5. Classification of Groups

5.1 Sylow Subgroups and Sylow Theorems

p is a prime and G is a group whose order is divisible by p. A subgroup H is a p-subgroup if $|H| = p^r$ for some positive integer r.

If $|G| = p^e m$ where p is a prime and $p \nmid m$. Then a subgroup H is a Sylow p-subgroup if $|H| = p^e$.

Sylow Theorem. G is a group. $|G| = p^e m$, where p is a prime and $p \nmid m$. Then:

1. There exists a Sylow p-subgroup of G.
2. If H is a Sylow p-subgroup of G, and K is a p-subgroup of G, then there exists $g \in G$ such that $K \subset gHg^{-1}$.
3. The number of Sylow p-subgroups divides m and congruent to 1 modulo p.

Cor. Any two Sylow p-subgroup of G are conjugate to each other, i.e. if H, K are Sylow p-subgroups, then there exists $g \in G$ such that $K = gHg^{-1}$.

Pf. By part (2) of the Theorem, $\exists g \in G$, $K \subset gHg^{-1}$. By part (1), $|H| = |K| = p^e$. Also $|gHg^{-1}| = |H| = p^e$.

Cor. H is a Sylow p-subgroup of G. Then H is the unique Sylow p-subgroup $\iff$ H is a normal subgroup of G.

Pf. By the above corollary, all the Sylow p-subgroups are of form gHg^{-1} for some $g \in G$. Then H is unique $\iff \forall g \in G, gHg^{-1} = H \iff H \lhd G$

Example: $|G| = 15 = 3 \times 5$

Let H be a Sylow 3-subgroup of G. $|H| = 3^1 = 3$.

Let K be a Sylow 5-subgroup of G. $|K| = 5^1 = 5$.

The number of Sylow 3-subgroup divides 5, and $\equiv 1 \pmod 3$, so it's 1. So $H \lhd G$.

The number of Sylow 5-subgroup divides 3, and $\equiv 1 \pmod 5$, so it's 1. So $K \lhd G$.

$|H \cap K| = 1$ since it divides both $|H| = 3$ and $|K| = 5$. → $H \cap K = \{1\}$

$|HK| = \frac{|H| \times |K|}{|H \cap K|} = 15 = |G|$ → $G = HK$

So $G = H \times K \cong C_3 \times C_5 = C_{15}$

Example: We will show that a group of order 30 is not simple.

Let $|G| = 30 = 2 \times 3 \times 5 = 3 \times 10 = 5 \times 6$.

The number of Sylow 3-subgroup divides 10, and $\equiv 1 \pmod 3$, so it's 1 or 10.

The number of Sylow 5-subgroup divides 6, and $\equiv 1 \pmod 5$, so it's 1 or 6.

If $n_3 = 10$, $n_5 = 6$, $H_1, ..., H_{10}$ are Sylow 3-sub, $K_1, ..., K_6$ are Sylow 5-sub

- $H_i \cap K_j = \{1\}$ since $\gcd(|H_i|, |K_j|) = 1$

- $H_i \cap H_j = \{1\}, K_i \cap K_j = \{1\}, \forall i \neq j$ since if $a \neq 1, a \in H_i \cap H_j$ → since $|H_i| = |H_j| = 3$ is prime, $H_i =< a >= H_j$ → contradiction

So the union of all these 16 subgroups has element $1 + 10 \times (3-1) + 6 \times (5-1) > 30$ → contradiction

So either $n_3 = 1$, then $H \lhd G$; or $n_5 = 1$, then $K \lhd G$ → proper normal subgroup → not simple.

5.2 Proof of Sylow Theorem

Omitted.

5.3 Semidirect Product Construction

G and G' are groups, and $\phi : G' \to Aut(G)$ is a homomorphism. The semidirect product of G and G' with respect to ϕ is the group $G \rtimes_\phi G'$ whose underlying set is same as that of $G \times G'$, and the law of composition is defined by

$(g_1, g_1')(g_2, g_2') = (g_1 \phi_{g_1'}(g_2), g_1' g_2')$

Prop. $G \rtimes_\phi G'$ defines a group.

Pf. 1. Associativity:

$$\begin{aligned}((g_1, g_1')(g_2, g_2'))(g_3, g_3') &= (g_1 \phi_{g_1'}(g_2), g_1' g_2')(g_3, g_3') \\ &= (g_1 \phi_{g_1'}(g_2) \phi_{g_1' g_2'}(g_3), g_1' g_2' g_3') \\ &= (g_1 \phi_{g_1'}(g_2) \phi_{g_1'}(\phi_{g_2'}(g_3)), g_1' g_2' g_3') \\ &= (g_1 \phi_{g_1'}(g_2 \phi_{g_2'}(g_3)), g_1' g_2' g_3') \\ &= (g_1, g_1')(g_2 \phi_{g_2'}(g_3), g_2' g_3') \\ &= (g_1, g_1')((g_2, g_2')(g_3, g_3'))\end{aligned}$$

