups of G such that $hKh^{-1} = K$ for any $h \in H$, i.e., (H is a subgroup of the normalizer of K). Then*

1. *HK is a subgroup of G;*
2. *K is a normal subgroup of HK;*
3. *$H \cap K$ is a normal subgroup of H;*
4. *$HK/K \cong H/(H \cap K)$.*

Theorem 2.5 (The Third Isomorphism Theorem) *Let G be a group. Let H and K be normal subgroups of G such that $H \leq K$. Then K/H is a normal subgroup of G/H and*

$$(G/H)/(K/H) \cong G/K.$$

Theorem 2.6 (The Fourth Isomorphism Theorem) *Let G be a group with a normal subgroup N. Let $\pi : G \to G/N$ be the quotient map. Then π induces a bijection between*

$$\{H \leq G \,|\, N \leq H\} \leftrightarrow \{\text{subgroups of } G/N\} = \{H/N \,|\, N \leq H \leq G\}$$

by $H \mapsto \pi(H)$, and $K \mapsto \pi^{-1}(K)$. Moreover, the bijection preserves the following properties ($N \leq A, B \leq G$):

1. *$\pi(A) \leq \pi(B) \Leftrightarrow A \leq B$;*
2. *$|A : B| = |\pi(A) : \pi(B)|$ if $B \leq A$.*
3. *$\pi(\langle A \cup B \rangle) = \langle \pi(A) \cup \pi(B) \rangle$;*
4. *$\pi(A \cap B) = \pi(A) \cap \pi(B)$;*
5. *A is normal in G if and only if $\pi(A)$ is normal in G/N.*

3 Some Special Groups

3.1 Symmetric Group

Definition: Let $X = \{1, 2, \cdots, n\}$. Then the symmetric group of n letters are defined as $S_n = \mathrm{Perm}(n)$. Where Perm is the set of all bijections on the set X.
Definition: Let A be an arbitrary set, we can define the symmetric group on A by $S_A = \mathrm{Perm}(A)$.

Lemma 3.1 *For any $\sigma \in S_n$, it can be written as a product of disjoint cycles. In particular, S_n is generated by the set*

$$\{(i, i+1) : 1 \leq i \leq n-1\}.$$

Lemma 3.2 *Suppose $(a_1 a_2 \cdots a_n)$ is a cycle, then it can be decomposed into the following ways:*

- $(a_1a_2)(a_2a_3)(a_3a_4)\cdots(a_{n-1}a_n)$
- $(a_1a_n)(a_1a_{n-1})\cdots(a_1a_2)$
- $(a_na_{n-1})(a_na_{n-2})\cdots(a_na_1)$

Lemma 3.3 *Every permutation can be expressed as a product of even number $(2, 4, \cdots)$ cycles. The recipe is to square the cycle and then follow up with the appropriate cycle. For example, $(12) = (1324)(1234)(1234)$.*

Lemma 3.4 *Let X be a set of n elements. Then $\mathrm{Perm}(X) \cong S_n$.*

Note one can think of a permutation of on the set $\{1, \cdots, n\}$ as a permutation matrix of size $n \times n$. Then we have a natural group homomorphism $S_n \to GL_n(\mathbb{C})$ mapping elements in S_n to the subgroup of permutation matrices.
Definition: we consider the composition of the group homormophism $S_n \to GL_n(\mathbb{C})$ with the determinant map, we obtain a group homomorphism $\mathrm{sgn} : S_n \to \mathbb{C}^*$. It is clear that the image of this map is $\{\pm 1\}$.
Definition: we define the alternating subgroup A_n of S_n as the kernel of the map sgn.

Lemma 3.5 *Suppose $\sigma \in S_n$ is the product of cycles $\sigma_1, \sigma_2, \cdots \sigma_n$ which are not necessarily disjoint, suppose σ_i is an k_i cycle, then*

$$\mathrm{sgn}(\sigma) = \prod_{i=1}^{n} \mathrm{sgn}(\sigma_i) = \prod_{i=1}^{n} (-1)^{k_i - 1} = (-1)^{\sum\limits_{i=1}^{n}(k_i-1)}.$$

Lemma 3.6 *Every element in the alternating group can be decomposed into a product of $2k$ many transpositions, and for each pair of transposition $(ab)(cd)$, we have $(ab)(bc)(bc)(cd) = (abc)(bcd)$, which means they can be decomposed into products of 3-cycles.*

Definition: let n be a positive integer. A partition of n, denoted by $\lambda \vdash n$, is a nondecreasing sequence $\lambda = (\lambda_1, \cdots, \lambda_k)$ of positive integers such that $\sum \lambda_i = n$. We denote the set of partitions by $\mathcal{P}(n)$.
Cycle Decomposition of Conjugate.

Conjugate Permutations have Same Cycle Type.

Theorem 3.7 *The set of conjugacy classes of S_n is in natural bijection with $\mathcal{P}(n)$.*

Proposition 3.8 *For $n \in \mathbb{Z}^+$, S_n is isomorphic to a subgroup of A_{n+2}.*

Proof: We construct an injective homomorphism ϕ from S_n to A_{n+2}, then S_n will be isomorphic to the image of ϕ. Define it in the following way: $\phi(\sigma) = \sigma$ if σ is an even permutation, $\phi(\sigma) = \sigma \circ ((n+1)(n+2))$ if σ is an odd permutation. □

Proposition 3.9 *The conjugacy class in S_n which consists of even permutations is either a single conjugacy class under the action of A_n or is a union of two classes of the same size in A_n. If $\sigma \in A_n$, then all elements in the conjugacy class of σ in S_n are conjugate in A_n if and only if σ commutes with an odd permutation.*

Proposition 3.10 *For $n \neq 6$, every automorphism on S_n is inner. $|Aut(S_6) : Inn(6)| = 2$.*

Lemma 3.11 *The center of the symmetric group S_n is trivial for $n \geq 3$; the center of the alternating group A_n, is trivial for $n \geq 4$.*

Theorem 3.12 *For $n \geq 5$, A_n is simple.*

Proof: We first prove that A_5 is simple. In fact, we show that if $|G| = 60$, and G has more than one Sylow $5-$subgroup, then G is simple.

Suppose $n_5 > 1$, then n_5 can only be 6. Let $P \in Syl5(G)$, then $|N_G(P)| = 10$. Now suppose H is a normal subgroup of G that is not $\{e\}$ or G. If $5|H$, then H contains a Sylow 5-subgroup of G. Since H is normal, then it contains all 6 conjugates of this subgroup, so $|H| \geq 1 + 6 \cdot 4 = 25$, which implies $|H| = 30$. But then any group of order 30 must have a unique Sylow $5-$subgroup (by some further analysis). Hence 5 doesn't divide the order of H.

Now if $|H| = 6$ or 12, H has a normal, hence characteristic Sylow subgroup, which is therefore also normal in G. Replacing H by this subgroup if necessary, we may assume that $|H| = 2, 3$ or 4. Let $\bar{G} = G/H$, so $|\bar{G}| = 30, 20$ or 15. In each case, $\bar{G}$ has a normal subgroup $\bar{P}$ of order 5. If we let H_1 be the complete preimage of $\bar{P}$ in G, then $H_1 \trianglelefteq G$, $H_1 \neq G$ and $5|H_1$, which contradicts the preceding paragraph. Hence G must be simple.
Now A_5 is simple because it has two distinct Sylow 5-subgroups, namely $\langle(12345)\rangle$ and $\langle(13245)\rangle$.

Next we show by induction that A_n is normal for $n > 5$. Assume there exists $H \trianglelefteq G = A_n$ with $H \neq \{e\}$ or G. Then for each $i \in \{1, 2, \cdots, n\}$ Let G_i be the stabilizer of i in the natural action of G on $i \in \{1, 2, \cdots, n\}$. Thus $G_i \leq G$ and $G_i \cong A_{n-1}$. By induction, G_i is simple for $1 \leq i \leq n$.
Suppose first that there is some $\tau \in H$ with $\tau \neq 1$ but $\tau(i) = i$ for some $i \in \{1, 2, \cdots, n\}$. Since $\tau \in H \cap G_i$ and $H \cap G_i \trianglelefteq G_i$, by the simplicity of G_i, we must have $H \cap G_i = G_i$, so $G_i \leq H$. But as H is normal, then

$$\sigma G_i \sigma^{-1} = G_{\sigma(i)} \leq \sigma H \sigma^{-1} = H.$$

So $G_j \leq H$ for all j. Note any $\lambda \in A_n$ can be written as a product of an even number, $2t$, of transpositions, so

$$\lambda = \lambda_1 \lambda_2 \cdots \lambda_t,$$

where λ_k is a product of two transpositions. Since $n > 4$, each λ_k is a three cycle, hence $\lambda_k \in G_j$ for some j, then we have that G is generated by $G_1, \cdots, G_n$, hence $G = H$ which is a contradiction. Therefore if $\tau \neq 1$ is an element of H, then $\tau(i) \neq i$ for all $i \in \{1, 2, \cdots, n\}$, i.e., any non-identity element of H does not fix any element of $\{1, 2, \cdots, n\}$.
It follows that if τ_1, τ_2 are elements of H with $\tau_1(i) = \tau_2(i)$ for some i, then $\tau_1 = \tau_2$, since $\tau_2^{-1}\tau_1(i) = i$. Suppose there exists a $\tau \in H$ such that the cycle decomposition of τ contains a cycle of length ≥ 3, say

$$\tau = (a_1 a_2 a_3 \cdots)(b_1 b_2 \cdots) \cdots$$

Let $\sigma \in G$ be an element with $\sigma(a_1) = a_1$, $\sigma(a_2) = a_2$ but $\sigma(a_3) \neq a_3$. Then

$$\tau_1 = \sigma \tau \sigma^{-1} = (a_1 a_2 \sigma(a_3) \cdots)(\sigma(b_1)\sigma(b_2) \cdots) \cdots$$

So τ and τ_1 are distinct elements of H with $\tau(a_1) = \tau_1(a_1) = a_2$, which is a contradiction. This proves that only $2-$cycles can appear in the cycle decomposition of non-identity elements of H.
Let $\tau \in H$ with $\tau \neq 1$, so

$$\tau = (a_1 a_2)(a_3 a_4)(a_5 a_6) \cdots .$$

Such representation exists because τ do not fix any indices. Let $\sigma = (a_1 a_2)(a_3 a_5) \in G$. Then

$$\tau_1 = \sigma\tau\sigma^{-1} = (a_1 a_2)(a_5 a_4)(a_3 a_6)\cdots,$$

Hence τ and τ_1 are distinct elements of H with $\tau(a_1) = \tau_1(a_1) = a_2$, again a contradiction. Hence we must have that A_n is simple. $\square$

3.2 The Quaternion Group

Definition: the Quarternion Group Q_8 is defined as follows. As a set we define

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

We then define the multiplication map $Q_8 \times Q_8 \to Q_8$ as follows:

$$\begin{aligned} \forall a \in Q_8 \;\; 1a = a1 &= a \\ \forall a \in Q_8 \;\; (-1)(-1) = 1,\, (-1)a = a(-1) &= -a \\ i \cdot i = j \cdot j = k \cdot k &= -1 \\ i \cdot j = k,\;\; j \cdot i &= -k, \\ j \cdot k = i,\;\; k \cdot j &= -i \\ k \cdot i = j,\;\; i \cdot k &= -j. \end{aligned}$$

The quaternion group can be represented as the following:

$$Q_8 = \langle a, b \,|\, a^2 = b^2,\, a^{-1}ba = b^{-1}\rangle.$$

3.3 Matrix Groups

Definition: let k be a field, the general linear group over k is defined as

$$GL_n(K) = \{A \in M_{n\times n}(k) \,|\, A \text{ is invertible}\}.$$

Definition: the orthogonal group over k is defined as

$$O_n(k) = \{A \in M_{n\times n}(k) \,|\, AA^T = A^T A = I\}.$$

Definition: over the complex numbers, we define the unitary group as follows:

$$U_n = \{A \in M_{n\times n}(\mathbb{C}) \,|\, AA^H = A^H A = I\}.$$

Definition: let $\mathbb{F}$ be any field in which the determinant of a matrix over the field can be calculated, then we define the special linear group to be

$$SL_n(\mathbb{F}) = \{A \in GL_n(\mathbb{F}) \mid \det(A) = 1\}.$$

Definition: we define $Gr_{k,n}(\mathbb{F})$ be the set of $k-$dimensional subspace of $\mathbb{F}^n$.

Lemma 3.13 *With A be an arbitrary matrix, we have the following results:*

1. $e_{ij}A = \begin{bmatrix} 0 \\ \vdots \\ a_j \\ \vdots \\ 0 \end{bmatrix}$, *i.e., the matrix whose ith row is the jth row of the matrix A.*
2. Ae_{ij} *is the matrix whose jth column is the ith column of A.*
3. e_jAe_k *is the number that is the jk-entry of A.*
4. $e_{ij}Ae_{kl}$ *is the matrix whose il-entry is the jk-entry from A.*

Lemma 3.14 *The product of elements of finite order is a group need not have finite order.*

Proof: Counter Example:

$$\begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

The two matrices on the left have order 2, but the matrix on the right has an infinite order. $\square$

Lemma 3.15 *Suppose $\mathbb{F}$ is a field with order q, where q is a prime, then the order of*

$$GL_n(\mathbb{F}) = \prod_{i=1}^{n}(q^n - q^{i-1}).$$

Lemma 3.16 *Suppose $\mathbb{F}$ is a field with order q, where q is a prime. Then $|GL_n(\mathbb{F}) : SL_n(\mathbb{F})| = q - 1$.*

Lemma 3.17 *The center of the general linear group over a field $\mathbb{F}$, $GL_n(\mathbb{F})$ is the collection of scalar matrices,*

$$\{\lambda I_n \,:\, \lambda \in \mathbb{F} \setminus \{0\}\}.$$

The center of the orthogonal group is $\{I_n, -I_n\}$.

3.4 The Group $\mathbb{Z}/n\mathbb{Z}$

Definition: let $n \in \mathbb{Z}$ be an integer. We define an equivalence relation on $\mathbb{Z}$ by $a \sim b$ iff $n|(a-b)$. We denote the equivalent classes by $\mathbb{Z}/n\mathbb{Z}$. Note, $\mathbb{Z}/n\mathbb{Z}$ form an abelian group with respect to the addition map.

Lemma 3.18 *The multiplication on $\mathbb{Z}/n\mathbb{Z}$ is well-defined. Moreover, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ forms a commutative ring.*

Definition: we define the set of units modulo n $(\mathbb{Z}/n\mathbb{Z})^*$ by

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \,|\, \text{there exists } \bar{b} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \bar{b}\bar{a} = \bar{1}\}.$$

Lemma 3.19 $(\mathbb{Z}/n\mathbb{Z})^*$ *forms an abelian group under the multiplication map, and the order of the group is $\varphi(n)$.*

3.5 Cyclic Groups

Definition: a group G is called cyclic if G can be generated by single element, i.e., $G = \langle x \rangle$ for some $x \in G$. Let $G = \langle x \rangle$ throughout this section, then $|G| = \mathrm{ord}(x)$.

