WEEK 2 LECTURE NOTES

Contents

1. Group actions

Definition 1.1. A (left) group action of a group G on a set A is a map from $G \times A$ to 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) $1 \cdot a = a$ for any $a \in A$.

Example 1.2. (1) We have the natural action of S_n on $\{1, \dots, n\}$.
(2) The multiplication map $G \times G \to G$ defines an action of G on itself.

Proposition 1.3. *Let a group G act on a set A. Then we have a group homomorphism*

$$G \to Perm(A), \quad g \mapsto (a \mapsto g \cdots a).$$

Proof. Let us write σ_g for the map $\sigma_g : A \to A$, $\sigma_g(a) = g \cdot a$.

We first check this is a bijection, hence a well-defined map from G to $Perm(A)$. We then check this is a group homomorphism. $\square$

Remark 1.4. It follows that a group action on a set is equivalent to a group homomorphism to the permutation group.

Example 1.5. Let G be a group and A be a set. We always have the trivial action of G on A, that is, $g \cdot a = a$ for any $g \in G$ and $a \in A$.

Example 1.6. Let G be a group. We define the conjugation action of G on its own by $g \cdot h = ghg^{-1}$. That is, for each $g \in G$, define $c_g \colon G \to G$ to be conjugation

$$c_g(x) = gxg^{-1}.$$

We show that it is an action. To verify axiom (1), note that for each $x \in G$,

$$\begin{aligned} (c_g \circ c_h)(x) =& c_g(c_h(x)) \\ =& c_g(hxh^{-1}) \\ =& g(hxh^{-1})g^{-1} \\ =& (gh)x(gh)^{-1} \\ =& c_g h(x). \end{aligned}$$

Therefore, $c_g \circ c_h = c_{gh}$. To prove axiom (2), note that for each $x \in G$, $c_1(x) = 1x1^{-1} = x$.

Example 1.7. Let H be any subgroup of G. Define an action of G on G/H by the left translation

$$\tau_g \colon aH \mapsto gaH \text{ for all } g \in G,\ aH \in G/H.$$

This satisfies the two axioms for a group action. Also, τ_g is a permutation in $S_{G/H}$ and the map $g \mapsto \tau_g$ is a homomorphism from G to $S_{G/H}$.

Definition 1.8 (Stabilizers)**.** Let a group G act on a set A.

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

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

(2) For any subset $B \subset A$, we define

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

(3) We define the kernel of the action by $\mathrm{Stab}_G(A)$.

Lemma 1.9. *Both G_a and $\mathrm{Stab}_G(B)$ are subgroups of G. The subgroup $\mathrm{Stab}_G(A)$ is the kernel of the corresponding group homomorphism $G \to Perm(A)$ of the group action.*

Proof. $\square$

Definition 1.10. (1) Let $A \subset G$ be a non-empty subset of G. Define $C_G(A) = \{g \in G | gag^{-1} = a \text{ for all } a \in A\}$. This subgroup is called the centralizer of A in G. (Check this is indeed a subgroup.)

(2) The center of G is defined to be the subgroup $Z(G) = \{g \in G | gag^{-1} = a \text{ for all } a \in G\}$. (Check this is indeed a subgroup.)

(3) Let $A \subset G$ be a non-empty subset of G. The normalization of A is defined to be $N_G(A) = \{g \in G | gAg^{-1} = A\}$. (Check this is indeed a subgroup.)

Lemma 1.11. *(1) We consider the action of G on itself by conjugation, that is, $g \cdot a = gag^{-1}$. The $Stab_G(A) = C_G(A)$ for any $A \subset G$.*

(2) Let $\mathcal{P}(G)$ be the power set of G. We consider the action of G on $\mathcal{P}(G)$ by conjugation. Then $N_G(A) = Stab_G(A)$ for any $A \subset G$.

Example 1.12. (1) Let G be an abelian group. Then $C_G(A) = N_G(A) = Z(G) = G$ for any subset $A \subset G$.

(2) Let S_4 acts on $\{1,2,3,4\}$ in the natural way. Then we have $Stab_G(4) = S_3$ and the kernel of this action is $\{e\}$.

(3) Let $(12) \in S_4$. We compute $C_{S_4}((12)) = \{e, (12), (34), (12)(34)\}$.
We have $N_{S_4}((12)) = C_{S_4}((12))$.

1.1. **Orbits.**

Definition 1.13. Let G act on a set A. Let $a \in A$. The orbit of a is defined as $\mathcal{O}(a) = G \cdot a = \{ga \in A | g \in G\}$.