2. Idendity: $(1, 1')$

   $(1, 1')(g, g') = (1\phi_{1'}(g), 1'g') = (g, g')$ and $(g, g')(1, 1') = (g\phi_{g'}(1), g'1') = (g, g')$

3. Inverse: $(g, g')^{-1} = (\phi_{(g')^{-1}}(g^{-1}), (g')^{-1})$

   $(g, g')(\phi_{(g')^{-1}}(g^{-1}), (g')^{-1}) = (g\phi_{g'}(\phi_{(g')^{-1}}(g^{-1})), g'(g')^{-1}) = (g\phi_{g'(g')^{-1}}(g^{-1})), 1') = (1, 1')$

   $(\phi_{(g')^{-1}}(g^{-1}), (g')^{-1})(g, g') = (\phi_{(g')^{-1}}(g^{-1})\phi_{(g')^{-1}}(g), (g')^{-1}g') = (\phi_{(g')^{-1}}(g^{-1}g), 1') = (1, 1')$

Similar to $G \times G'$, we can identify G with $G \times \{1'\} \subseteq G \rtimes_\phi G'$

G' with $\{1\} \times G' \subseteq G \rtimes_\phi G'$

and it's easy to verify G, G' are subgroups of $G \rtimes_\phi G'$ under this identification.

Prop. Under the above identification, G is a normal subgroup of $G \rtimes_\phi G'$, and $(1, g')(g, 1')(1, g')^{-1} = (\phi_{g'}(g), 1')$.

Pf. $\forall (x, y) \in G \rtimes_\phi G'$, $\forall (g, 1') \in G \times \{1\}$,

$(x, y)(g, 1')(x, y)^{-1} = (x\phi_y(g), y)(\phi_{y^{-1}}(x^{-1}), y^{-1}) = (x\phi_y(g)\phi_y(\phi_{y^{-1}}(x^{-1})), yy^{-1}) = (x\phi_y(g)x^{-1}, 1') \in G \times \{1'\}$

so $G \times \{1'\}$ is a normal subgroup of $G \rtimes_\phi G'$

In particular, taking $(x, y) = (1, g')$,

$(1, g')(g, 1')(1, g')^{-1} = (1\phi_{g'}(g)1^{-1}, 1') = (\phi_{g'}(g), 1')$

We want to identify G as a semidirect product of its subgroups H and K. By the Prop above, the action of K on H in G should be conjugation, so let $\phi : K \to Aut(H)$ be $\phi_k : H \to H$, $h \mapsto khk^{-1}$. Define $f : H \rtimes_\phi K \to G$, $(h, k) \mapsto hk$.

Prop. H is a normal subgroup of G and K is a subgroup of G. Then f defined above is a semidirect product $\iff H \cap K = \{1\}$ and $HK = G$.

Notation. If the above f is an isomorphism, we write $G = H \rtimes K$. The symbol ϕ, which stands for the conjugation action of K on H, is omitted.

Example: S_3. $H =< (123) >$. $K =< (12) >$. $S_3 = H \rtimes K$ since

- H is a normal subgroup of S_3. K is a subgroup of S_3.
- $H \cap K = \{1\}$
- $|HK| = \frac{|H| \times |K|}{|H \cap K|} = 6 = |S_3| \to S_3 = HK$

5.4 Rubik's Cube Group

The Rubik's Cube Groups G is the group of all moves of a $3 \times 3 \times 3$ Rubik's Cube, with the law of composition be the composition of moves.

Each element in G can be written as a finite sequence of composition of the following elements: U, D, F, B, L, R, which denotes the clockwise rotation by 90 degree of the Up, Down, Front, Back, Left and Right face respectively. Each is of order 4.

Let V denote the set of 8 corner blocks and E the set of 12 edge blocks. Each move will induce a permutation on V and on E respectively. We obtain a homomorphism $G \to S_8 \times S_{12}$.

Let γ_0 be the kernel of this map, then it consists of moves that do not permute the blocks.

If we assign an orientation to each of the subcube, then let γ_1 be the subgroup of G that preserves the orientation of each subcube.

Then $G = \gamma_0 \times \gamma_1$.

5.5 Groups of Order 2p

If p is a prime and G is a group of order $2p$, then G is isomorphic to either $\mathbb{Z}/2p\mathbb{Z}$ or D_p.

5.6 Groups of Order 12

There are five isomorphic classes of groups of order 12.

$\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_6, A_4, another with no name.

Pf. $|G| = 12 = 2^2 \times 3$

Let H be a Sylow 2-subgroup of G. $|H| = 4$.

Let K be a Sylow 3-subgroup of G. $|K| = 3$.

$n_2 \mid 3$, $n_2 \equiv 1 \pmod 2$ → $n_2 = 1/3$

$n_3 \mid 4$, $n_3 \equiv 1 \pmod 3$ → $n_3 = 1/4$

Tf there are 4 subgroups of order 3, then there are only 12−1−4×(3−1) = 3 elements outside the union of there four Sylow 3-subgroups, so there is only space for at most 1 Sylow 2-subgroup. We conclude either H or K is a normal subgroup of G.