Lemma 3.20 *If $|G| = n$, then $G \cong \mathbb{Z}/n\mathbb{Z}$, if $|G| = \infty$, then we have $G \cong \mathbb{Z}$.*

Lemma 3.21 *Let $p \in \mathbb{Z}$ be a prime. If G is a group of order p, then G is isomorphic to the cyclic group $\mathbb{Z}/p\mathbb{Z}$.*

Lemma 3.22 *The only group H that does not contain a proper subgroup are cyclic groups of prime order.*

Proposition 3.23 *Let $H \leq G$ be a subgroup. Then $H = \langle x^a \rangle$ for some $a \in \mathbb{Z}$ is also cyclic. Let $d \geq 0$ be the gcd of a and $|G|$, if $|G| = \infty$, then we set $d = a$. Then $H = \langle x^d \rangle$.*

Corollary 3.23.1 *Let $H = \langle x^d \rangle$ be a subgroup of G such that $d \geq 0$ and $d|n$. Then $|G : H| = d$.*

Lemma 3.24 *Suppose G is an arbitrary group and $x \in G$. If $m, n \in \mathbb{Z}$ is such that $x^n = 1$ and $x^m = 1$, then $x^{\gcd(m,n)} = 1$.*

Corollary 3.24.1 *Suppose $G = \langle x \rangle$ is a cyclic group of order n. Then $H = \langle x^s \rangle$ is a cyclic group of order $n/\gcd(s, n)$.*

Theorem 3.25 *Let $G = \langle x \rangle$ be a cyclic group of order n. Then $\{\langle x^d \rangle \,|\, d \geq 0,\, d|n\}$ is the set of all non-identical subgroups of G.*

Proposition 3.26 *Let $H_1 = \langle x^p \rangle$ and $H_2 = \langle x^q \rangle$, with $p, q \geq 0$, and $p, q|n$. Then we have*

$$H_1 \cap H_2 = \langle x^{\mathrm{lcm}(p,q)} \rangle, \quad \langle H_1 \cup H_2 \rangle = \langle x^{\gcd(p,q)} \rangle.$$

Lemma 3.27 *Suppose G is cyclic with order n. Let $End(G)$ be the set of endomorphisms of G, we have a bijection*

$$End(G) \cong \mathbb{Z}/n\mathbb{Z},\ \sigma \mapsto a(\sigma) = \sigma(x), \quad \text{such that } \sigma \circ \sigma' \mapsto a(\sigma)a(\sigma').$$

Corollary 3.27.1 *We have a group isomorphism*

$$Aut(G) \cong (\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/nZ \mid \gcd(a,n) = 1\}.$$

Proposition 3.28 *If G is abelian and simple, then $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p.*

Proof: Suppose G is abelian and simple. Let $x \neq e \in G$, we can find this x since G cannot be trivial (as it is simple). Now consider $\langle x \rangle$, we must have $\langle x \rangle \trianglelefteq G$, so $\langle x \rangle = G$. So G is cyclic, so G is congruent to a subgroup of $\mathbb{Z}$. If G is infinite, then $G \cong \mathbb{Z}$ which is not simple. If $|G| = n$ is a composite number, then $|G|$ has an element of order p, where p is the smallest prime dividing n (By Cauchy's Theorem). Then the subgroup generated by that element is a proper normal subgroup of G, so G is not simple. Hence $|G| = p$ for some prime p, i.e., $G \cong \mathbb{Z}/p\mathbb{Z}$. $\square$

3.6 Dihedral Group

Definition: we define the Dihedral group of order $2n$ by the following presentation: $\langle s, r \mid r^n = s^2 = e, rs = sr^{-1} \Leftrightarrow (rs)^2 = e\rangle$. The elements of the dihedral group of of order $2n$ are

$$D_{2n} = \{1, r, r^2, \cdots, r^{n-1}, s, sr, sr^2, \cdots, sr^{n-1}\}.$$

Lemma 3.29 *In any dihedral group, $r^i s = sr^{-i}$.*

Lemma 3.30 *Let r_i denote r^i and s_i denote $r^i s$ in a dihedral group, then the following holds:*

$$r_i r_j = r_{i+j}, \quad r_i s_j = s_{i+j}, \quad s_i r_j = s_{i-j}, \quad s_i s_j = r_{i-j}.$$

Proposition 3.31 *Suppose $n = 2k$, then the conjugacy classes in D_{2n} are the following:*

$$\{1\}, \{r^k\}, \{r^{\pm 1}\}, \cdots, \{r^{\pm(k-1)}\}, \{sr^{2b} \mid b = 1, \cdots, k\} \text{ and } \{sr^{2b-1} \mid b = 1, \cdots, k\}.$$

Suppose $n = 2k+1$, then the conjugacy classes in D_{2n} are the following:

$$\{1\}, \{r^{\pm 1}\}, \cdots, \{r^{\pm(k-1)}\}, \{r^{\pm k}\}, \{sr^b \mid b = 1, \cdots, n\}.$$

4 Group Actions

4.1 Basics of Group Actions

Definition: a (left) group action of a group G on a set A is a map from $G \times A \Rightarrow A$ such that $(g, a) \mapsto g \cdot a = ga$ satisfying the following properties:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for any $g_1, g_2 \in G$ and $a \in A$.

2. $e \cdot a = a$ for any $a \in A$.

If this is the case, we denote $G \curvearrowright A$.

Definition: a group $(G, \times)$ act on itself by left multiplication if the map is from $G \times G \to G$ is defined to be $g \cdot h = g \times h$.

Theorem 4.1 *Let G be a group acting on a set A. Then we have a group homomorphism $\varphi : G \to \mathrm{Perm}(A)$, $g \mapsto \varphi(g) = \sigma_g = (a \mapsto g \cdot a,\ \forall a \in A)$. In particular, each $g \in G$ is mapped to a bijective map $\sigma_g : A \to A$.*

Corollary 4.1.1 *Let $\varphi : G \to \mathrm{Perm}(A)$ be a group homomorphism. Then $g \cdot a = \varphi(g)(a)$ defines a group action of G on A.*

Definition: let G be a group, we say G act on itself by conjugation if the map $G \times G \to G$ is defined by $g \cdot h = ghg^{-1}$.

Definition: a right action of a group G on a set A is a map from $A \times G \to A$ such that $(a, g) \mapsto a \cdot g = ag$ satisfying the following properties:

1. $(a \cdot g_1) \cdot g_2 = a \cdot (g_1 g_2)$;
2. $a \cdot e = a$.

Lemma 4.2 *Let G acts on A from the right. The map $(g, a) \mapsto a \cdot g^{-1}$ defines a left action of G on A.*

Lemma 4.3 *$GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ naturally by left multiplication. $GL_n(\mathbb{R}) \curvearrowright Gr_{k,n}(\mathbb{R})$ naturally by sending it to the image of the linear transformation.*

Proposition 4.4 (Burnside's Lemma) *Let G be a finite group that acts on a set X. For each $g \in G$, let X^g denote the set of elements in X that are fixed by g and let $|X/G|$ denote the number of orbits of this action, then*

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

Proof: Note $\sum_{g \in G} |X^g| = \sum_{x \in X} |\,\mathrm{Stab}_G(x)|$, and so by orbit stabilizer theorem, we have

$$|G \cdot x| = |G : \mathrm{Stab}_G(x)| = \frac{|G|}{|\,\mathrm{Stab}_G(x)|}.$$

Then the sum may therefore be rewritten as

$$\sum_{x \in X} \frac{|G|}{|G \cdot x|} = |G| \sum_{x \in X} \frac{1}{|G \cdot x|} = |G| \sum_{A \in X/G} \sum_{x \in A} \frac{1}{|A|}.$$

Note $\sum_{x \in A} \frac{1}{|A|} = 1$, so the term on the previous equation is equal to $|G||X/G|$ and the desired equality follows. □

Lemma 4.5 *Let H be a subgroup of G with index n, then there exists a subgroup N of G, s.t., $N \leq H$ and $N \trianglelefteq G$ with $|G : N| \leq n!$.*

Proof: Let G act on the G/H by left multiplication. Then this establishes a homomorphism between G and S_n. Let N be the kernel of this homomorphism, then N is normal with $|G : N| \leq n!$ by the first isomorphism theorem. $N \leq H$ as if $ngH = gH$ for all gH, then we must have $nH = H$, i.e., $n \in H$.

□

4.2 Stabilizers, Normalizers, Centralizers, Centers and Orbits

Definition: let $G \curvearrowright A$,

- For any $a \in A$, we define the stabilizer subgroup of G by

$$G_a = \mathrm{Stab}_G(a) = \{g \in G \,|\, g \cdot a = a\}.$$

- For any subset $B \subset A$, we define the pointwise

$$\mathrm{Stab}_G(B) = \bigcap_{a \in B} \mathrm{Stab}_G(a) = \{g \in G \,|\, g \cdot a, \text{ for any } a \in B\}.$$

- We define the kernel of the action as

$$\mathrm{Stab}_G(A) = \{g \in G \,|\, g \cdot a = a \ \ \forall a \in A\}.$$

Lemma 4.6 *$G_a, \mathrm{Stab}_G(B)$ are both subgroups of G and $\mathrm{Stab}_G(A) = \ker(G \to \mathrm{Perm}(A))$.*

Definition: let $\phi \neq A \subset G$ be a subset. We define the centralizer of A,

$$C_G(A) = \{g \in G \,|\, gag^{-1} = a, \ \forall a \in A\}.$$

Definition: the center of G is defined as

$$Z(G) = \{g \in G \,|, \ gag^{-1} = a \ \ \forall a \in G\} = C_G(G).$$

I.e., if $G \curvearrowright G$ by the conjugate action, then $Z(G)$ is the kernel of this action so $Z(G)$ is normal in G, and $C_G(A) = \mathrm{Stab}_G(A)$.
Definition: We define the normalizer of A to be

$$N_G(A) = \{g \in G \,|\, gAg^{-1} = A\} \supset \bigcap_{a \in A} C_G(a).$$

If we consider the conjugation action $G \curvearrowright \mathcal{P}(G)$, then the normalizer of a subset A is equal to the stabilizer of A under this action, as under this action, we have $\mathrm{Stab}_G(A) = \{g \in G \,|\, g \cdot A = gAg^{-1} = A\}$.

Lemma 4.7 *Suppose A is a subset of G, then $C_G(A) \leq N_G(A)$. If H is a subgroup of G, then $H \leq N_G(H)$ and H is normal in $N_G(H)$.*

Definition: let $G \curvearrowright A$. Let $a \in A$. The orbit of a is defined as $\mathcal{O}(a) = G \cdot a = \{g \cdot a \,|\, g \in G\}$.
Definition: we say G act on A transitively if $G \cdot a = A$ for some $a \in A$.
Definition: a group action is called faithful if the kernel of the action is only the identity.

Theorem 4.8 *Let G act on A, then*

1. *for any two orbits $\mathcal{O}(a)$ and $\mathcal{O}(b)$, we have either $\mathcal{O}(a) = \mathcal{O}(b)$, or $\mathcal{O}(a) \cap \mathcal{O}(b) = \emptyset$. So we have an equivalence relation $\sim$ on A by $a \sim b$ if there is a $g \in G$ such that $a = g \cdot b$, i.e., A is partitioned by orbits.*

2. *For any $a \in A$, we have a bijection between*
$$G/\operatorname{Stab}_G(a) \leftrightarrow \mathcal{O}(a).$$
(Note the stabilizer subgroup is generally not normal, $G/\operatorname{Stab}_G(a)$ denotes the set of left cosets).

3. *Assume G is a finite group, then the cardinality of $\mathcal{O}(a)$ has to be finite.*

4. *Let $G \curvearrowright A$, where A is finite. Let $I \subset A$ be a set of representatives of $G-$orbits, that is $A = \bigsqcup_{a \in I} \mathcal{O}(a)$. Ten*
$$|A| = \sum_I |\mathcal{O}(a)|.$$

Lemma 4.9 *Suppose G is a group acting on a set A, and $a, b \in A$ are in the same orbit. Then*
$$\operatorname{Stab}_G(a) \cong \operatorname{Stab}_G(b).$$
In particular, if $b = g \cdot a$, then $\operatorname{Stab}_G(b) = g \operatorname{Stab}_G(a) g^{-1}$.

Proposition 4.10 *Let H be a normal subgroup of prime order p in a finite group G. Suppose that p is the smallest prime that divides the order of G, then $H \leq Z(G)$.*

Proof: Consider G acting on elements of H by conjugation, let $e, a_1, \cdots, a_k$ be the complete list of representatives of the orbits, then
$$p = |H| = |\{e\}| + \sum_k |\mathcal{O}(a_k)|.$$
Now the size of each orbit divides $|G|$ and is less than p. Hence the size of each orbit must be 1, which implies $H \leq Z(G)$. $\square$

4.3 Action by Conjugation

Definition: let G be a group, we say a map $\phi : G \to G$ is an Endomorphism if ϕ is a homomorphism. We say ϕ is an automorphism if ϕ is an isomorphism. We denote the set of all endomorphisms on G by $\operatorname{End}(G)$, and the set of all automorphism by Aut(G).
Definition: let $g \in G$, a map ψ_g defined by $\psi_g : G \to G$, $h \mapsto ghg^{-1}$ is known as an inner automorphism. We denote the set of all inner automorphism on G by $\operatorname{Inn}(G)$.

Lemma 4.11 *Suppose $g, x \in G$, $H \leq G$, then $|gxg^{-1}| = |x|$ and $|gHg^{-1}| = |H|$. If H is the unique subgroup of order n in G, then $H \trianglelefteq G$.*

Lemma 4.12 *End(G), Aut(G), Inn(G) are groups. And Inn(G) is normal in Aut(G).*

Definition: we define the set of outer automorphism to be Aut(G)/Inn(G).

Theorem 4.13 (Cayley's Theorem) *Any group is isomorphic to a subgroup of some permutation group. If G is finite of order n, then G is isomorphic to a subgroup of S_n.*

Proposition 4.14 *Let G be a finite group of order n. Let p be the smallest prime factor of n. Then any subgroup of index p is normal (provided such a subgroup exists).*

Proof: Let H be a subgroup of G with such index p. Then consider G acting on G/H by left multiplication. Let K be the kernel of this action, then $\forall k \in K$, we have $kgH = gH$ for all $g \in G$, so $g^{-1}kg \in H$, $k \in gHg^{-1}$. Thus $K = \bigcap_{g \in G} gHg^{-1} \subset H$. Now the action induce a group homomorphism $\phi : G \to S_p$ such that $G/K \cong \phi(G)$. Since $\phi(G) | p!$ and p is the smallest prime that divides $|G|$, then we must have $|G : K| = p$ or 1. But as $K \leq H$, then it follows that $|G : K| = p$ and $K = H$. $\square$

Corollary 4.14.1 *Let G be a finite group. Then any subgroup of index 2 must be normal.*

Definition: the orbits of G acting on itself by conjugation is called conjugacy class of G.

Lemma 4.15 *The number of conjugates of a subset S in a group G is the index of normalizer of S, $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is the index of the centralizer of s, $|G : C_G(s)|$.*

Proposition 4.16 *Let G be a finite group and let $g_1, \cdots, g_n$ be representations of conjugacy classes of G not contained in the center. Then we have*

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(g_i)|.$$

Corollary 4.16.1 *Let G be a group of order p^n for some prime p. Then $Z(G)$ is non-trivial.*

Proposition 4.17 *Suppose $S \subseteq G$ and $g \in G$, then $gN_G(S)g^{-1} = N_G(gSg^{-1})$ and $gC_G(S)g^{-1} = C_G(gSg^{-1})$.*

Proposition 4.18 *Assume H is a normal subgroup of G, $\mathcal{K}$ is a conjugacy class of G contained in H and $x \in \mathcal{K}$. Then $\mathcal{K}$ is a union of k conjugacy class of equal size in H, where $k = |G : HC_G(x)|$.*

Proof: Let $x \in \mathcal{K}$. Then

$$|\mathcal{K}| = \frac{|G|}{|C_G(x)|}.$$

Now we consider the orbit of x under conjugation by H.

$$|\mathcal{O}_H(x)| = \frac{|H|}{|C_H(x)|}.$$

We first show that each H orbit have the same size. Let $g \in G$, then $gxg^{-1} \in \mathcal{K}$. So $C_H(gxg^{-1}) = gC_H(x)g^{-1}$. As $C_H(gxg^{-1}) \leq H$, H is normal, then $gC_H(x)g^{-1} \leq H$. Thus there is a bijection between the two, then by the orbit stabilizer theorem, we know there orbit have the same size.
Next since H is normal in G, then by the second isomorphism theorem

$$\frac{C_G(x)H}{H} \cong \frac{C_G(x)}{C_G(x) \cap H} = \frac{C_G(x)}{C_H(x)}.$$

Then

$$\begin{aligned}
\frac{|\mathcal{K}|}{|\mathcal{O}_H(x)|} &= \frac{|G|}{|C_G(x)|} \cdot \frac{|C_H(x)|}{|H|} \\
&= \frac{|G|}{|H|} \cdot \frac{|H|}{|C_G(x)H|} \\
&= \frac{|G|}{|C_G(x)H|} \\
&= |G : HC_G(x)|
\end{aligned}$$

□

Lemma 4.19 *Suppose M is a maximal subgroup of G, then either $N_G(M) = M$ or $N_G(M) = G$. If M is a maximal subgroup of G that is not normal in G, then the number of nonidentity elements of G that are contained in conjugates of M is at most $(|M| - 1)|G : M|$.*

Corollary 4.19.1 *Assume H is a proper subgroup of the finite group G, then G is not the union of conjugates of H, that is*

$$G \neq \bigcup_{g \in G} gHg^{-1}.$$

Corollary 4.19.2 *Let $g_1, g_2, \cdots, g_r$ be representatives of the conjugacy class of the finite group G and assume these elements pairwise commutes, then G is abelian.*

4.4 Automorphism

Proposition 4.20 *Let H be a normal subgroup of the group G. Then G acts by conjugation on H as automorphisms of H. More specifically, the action of G on H by conjugation is defined for each $g \in G$ by $h \mapsto ghg^{-1}$. The kernel of the homomorphism is $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $Aut(H)$.*

Corollary 4.20.1 *For any subgroup H of a group G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of Aut(H). In particular, $G/Z(G)$ is isomorphic to a subgroup of $Aut(G)$.*

Definition: a subgroup H of a group G is called characteristic in G, denoted H char G, if every automorphism of G maps H to itself, i.e., $\sigma(H) = H$ for all $\sigma \in \text{Aut}(G)$.