We say the action of G on A is transitive if $A = G \cdot a$ for some $a \in A$.

Example 1.14. (1) The left multiplication of G on itself is transitive.

(2) The natural action of S_n on $\{1, 2, \ldots, n\}$ is transitive.

(3) The conjugation action of S_3 on itself has 3 orbits.

Lemma 1.15. *Let G act on a set A.*

(1) For any two orbits $\mathcal{O}(a)$ and $\mathcal{O}(b)$, we have either $\mathcal{O}(a) = \mathcal{O}(b)$ or $\mathcal{O}(a) \cap \mathcal{O}(b) = \emptyset$. Therefore we have a parition of A by orbits.

(2) For any $a \in A$, we have bijection between the set of cosets $G/Stab_G(a)$ and the $\mathcal{O}(a)$ orbit of a.

(3) Assume G is a finite group. Then the cardinality of any orbit must divide $|G|$.

Proof. $\square$

Corollary 1.16. *Let G act on a finite set A. Let $I \subset A$ be a set of representative of G-orbits. Then we have*

$$|A| = \sum_{a \in I} |\mathcal{O}(a)|.$$

1.2. **More on group actions.**

Theorem 1.17. *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 $|G|/|H|$.*

In particular, we have $|H| \mid |G|$ if $|G|$ is finite.

Proof. □

Definition 1.18. 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 $|G : H|$.

Example 1.19. We have $|\mathbb{Z} : 2\mathbb{Z}| = 2$. Note that both $\mathbb{Z}$ and $2\mathbb{Z}$ are infinite.

Example 1.20.
(1) We consider the conjugation action of G on G. Then we have $Stab_G(G) = G$ and $\cap_{g\in G} Stab_G(a) = Z(G)$.
(2) We consider the action G on G/H via left multiplication. This action is transitive. We have $Stab_G(H) = H$. However, the kernel of this action is $\cap_{g\in G} gHg^{-1}$.

Theorem 1.21 (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.*

Proof. □

Proposition 1.22. *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 index p. We consider the action of G on G/H. Let $K = \cap_{g\in G} gHg^{-1} \subset H$ be the kernel of this action. Then we have a group homomorphism $\phi : G \to S_p$ such that $G/K \cong \phi(G)$ by the first isomorphism theorem.

We see that $|G/K| = |\phi(G)|$ must be a factor of $|S_p| = p!$. We have $n = |G| = |K||\phi(G)|$. Since the smallest prime factor of n is p. We can only have $|G/K| = p$, or $|K| = n/p = |H|$. We have $K = H$. □

Corollary 1.23. *Let G be a finite group. Then any subgroup of index 2 must be normal.*

1.3. **Conjugacy classes.**

Definition 1.24. The orbits of G acting on itself by conjugation is called conjugacy classes of G.

Example 1.25.
(1) Let G be abelian. Then each conjugacy class consists of a single element of G.
(2) The group S_3 has three conjugacy classes.
(3) Let $z \in Z(G)$. Then the conjugacy of z is precisely $\{z\}$.

Proposition 1.26. *Let G be a finite group and let $g_1, \ldots, g_n$ be representatives of conjugacy classes of G not contained in the center. Then we have*

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

Proof. □

Corollary 1.27. *Let G be a group of order p^n for some prime p. Then $Z(G)$ is non-trivial.*

Proof. We know $|Z(G)| \geq 1$, since the identity element is in the center. Recall the class equation:

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

Note that $|G : C_G(g_i)| > 1$, since $C_G(g_i) \neq G$ by definition. Therefore $p \mid |Z(G)|$. Since $|Z(G)| \neq 0$, we must have $|Z(G)| > 1$. This finishes the proof. □

Let us next give an explicit description of conjugacy classes of the symmetric S_n.

Definition 1.28. Let n be positive integer. A partition of n, denoted by $\lambda \vdash n$, is a nondecreasing sequence $\lambda = (\lambda_1, \dots, \lambda_k)$ of positive intergers such that $\sum \lambda_i = n$. We denote the set of partitions of n by $\mathcal{P}(n)$.

Theorem 1.29. *The set of conjugacy classes of S_n is in natural bijection with $\mathcal{P}(n)$.*

Proof. □

1.4. **Subgroups of cyclic groups.**

Definition 1.30. A group G is called cyclic if G can be generated by a single element, i.e., $G = \langle x \rangle$ for some $x \in G$.