Case 1. $H \lhd G$, $K \lhd G$.

$G = H \times K$

Case 1a. $G = H \times K \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$

Case 1b. $G = H \times K \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Case 2. $H \lhd G$, K is not normal.

$G = H \rtimes K$

Case 2a. $G \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\phi \mathbb{Z}/3\mathbb{Z}$, $\phi : \mathbb{Z}/3\mathbb{Z} \to Aut(\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/4\mathbb{Z})^\times \cong \{\bar{1}, \bar{3}\}$. So $|Aut(\mathbb{Z}/4\mathbb{Z})| = 2$ and $|\mathbb{Z}/3\mathbb{Z}| = 3$, there is no nontrivial homomorphism ϕ in this case.

Case 2b. $G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_\phi \mathbb{Z}/3\mathbb{Z}$, $\phi : (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \to Aut(\mathbb{Z}/4\mathbb{Z}) \cong Aut(K_4) \cong S_3$. ϕ is determined by $\phi(\bar{1}_3)$, and $|\bar{1}_3| = 3$, so $\bar{1}$ is mapped to one of the two 3-cycles in S_3. These two choices will give isomorphic semi-direct product group structure since there is an automorphism of S_3 switching the two 3-cycles. In this case there is a unique semi-direct product structure.

Case 3. $K \lhd G$, H is not normal.

$G = K \rtimes H$

Case 3a. $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi \mathbb{Z}/4\mathbb{Z}$, $\phi : \mathbb{Z}/4\mathbb{Z} \to Aut(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^\times \cong \{\bar{1}, \bar{2}\}$. ϕ is determined by $\phi(\bar{1}_4)$ and ϕ is not trivial, so $\phi(\bar{1}_4)$ is the map $\bar{k}_3 \to 2\bar{k}_3 = -\bar{k}_3$, and $\phi(\bar{m}_4) = (\bar{k}_3 \mapsto (-1)^m \bar{k}_3)$. In this case there is a unique semi-direct product structure.

Case 3b. $G \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \rtimes_\phi K_4$. $\phi : K_4 \to Aut(\mathbb{Z}/3\mathbb{Z}) \cong (\mathbb{Z}/3\mathbb{Z})^\times \cong \{\bar{1}, \bar{2}\}$. The three non-identity elements in K_4 are all of order 2, so if ϕ is not trivial, it has to be the case two of these three elements map to $\bar{2}_3$ and the remaining one maps to $\bar{1}_3$. And the difference choices of the element sending to $\bar{1}_4$ give isomorphic semidirect product groups. In this case this is a unique semi-direct product structure.

5.6 Groups of Order 8

There are 5 isomorphic classes of groups of order 12.

$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_4, Q_8.

G is a group of order 8. Let $m = \max_{g \in G} |g|$, the maximal order of elements in G. The possibilities are $m = 2$, $m = 4$ or $m = 8$.

Case 1. $m = 8$. $G \cong \mathbb{Z}/8\mathbb{Z}$.

Case 2. $m = 2$. $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Case 3. $m = 4$. $G \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$G \cong \mathbb{Z}/4\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z} \cong D_4$.

$G \cong Q_8$.

Lemma. If all the non-identity elements of a group G are of order 2, then G is abelian.

Pf. $\forall x, y \in G$, $x^2 = 1$, $y^2 = 1 \to x = x^{-1}$, $y = y^{-1}$, $(xy)^2 = 1 \to xy = (xy)^{-1} = y^{-1}x^{-1} = yx$

Lemma. H, K are subgroups of a group G. Then HK is a subgroup of $G \iff HK = KH$.

Pf. If $HK = KH$, $\forall h_1k_1, h_2k_2 \in HK$, $(h_1k_1)^{-1}(h_2k_2) = k_1^{-1}h_1^{-1}h_2k_2$.

$k_1^{-1} \in K$, $h_1^{-1}h_2 \in H$, so $k_1^{-1}h_1^{-1}h_2 \in KH = HK$, there exists $h \in H$ and $k \in K$ such that $k_1^{-1}h_1^{-1}h_2 = hk$. Therefore, $k_1^{-1}h_1^{-1}h_2k_2 = hkk_2 \in HK$.

If HK is a subgroup of G, for any $kh \in KH$, $kh = (h^{-1}k^{-1})^{-1} \in HK$ since $h^{-1}k^{-1} \in HK$ and HK is a subgroup. So $KH \subseteq HK$.

For any $hk \in HK$, $(hk)^{-1} \in HK$ since HK is a subgroup, so $(hk)^{-1} = h'k'$ for $h' \in H$ and $k' \in K$, so $hk = k'^{-1}h'^{-1} \in KH$. So $HK \subseteq KH$. Therefore, $HK = KH$.