Lemma 4.21

1. *Characteristic subgroups are normal.*
2. *If H is the unique subgroup of G of a given order, then H is characteristic in G.*
3. *If K char H and $H \trianglelefteq G$, then $K \trianglelefteq G$.*
4. *If K char H and H char G, then K char G.*
5. *If $K \trianglelefteq H$ and H char G, then K is not necessarily normal in G.*

Lemma 4.22 *Let G be a group. Then $Z(G)$ char G.*

Proof: We show for any $\phi : G \to G \in \mathrm{Aut}(G)$, $\phi(Z(G)) \leq Z(G)$. Then apply ϕ^{-1}, we would get $\phi^{-1}(Z(G)) \leq Z(G)$, so $Z(G) \leq \phi(Z(G))$, which implies $\phi(Z(G)) = Z(G)$ for all ϕ.
Let $x \in Z(G)$ and $y \in G$ be arbitrary. Since $\phi(y)\phi(x) = \phi(yx) = \phi(xy) = \phi(x)\phi(y)$. And ϕ is an automorphism, then $\phi(x)$ commutes with every element in G hence $\phi(x) \in Z(G)$, thus $\phi(Z(G)) \leq Z(G)$. Then $Z(G)$ is characteristic in G. □

Proposition 4.23 *Let $n \in \mathbb{Z}^+$, then $|\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$ and $\mathrm{Aut}(Z/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Moreover, if G is cyclic of order p^k, then $\mathrm{Aut}(G) \cong Z_{p^{k-1}(p-1)}$.*

Proof: An automorphism on $\mathbb{Z}/n\mathbb{Z}$ is uniquely determined by the image of $\bar{1}$, which must be mapped to a generator of $\mathbb{Z}/n\mathbb{Z}$, thus $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, so $|\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$. □

Proposition 4.24 *Let p be a prime and let V be an abelian group with the property that $pv = (v)^p = 0$ for all $v \in V$. If $|V| = p^n$, then V is an n-dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The automorphisms of V are precisely the nonsingular linear transformations from V to itself, that is*

$$Aut(V) \cong GL(V) \cong GL_n(\mathbb{F}_p).$$

Corollary 4.24.1 $\mathrm{Aut}(\prod_{i=1}^{n} \mathbb{Z}/p\mathbb{Z}) \cong GL_n(\mathbb{F}_p)$.

5 Free Groups

Definition: let S be a set. A free group $F(S)$ over S is a group generated by $S \subset F(S)$ satisfying the following universal property: for any group G with a map of sets $\phi : S \to G$, there exists a unique group homomorphism $\tilde{\phi}$ such that the following diagram commutes:

$$\begin{tikzcd} S \arrow[r, "i"] \arrow[dr, "\phi"'] & F(S) \arrow[d, "\tilde{\phi}"] \\ & G \end{tikzcd}$$

The set S is often called a basis of $F(S)$.

Theorem 5.1 *For any set S, the free group $F(S)$ exists and $F(S)$ is unique up to isomorphism.*

Definition: let G be a group with a generating set S, that is $\langle S \rangle = G$.

1. A presentation of G is a pair (S, R), where R is a set of relations in $F(S)$ such that the normal closure of R is the kernel of the natural map $F(S) \to G$.

2. We say G is finitely generated if there exists a presentation (S, R) such that both S and R are finite.

Theorem 5.2 (Nielsen–Schreier theorem) *Subgroups of free groups are free.*

5.1 Coproduct

Theorem 5.3 *For any two groups G and H, there exists a unique (up to isomorphism) $G * H$ together with group homomorphisms $H \to G * H$ and $G \to G * H$ satisfying the following properties: for any group homomorphisms $\phi_1 : G \to K$ and $\phi_2 : H \to K$, there exists a unique group homomorphism $\phi : G * H \to K$ such that the following diagram commutes:*

$$\begin{tikzcd}
 & K & \\
H \arrow[ur, "\phi_1"] \arrow[r] & G * H \arrow[u, "\phi"] & G \arrow[ul, "\phi_2"'] \arrow[l]
\end{tikzcd}$$

Let $G \cong F(G)/R(G)$ for a free group G. Similarly, we have $H \cong F(H)/R(H)$. Then we claim that $G * H = F(G \bigsqcup H)/N$, where N is the normal subgroup generated by $R(G) \cup R(H)$.

6 Structure of Finite Groups

6.1 Sylow's Theorem

Definition: let G be a finite group with order p^n, where p is a prime, then it is called a $p-$group.
Definition: a subgroup of a group G that has order p^n is known as a p-subgroup.
Definition: assume $|G| = p^n m$, where $p \nmid m$, $n > 0$, then a subgroup of G of order p^n is known as a Sylow $p-$subgroup.
Definition: the set of all Sylow p-subgroup of G is denoted by Sylp(G). We denote the cardinality of the set of all Sylp(G), by $n_p = n_p(G)$.

Lemma 6.1 *Let G be an abelian finite group, and let p be prime that divides the order of $|G|$, then Sylow $p-$subgroup exists.*

Theorem 6.2 (First Sylow Theorem) *Let G be a finite group and let p be a prime such that $p||G|$, then a Sylow $p-$subgroup of G exists.*

Lemma 6.3 *Let G be a finite group and p be a prime such that $p||G|$, let Q be Sylow $p-$subgroup. Let P be a $p-$subgroup of G. Then we have $P \cap N_G(Q) = P \cap Q$.*

Theorem 6.4 (Second Sylow Theorem) *Any two Sylow $p-$subgroup are conjugate to each other. In other words, the conjugate action $G \curvearrowright$Sylp(G) is transitive, i.e., $G \cdot Q =$Sylp(G) for any Sylow p-subgroup Q.*

Theorem 6.5 (Thrid Sylow Theorem) $|Sylp| = n_p \equiv 1 \mod p$, $n_p | \frac{|G|}{|Q|}$, *in particular* $n_p = |G : N_G(Q)|$, *where Q is any Sylow $p-$subgroup.*

Corollary 6.5.1 *Let $Q \in$Sylp(G) be a Sylow $p-$subgroup, then $|G \cdot Q| \equiv 1 \mod p$, we can show this by considering $Q \curvearrowright G \cdot Q$ by conjugation.*

Theorem 6.6 *Any $p-$subgroup is contained in some Sylow $p-$subgroup of G.*

Corollary 6.6.1 *Let G be a finite group and p be a prime, then*

1. *let P be a $p-$subgroup and Q be a Sylow $p-$subgroup. Then $P \subset gQg^{-1}$ for some $g \in G$.*
2. *G has a unique Sylow $p-$subgroup if and only if a Sylow p-subgroup is normal, if and only if a Sylow p-subgroup is characteristic in G, if and only if all subgroups generated by elements of p-power order are p-groups, i.e., if X is any subset of G such that $|x|$ is a power of p for all $x \in X$, then $\langle X \rangle$ is a p-group.*

6.2 Semi-direct Products

Definition: let H and K be two groups. Let $\phi : K \to \mathrm{Aut}(H)$ be a group homomorphism, we define a binary operation on the set $H \times K$ by $(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot \phi(k_1)(h_2), k_1 k_2)$ and setting the inverse of (h, k) to be $((\phi(k^{-1})(h))^{-1}, k^{-1})$.

Theorem 6.7 *The binary operation above defines a group structure on $H \times K$.*

Definition: we denote this group by $H \rtimes_\phi K$ ($H \rtimes K$ if ϕ is clear). This is called the semi-direct product of H and K with respect to ϕ.
Remark: if ϕ is the trivial group homomorphism, then $H \rtimes_\phi K = H \times K$ is the direct product.
Remark: we could have $H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K$ for different homomorphism $\phi_1 \neq \phi_2$.

Proposition 6.8 *Let $H \rtimes_\phi k$ be the semi-direct product, then*

1. *$|H \rtimes_\phi K| = |H||K|$.*
2. *$\{(h, e_K) \,|\, h \in H\}$ is a normal subgroup in $H \rtimes_\phi K$ isomorphic to H. We often identify this subgroup with H ($H \leq H \rtimes_\phi K$).*
3. *$\{(e_H, k) \,|\, k \in K\}$ is a subgroup of $H \rtimes_\phi K$ isomorphic to K, we identify this group with K ($K \leq H \rtimes_\phi K$).*
4. *$H \cap K = \{e\}$.*
5. *For any $k \in K$ and $h \in H$, we have $khk^{-1} = \phi(k)(h)$, i.e., $(e_H, k)(h, e_K)(e_H, k^{-1}) = (\phi(k)(h), e_K)$.*
6. *$C_K(H) = \ker \phi$ and $C_H(K) = N_H(K)$.*

Remark: let $H \trianglelefteq G$, then we have $G \to \mathrm{Aut}(H)$, $g \mapsto (h \mapsto ghg^{-1})$, where $K \subset G$.

Example: let G be a group, we consider the product $G^n = G \times G \times \cdots \times G$. Then we define $\phi : S_n \to \mathrm{Aut}(G^n)$, $\sigma \mapsto ((g_i) \mapsto (g_{\sigma(i)}))$. Then we have $(G^n) \rtimes_\phi S_n$, this is called the wreath product of G by S_n, denoted $G \wr S_n$. We have

$$((g_i), \sigma) \cdot ((h_i), \tau) = ((g_i h_{\sigma(i)}), \sigma\tau).$$

Proposition 6.9 *Let G be a group with two subgroups H and K. Assume*

1. *H is normal in G;*
2. *$H \cap K = \{e\}$;*
3. *$H \cdot K = G$.*

Then $G \cong H \rtimes_\phi K$, where $\phi : K \to \mathrm{Aut}(H)$, $k \mapsto (h \mapsto khk^{-1})$.

Proof: consider the map $\psi : H \rtimes_\phi K \to G$, $(h, k) \mapsto hk$. Then one can show ϕ is an isomorphism. $\square$

Proposition 6.10 *Let H and K be groups and let $\varphi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then the following are equivalent:*

1. *The identity (set) map between $H \rtimes_\varphi K$ and $H \times K$ is a group homomorphism.*
2. *φ is the trivial homomorphism from K into $\mathrm{Aut}(H)$.*
3. *$K \trianglelefteq H \rtimes_\varphi K$.*

Proposition 6.11 *Let p and q both be primes. Let $H = \mathbb{Z}/p\mathbb{Z}$ and $K = \mathbb{Z}/q\mathbb{Z}$. Given two group homomorphism*

$$\phi_i : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}), \quad i = 1, 2,$$

such that $\phi_1(H) = \phi_2(H)$. Then $K \rtimes_{\phi_1} H \cong K \rtimes_{\phi_2} H$.

Proposition 6.12 *Suppose K is a cyclic group, H is arbitrary. Let ϕ_1 and ϕ_2 be homomorphism from K into $\mathrm{Aut}(H)$, such that $\phi_1(K)$ and $\phi_2(K)$ are conjugate subgroups of $\mathrm{Aut}(H)$. (If K is infinite, then assume ϕ_1 and ϕ_2 are also injective). Then $H \rtimes_{\phi_1} K \cong H \rtimes_{\phi_2} K$.*

Proof: Let $\sigma \in \mathrm{Aut}(H)$, s.t., $\sigma\phi_1(K)\sigma^{-1} = \phi_2(K)$. Let p the generator of K, then $\phi_1(K)$, $\phi_2(K)$ is generator by $\phi_1(p)$, $\phi_2(p)$ respectively. Furthermore, since $\sigma\phi_1(p)\sigma^{-1} \in \phi_2(K)$, then $\sigma\phi_1(p)\sigma^{-1} = \phi_2(p)^a$ for some $a \in \mathbb{Z}$. Then we can easily show that $\sigma\phi_1(k)\sigma^{-1} = \phi_2(k)^a$ for all $k \in K$.
Now we define a map $\psi : H \rtimes_{\phi_1} K \to H \rtimes_{\phi_2} K$, by $(h, k) \mapsto (\sigma(h), k^a)$ and it has inverse $\psi^{-1}((h, k)) = (\sigma^{-1}(h), k^{-a})$. We show ψ is a homomorphism, clearly identity is mapped to identity. Now suppose $(h_1, k_1), (h_2, k_2) \in H \rtimes_{\phi_1} K$,

then

$$\begin{aligned}
\psi((h_1,k_1)(h_2,k_2)) &= \psi((h_1\phi_1(k_1)(h_2),k_1k_2)) \\
&= (\sigma(h_1\phi_1(k_1)(h_2)),(k_1k_2)^a) \\
\psi((h_1,k_1))\psi((h_2,k_2)) &= (\sigma(h_1),k_1^a)(\sigma(h_2),k_2^a) \\
&= (\sigma(h_1)\phi_2(k_1^a)(\sigma(h_2)),k_1^ak_2^a) \\
&= (\sigma(h_1)\phi_1(k_1)(\sigma(h_2)),(k_1k_2)^a) \\
&= (\sigma(h_1)\sigma(\phi_1(k_1)(\sigma^{-1}(\sigma(h_2)))),(k_1k_2)^a) \\
&= (\sigma(h_1\phi_1(k_1)(h_2)),(k_1k_2)^a)
\end{aligned}$$

As desired. □

Definition: Let H be a group, we define the semidirect product $H \rtimes_\phi \mathrm{Aut}(H)$, where $\phi : \mathrm{Aut}(H) \to \mathrm{Aut}(H)$ is the identity map, to be the Holomorph of H, denoted $\mathrm{Hol}(H)$.

Proposition 6.13 *If H is any group, then there is a group G contains H as a normal subgroup with the property that for every automorphism σ of H there is an element $g \in G$, such that conjugation by g when restricted to H is the given automorphism σ , i.e., every automorphism of H is obtained as an inner automorphism of G restricted to H.*

Proof: Take $\mathrm{Hol}(H)$. □

6.3 More on Sylow Theorems

Definition: a simple group is a nontrivial group whose only normal subgroups are the trivial group and the group itself.