Let G be an arbitrary group and $x \in G$. Then the subgroup $\langle x \rangle$ generated by x is a cyclic group. So we are studying the easieast subgroups of a group G.
Let $G = \langle x \rangle$ be a cyclic group throughout this section.

Lemma 1.31. *Let $G = \langle x \rangle$. Then $|G| = ord(x)$.*

Proof. □

Corollary 1.32. *If $|G| = n$, then we have $G \cong \mathbb{Z}/n\mathbb{Z}$. If $|G| = \infty$, then we have $G \cong \mathbb{Z}$.*

Example 1.33.
(1) For any $n \in \mathbb{Z}$, the quotient group $\mathbb{Z}/n\mathbb{Z}$ is cyclic. We can take $\overline{1}$ as the cyclic generator.
(2) The group S_3 is NOT cyclic.

Lemma 1.34. *Let $p \in \mathbb{Z}$ be a prime. If G is a group of order p, then G is isomorphic to the cyclic group $\mathbb{Z}/p\mathbb{Z}$.*
In other words, there is a unique group of order p up to isomorphism.

Proposition 1.35. *Let $H \leq G$ be a subgroup. Then $H = \langle x^a \rangle$ for some $a \in \mathbb{Z}$ is also cyclic.*

Proof. □

Corollary 1.36. *Let $H = \langle x^a \rangle$ be a subgroup of G. Let $d \geq 0$ be the g.c.d. of a and n. Then $H = \langle x^d \rangle$.*

Proof. □

Corollary 1.37. *Let $H = \langle x^d \rangle$ be a subgroup of G such that $d \geq 0$ and $d \mid n$. Then $|H| = n/d$.*

Proof. □

We summarize the discussion above as the following theorem.

Theorem 1.38. *Let $G = \langle x \rangle$ be a cyclic group of order n. Then $\{\langle x^d \rangle | d \geq 0, d \mid n\}$ is the set of all non-identical subgroups of G.*

Proof. □

Proposition 1.39. *Let $H_1 = \langle x^{d_1} \rangle$ and $H_2 = \langle x^{d_2} \rangle$ be subgroups of G with $d_i \geq 0$ and $d_i \mid n$. Then we have*

$$H_1 \cap H_2 = \langle x^s \rangle, \qquad \langle H_1 \cup H_2 \rangle = x^t.$$

Here $t = gcd(d_1, d_2)$ and $t = lcm(d_1, d_2)$.

1.5. **Automorphisms of cyclic groups.** Let $G = \langle x \rangle$ be a cyclic group of order n. Recall the ring $\mathbb{Z}/n\mathbb{Z}$.

Lemma 1.40. *Let $End(G)$ be the set endomorphisms of G, i.e., group homomorphisms from G to G. We have a bijection*

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

Proof. □

Let $Aut(G)$ be the automorphism group of G.

Theorem 1.41. *We have a group isomorphism*

$$Aut(G) \cong (\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} | gcd(a, n) = 1\}$$

Proof. □

As we have seen in the proof, to understand the precise structure of the group $Aut(G)$ we need to understand the ring $\mathbb{Z}/n\mathbb{Z}$. This will be the topic for the future semester.

2. Sylow theorems I

Definition 2.1. Let G be a finite group and let p be a prime.

(1) A group of order $p^n (n > 0)$ is called a p-group. Subgroups of G of order p^n is called p-subgroups.
(2) Assume $|G| = p^n m$ with $p \nmid m$. Then a subgroup of G of order p^n is called a Sylow p-subgroup of G.
(3) The set of all Sylow p-subgroups of G is denoted by $Syl_p(G)$. We denote the cardinality of $Syl_p(G)$ by $n_p = n_p(G)$.

Lemma 2.2. *Let G be a finite abelian group and let p be a prime that divides the order of G. Then G contains an element of order p.*

Proof. We proceed by induction on $|G| = p^n m$. Let $x \in G$ be a non-trivial element, and write $\langle x \rangle = H$. Then H is not trivial by assumption. If $H = G$, then we can take $P = \langle x^{p^{n-1}m} \rangle$. If $H \neq G$ with $p||H|$, we can proceed with induction hypothesis. In any case, if $p||H|$, we are done.

So we can assume $p \nmid |H|$. Note that since G is abelian, H is normal. We have $p \mid |G/H|$ and $1 < |G/H| < |G|$. By induction hypothesis, we can find $yH \in G/H$ of order p. This means

$$y^p = h \in H, \text{with } y \neq e.$$

In particular, we have $y^a \notin H$ for any a coprime to p. Let $ord(h) = a$. Since a is a factor of $|H|$, it must be coprime to p. Therefore $y^a \neq e$. We further have

$$(y^a)^p = (y^p)^a = e.$$

We conclude that y^a is of order p in G. □

Corollary 2.3. *Let G be a finite abelian group and let p be a prime that divides the order of G. Then Sylow p-subgroup of G exists.*

Proof. □

Theorem 2.4. *Let G be a finite group and let p be a prime. Then Sylow p-subgroup of G exists.*

Proof. We can assume $p||G|$, otherwise there is nothing to show. Let us assume $p^n||G|$ but $p^{n+1} \nmid |G|$. We proceed by induction on $|G|$. The base case is trivial.

If $p \mid |Z(G)|$, then we have an element $x \in Z(G)$ of order p. This is because $Z(G)$ is abelian, hence we can apply the previous lemma. Then if $P' \leq G/\langle x \rangle$ is a Sylow p-subgroup of the quotient, $\pi^{-1}(P')$ will the Sylow p-subgroup of G.

Assume $p \nmid |Z(G)|$. We write

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

Here $\{g_1, \ldots, g_n\}$ is a set of representatives of non-trivial conjugacy classes. Since $p||G|$ and $p \nmid |Z(G)|$, we must have $p \nmid |G/C_G(g_i)|$ for some i.

Let us assume $p \nmid |G/C_G(g_1)|$. Then $p^n \nmid |C_G(g_1)|$. By assumption of g_1 (non-trivial conjugacy class), we must have have $C_G(g_1) \neq G$, or $|C_G(g_1)| < |G|$. We apply induction hypothesis to obtain a Sylow p-subgroup of $|C_G(g_1)|$ of order p^n. This is clearly the Sylow p-subgroup of G as well. □

2.1. **Sylow theorems II.** Let S be the set of all Sylow p-subgroups. Then $|S| = n_p$ by definition. We know S is not empty now. We consider the action of G on S by conjugation. Let $Q \in S$ and $G \cdot Q$ be the orbit of Q. The next few theorems explore the action of a p-subgroup (could be a Sylow p-subgroup as well) P on S and $G \cdot Q$.

Let us record a useful lemma here.

Lemma 2.5. *Let Q be a Sylow p-subgroup of G. Let P be any p-subgroup of G, then we have $(N_P(Q) =)P \cap N_G(Q) = P \cap Q$.*

Proof. Let $H = P \cap N_G(Q) = \{g \in P | gQg^{-1} = Q\}$. It is clear that $Q \cap P \subset H$. We show the reverse inclusion.

We claim HQ is a p-subgroup of G. It is straightforward to check that HQ is a subgroup of G and Q is a normal subgroup of H. By the isomorphism theorem, we have

$$HQ/Q \cong H/H \cap Q.$$

We conclude that $|HQ| = \frac{|H||Q|}{|H \cap Q|}$. Note that $|H|$, $|Q|$, $|H \cap Q|$ are all powers of p. So HQ is a p-subgroup of G containing the Sylow p-subgroup Q. We must have $HQ = Q$, that is, $H \subset Q$. Hence $H \subset P \cap Q$. □

Proposition 2.6. *Let G be a finite group and let p be a prime. Then we have*

$$n_p \equiv 1 \mod p.$$

Proof. Let P be a Sylow p-subgroup of G. We consider the action of P on S by restriction.

We consider the partition of S into P-orbits, say

$$S = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \cdots \sqcup \mathcal{O}_n.$$

Of course $P \in S$ is an orbit consists of a single element. Let us just call this orbit $\mathcal{O}_1$. Then we have

$$n_p = |S| = 1 + |\mathcal{O}_2| + \cdots |\mathcal{O}_n|.$$

For any $\mathcal{O}_i$ with $i \neq 1$, we have bijections

$$P/Stab_P(Q_i) \cong \mathcal{O}_i, \quad \text{for any } P \neq Q_i \in \mathcal{O}_i$$

Here $Stab_P(Q_i) = \{g \in P | gQ_ig^{-1} = Q_i\}$. We have $Stab_P(Q_i) = P \cap Q_i$ by the lemma. Then we see that $p \mid |P/Stab_P(Q_i)|$. Hence

$$|S| \equiv 1 \mod p.$$

□

Corollary 2.7. *We have*

$$|G \cdot Q| \equiv 1 \mod p.$$

Proof. We consider the action of Q on $G \cdot Q$. Then the same argument as the preivous theorem applies. □