Proposition 6.14 *Let P be a Sylow $p-$subgroup of H and H be a subgroup of K. If $P \trianglelefteq H$ and $H \trianglelefteq K$, then P is normal in K. If $P \in$Sylp(G), and $H = N_G(P)$, then $N_G(H) = H$.*

Proof: Since P is normal in H, then P is characteristic in H and $H \trianglelefteq K$, so $P \trianglelefteq K$. Next, if $P \in \mathrm{Sylp}(G)$, and $H = N_G(P)$. Suppose $g \in G$ is such that $gHg^{-1} = H$, then $gPg^{-1} = P$, since P is characteristic in H. Therefore, we conclude that $g \in N_G(P) = H$. □

Proposition 6.15 *There are exactly 2 groups (up to isomorphism) of order 6, namely $\mathbb{Z}/6\mathbb{Z}$ and S_3. Any groups of order 15 is cyclic.*

Lemma 6.16 *Let p be a prime and G be a group of order p^2. Then $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$. In particular, such group has to be abelian.*

Lemma 6.17 *Let G be a group (potentially infinite), such that $G/Z(G)$ is cyclic, then G is abelian. In other words, $G/Z(G)$ cannot be a non-trivial cyclic group.*

Proposition 6.18 *Suppose G is a group of order 12, then one of the following holds:*

- $G \cong A_4$.
- $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
- $G \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
- $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$, *where* $\phi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ *is given by* $(a, b) \mapsto a$.
- $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$, *where* $\phi : \mathbb{Z}/4\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$, $x \mapsto y$, *where* x, y *are the generators for* $\mathbb{Z}/4\mathbb{Z}$ *and* $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$ *respectively.*

Lemma 6.19 *Let G be a finite group with $H \trianglelefteq G$ and $P \in Sylp(G)$. Then $H \cap P$ is a Sylow $p-$subgroup of H and HP/H is a Sylow $p-$subgroup of G/H.*

Proof: By the second isomorphism theorem, we have

$$PH/H \cong P/(P \cap H).$$

Then $|PH||P \cap H| = |H||P|$. Now $P \cap H \subset H$, and $|PH|$ divides p at most as many times as $|P|$, as $PH \leq G$. Hence it must be the case that $|P \cap H|$ divides p as many times as H, as $H \cap P$ is a p-group, $((H \cap P) \leq P)$ so $H \cap P$ is a Sylow p-subgroup of H. Then HP/H is a Sylow $p-$subgroup is clear by the above isomorphism. $\square$

Proposition 6.20

1. *If $P \in \mathrm{Sylp}(G)$ and $H \leq G$. Then there exists some $g \in G$, s.t., $gPg^{-1} \cap H$ is a Sylow $p-$subgroup of H.*
2. *If P is a normal Sylow $p-$subgroup of G and H is any subgroup of G, then $P \cap H$ is the unique Sylow $p-$subgroup of H.*

Proposition 6.21 *Let N be a normal subgroup of a finite group G. Then $n_p(G/N)|n_p(G)$ for any prime p.*

Proof: Firstly, note that for any Sylow $p-$subgroup Q of G/N, let $K = \pi^{-1}(Q)$. Then $\pi(K) = Q$, and for any Sylow $p-$subgroup of K, call it P, we have $\pi(PN) = Q$ (the projection map maps Sylow $p-$subgroups to Sylow $p-$subgroups). Finally, we show that for any Sylow $p-$subgroup Q of G/N, equal number of Sylow $p-$subgroup in G maps to Q. Let Q_1, Q_2 be two Sylow $p-$subgroup of G/N, s.t., $Q_1 = xNQ_1x^{-1}N$, then we can show that there is a bijection between the Sylow $p-$subgroup of $\pi^{-1}(Q_1)$ and $\pi^{-1}(Q_2)$ constructed using conjugation by x and x^{-1} respectively. $\square$

6.4 Groups of Finite order

Proposition 6.22 *let G be of order $2n$ for an odd integer $n > 1$. Then G is not simple.*

Proof: Let G be of order $2n$, we know G is isomorphic to a subgroup of S_{2n}, denote this isomorphism to be ϕ. Then we would have a natural homomorphism $\psi : G \to S_{2n}$, $g \mapsto \phi(g)$, since $\phi(G) \leq S_{2n}$, and ϕ is a homomorphism. Again recall the homomorphism $\text{sgn} : S_{2n} \to \mathbb{Z}/2\mathbb{Z}$ defined in class, then by composing ψ and sgn, we get the a new homomorphism $f = \text{sgn} \circ \psi : G \to \mathbb{Z}/2\mathbb{Z}$, $f(g) = \text{sgn}(\phi(g))$.

Next, to show G is not simple, it suffices to show f is not the trivial map. We know $\ker(f) \trianglelefteq G$. If f is not trivial, then $\ker(f) \neq G$. Since $n > 1$, and the order of G is $2n$ which is greater than the order of $\mathbb{Z}/2\mathbb{Z}$, then $\ker(f) \neq \{e\}$, as the map cannot be injective. So we get that $\ker(f)$ is a normal subgroup of G that is not $\{e\}$ or G itself, hence G is not simple.

We proceed to show this map is trivial. By Sylow's Theorem, we know that G has a Sylow $2-$group P_2, since n is odd, then $|P_2| = 2$. Hence P_2 is cyclic and contains an element x with order 2. We show $f(x) = 1$ by showing $\phi(x)$ is an odd permutation. Since x is order 2, and ϕ being an isomorphism, then $\phi(x)$ order 2. As $\phi(x)$ is a permutation, we can write it as the product of disjoint cycles. As $|\phi(x)| = 2$, then these cycles have length 2. Now recall the isomorphism ϕ is constructed from the group action G acting on itself by left multiplication. Then for any $g \in G$, $xg \neq g$, since $x \neq e_G$. So x permutes every element of G, i.e., $\phi(x)$ do not fix any element, that is every number from $\{1, \cdots, 2n\}$ appears in some cycle of the disjoint cycle representation for $\phi(x)$. And because each cycle is length 2, every number $\{1, \cdots, 2n\}$ appears in some cycles and the cycles are disjoint, then there are exactly $2n/2 = n$ transpositions. As n is odd, then we conclude $\phi(x)$ is an odd permutation. Hence $f(x) = \text{sgn}(\phi(x)) = 1$. So f is not trivial, and it follows from the previous analysis that G is not simple $\square$

Proposition 6.23 (Group of order pq, $p < q$) *Suppose a group G is of order pq, where p and q are primes. Then either $G \cong Z_{pq}$ or $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. If $p \nmid q-1$, then $G \cong Z_{pq}$.*

Proof: G has a normal Sylow q-subgroup, since $n_q = 1 \mod q$ and $n_q | pq$, so $n_q | p$, but as $p < q$, we have $n_p = 1$. Thus the only Sylow p- subgroup is normal in G. If $p \nmid q - 1$, then it follows that the Sylow $p-$subgroup is also normal, hence G must be cyclic of order pq. Otherwise, we may have $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$. $\square$

Remark: the case when $p = 2$ and $q = 3$ is shown in the previous section.

Proposition 6.24 (Group of order p^3) *Suppose a group G is of order p^3, where p is a prime, then one of the following holds:*

1. $G \cong \mathbb{Z}/p^3\mathbb{Z}$.
2. $G \cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
3. $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
4. $G \cong (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/p\mathbb{Z}$.
5. $G \cong \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/p\mathbb{Z}$.

Proof: If G is of order p^3, then G is a p-group, hence it has non-trivial center. If $Z(G) = p^2$ or p^3 then $G/Z(G)$ is cyclic, hence G is abelian, in this case $G \cong \mathbb{Z}/p^3\mathbb{Z}$ or $G \cong \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
Now suppose G is not abelian, then $Z(G) = p$. Hence $|G/Z(G)| = p^2$ and cannot be cyclic. So, we have $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. We consider two cases:

Case 1: G has an element of order p^2, denote it by x.
Let $H = \langle x \rangle$, then H is normal as it is index p. If E is the kernel of the pth power map, that is $g \mapsto g^p$, then $E \cong Z_p \times Z_p$ and $E \cap H = \langle x^p \rangle$. Let y be any element of $E - H$ and let $K = \langle y \rangle$. By construction, $H \cap K = 1$ and so G is isomorphic to $Z_{p^2} \rtimes Z_p$, for some $\varphi : K \to \mathrm{Aut}(H)$. However,up to the choice of a generator for the cyclic group K, there is only one nontrivial homomorphism, given by

$$\varphi(y)(g) = g^{1+p}.$$

Hence up to isomorphism, there is a unique non-abelian group $H \rtimes K$ in this case.

Case 2: every nonidentity element of G has order p.
In this case, let H be any subgroup of G of order p^2. Then $H \cong Z_p \times Z_p$ (no element of p^2). Let $K = \langle y \rangle$ for any element y of $G - H$. Since H has index p, then $H \trianglelefteq G$, and K is not contained in H, so $H \cap K = 1$. Then $G \cong (Z_p \times Z_p) \rtimes Z_p$ for some $\varphi : K \to \mathrm{Aut}(H)$. But we know

$$\mathrm{Aut}(H) \cong GL_2(\mathbb{F}_p)$$

So $|\mathrm{Aut}(H)| = (p^2 - 1)(p^2 - p)$. Note that a Sylow p-subgroup of $\mathrm{Aut}(H)$ has order p so all subgroups of order p in are conjugate in $\mathrm{Aut}(H)$ by Sylow's Theorem. Hence no matter what φ is, the resulting group are all isomorphic. We pick one representative of this, if $H = \langle a \rangle \times \langle b \rangle$. Let $\langle \gamma \rangle$ generated the image of φ, then

$$\gamma(a) = ab \text{ and } \gamma(b) = b.$$

Finally, since the two non-abelian groups have different orders for the kernels of the pth power map, they are not isomorphic. □

Proposition 6.25 (Groups of order p^2q) *Let G be a non-abelian group of order p^2q.*

1. *If $p > q$, then $G \cong \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$ or $G \cong (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/q\mathbb{Z}$*
2. *If $p < q$, if the Sylow $q-$subgroup is not normal, then $|G| = 12$, and $G \cong A_4$; if the Sylow q-subgroup is normal, then $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$.*

Proof: Suppose G is of order p^2q:

1. If $p > q$, then the Sylow p-subgroup of G is normal and it is abelian as it is of order p^2. Since G is non-abelian, then the Sylow q-subgroup of G is not normal otherwise G is the direct product of two abelian groups. Hence $G \cong \mathbb{Z}/p^2\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$ or $G \cong (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes \mathbb{Z}/q\mathbb{Z}$.
2. If $p < q$, then $n_q = 1$ or p^2. $n_q = p^2$ if and only if $q | p^2 - 1$ so $q | p + 1$. But as p, q are prime, then we conclude that p, q $p = 2$, $q = 3$. So $|G| = 12$. But then by Proposition 6.18, we know $G \cong A_4$. In this case the Sylow

2− subgroup is normal.

Now suppose $n_q = 1$. Then the Sylow $q-$subgroup is normal again, so $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/q\mathbb{Z} \rtimes (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z})$. Of course further analysis can be made based on the kernel and image of φ.

$\square$

Proposition 6.26 *Let G be a finite nonabelian simple group. Let $H \leq G$ by a proper subgroup, then $|G : H| \geq 5$.*

Proof: G acts on the left cosets of H by left multiplication. This action is nontrivial, since H is a proper subgroup. Since G is simple, the action has trivial kernel. It thus defines an embedding of G into $S_{|G:H|}$. Since S_4 (S_4 is not simple, subgroup of order 12 is A_4 and not simple, subgroup of order 6 is isomorphic to S_3), S_3 (S_3 is not simple, and any proper subgroup of S_3 is abelian), S_2 (abelian) and S_1 have no nonabelian simple subgroups, hence $|G : H| \geq 5$. $\square$

Ways to prove a groups is not normal: Under the assumption that $|G|$ is not a cyclic group of order p, then we can use the following to determine when G is not a simple group.

1. Group of order $2n$, n being odd, is not simple.
2. Group of order pq is not simple.
3. p-group is not simple.
4. Group of order p^2q is not simple.
5. If G has a subgroup H of index p, where p is the smallest prime dividing G, then H is normal, hence G is not simple.
6. Let p be a prime dividing $|G|$. If the only solution to $n_p \equiv 1 \mod p$, and $n_p | \frac{n}{p^m}$, is $n_p = 1$, then the Sylow p-subgroup must be normal, hence G is not simple.
7. Counting elements of each order: if $|G| = p^m e$, where $p \nmid e$. Then when $m = 1$, then every Sylow p-subgroup is a cyclic group of order p, hence they do not intersect, which contributes to $(p-1) \cdot n_p$ elements. If $m > 1$, then the Sylow $p-$subgroups may intersect, which contributes to at least $p^m - 1 + p$ elements. Using a counting argument, we can conclude that certain Sylow p-subgroup must be normal, hence G is not simple.
8. Suppose the Sylow p-subgroup of G be $P = \{P_1, \cdots, P_m\}$. Then consider G acting on P by conjugation, which induce a map $\varphi : G \to S_m$. If $|G| \nmid m!$, then the kernel of φ cannot be trivial, thus $\ker(\varphi)$ is a normal subgroup of G. So G is not simple.
9. Suppose the Sylow p-subgroup of G be $P = \{P_1, \cdots, P_m\}$. Then consider G acting on P by conjugation, which induce a map $\varphi : G \to S_m$. G should not contain a subgroup of index 2 (as that subgroup would be normal), then $\varphi(G) \leq A_m$. So if $|G| \nmid |A_m| = m!/2$, then G is not simple.

   We show a quick proof why $\varphi(G) \leq A_m$ or more simply denote $G \leq A_n$:
   If G is not contained in A_m, then A_m is a proper subgroup of GA_m, so $GA_m = S_m$. But now by the second isomorphism thoerem.
   $$2 = |S_m : A_m| = |GA_m : A_m| = |G : G \cap A_m|.$$

So G has a subgroup $G \cap A_m$ of index 2.

10. Let P be a Sylow p-subgroup, then $N_G(P) \leq G$. Then consider G acting on $G/N_G(P)$ by left multiplication, which induces a homomorphism $\varphi : G \to S_i$ where $i = |G : N_G(P)|$. If φ is not injective, then $\ker(\varphi)$ is a normal subgroup of G hence G is not simple. We can even expand this by applying the action to the left cosets of any subgroup of G. So if a group G is of order n, then it cannot have any subgroup with index m where $n \nmid m!$, otherwise the action by left multiplication on the cosets of this subgroup has non-trivial kernel.

11. We first prove a lemma which states: in a finite group G, if $n_p \neq 1 \mod p^2$, then there are distinct Sylow p-subgroup P and R of G such that $P \cap R$ is of index p in both P and R (hence is normal in each).
Proof: Let P act by conjugation on the set $Sylp(G)$. Let $\mathcal{O}_1, \cdots, \mathcal{O}_s$ be the orbits under this actions with $\mathcal{O}_1 = \{P\}$. If p^2 divides $|P : P \cap R|$ for all Sylow p-subgroups R of G different from P, then each $\mathcal{O}_i$ has size divisible by p^2, $i = 2, 3, \cdots, s$. In this case, since n_p is the sum of the lengths of the orbits we have $n_p = 1 + kp^2$ which is a contradiction.
Now suppose two Sylow $p-$subgroups P and Q be such that $K = P \cap Q$ have index p in P and Q respectively. Then K is normal in P and Q. Then consider $N = N_G(K)$ which contains P and Q. Now if N has only one Sylow p-subgroup, then we immediately get a contradiction. Otherwise, $|P|||N|$ and $|N| > |P|$. Now if $|N| = |G|$, then $P \cap Q$ is normal, hence G is not simple; If $|N| < |G|$, then consider $|G : N|$ which is small enough. Then we can apply the previous technique to analysis the group.

12. Let the sylow p-subgroup of G be $X = \{P_1, \cdots, P_m\}$, where $m < 2p$. Then consider $\varphi : G \to S_m$ which has image in A_m. $|N_G(P)| = \frac{|G|}{n_p}$. Now we claim that $|N_{A_m}(P_i)| = \frac{1}{2}|N_{S_m} P_i|$ when p is an odd prime.
Proof: we know $\varphi(P_i)$ need to be a Sylow p-subgroup of S_m and A_m (if φ is not injective, then G is not simple), because $m \leq 2p$. Then by Frattini's Argument, we have

$$S_m = N_{S_m}(P_i)A_m$$

so $N_{s_m}(P_i)$ is not contained in A_m, hence $N_{S_m}(P_i) \cap A_m = N_{A_m}(P_i)$ has index 2 in $N_{s_m}(P_i)$.
Next we compute $|N_{s_m}(P_i)|$, since it is a p-group, then $|O_{p_i}|$ under the conjugation action is $\frac{m!}{p(p-1)(m-p)!}$, which gives $|N_{s_m}(P_i)| = p(p-1)(m-p)!$. Then $|N_{A_m}(P_i)| = \frac{1}{2}p(p-1)(m-p)!$ which must be divisible by $\frac{|G|}{n_p}$. Now if $m = p+1$, this implies $\frac{1}{2}p(p-1)$ must be divisible by $\frac{|G|}{n_p}$.

13. Suppose the normalizer N of a Sylow $p-$subgroup P of G is cyclic of order pq where q is also a prime. Then N is cyclic, consider $\varphi : G \to S_{|G:P|}$ induced by G acting on the Sylow $p-$subgroups by conjugation. The image of N under this map is of order pq if φ is injective, which requires $|G : P| > p + q$.