Theorem 2.8. *Let G be a finite group and let p be a prime. Any p-subgroup is contained in some Sylow p-subgroup.*

Proof. Let P be a p-subgroup of G. We consider the action of P on S. We consider the partition of S by P-orbits, say

$$S = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \cdots \sqcup \mathcal{O}_n.$$

We have bijections

$$P/Stab_P(Q_i) \cong \mathcal{O}_i, \quad Q_i \in \mathcal{O}_i.$$

Recall $Stab_P(Q_i) = \{g \in P | gQ_ig^{-1} = Q_i\} = P \cap Q_i$ by the previous lemma. We see thave

$$\begin{cases} p \mid |P/Stab_P(Q_i)| = |\mathcal{O}_i|, & \text{if } P \not\subset Q_i; \\ 1 = |P/Stab_P(Q_i)| = |\mathcal{O}_i|, & \text{if } P \subset Q_i. \end{cases}$$

Since $|S| = |\mathcal{O}_1| + \cdots + |\mathcal{O}_n|$ is 1 mod p, we must have $1 = |P/Stab_P(Q_i)|$ for some i. Hence P is contained in some Sylow p-subgroup. □

Theorem 2.9. *Let G be a finite group and let p be a prime. Any two Sylow p-subgroups are conjugate to each other. In other words, the action of G on S is transitive.*

Proof. Let P and Q be Sylow p-subgroups. We consider the action of P on $G \cdot Q$. By definition $G \cdot Q = \{gQg^{-1} | g \in G\}$. We can then apply the same argument as the previous one thanks to Corollary 2.7. $\square$

Theorem 2.10. *Let G be a finite group and let p be a prime. Then we have*

$$n_p \mid |G|.$$

Proof. We know now S is a single G-orbit. So we have a bijection

$$G/Stab_G(P) \cong S, \quad \text{for any } P \in S.$$

Then since $|G/Stab_G(P)|$ divides $|G|$, n_p divides $|G|$. $\square$

2.2. **Consequences of Sylow theorems.** We next discuss some consequences of Sylow theorems.

Corollary 2.11. *Let G be a finite group and let p be a prime.*

(1) Let P be a p-subgroup of G and Q be a Sylow p-subgroup of G. Then we have

$$P \subset gQg^{-1}, \textit{for some } g \in G.$$

(2) G has a unique Sylow p-subgroup P if and only if the Sylow p-subgroup P is normal.

Example 2.12. We consider the symmetric group S_3. There are three Sylow 2-subgroups: $\langle(12)\rangle$, $\langle(23)\rangle$, $\langle(13)\rangle$. There is only one Sylow 3-subgroup $\langle(123)\rangle \cong A_3$, which is normal.

Example 2.13. Let us classify groups of order 15 (up to isomorphism).

Let G be such a group. We know

$$n_3 \equiv 1 \mod 5 \quad \text{and} \quad n_3 | 15.$$

We must have $n_3 = 1$. So we have a unique normal Sylow 3-subgroup P_3. Similarly we see that we have a unique normal Sylow 5-subgroup P_5. Note that since $|P_3| = 3$ and $|P_5| = 5$ are both primes, we must have $P_3 \cong \mathbb{Z}/3\mathbb{Z}$ and $P_5 \cong \mathbb{Z}/5\mathbb{Z}$.

We then make the following claims

(1) P_3P_5 is a subgroup of G
(2) We have $|P_3P_5| = \frac{|P_3||P_5|}{|P_3 \cap P_5|} = 15$. (This is a special case of double cosets.)
(3) We have $P_3P_5 = G$ for numerical reason.
(4) We have $G \cong P_3 \times P_5 \cong \mathbb{Z}/15\mathbb{Z}$.

So we have only one group of order 15.

2.3. **Semi-direct products.**

Definition 2.14. Let H and K be two groups. Let $\phi : K \to Aut(H)$ be a group homomorphism. We define a binary operation on $H \times K$ by

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1\phi(k_1)(h_2), k_1k_2).$$

Theorem 2.15. *The binary operation defines a group structure on the set $H \times G$. We denote this group by $H \rtimes_\phi K$ (or simply $H \rtimes K$). This is called the semi-direct product of H and K with respect to ϕ.*

Proof. Intuitively, we want to think of $\phi(k_1)(h_2)$ as $k_1 h_2 k_1^{-1}$. □

Remark 2.16. We could have $H \rtimes_\phi K \cong H \rtimes_\psi K$ for two different group homomorphisms $K \to Aut(H)$. This will be precise in the next Proposition.

Proposition 2.17. *Let $H \rtimes_\phi K$ be the semi-direct product of H and K with respect to ϕ.*

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

Proof. □

Example 2.18. (1) Let $\phi : K \to Aut(H)$ be the trivial group homomorphism. Then $H \rtimes_\phi K \cong H \times K$.
(2) Let G be a group. We consider the permutation map $\phi : S_n \to Aut(G^n)$. Then the semi-direct product $(G^n) \rtimes_\phi S_n$ is called the wreath product of G by S_n, and often denoted by $G \wr S_n$.
The multiplication behaves as follows

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

Proposition 2.19. *Let G be a group with two subgroups H and K. Assume*

(1) H *is normal in* G,
(2) $H \cap K = \{e\}$,
(3) $HK = G$.

Then we have $G \cong H \rtimes_\phi K$. Here $\phi : K \to Aut(H)$ is given by $k \mapsto (h \mapsto khk^{-1})$.

Proof. □

Proposition 2.20. *There are exactly two groups (up to isomorphism) of order* 6.

Proof. We know we have two such groups $\mathbb{Z}/6\mathbb{Z}$ and S_3.

Let G be such a group. We know

$$n_3 \equiv 1 \mod 3 \quad \text{and} \quad n_3 | 6.$$

We must have $n_3 = 1$. So we have a unique normal Sylow 3-subgroup $P_3 \cong \mathbb{Z}/3\mathbb{Z}$.

We similarly know

$$n_2 \equiv 1 \mod 2 \quad \text{and} \quad n_2 | 6.$$

We have two cases for n_2. We have either $n_2 = 1$ or $n_2 = 3$.

If $n_2 = 1$, then very much similar to the previous example, we have $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$.

Assume $n_2 = 3$ now. Let P_2 be any one of the three Sylow 2-subgroups. We still have following claims

(1) P_2P_3 is a groups.
(2) We have $|P_2P_3| = \frac{|P_2||P_3|}{|P_2 \cap P_3|} = 6$. (This is a special case of double cosets.)
(3) We have $P_2P_3 = G$ for numerical reason.

However, $G \ncong P_2 \times P_3$. Let us consider the conjugation action of P_2 on P_3. This is well-defined, since P_3 is normal. (Recall from Midterm, if P_2 is also normal, then this action is trivial.) So now we have a group homomorphism $\phi : P_2 \to Aut(P_3) = Aut(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

We further divide into two cases.

(1) If ϕ is the trivial group homomorphis, then we have $G \cong P_2 \times P_3$. We actually have a contradiction here, or we can relax the assumption. In any case, we have considered this case before.
(2) If ϕ is the non-trivial group homomorphism, this means $xyx^{-1} = y^2$, there x is the generator P_2 and y is the generator of P_3.

    In this case, we have a group homomorphism $P_3 \rtimes_\phi P_2 \to G$. We see that this is an isomorphism by cardinality reason.

□

2.4. **Applications of Sylow's theorems.**

Definition 2.21. A simple group is a nontrivial group whose only normal subgroups are the trivial group and the group itself.

Example 2.22. Let G be a group of order 132. Then G can not be simple.

We have $132 = 11 \times 2^2 \times 3$. We have

$$n_3 \equiv 1 \mod 3 \quad \text{and} \quad n_3 \mid 132$$

$$n_2 \equiv 1 \mod 2 \quad \text{and} \quad n_2 \mid 132$$

$$n_{11} \equiv 1 \mod 11 \quad \text{and} \quad n_{11} \mid 132$$

Assume the contrary that G is simple. Then we must have $n_{11} = 12$. Note that two Sylow 11-subgroups intersection trivially. So there are $12 \times 10 = 120$ elements of order 11.

Now we look at $n_3 \in \{1, 4, 22\}$. We know $n_3 \neq 1$ by assumption. If $n_3 = 4$, then we have $4 \times 2 = 8$ elements of order 3. So the Sylow 2-subgroup must be normal. If $n_3 = 22$, then we clearly have too many elements beyond the cardinality of G.

Example 2.23. Let G be a group of order $12 = 2^2 \times 3$. Then we claim either G has a normal Sylow 3-subgroup or G has a normal Sylow 2-subgroup. So this group can not be simple.