14. Suppose the normalizer of N of a Sylow $p-$subgroup P of G is of order $pqr \cdots$. Then let Q be a Sylow $q-$subgroup of N. If $q \nmid p - 1$, then PQ is a cyclic subgroup of N hence abelian. This implies the Sylow $q-$subgroup of G, if it is of order q, will have P lying inside the normalizer of Q. Hence we can restrict the possible index of $N_G(Q)$.

15. Burnside's normal complement theorem: Suppose G is a finite group and P is a Sylow p-subgroup of G. Then if $C_G(P) = N_G(P)$, then there exists $Q \trianglelefteq G$ such that $P \cap Q = \{e\}$ and $G = PQ$.
So if $C_G(P) = N_G(P)$, then G is not simple.

16. Recall proposition: Suppose H is a subgroup of G, then $N_G(H)/C_G(H) \subseteq \mathrm{Aut}(H)$. E.g.: consider group of order $525 = 3 \cdot 5^2 \cdot 7$. Then $n_3 \in \{1, 7, 25, 175\}$.

    - $n_3 = 7$, then $|N(P_3)| = 3 \cdot 5^2$. But $\gcd(5, 2) = 1$, then $C(P_3) = N(P_3)$, then by the Burnside's normal complement theorem, G is not simple.
    - $n_3 = 25$, then $N_G(P_3)/C_G(P_3) \subset \mathrm{Aut}(P_3) = Z_2$. And $|N_G(P_3)| = 21$, $\gcd(21, 2) = 1$, hence $C_G(P_3) = N_G(P_3)$. So G is not simple.
    - $n_3 = 175$, similar to the previous case, we have $N_G(P_3) = C_G(P_3)$, so G is simple.

Further Techniques for analysing the structure of a group:

1. Suppose we know a group G has a normal Sylow p-subgroup P of order p, and Q is a Sylow $q-$subgroup of order q. Then consider the group PQ which has order pq. If PQ is normal in G, then P and Q are characteristic in PQ, hence normal in G. We know PQ has to be normal if $|G : PQ|$ is equal to the smallest prime dividing $|G|$.

2. Once we establish PQ is a subgroup of G as above, we can also proceed with counting argument, as PQ is cyclic hence can only contain 1 Sylow subgroup of each type.

3. We can also study the centralizer of an element of a Sylow $p-$subgroup P, where $|P| = p$. Let $x \in P$, then $x \in C_G(x) \leq N_G(P)$. Since $N_G(P)$ acts on P by conjugation, then if some element of $N_G(P)$ has order that doesn't divides $p - 1$ then it must commute with every element in P.

4. Let H be a normal subgroup of prime order p in a finite group G. Suppose that p is the smallest prime that divides the order of G, then $H \leq Z(G)$.

5. Suppose P is a normal Sylow p-subgroup of G. Then G act on P by conjugation, hence there is homomorphism from G to $\mathrm{Aut}(P)$, thus an isomorphism from $G/C_G(P)$ to a subgroup of $\mathrm{Aut}(P)$. However, if $\gcd(|\mathrm{Aut}(P)|, |G|/p)$ is 1, then the map has to be trivial. Hence $P \leq Z(G)$.

6. Recall for any subgroup H of a group G, the quotient group $N_G(H)/C_G(H)$ is isomorphic to a subgroup of Aut(H).

Theorem 6.27 *For $n < 100$, if $|G| = n$ is a non-abelian simple group, then $|G| = 60$ and $G \cong A_5$.*

Proof: By using the preceding techniques, we can rule out all possibility except $|G| = 60$. Now we show that if G is a simple group of order 60, then $G \cong A_5$.
Firstly G has no proper subgroup H of index less than 5 by Proposition 6.26. So $n_2 = 5$ or 15. Let $P \in Syl2(G)$ and let $N = N_G(P)$, so $|G : N| = n_2$.
If $n_2 = 5$, then N has index 5 so the action of G by left multiplication on the set of left cosets of N gives a permutation representation of G into S_5. The kernel must be trivial, then G is isomorphic to a subgroup of S_5.

Then $G \leq A_5 \Rightarrow G \cong A_5$. ($G$ cannot be another subgroup of order 2 in S_5).
If $n_2 = 15$. Then if for every pair of distinct Sylow 2-subgroups P and Q of G, $P \cap Q = 1$. Then the number of nonidentity elements in Sylow 2-subgroups would be $(4-1) \cdot 15 = 45$ which is not possible. This contradiction proves that there exists distinct Sylow 2-subgroups P and Q such that $|P \cap Q| = 2$. Let $M = N_G(P \cap Q)$, then $P, Q \leq M$. So $|M| > 4$ and $4|M$, which implies $|M| = 12$. I.e., M has index 5 in G. But now the argument of the preceding paragraph applied to M in place of N gives $G \cong A_5$. This leads to a contradiction because $n_2(A_5) = 5$.
□

7 Group Decompositions

7.1 Solvable Groups

Definition: let G be a group,

- A (normal) tower/series of G is a sequence of subgroups $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m = \{e\}$. Such that G_{i+1} is a normal subgroup of G_i. We have the subquotient/factor group G_i/G_{i+1}.
- The normal tower is called abelian (resp. cyclic) if G_i/G_{i+1} is abelian (resp. cyclic) for all i.
- a refinement of a given tower of G is a tower obtained by inserting a finite number of subgroups in the given tower.
- Let $G = G_0 \supset G_1 \supset \cdots \supset G_m = \{e\}$ and $G = H_0 \supset H_1 \supset \cdots \supset H_n = \{e\}$, be normal towers of G. They are called equivalent if $m = n$, and up to permutation of indices $i \mapsto i' \in S_n$, we have

$$G_i/G_{i+1} \cong H_{i'}/H_{i'+1}$$

  for all i.
- A group G is called solvable if it admits a normal tower $G = G_0 \supset G_1 \supset \cdots \supset G_m = \{e\}$ such that G_i/G_{i+1} is abelian.

Lemma 7.1 *S_3 is solvable, we have $S_3 \supset A_3 \cong \mathbb{Z}/3\mathbb{Z} \supset \{e\}$. S_5 is NOT solvable.*

Lemma 7.2 *Let G be a finite group. Then any abelian tower of G admits a cyclic refinement.*

Corollary 7.2.1 *Let G be finite. Then G is solvable if and only if G admits a cyclic tower.*

Definition: suppose $x, y \in G$, then $x^{-1}y^{-1}xy$ is called the commutator of x and y and is denoted $[x, y]$. The group generated by the set of all commutators in G is known as the commutator subgroup of G and is denoted by $G^{(1)} = [G, G]$.

Lemma 7.3 *Let $G^{(1)}$ denote the commutator subgroup of G. Then $G^{(1)} \trianglelefteq G$, and $G/G^{(1)}$ is an abelian group. In particular, any group homomorphism from G to an abelian group factors through $G/[G, G]$.*

Notation: $G^{(1)} = [G, G]$, $G^{(0)} = G$, $G^{(i+1)} = [G^{(i)}, G^{(i)}] \trianglelefteq G_i$.

Theorem 7.4 *A group G is solvable, if and only if $G^{(n)} = \{e\}$ for some n.*

Proof: $\Leftarrow$: we consider the normal tower

$$G = G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots \supset G^{(n)} = \{e\}.$$

We know $G^{(i)}/G^{(i+1)}$ is abelian, so G is solvable.
$\Rightarrow$: assume G is solvable. Then we have an abelian tower. $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$, such that G_i/G_{i+1} is abelian for all i. We claim $G^{(i)} \subset G_i$. By induction on n.
The base case is trivial, $G^{(0)} = G_0$ by definition. Note that since G_i/G_{i+1} is abelian, we have $[G_i, G_i] \subset G_{i+1}$ (The image of $[G_i, G_i]$ under the quotient map $G_i \to G_i/G_{i+1}$ is $e \cdot G_{i+1}$). Then by induction hypothesis, $G^{(i)} \subset G_i$. Then $G^{(i+1)} = [G^{(i)}, G^{(i)}] \subset [G_i, G_i] \subseteq G_{i+1}$.
Then $G^{(n)} \subseteq G_n = \{e\} \Rightarrow G^{(n)} = \{e\}$. □

Lemma 7.5 *Let G be a group and $N \trianglelefteq G$, then $\forall n \in \mathbb{N}$, $(G/N)^{(n)} = G^{(n)}N/N$.*

Proof: When $n = 0$, the statement clearly holds.
Suppose the statement holds for some $n \in \mathbb{N}$, then consider the case for $n+1$. Firstly, it is clear that N is normal in $G^{(n+1)}N$ because it is normal in G.
Now since $(G/N)^{(n+1)} = [(G/N)^n, (G/N)^n] = [G^{(n)}N/N, G^{(n)}N/N]$. We show that generator of $(G/N)^{(n+1)}$ is in $G^{(n+1)}N/N$. Let $xnN, y\tilde{n}N \in G^{(n)}N/N$, then

$$xnN \cdot y\tilde{n}N \cdot n^{-1}x^{-1}N \cdot \tilde{n}^{-1}y^{-1}N = xyx^{-1}y^{-1}n'N \in G^{(n+1)}N/N.$$

Now if $gnN \in G^{(n+1)}N/N$, then $g = \prod_{i=1}^{k}(x_i y_i x_i^{-1} y_i^{-1})$, so

$$gnN = \prod_{i=1}^{k}(x_i y_i x_i^{-1} y_i^{-1})nN = \prod_{i=1}^{k}(x_i y_i x_i^{-1} y_i^{-1})N = \prod_{i=1}^{k}\left[x_i N y_i N x_i^{-1} N y_i^{-1} N\right] \in [G^{(n)}N/N, G^{(n)}N/N].$$

Hence by induction the statement holds for all $n \in \mathbb{N}$. □

Theorem 7.6 *Let G be a solvable group, then any subgroup of G or any quotient group of G is solvable. Conversely, if a normal subgroup N of G is solvable, and G/N is solvable, then G is solvable.*

Proof: Let H be a subgroup of G, suppose G is solvable, then let

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

be a normal tower such that G_i/G_{i+1} is abelian. Then consider $H_i = H \cap G_i$. Then clearly

$$H = H_0 \supset H_1 \supset \cdots \supset H_n = \{e\}.$$

H_{i+1} is normal in H_i, because let $h \in H_{i+1}$ and $g \in H_i$, then $h \in H$ and $h \in G_{i+1}$, $g \in H$ and $g \in G_i$, so $ghg^{-1} \in H$ and $ghg^{-1} \in G_{i+1}$ as G_{i+1} is normal in G_i. Next, G_{i+1} is normal in $H \cap G_i$ as it is normal in G_i, then by the second isomorphism theorem, we have

$$\frac{(H\cap G_i)}{G_{i+1}} \cong \frac{H\cap G_i}{H\cap G_i\cap G_{i+1}} = \frac{H\cap G_i}{H\cap G_{i+1}}.$$

But notice $\frac{H\cap G_i}{G_{i+1}} \leq \frac{G_i}{G_{i+1}}$ which is abelian, then we conclude that $\frac{H_i}{H_{i+1}} = \frac{H\cap G_i}{H\cap G_{i+1}}$ is abelian.

Next, let $Q = G/N$ be a quotient group of G, then $N \trianglelefteq G$. Consider $Q_i = G_iN/N$, then $Q_i \trianglelefteq Q_{i+1}$ because N is normal in G_iN (since it is normal in G) and $G_{i+1}N$ is normal in G_iN (can do direct verification), so Q_i is normal in Q_{i+1}. Also by the third isomorphism theorem, we have

$$\frac{G_iN/N}{G_{i+1}N/N} \cong \frac{G_iN}{G_{i+1}N}.$$

Now we show for any $x, y \in G_{i+1}$ and $n, m \in N$, the commutator $[xn, ym]$ is in G_iN, then it would imply $G_iN/G_{i+1}N$ is abelian.

$$\begin{aligned}[xn, ym] &= xnymn^{-1}x^{-1}m^{-1}y^{-1}\\ &= xyx^{-1}y^{-1}\tilde{n} \in G_{i+1}N\end{aligned}$$

This is because N is normal, so we can shift every element of n to the right, and $xyx^{-1}y^{-1} \in G_iN$ because G_i/G_{i+1} is abelian. Hence we conclude Q_i/Q_{i+1} is also abelian.

On the other hand, if $N \trianglelefteq G$ and both N and G/N are solvable. Then $(G/N)^{(n)} = e = \{N\}$ for some $n \in \mathbb{N}$, by Theorem 7.4. So by theorem 7.5, we have

$$G^{(n)}N/N = (G/N)^{(n)} = \{N\}.$$

That is $G^{(n)} \leq N$. Then $G^{(n)}$ is solvable because it is a subgroup of N, so $(G^{(n)})^{(m)} = \{e\}$ for some $m \in \mathbb{N}$. But then observe $(G^{(n)})^{(m)} = G^{(m+n)} = \{e\}$. Hence G is solvable. □

Proposition 7.7 *Let G and K be groups, let H be a subgroup of G and let $\varphi : G \to K$ be a surjective homomorphism.*

1. *$H^{(i)} \leq G^{(i)}$ for all $i \geq 0$. In particular, if G is solvable, then so is H, i.e., subgroups of solvable groups are solvable (and the solvable length of H is less than or equal to the solvable length of G).*

2. *$\varphi(G^{(i)}) = K^{(i)}$. In particular, homomorphic images and quotient groups of solvable groups are solvable (of solvable length less than or equal to that of the domain group).*

Theorem 7.8 *Let G be a finite group*

1. *(Burnside) If $|G| = p^aq^b$ for some primes p and q, then G is solvable.*

2. *(Philip Hall) If for every prime p dividing $|G|$ we factor the order of G as $|G| = p^am$ where $(p, m) = 1$, and G has a subgroup of order m, then G is solvable.*

3. *(Feit-Thompson) If $|G|$ is odd then G is solvable.*

4. *(Thompson) If for every pair of elements $x, y \in G$, $\langle x, y\rangle$ is a solvable group, then G is solvable.*

Remark: the proof of these theorems are generally difficult!

Theorem 7.9 *A finite group G is solvable if and only if for every divisor n of $|G|$ such that $\gcd(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n.*

Proposition 7.10 *Let G be any group, then $G^{(i)}$ is characteristic in G.*

Proof: G is clearly characteristic in G. Now suppose $G^{(n)}$ is characteristic in G, we show $G^{(n+1)}$ is characteristic in G. Let $\phi : G \to G$ be any automorphism, we show that any generator element of $G^{(n+1)}$ is mapped to $G^{(n+1)}$ under ϕ. But this is clear, as if $x, y \in G^{(n)}$, then $\phi(x), \phi(y) \in G^{(n)}$ as $G^{(n)}$ is characteristic in G. Hence $\phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} \in G^{(n+1)}$. □

Lemma 7.11 *Let G be a group and $H \trianglelefteq G$, then $H^{(n)} \trianglelefteq G$.*

Proof: When $n = 0$, then $H \trianglelefteq G$. Suppose the statement hold for some n, we show it holds for $n + 1$.
It suffices to show that for any $g \in G$, and $x, y \in H^{(n)}$, we have $gxyx^{-1}y^{-1}g^{-1} \in H^{(n+1)}$, as such $xyx^{-1}y^{-1}$ generates $H^{(n+1)}$. Notice

$$gxyx^{-1}y^{-1}g^{-1} = gxg^{-1}gyg^{-1}gx^{-1}g^{-1}gy^{-1}g^{-1}.$$

Since $H^{(n)}$ is normal in G, then $gxg^{-1} = x' \in H^{(n)}$ and $gyg^{-1} = y' \in H^{(n)}$, so $gxyx^{-1}y^{-1}g^{-1} = x'y'(x')^{-1}(y')^{-1} \in H^{(n+1)}$ as desired.
□

Proposition 7.12 *Suppose H is a nontrivial normal subgroup of a solvable group G, then there is a nontrivial subgroup A of H with $A \trianglelefteq G$ and A abelian.*

Proof: If H is abelian, then we done. Otherwise $[H, H] \neq \{e\}$. Since G is solvable, then $H^{(n)} = \{e\}$ for some $n \in \mathbb{N}$. Then consider $H^{(n-1)}$ which is abelian. Then $A := H^{(n-1)}$ is the group we are looking for. □

7.2 Composition Series

Definition: a normal tower $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m = \{e\}$ is called a composition series if each factor group G_i/G_{i+1} is simple. The factor groups G_i/G_{i+1} are called composition factors of G.
Note: later we will show that the composition factors are well-defined independent of the normal tower we choose. The composition series always exist if G is finite. However the group $(\mathbb{Z}, +)$ has no composition series.

Theorem 7.13 *Every finite non-trivial group G has a composition series. In particular, if $H \trianglelefteq G$, then there is a composition series of G containing H.*

Proof: We proceed with induction on $|G|$. Firstly, note if G is simple then $G = G_0 \supset G_1 = \{e\}$ is a composition series. And if G is of prime order, then G is simple. Now suppose G it not simple, then let H be a nontrivial normal subgroup of G. Then $|H| \leq |G|$ and $|G/H| \leq G$. Then let

$$H = H_0 \supset H_1 \supset \cdots \supset H_n = \{e\};$$

$$G/H = K_0 \supset K_1 \supset \cdots \supset K_m = \{e\}.$$

Then consider the tower:

$$G = \pi^{-1}(K_0) \supset \cdots \supset \pi^{-1}(K_m) = H = H_0 \supset \cdots \supset H_n = \{e\}.$$

The tower is normal because $K_{i+1} \trianglelefteq K_i$ so $\pi^{-1}(K_{i+1}) \trianglelefteq \pi^{-1}(K_i)$ by the fourth isomorphism theorem. Moreover, $\pi^{-1}(K_i)/\pi^{-1}(K_{i+1})$ is simple, because

$$\pi^{-1}(K_i)/\pi^{-1}(K_{i+1}) \cong K_i/K_{i+1}$$

by the third isomorphism theorem. Thus we have derived a composition series for G. $\square$

Theorem 7.14 (Jordan-Hölder Theorem) *Let G be a group with two composition series.*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\};$$

$$G = H_0 \supset H_1 \supset \cdots \supset H_m = \{e\}.$$

Then they are equivalent. So the composition factors of G is well-defined if G has a composition series.

Definition: let G be a group with a composition series

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}.$$

Then the composition factors of G is $\{G_i/G_{i+1}\}$.

Proposition 7.15 *Let G be a group with two (normal) towers,*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\};$$

$$G = H_0 \supset H_1 \supset \cdots \supset H_m = \{e\}.$$

Then they have equivalent refinement.

Proof: Consider

$$(G_0 \cap H_0)G_1 \supset (G_0 \cap H_1)G_1 \supset \cdots \supset (G_0 \cap H_m)G_1 \cup (G_1 \cap H_0)G_2 \supset \cdots.$$

$$(H_0 \cap G_0)H_1 \supset (H_0 \cap G_1)H_1 \supset \cdots \supset (H_0 \cap G_n)H_1 \supset (H_1 \cap G_0)H_2 \supset \cdots.$$

More specifically, define $G_{i,j} = (H_i \cap G_i)G_{i+1}$, $H_{j,i} = (G_i \cap H_j)H_{j+1}$. Since G_1 is normal in G_0, then $G_0 \cap H_0 \subset N(G_1)$, hence $(G_0 \cap H_0)G_1$ is a group. Similarly, we have $G_{i,j}$, $H_{j,i}$ are groups. And $G_{i,j+1} \supset G_{i,j}$, $H_{j,i+1} \supset H_{j,i}$. (This is just a sketch, we also need to consider when the other index changes).
We claim that $G_{i,j+1}$ is normal in $G_{i,j}$; $H_{j,i+1}$ is normal in $H_{j,i}$, and $G_{i,j}/G_{i,j+1} \cong H_{j,i}/H_{j,i+1}$. This follows precisely from the Butterfly Lemma. □

Lemma 7.16 (Butterfly Lemma) *Let G be a group, let U, V be subgroups of G, and let $u \trianglelefteq U$, and $v \trianglelefteq V$. Then $u(U \cap v)$ is normal in $u(U \cap V)$; $(u \cap V)v$ is normal in $(U \cap V)v$. We also have $u(U \cap V)/u(U \cap v) \cong (U \cap V)v/(u \cap V)v$.*

Theorem 7.17 *If G is finite, then the following are equivalent:*

1. *G is solvable;*
2. *G has a normal tower:*
$$\{e\} = H_s \trianglelefteq H_{s-1} \trianglelefteq \cdots H_0 = G$$
such that H_{i+1}/H_i is cyclic;
3. *All compositions factors of G are of prime order;*
4. *G has a normal tower:*
$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_t = G$$
such that N_i is normal in G and N_i/N_{i+1} is abelian.

Proof: $1 \Rightarrow 2$: suppose G is solvable, then

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = \{e\}$$

and G_i/G_{i+1} is abelian. Then for any i, if G_i/G_{i+1} is simple, then $G_i/G_{i+1} \cong \mathbb{Z}/p\mathbb{Z}$, so it is cyclic. Suppose not, then let P be any normal group of G_i/G_{i+1} that is not $\{e\}$ or G_i/G_{i+1}. Then consider $G_{i+1} \trianglelefteq \pi^{-1}(P) \trianglelefteq G_i$, it is clear that $\pi^{-1}(P)/G_{i+1}$ and $G_i/\pi^{-1}(P)$ are abelian. Hence by inserting $\pi^{-1}(P)$, we get an refined of the normal tower. Repeating this process, evetually we get that

$$G = G'_0 \supset G'_1 \supset \cdots \supset G'_n = \{e\}$$

and G'_i/G'_{i+1} is simple hence cyclic. Thus we have $1 \Rightarrow 2$.

$2 \Rightarrow 3$: Similar to the previous part, we can extend the normal tower by finding an refinement each time. H_{i+1}/H_i is cyclic, hence abelian. It is simple iff $|H_i/H_{i+1}| = p$ for some prime p. So if the quotient is not simple, then we can find a P that is normal in H_i/H_{i+1}.

$3 \Rightarrow 4$: If G is simple, then we done (we can easily see that G is abelian), otherwise, let N_0 be a nontrivial normal group of G with smallest order. We can always find such N_0 by the well-ordering principle. Now we know there exists a composition series of G that contains N_0, denote it

$$\{e\} = G_0 \trianglelefteq \cdots \trianglelefteq G_k \trianglelefteq N_0 \trianglelefteq G_{k+1} \trianglelefteq \cdots G_v = G.$$

We show N_0 has to be abelian. This is because $N_0/G_k \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p. Then let $x, y \in N_0$, we consider $xyx^{-1}y^{-1}$ acting on the cosets N_0/G_k by left multiplication. Since $|N_0 : G_k| = p$ is a prime, by some thinking, we conclude that $xyx^{-1}y^{-1}G_k = G_k$, so $xyx^{-1}y^{-1} \in G_k$. Since N_0, is normal in G, $gG_kg^{-1} \leq N_0$ with index p. Then by a similar argument, we have $xyx^{-1}y^{-1} \in gG_kg^{-1}$ (acting on the subgroup gG_kg^{-1}). So consider $\bigcap_{g\in G} gG_kg^{-1}$ which contains $xyx^{-1}y^{-1}$. But $\bigcap_{g\in G} gG_kg^{-1}$ is normal, then by the minimality of N_0, we conclude that $xyx^{-1}y^{-1} = e$, thus $[N_0, N_0] = \{e\}$. Hence N_0 is abelian.
Lastly, we proceed the same procedure on G/N_0, to get N_1, N_2 and so on, and resultingly, we get the normal tower

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots N_t = G$$

such that N_i is normal in G and N_i/N_{i+1} is abelian.

$4 \Rightarrow 1$: Clear. $\square$

7.3 Nilpotent Group

Definition: for any group G, we define the following subgroups of G inductively:

- $Z_0(G) = \{e\}$,
- $Z_1(G) = Z(G)$,
- Then consider $\pi : G \to G/Z(G)$ and define $Z_2(G)$ to be $\pi^{-1}(Z(G/Z(G))$ Then note that $Z_2(G)$ is normal in G.
- We define $Z_{i+1}(G) = \pi^{-1}(Z(G/Z_i(G)))$.
- And we get a tower of (normal) subgroups:

$$Z_0(G) = \{e\} \leq Z_1(G) = Z(G) \leq Z_2(G) \leq Z_3(G) \leq \cdots .$$

  This tower is called the upper central series of G.

Definition: a group is called nilpotent if $Z_n(G) = G$ for some n. The smallest such n is called the nilpotence class of G. In other words, we have

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq Z_n(G) = G \leq Z_{n+1}(G) = G.$$

Remark: there are various other equivalent characterization of nilpotent groups.
Remark: if G is a finite group, then eventually $Z_n(G) = Z_{n+1}(G) = Z_{n+2}(G) = \cdots$, for some $n \in \mathbb{Z}^+$. If G is infinite, then it may happen that $Z_n(G) \neq G$ for any $n \in \mathbb{Z}$, but $G = \bigcup_{i=0}^{\infty} Z_i(G)$. Such group is known as hypernilpotent.

Lemma 7.18 *$Z_i(G)$ is a characteristic hence normal group in G.*

Proof: Note $Z_1(G) = Z(G)$ char in G by Lemma 4.22. Now suppose $Z_i(G)$ is characteristic, we show $Z_{i+1}(G)$ is also characteristic in G. $Z(G/Z_i(G))$ is characteristic in $G/Z_i(G)$ again by Lemma 4.22. Now consider an automorphism ϕ on G. $\phi(Z_i(G)) = Z_i(G)$. Now if $x \in Z_{i+1}(G)$, then for any $y \in G$, we have $xyx^{-1}y^{-1} \in Z_i(G)$, as $xyZ_i(G) = yxZ_i(G)$. We show $\phi(x) \in Z_{i+1}(G)$. suffices to show $\phi(xyx^{-1}y^{-1}) \in Z_i(G)$ for any $y \in G$. But since $xyx^{-1}y^{-1} = g \in Z_i(G)$, and $\phi(g) = g' \in Z_i(G)$, then $\phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = \phi(xyx^{-1}y^{-1}) = g' \in Z_i(G)$. Hence we conclude that $\phi(x) \in Z_{i+1}(G)$, so $Z_{i+1}(G)$ is characteristic in G. □

Lemma 7.19 *If G is nilpotent, then G is solvable. If G is abelian, then G is nilpotent.*

Lemma 7.20 *Let G be a finite p-group for some prime p, then G is nilpotent of nilpotence class at most $n-1$, where $|G| = p^n$.*

Theorem 7.21 *Let G be a finite group of order $p_1^{n_1} \cdots p_k^{n_k}$ for primes p_i and $n_i > 0$. Let P_i be a Sylow p_i-subgroup of G, then the following are equivalent:*

- *G is nilpotent;*
- *If H is a proper subgroup of G, then H is a proper subgroup of $N_G(H)$.*
- *Every Sylow p_i-subgroup is normal.*
- *$G \cong P_1 \times P_2 \times \cdots \times P_k$.*

Proof:

1. $1 \Rightarrow 2$: we proceed by induction on $|G|$. The base case is vacuously true (no proper subgroup).
   We know $Z(G) \neq \{e\}$, as G is nilpotent. Note $Z(G) \subset N_G(H)$, hence $HZ(G) \subset N_G(H)$. We can assume $Z(G) \subset H$, otherwise H is clearly a proper subgroup of $N_G(H)$. We consider the quotients $H/Z(G)$ which is a proper subgroup of $G/Z(G)$. Let $K/Z(G)$ be the normalizer of $H/Z(G)$, then $H/Z(G)$ is a proper subgroup of $K/Z(G)$ by induction hypothesis (since $G/Z(G)$ is also nilpotent). Hence H is a proper subgroup of K, and clearly $K \subset N_G(H)$.
2. $2 \Rightarrow 3$: Let P_I by any Sylow p_i-subgroup of G. Let $N = N_G(P_i)$. We know $N_G(N) = N$, hence N must be G. So P_i is normal in G.
3. $3 \Rightarrow 4$: Direct Product.
4. $4 \Rightarrow 1$: Clear.

□

Corollary 7.21.1 *Let p be a prime and let P be a group of order p^a, $a \geq 1$. Then every proper subgroup H of P is a proper subgroup of $N_P(H)$.*

Corollary 7.21.2 *A finite abelian group is the direct product of its Sylow subgroups.*

Lemma 7.22 (Frattini's Argument) *Let G be a finite group, H be normal in G, P be a Sylow $p-$subgroup of H. Then $G = HN_G(P)$ and $|G : H|$ divides $|N_G(P)|$.*

Proof: Firstly $HN_G(P)$ is a subgroup of G and $HN_G(P) = N_G(P)H$. Let $g \in G$. Since $gPg^{-1} \leq gHg^{-1} = H$, both P and gPg^{-1} are Sylow $p-$subgroups of H. Then there exists $x \in H$, s.t., $gPg^{-1} = xPx^{-1}$ that is $gx^{-1} \in N_G(p)$. Hence $g \in N_G(P)x$. Since g is arbitrary, then $G = N_G(P)H$.
Next apply the second isomorphism theorem to $G = N_G(P)H$, we obtain

$$|G : H| = |N_G(P) \,:\, N_G(P) \cap H|.$$

So $|G : H|$ divides $|N_G(P)|$. $\square$

Definition: let G be a group. A proper subgroup M of G is called maximal if whenever $M \leq H \leq G$, then $H = M$ or $H = G$.
Let S be the set of all proper subgroup ordered by inclusion.

Proposition 7.23 *Let G be a finite group. Then G is nilpotent if and only if all maximum subgroups of G are normal.*

Proposition 7.24 *If G is a finite group such that for all positive integers n dividing its order, G contains at most n elements x satisfying $x^n = 1$, then G is cyclic.*

Proof: Let $|G| = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ and let P_i be a Sylow p_i-subgropu of G for $i = 1, 2, \cdots, s$. Since $p_i^{\alpha_i} || G|$ and the $p_i^{\alpha_i}$ elements of P_i are solutions of $x^{{p_i}^{\alpha_i}} = 1$, by hypothesis P_i must contain all solutions to this equation in G. It follows P_i is the unique (hence normal) Sylow p_i-subgroup of G. Then G is the direct product of its Sylow subgroups. Now each P_i possesses a normal subgroup M_i of index p_i, that is $|M_i| = p_i^{\alpha_i - 1}$ and G has at most $p_i^{\alpha_i - 1}$ solutions to $x^{{p_i}^{\alpha_i - 1}} = 1$. So M_i contains all elements x satisfying this equation, then for any elements in P_i but not contained in M_i, it must satisfy $x^{{p_i}^{a_i}} = 1$ but $x^{{p_i}^{\alpha_i - 1}} \neq 1$, i.e., x is an element of order $p_i^{\alpha_i}$. This proves P_i is cyclic for all i. So G is the direct product of cyclic groups of relatively prime order, hence is cyclic. $\square$

Definition: for any group G, we define the following subgroups inductively:

$$G^0 = G, \;\; G^1 = [G, G] \;\text{ and }\; G^{i+1} = [G, G^i].$$

The chain of groups

$$G^0 \geq G^1 \geq G^2 \geq \cdots$$

is called the lower central series of G.

Lemma 7.25 *G^i is characteristic in G for all $i \in \mathbb{N}$.*

Proof: It is clear that G^1 is characteristic in G. Next if G^i is characteristic in G, we show G^{i+1} is characteristic in G. Let $\phi \in Aut(G^{i+1})$ It suffices to show that the image under ϕ for set of generators of G^{i+1} is contained G^{i+1}. Let $x \in G$ and $y \in G^i$. Then

$$\phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = \phi(x)y'\phi(x)^{-1}(y')^{-1} \in G^{i+1}$$

as G^i is characteristic in G. Hence we conclude that G^{i+1} is characteristic in G for all $i \in \mathbb{N}$. $\square$

Lemma 7.26 *Let H be a subgroup of G, if $[H,G]$ or $[G,H]$ is trivial, then $H \leq Z(G)$.*

Proof: If $[H,G] = \{e\}$ then $\forall g \in G$ and $h \in H$, we have $gh = hg$. Hence $h \in Z(G)$. Similarly, the statement holds for $[G,H] = \{e\}$. □

Theorem 7.27 *The following are equivalent:*

1. *G has an upper central series with $Z_n(G) = G$ for some $n \in N$.*
2. *G has a central series of finite length, that is*

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n = G$$

such that $G_{i+1}/G_i \leq Z(G/G_i)$;

3. *G has a lower central series with $G^n = \{e\}$ for some $n \in \mathbb{N}$.*

Proof: $1 \Rightarrow 2$: Suppose 1 holds, then

$$Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq Z_n(G) = G.$$

And $Z_i(G) \trianglelefteq Z_{i+1}(G)$ with $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)) \leq Z(G/G_i)$. Hence 2 holds.