Assume $n_3 \neq 1$. Then we know

$$n_3 \equiv 1 \mod 3 \quad n_3 \mid 12.$$

We can only have $n_3 = 4$. Note that different Sylow 3-subgroups have trivial intersections. So the union of the four Sylow 3-subgroups contains 9 elements. We have only $3 + 1$ elements left for the Sylow 2-subgroups. It has to be normal.

Let us determine the group in this case. Let $S = \{Q_1, Q_2, Q_3, Q_4\}$ be the set of Sylow 3-subgroups. We have the conjugation action of G on S, hence a group homomorphism

$$G \to S_4.$$

Recall $Stab_{Q_i}(Q_j) = Q_i \cap Q_j$. Therefore the image of Q_i consisting of 3-cycles fixing Q_i while permuting the other three subgroups.

There are exactly four Sylow 3-subgroups contained in S_4, and they generate $A_4 = H$. Then since $|A_4| = 12$, we have $G \cong A_4$ for cardinality reason.

Let us try to classify groups of order 12.

Lemma 2.24. *Let p be a prime. Then any group G of order p^2 must be abelian. Moreover, we have either $G \cong \mathbb{Z}/p^2\mathbb{Z}$ or $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.*

Proof. We know G must have non-trivial center. Let $x \in Z(G)$ be a non-trivial elements, and let $H = \langle x \rangle$. If $H = G$, we are done. In this case we have $G \cong \mathbb{Z}/p^2\mathbb{Z}$.

Otherwise we have $|H| = p$ and $H \cong \mathbb{Z}/p\mathbb{Z}$. Let $y \in G$ and $y \notin H$. And consider $K = \langle y \rangle$. If $K = G$, we done again. In this case we have again $G \cong \mathbb{Z}/p^2\mathbb{Z}$.

Now we are left with the case $H \cong \mathbb{Z}/p\mathbb{Z}$ and $K \cong \mathbb{Z}/p\mathbb{Z}$. Note that $H \cap K$ is trivial. We also have $xy = yx$ for any $x \in H$ and $y \in K$, since any group homomorphsim $K \to Aut(H)$ is trivial ($|Aut(H)| = p - 1$). Therefore the map $H \times K \to G$, $(x, y) \mapsto xy$ is a group isomorphism. ☐

Lemma 2.25. *Let G be a group (potentially infinite) such that $G/Z(G)$ is cyclic (including the trivial case). Then G is abelian.*

In other words, $G/Z(G)$ can be not a non-trivial cyclic group.

Proof. HW 5. ☐

Example 2.26. Let us now classify groups of order 12. Let G be such a group. We already know that if $n_3 \neq 1$ then we have $G \cong A_4$. We assume $n_3 = 1$ now, and let P_3 be the Sylow 3-subgroup.

Assume $n_2 = 1$. Let P_4 be the unique normal Sylow 2-subgroup. We know $P_4 \cong \mathbb{Z}/2^2\mathbb{Z}$ or $P_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then we have $G \cong P_4 \times P_3$, since $P_4 \cap P_3 = \{e\}$ and both of them are normal.

Assume $n_2 \neq 1$. Let P_4 be a Sylow 2-subgroup. We know $P_4 P_3 = G$. So we need to determine the multiplication of G, which is essentially the group homomorphism $P_4 \to Aut(P_3) \cong \mathbb{Z}/2\mathbb{Z}$.

(1) Assume $P_4 \cong \mathbb{Z}/2^2\mathbb{Z}$. We consider group homomorphisms $\phi : P_4 \to Aut(P_3) \cong \mathbb{Z}/2\mathbb{Z}$. There are only two of them, denoted by ϕ_1 and ϕ_2, where ϕ_1 is the trivial one. We have $P_3 \rtimes_{\phi_1} P_4 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \rtimes_{\phi_2} \mathbb{Z}/2^2\mathbb{Z}$.

(2) Assume $P_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We consider group homomorphisms $\phi : P_4 \to Aut(P_3) \cong \mathbb{Z}/2\mathbb{Z}$. There are four of them ϕ_1, ϕ_2, ϕ_3, ϕ_4. Here ϕ_1 is the trivial one. We assume ϕ_2 maps (a, b) to a, and ϕ_2 maps (a, b) to b, and ϕ_4 maps (a, b) to $a + b$.