$2 \Rightarrow 1$: Suppose G has a central series of finite length, that is

$$\{e\} = G_0 \leq G_1 \leq G_2 \leq \cdots \leq G_n = G$$

such that $G_{i+1}/G_i \leq Z(G/G_i)$. We prove $G_i \leq Z_i(G)$.
When $i = 0$, The statement clearly holds, as $Z_0(G) = G_0 = \{e\}$. Now assume $Z_i(G) \geq G_i$ for some $i \in \mathbb{N}$, we show $Z_{i+1}(G) \geq G_{i+1}$. Since $G_{i+1}/G_i \leq Z(G/G_i)$, then $[G, G_{i+1}] \leq G_i \leq Z_i(G)$. So under the projection $\pi : G \to G/Z_i(G)$, the image of elements of G_i are in the center of $G/Z_i(G)$ (as they are mapped to identity in $G/Z_i(G)$. Thus $G_{i+1}Z_i(G)/Z_i(G)$ is in the center of $G/Z_i(G)$ (since $[G, G_{i+1}] \leq Z_i(G)$), so $G_{i+1}Z_i(G) \leq Z_{i+1}(G) \Rightarrow G_{i+1} \leq Z_{i+1}(G)$.)

$2 \Rightarrow 3$: Suppose G has a finite central series, by reordering we have

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_n = \{e\}$$

for some $n \in \mathbb{N}$. Then we show that $G^i \leq G_i$. Then we could conclude that $G^n \leq G_n = \{e\}$, so $G^n = \{e\}$.
When $i = 0$, the $G = G_0 \geq G^0 = G$. Suppose $G_i \geq G^i$ for some $i \in \mathbb{N}$, consider the case for $i+1$. $G^{i+1} = [G, G^i]$, because $G_i \geq G^i$, then $[G, G_i] \geq [G, G^i]$. Now since $G_i/G_{i+1} \leq Z(G/G_{i+1})$ (as we reordered), then $[G/G_{i+1}, G_i/G_{i+1}] = G_{i+1}/G_{i+1}$ (easy evaluation), so $[G, G_i] \leq G_{i+1}$, hence $G_{i+1} \geq G^{i+1}$.

$3 \Rightarrow 2$: A lower central series is a central series in inverse order, that is we claim that

$$\{e\} = G^n \leq G^{n-1} \leq \cdots \leq G^0 = G$$

is a central series. We just need to verify $G^i/G^{i+1} \leq Z(G/G^{i+1})$. Suffices to show

$$[G/G^{i+1}, G^i/G^{i+1}] \leq G^{i+1}/G^{i+1} = \{e\} \implies [G, G^i] \leq G^{i+1},$$

but this is clear from the definition of G^i's. □

Corollary 7.27.1 *G is nilpotent of class c if and only if c is the smallest nonnegative integer such that $G^c = 1$. If G is nilpotent of class c, then*

$$Z_i(G) \leq G^{c-i-1} \leq Z_{i+1}(G) \ \textit{ for all } i \in \{0, 1, \cdots, c-1\}.$$

Corollary 7.27.2 *Let G be a nilpotent group and N be a normal subgroup of G, then N and G/N are both nilpotent. If $N \trianglelefteq G$ is nilpotent, and G/N is nilpotent, then G is not necessarily nilpotent.*

Proof: Suppose G is nilpotent, then $G^i = 1$ for some $i \in \mathbb{N}$. Then it is easy to show that for any $N \trianglelefteq G$, we have $N^k \leq G^k$, $\forall k \in \mathbb{N}$ by an argument using generators and induction. Hence $N^i \leq G^i = 1$, hence N is nilpotent.

Next if N is normal. It is easy to show that $(G/N)^n = (G^n N)/N$. Then it follows that $(G/N)^i \leq G^i N/N = 1$. Hence G/N is nilpotent .

Lastly consider S_3 as a counter example for the last statement. $A_3 \trianglelefteq S_3$, and $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ are both nilpotent, but S_3 is not nilpotent. □

Proposition 7.28 *Let G be a nilpotent group, then for any nontrivial $N \trianglelefteq G$, $N \cap Z(G)$ is non-trivial.*

Proof: Consider the upper central series of G, since G is nilpotent, then $\exists c \in \mathbb{N}$, s.t., $Z_c(G) = G$. Then there exists some $i \geq 0$, s.t., $N \cap Z_i(G)$ is trivial and $N \cap Z_{i+1}(G)$ is nontrivial, as N is nontrivial. Now by definition of upper central series, we have $[G, Z_{i+1}(G)] \leq Z_i(G)$. Now since N is normal in G, we also have $[G, N] \leq N$. Note

$$[G, N \cap Z_{i+1}(G)] \leq [G, N] \cap [G, Z_{i+1}(G)] \leq N \cap Z_i(G).$$

So

$$[G, N \cap Z_{i+1}(G)]$$

is trivial by assumption, which implies $N \cap Z_{i+1}(G) \leq Z(G)$. But as $N \cap Z_{i+1}(G)$ is nontrivial, then $N \cap Z(G) \neq \{e\}$. Moreover, we conclude that $i = 1$. □

7.4 Finitely Generated Abelian Groups

Definition: for each $r \in \mathbb{Z}$ with $r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ be the direct product of $\mathbb{R}$ copies of the group $\mathbb{Z}$, where $\mathbb{Z}^0 = 1$. The group $\mathbb{Z}^r$ is called the free abelian group of rank r.

Theorem 7.29 (Fundamental Theorem of Finitely Generated Abelian Groups) *Let G be a finitely generated abelian group. Then*

1. $$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}.$$

   for some integers $r, n_1, n_2, \cdots, n_s$, satisfying the following condition:

   (a) *$r \geq 0$ and $n_j \geq 2$ for all j;*

   (b) *$n_{i+1} | n_i$ for $1 \leq i \leq s-1$.*

2. *the representation in (1) is unique. And we call the integer r be the free rank or Betti Number of G, and the integers $n_1, \cdots, n_s$ the invariant factors of G. Such Decomposition is called the invariant factor decomposition of G.*

Theorem 7.30 *Let G be a finite abelian group of order $n > 1$ and $|G| = n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Then*

1. *$G \cong A_1 \times A_2 \times \cdots \times A_k$, where $|A_i| = p_i^{a_i}$.*

2. *for each A_i,*
   $$A_i \cong Z_{p_i^{b_1}} \times \cdots \times Z_{p_i^{b_t}}$$
   with $b_1 \geq b_2 \geq \cdots \geq b_t \geq 1$ and $b_1 + b_2 + \cdots + b_t = a_i$. These are known as the elementary divisors of G.

3. *the decomposition is unique, and is known as the elementary divisor decomposition of G.*

Proof: Suffices to prove the statement on abelian p-groups. We denote $|G|$ by p^n and induct on n. We show G can be written as the direct product of $\langle a \rangle$ and K. If $n = 1$, then $G = \langle a \rangle \times \langle e \rangle$, where a is an element of maximum order in G. Now assume that the statement is true for all Abelian p-groups of order p^k, where $k < n$. Among all elements of G, let a have the maximum order, denote $|a| = p^m$. If $m = n$, then G is cyclic, then $G = \langle a \rangle \times \langle e \rangle$. So assume $m < n$, then $x^{p^m} = e$ for all $x \in G$. Now we choose b to be an element of the smallest order such that $b \notin \langle a \rangle$. Then $|b^p| = |b|/p$ which has order less than b (note clearly $p||b|$). This implies $|b^p| \in \langle a \rangle$ Now say $b^p = a^i$, then $e = b^{p^m} = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}}$, so $|a^i| \leq p^{m-1}$. Thus a^i is not a generator of $\langle a \rangle$, therefore $\gcd(p^m, i) \neq 1$, so $p|i$. Let $i = pj$, then $b^p = a^i = a^{pj}$. But then if $j \neq 1$, then $b \in \langle a \rangle$ which is a contradiction, hence $|b| = p$, thus $\langle a \rangle \cap \langle b \rangle = e$ (As any element in $\langle b \rangle b$ would generate $\langle b \rangle$).
Now consider $\bar{G} = G/\langle b \rangle$. Denote $\bar{x} = x\langle b \rangle\ in G/\langle b \rangle$, $x \in G$. If $|\bar{a}| < |a| = p^m$, $\bar{a}^{p^{m-1}} = \bar{e}$. This means that $(a\langle b \rangle)^{p^{m-1}} = a^{p^{m-1}}\langle b \rangle = \langle b \rangle$, which implies the order of a is p^{m-1}. So order of $\bar{a}$ is equal to p^m, therefore $\bar{a}$ is an element of maximum order in $\bar{G}$.
By induction, we know that $\bar{G} = \langle a \rangle \times \bar{K}$ for some subgroup $\bar{K} \leq \bar{G}$. Then let K be the pullback of $\bar{K}$ under the canonical projection. We claim that $\langle a \rangle \cap K = e$. As if $x \in \langle a \rangle \cap K$, then $\bar{x} \in \langle \bar{a} \rangle \cap \bar{K} = e = \langle b \rangle$, so $x \in \langle a \rangle \cap \langle b \rangle b = e$. lastly, by an order argument we have $G = \langle a \rangle K$, because $|K| = |\bar{K}| \cdot |\langle b \rangle|$, and $|a||\bar{K}| = |G|/|\langle b \rangle|$. So $G = \langle a \rangle \times K$, as $\langle a \rangle$, K are both normal and their intersection is trivial. ☐

Proposition 7.31 *Suppose $m, n \in \mathbb{Z}^+$, then $Z_m \times \mathbb{Z}_n \cong Z_{mn}$ if and only if $(m, n) = 1$.*

7.5 Inverse Limit

Definition: We consider a sequence of groups $\{G_n\}_{n=1}^{\infty}$ together with group homomorphism $f_n : G_n \to G_{n-1}$. We define the inverse limit, $\lim\limits_{\leftarrow} G_i$ of the sequence as follows:

- As a set, $\lim\limits_{\leftarrow} G_i = \{(x_i)_{i=1}^{\infty} | x_i \in G_i,\ f_i(x_i) = x_{i-1}\}$.
- We define multiplication on $\lim\limits_{\leftarrow} G_i$ as $(x_i) \cdot (y_i) = (x_i y_i)$

Proposition 7.32 $\lim\limits_{\leftarrow} G_i$ *is a group.*

Definition: let $G_n = \mathbb{Z}/p^n\mathbb{Z}$ and $\pi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$ be the quotient map. Then $\lim\limits_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p$ is called the $p-$adic integers.

Take $P = 3$. Then elements in Z_3 is a sequence (x_n) such that $x_n \mapsto x_{n-1}$ under the quotient. E.g.,

$$(0, 2 \times 3 + 0, 3^2 + 2 \times 3 + 0, \cdots).$$

So we often write $x \in \mathbb{Z}_p$ as a power series, $x = \sum\limits_{n=0}^{\infty} a_n p^n$. Then (x_n) is obtained by $x_n = \sum\limits_{i=0}^{n-1} a_i p^i$.

Proposition 7.33 *Let $\{G_n\}_{n=1}^{\infty}$ with $f_n : G_n \to G_{n-1}$ be a sequence of groups. Let H be a group with group homomorphisms $h_i : H \to G_i$ such that the following diagram commute for all i:*

$$\begin{tikzcd}
H \arrow[d, "h_i"] \arrow[dr, "h_{i-1}"] & \\
G_i \arrow[r, "f_n"] & G_{i-1}
\end{tikzcd}$$

Then there exists a unique group homomorphism $\phi : H \to \lim\limits_{\leftarrow} G$ such that following diagrams commute:

$$\begin{tikzcd}
 & \lim\limits_{\leftarrow} G_i \arrow[d] \arrow[dr] \arrow[drr] & & H \arrow[ll, "\phi"'] \arrow[dll] \arrow[dl] \arrow[d] & \\
{} \arrow[r] & G_{i+1} \arrow[r] & G_i \arrow[r] & G_{i-1} \arrow[r] & {}
\end{tikzcd}$$

In addition $\phi(h) = (h_i(h)) \in \lim\limits_{\leftarrow} G$ and $\ker\phi = \bigcap \ker h_i$.

8 Category Theory

Definition: a category $\mathfrak{C}$ consists of a collection of objects $\text{ob}(\mathfrak{C})$ and for any two objects $A, B \in \text{ob}(\mathfrak{C})$ a set of morphisms $\text{Mor}(A, B) = \text{Hom}(A, B)$; and for any $A, B, C \in \text{ob}(\mathfrak{C})$ a composition map:

$$\text{Mor}(B, C) \times \text{Mor}(A, B) \to \text{Mor}(A, C), \quad g \times f \mapsto g \circ f$$

such that

1. two sets $\text{Mor}(A, B)$ and $\text{Mor}(A', B')$ are disjoint, unless $A = A'$ and $B = B'$.
2. For any $A \in \text{ob}(\mathfrak{C})$, there exists $1_A \in \text{Mor}(A, A)$ such that for any $f \in \text{Mor}(A, B)$, $f \circ 1_A = f$; and for any $g \in \text{Mor}(B, A)$, $1_A \circ g = g$.
3. The composition is associative, $(f \circ g) \circ h = f \circ (g \circ h)$.

Examples:

1. We have the category of sets, denoted by Set. $\text{ob}(Set)$: is all sets. For any $A, B \in \text{ob}(Set)$, we define $\text{Mor}(A, B) =$ functions from A to B.
2. We have the category of groups denoted Grp. $\text{ob}(Grp)$: is all groups. $A, B \in \text{ob}(Grp)$: $\text{Mor}(A, B)$ is all the group homomorphism from A to B.
3. We have the category of abelian groups, denoted Ab.
4. We can define a category by diagrams:

$$\begin{tikzcd}
 & \bullet & \\
\bullet \arrow[ur] & \bullet \arrow[l] \arrow[u, "h"] \arrow[r, "f"'] & \bullet \arrow[ul, "g"']
\end{tikzcd}$$

   The objects are the dots, the Morphism are the arrows, e.g., $\text{Hom}(A, B) = \{f\}$, $\text{Hom}(B, A) = \emptyset$, and $g \circ f = h$.

5. Let k be a field. Then we have the category of all $k-$vector spaces, denoted by $Vect_k$. The object consists of all vector spaces over k. For $V, W \in \text{ob}$, we have $\text{Mor}(V, W) =$ all $k-$liner maps between V and W.
6. Let P be a poset (partially ordered set). We can define a category associated to P. The object is the set P, for any $a, b \in \text{ob}$, we define $\text{Mor}(a, b) = \{*_{a,b}\}$ if $a \leq b$, $\text{Mor}(a, b) = \emptyset$ if $a \not\leq b$.
7. Let G be a group, we define a category G with one object $*$ and $\text{Mor}(*, *) = G$ (the set of elements of G). The composition is given by group multiplication.

Definition: let $\mathfrak{C}$ be a category. A morphism $f : A \to B$ is called an isomorphism if there exists $g : B \to A$ such that $f \circ g : B \to B = id_B$ and $g \circ f : A \to A = id_A$.
Example:

1. Set, Grp, Ab.

2. Let P be a poset. Then if $a \cong b$, we have $a = b$.

3. Let $\mathfrak{C}$ be a category with $A \in \text{ob}(\mathfrak{C})$, then $\text{Aut}(A)$ =the set of isomorphism from A to A is a group. If $\mathfrak{C}$ is a set, then $\text{Aut}(A) = \text{Perm}(A)$.

Definition: let $\mathfrak{C}$ be a category.

1. We say an object I of $\mathfrak{C}$ is initial in $\mathfrak{C}$ if for any object A in $\mathfrak{C}$, there exists a unique morphism $I_A : I \to A$.

2. We say an object T of $\mathfrak{C}$ is terminal in $\mathfrak{C}$ if for any object $A \in \mathfrak{C}$, there exists a unique morphism $T_A : A \to T$.

Example:

1. In Grp, the trivial group $\{e\}$ is both initial and terminal.

2. Let $A = \{a, b\}$ and $\mathcal{P}(A)$ be a poset, then $\{a, b\}$ is the initial element, and $\emptyset$ is the terminal element.

3. In Set, the empty set $\emptyset$ is an initial object, and any singleton set is a terminal object.

Lemma 8.1 *If $\mathfrak{C}$ be a category. If $\mathfrak{C}$ has an initial (terminal) object, then it is unique up to isomorphism.*

Proof: Let I, I' be initial objects in $\mathfrak{C}$. Then we have unique $f : I \to I'$ and $g : I' \to I$. Then $f \circ g : I \to I = id_I$, since $f \circ g \in \text{Mor}(I, I)$ is unique. Similarly, we get $g \circ f = id_{I'}$. Hence I and I' are isomorphic. □

Definition: let $\mathfrak{C}$ and $\mathfrak{B}$ be categories. A (covariant) functor $F : \mathfrak{C} \to \mathfrak{B}$ consists of the following data:

1. A map $F : \text{ob}(\mathfrak{C}) \to \text{ob}(\mathfrak{B})$, $A \mapsto F(A)$.

2. For any $A, B \in \text{ob}(\mathfrak{C})$, we have a map

$$F : \text{Mor}(A, B) \to \text{Mor}(F(A), F(B)), \quad f \mapsto F(f)$$

and maps identity to identity. Note we are abusing notation a little bit here.

3. For any $A, B, C \in \text{ob}(\mathfrak{C})$ and $f : A \to B$, $g : B \to C$. We have $F(g \circ f) = F(g) \circ F(f)$.

Example:

1. We have the forgetful functor:

$$For : Grp \to Set, \quad G \mapsto G, \quad f : G \to H \mapsto f : G \to H.$$

2. (Adjoint Functor) we have the free group functor

$$F : Set \to Grp, \quad A \mapsto F(A) \text{ free group over } A, f : A \to B \mapsto F(f) : F(A) \to F(B).$$

We have a natural bijection $\text{Hom}_{Set}(A, For(G)) \cong \text{Hom}_{Grp}(F(A), G)$.
Suppose $f \in \text{Hom}_{Set}(A, For(G))$, then by universal property, we have a homomorphism from $F(A)$ to G (G is a group).

3. We have the forgetful functor from Ab to Grp.

4. We have the abelization functor:

$$F : Grp \to Ab, \quad G \mapsto G/[G,G], \quad f : G \to H \mapsto F(f) : G/[G,G] \to H/[H,H]$$

   Where $F(f)$ is induced by first mapping G to H, then to $H/[H,H]$, then $[G,G]$ will be mapped to a subgroup of $[H,H]$.
   We have the trivial functor: $Grp \to Ab$, $G \mapsto \{e\}$, $f : G \to H \mapsto id : \{e\} \to \{e\}$.

5. We have a forgetful functor $Ab \to Set$, $G \mapsto G$. We have the free abelian group functor, $Set \to Ab$, $A \mapsto \prod_A \mathbb{Z}$, $\{a,b\} \mapsto \mathbb{Z} \times \mathbb{Z}$.

6. Let $\mathfrak{C}$ be a category with $A \in \text{ob}(\mathfrak{C})$. Then we have a functor $\text{Hom}_{\mathfrak{C}}(A,-) : \mathfrak{C} \to Set$, $B \mapsto \text{Hom}_{\mathfrak{C}}(A,B)$, $f : B \to C \mapsto \text{Hom}_{\mathfrak{C}}(A,f) : \text{Hom}_{\mathfrak{C}}(A,B) \to \text{Hom}_{\mathfrak{C}}(A,C)$, induced by $g \mapsto f \circ g$.

7. We have the functor of taking invertible elements from Ring (the category of rings) to Grp, $R \mapsto R^*$.

8. The general linear group is a functor $GLn : Ring \to Grp$, $R \to GL_n(R)$, e.g., $\mathbb{Z} \mapsto GL_n(\mathbb{Z})$.

9. Let G be a group. Then we have the category $\underline{G}$ ($\text{ob}(\underline{G} = \{*\}$, and $\text{Mor}(*,*) = G$). Then a functor $f : \underline{G} \to Set$, $* \mapsto A$ is just a group on $F(A)$ if $F(1_*) = F(e) = 1_A$. $F : \text{Mor}(*,*) \to (F(*), F(*)) = \text{Mor}(A,A)$. Then we have $F(f \circ g) = F(f) \circ F(g)$, $F : G \to Perm(A) \subset \text{Mor}(A,A)$ is a group homomorphism.

10. A functor $F : G \to Vect_k$ such that $F(e) = 1_V$, $* \mapsto V$ is the same as a group representation on V, is the same as a group homomorphism $G \to GL(V)$.

11. We have the category of all categories, denoted by Cat. $\text{ob}(Cat)$ is the set of all categories, $\text{Mor}(\mathfrak{C}, \mathfrak{B})$: functors between $\mathfrak{C}$ and $\mathfrak{B}$.

Proposition 8.2 *Let $G : \mathfrak{C} \to \mathfrak{D}$ and $F : \mathfrak{B} \to \mathfrak{C}$ be two functors. Then $G \circ F$ is a functor from $\mathfrak{B} \to \mathfrak{D}$.*

Definition: let $\mathfrak{C}$ and $\mathfrak{B}$ be two categories. A contravariant functor $F : \mathfrak{C} \to \mathfrak{B}$ consists of the following data:

- $F : \text{ob}(\mathfrak{C}) \to \text{ob}(\mathfrak{B})$
- $F : \text{Mor}(A,B) \to \text{Mor}(F(B), F(A))$ such that the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[dr, "g\circ f"'] & B \arrow[d, "g"] & & F(A) & F(B) \arrow[l, "F(f)"'] \\
& C & \to & & F(C) \arrow[u, "F(g)"'] \arrow[ul, "F(g\circ f)=F(f)\circ F(g)"]
\end{tikzcd}$$

Example:

1. Let $\mathfrak{C}$ be a category and $A \in ob(\mathfrak{C})$, we have the ocntravariant functor $\text{Hom}(-,A) : \mathfrak{C} \to Set$, $\text{Hom}(-,A) : \text{ob}(\mathfrak{C}) \to \text{ob}(Set)$, $B \mapsto \text{Hom}(B,A)$; $\text{Hom}(-,A) : \text{Mor}(B,C) \to \text{Mor}(\text{Hom}(C,A), \text{Hom}(B,A))$, $f : B \to C \mapsto (g : C \to A \mapsto g \circ f : B \to A)$.

2. Let $Vect_k$ be the category of $k-$vector spaces. We consider the functor $(\cdot)^* : Vect_k \to Vect_k$, $V \mapsto \mathrm{Hom}_k(V, k) = V^*$ (the dual of V).

We define categories in order to define functors and we define functors in order to define natural transformations.

Definition: Let $\mathfrak{C}$ and $\mathfrak{B}$ be categories. Let $F, G : \mathfrak{C} \to \mathfrak{B}$ be functors, a natural transformation $\alpha : F \to G$ consists of a collection of morphisms $\alpha_A : F(A) \to G(A)$ for any $A \in \mathfrak{C}$, such that the following diagram commutes: for any $A, B \in \mathfrak{C}$, $f : A \to B$,

$$\begin{tikzcd}
F(A) \arrow[r, "\alpha_A"] \arrow[d, "F(f)"'] & G(A) \arrow[d, "G(f)"] \\
F(B) \arrow[r, "\alpha_B"'] & G(B)
\end{tikzcd}$$

Example:

1. We have two functors $(\cdot)^*$, $GL_n(\cdot) : CommutRing \to Grp$, then $\det : GL_n(\cdot) \to (\cdot)^*$ is a natural transformation. E.g. $\det_{\mathbb{R}} : GL_n(\mathbb{R}) \to \mathbb{R}^*$, $\det_{\mathbb{C}} : GL_n(\mathbb{C}) \to \mathbb{C}^*$.

2. For any categories $\mathfrak{C}$ (and Set). $A, B \in \mathfrak{C}$, we consider the functors: $\mathrm{Hom}(A, -) : \mathfrak{C} \to Set$ and $\mathrm{Hom}(B, -) : \mathfrak{C} \to Set$. Then any $\alpha : A \to B$ (in $\mathfrak{C}$) defines a natural transformation $\alpha : \mathrm{Hom}(A, -) \to \mathrm{Hom}(B, -)$, by for any $x \in \mathfrak{C}$, $\alpha_x : \mathrm{Hom}(A, x) \to \mathrm{Hom}(B, x)$, $f \mapsto f \circ \alpha$.
   We check this is indeed a natural transformation. For any $g : x \to y$, we have the following diagram commute:

$$\begin{tikzcd}
f \arrow[rrr, mapsto] \arrow[ddd, mapsto] & & & f \circ \alpha \arrow[dd, mapsto] \\
& Hom(A, x) \arrow[r, "\alpha_x"] \arrow[d] & Hom(B, x) \arrow[d] & \\
& Hom(A, Y) \arrow[r] & Hom(B, Y) & g \circ (f \circ \alpha) \\
g \circ f \arrow[rr, mapsto] & & (g \circ f) \circ \alpha &
\end{tikzcd}$$

Definition: let $\mathfrak{C}$ be a category, let H and G be two objects. The product of H and G (if exists) is an object denoted $H \times G$ in $\mathfrak{C}$ together with morphisms $H \times G \to H$ and $H \times G \to G$ satisfying the following universal property:

For any $\phi_1 : K \to G$ and $\phi_2 : K \to H$, there exists a unique morphism $\phi : K \to H \times G$ such that the following diagram commutes:

$$\begin{tikzcd}
& K \arrow[dl, "\phi_1"'] \arrow[d, dashed] \arrow[dr, "\phi_2"] & \\
H & H \times G \arrow[l] \arrow[r] & G
\end{tikzcd}$$

Example:

1. In Set, we know $H \times G$ is the Cartesian Product.
2. In Grp, we know $H \times G$ is just the product group.
3. In Ab, we know $H \times G$ is also the product group.
4. Let $\mathbb{Z}$ be a poset with the usual ordering. We consider $\mathbb{Z}$ as a category $\underline{\mathbb{Z}}$, we show the product exists in $\underline{\mathbb{Z}}$ for any a, b. We define $a \times b = \max(a, b)$. Then one can show that this definition is the desired definition we want.

Definition: we say a category $\mathfrak{C}$ has (finite) product, if any two object in $\mathfrak{C}$ admits a product.

Lemma 8.3 *Let $\mathfrak{C}$ be a category with product. Then for any A, B, C in $\mathfrak{C}$, we have a canonical isomorphism $A \times (B \times C) \cong (A \times B) \times C$.*

Lemma 8.4 *Let $\mathfrak{C}$ be a category with a terminal object T, then we have $T \times A \cong$ for any object A. And there is a canonical choice of this isomorphism.*

Definition: let $\mathfrak{C}$ be a category. Let H and G be two objects. The coproduct of H and G (if exists), is an object $H \sqcup G$ in $\mathfrak{C}$ together with two morphisms $f_1 : H \to H \sqcup G$, $f_2 : G \to H \sqcup G$ satisfying the following universal properties:

For any $\phi_1 : G \to K$, and $\phi_2 : H \to K$ there exists a unique $\phi : H \sqcup G \to K$ such that the following diagram commutes:

$$\begin{tikzcd}
& K & \\
H \arrow[ur, "\phi_1"] \arrow[r, "f_1"'] & H \sqcup G \arrow[u, dashed, "\phi"] & G \arrow[ul, "\phi_2"'] \arrow[l, "f_2"]
\end{tikzcd}$$

Examples:

1. In Set, the coproduct $H \sqcup G$ is the disjoint union.
2. In Grp, $H \sqcup G$ is the free product. Assume $H = F\langle H \rangle / \langle R(H) \rangle$, $G = F\langle G \rangle / \langle R(G) \rangle$, then $H \sqcup G = F\langle H \cup G \rangle / \langle R(H) \sqcup R(G) \rangle$.
3. In Ab, $H \sqcup G \cong H \times G$.
4. We consider $\mathbb{Z}$ as a poset, we have a category $\underline{\mathbb{Z}}$. Then $a \sqcup b = \min(a, b)$.

Definition: Let $\mathfrak{C}$ be a category with (finite) product and a terminal object I. A group object in $\mathfrak{C}$ consists of an object $G \in \mathfrak{C}$ together with morphisms

$$m : G \times G \to G, \;\; e : I \to G, \;\; \iota : G \to G$$

such that the following diagrams commutes: Associativity:

$$\begin{tikzcd}
G \times (G \times G) \arrow[r, "id \times m"'] \arrow[d, leftrightarrow, "\cong"'] & G \times G \arrow[dr, "m"] & \\
& & G \\
(G \times G) \times G \arrow[r, "m \times id"'] & G \times G \arrow[ur, "m"'] &
\end{tikzcd}$$

and Identity:

$$\begin{tikzcd}
I \times G \arrow[r, "e \times id"'] \arrow[dr, "\cong"'] & G \times G \arrow[d, "m"] \\
& G
\end{tikzcd}
\qquad
\begin{tikzcd}
G \times I \arrow[r, "id \times e"'] \arrow[dr, "\cong"'] & G \times G \arrow[d, "m"'] \\
& G
\end{tikzcd}$$

and Inverse:

$$\begin{tikzcd}
G \arrow[r, "\triangle"] \arrow[d] & G \times G \arrow[r, "id \times \iota"] & G \times G \arrow[d, "m"] \\
I \arrow[rr, "e"'] & & G
\end{tikzcd}
\qquad
\begin{tikzcd}
G \arrow[r, "\triangle"] \arrow[d] & G \times G \arrow[r, "\iota \times id"] & G \times G \arrow[d, "m"] \\
I \arrow[rr, "e"'] & & G
\end{tikzcd}$$

where $id \times m$ is defined as follows, and $m \times id$ is defined similarly

$$\begin{tikzcd}
G \arrow[d, "id"'] & G \times (G \times G) \arrow[l] \arrow[r] \arrow[dl] \arrow[d, "id \times m"] \arrow[dr] & G \times G \arrow[d, "m"] \\
G & G \times G \arrow[l] \arrow[r] & G
\end{tikzcd}$$

and $\triangle$ is defined as follows:

$$\begin{tikzcd}
& G \arrow[dl, "id"'] \arrow[d, dashed, "\triangle"] \arrow[dr, "id"] & \\
G & G \times G \arrow[l] \arrow[r] & G
\end{tikzcd}$$

Examples:

1. A group object G in Set is a (traditional) group.

2. A group object G in the category of topological spaces is a topological group.

3. A group object G in the category of Grp is an abelian group.

4. Let G and H be group objects in $\mathfrak{C}$. A group homomorphism $f : G \to H$ is a morphism $f : G \to H$ such that

the following diagram commute

$$\begin{tikzcd}
G \times G \arrow[r, "f\times f"'] \arrow[d, "m_G"'] & H \times H \arrow[d, "m_H"'] \\
G \arrow[r, "f"'] & H
\end{tikzcd}$$

Definition: let J be an index category (a category used for index). Let $\mathfrak{C}$ be a category and $F : J \to \mathfrak{C}$ be a functor. An (inverse) limit of $F : J \to \mathfrak{C}$ consists of an object $\lim\limits_{\leftarrow} F \in \mathfrak{C}$ together with a cone $\lim\limits_{\leftarrow} F \to F$ (a cone is such that $\forall i, j \in J$, $f : i \to j$, the following diagram commutes)

$$\begin{tikzcd}
& \lim\limits_{\leftarrow} F \arrow[dl] \arrow[dr] & \\
F(i) \arrow[rr, "F(f)"'] & & F(j)
\end{tikzcd}$$

The cone need to satisfy the following universal property: For any cone $c \to F$, $c \in \mathfrak{C}$, there exists a unique $\phi : c \to \lim\limits_{\leftarrow} F$ such that the following diagram commutes, $\forall i \xrightarrow{f} j$,

$$\begin{tikzcd}
c \arrow[r, dashed, "\phi"] \arrow[d] \arrow[dr] & \lim\limits_{\leftarrow} F \arrow[dl] \arrow[d] \\
F(i) \arrow[r, "F(f)"'] & F(j)
\end{tikzcd}$$

Definition: a colimit is defined similarly as the (inverse) limit but reversing the arrows.