Then we have $P_3 \rtimes_{\phi_1} P_4 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then we can check by direct computation that $P_3 \rtimes_{\phi_2} P_4 \cong P_3 \rtimes_{\phi_3} P_4 \cong P_3 \rtimes_{\phi_4} P_4$. We see that $P_3 \rtimes_{\phi_2} P_4 \cong G' \times \mathbb{Z}/2\mathbb{Z}$ for a non-abelian group G' of order 6. We see that $G' \cong S_3$ by our earlier result. We conclude that $P_3 \rtimes_{\phi_2} P_4 \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$.

Now we can conclude that there are 5 groups of order 12, up to isomorphism.

2.5. **Solvable groups.**

Definition 2.27. Let G be a group.

(1) 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 (not necessarily of G). We have the *subquotient/factor* groups G_i/G_{i+1}. The normal tower is called abelian (resp. cyclic), if each factor group G_i/G_{i+1} is abelian (resp. cyclic).

(2) A *refinement* of a given tower is a tower obtained by inserting a finite number of subgroups in the given tower.

(3) Let

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_n = \{e\},$$
$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m = \{e\}$$

be normal towers. Two normal towers are called *equivalent* if $m = n$ and up to permutation of indices $i \mapsto i'$, we have

$$G_i/G_{i+1} \cong H_{i'}/H_{i'+1}, \qquad \text{for all } i.$$

Lemma 2.28. *Let G be a finite group. An abelian tower of G admits a cyclic refinement.*

Proof. □

Definition 2.29. A normal tower

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_m = \{e\}$$

is called a *composition series* of G is each factor group G_i/G_{i+1} is simple. The factor groups are called *composition factors* of G. Note that this is NOT well-defined yet.

(Recall a group H is called simple if $H \neq \{e\}$ and it does not contain any other normal subgroups besides $\{e\}$ and H.)

Remark 2.30. The composition series always exist for a finite group G. The group $\mathbb{Z}$ has no composition series.

Example 2.31. (1) Let $G = \mathbb{Z}/6\mathbb{Z}$. We have two equivalent normal towers

$$G \supset \mathbb{Z}/3\mathbb{Z} \supset \{e\}, \quad G \supset \mathbb{Z}/2\mathbb{Z} \supset \{e\}.$$

(2) The two groups $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ have the same composition factors, while non-isomorphic.

(3) 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.

We claim S_3 is solvable. We actually have the normal tower

$$S_3 \supset A_3 \supset \{e\}.$$

(4) S_5 is not solvable (Google this). This plays a VERY important role in Galois theory.

Lemma 2.32. *Let G be a group. The commutator subgroup $G^{(1)} = [G, G]$ of G is defined to be the subgroup generated by $[a, b] = aba^{-1}b^{-1}$ for all $a, b \in G$. Then $G^{(1)}$ is normal in G. In particular, any group homomorphism from G to an abelian group factors through $G/[G, G]$.*

We similarly define $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.

Proof. Let $u \in [G,G]$. Then

$$gug^{-1} = u \cdot u^{-1}gug^{-1} = u \cdot [u^{-1}, g] \in [G,G].$$

This shows the normality. The rest follows from the universal property of the quotient. □

We often write $G^{(0)} = G$.

Proposition 2.33. *A group G is solvable if and only if $G^{(n)} = \{e\}$ for some n.*

Proof. We assume $G^{(n)} = \{e\}$ for some n. Since $G/[G,G]$ is always abelian, the claim follows.

Now we prove the other direction. Let

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

be a normal tower with abelian factor groups. Since H_i/H_{i+1} is abelian, we must have

$$H_{i+1} \supset [H_i, H_i].$$

We then claim $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subset [H_{(i-1)}, H_{(i-1)}] \subset H_i$ by induction. This is immediate, since $G^{(0)} = H_0$. □

3. Nilpotent groups

Definition 3.1. (1) For any (finite or infinite) group G we define the following subgroups inductively:

$$Z_0(G) = 1, Z_1(G) = Z(G)$$

and $Z_{i+1}(G)$ is the subgroup $\pi^{-1}(Z(G/Z_i(G)))$ for the canonical quotient $\pi : G \to G/Z_i(G)$.

The chain of (normal) subgroups

$$Z_0 \le Z_1 \le Z_2 \le \cdots$$

is called the upper central series of G.

(2) A group G is called nilpotent if $Z_n(G) = G$ for some n. The smallest such n is called the nilpotence class of G.

Corollary 3.2. *If G is nilpotent, then G is solvable.*

Example 3.3. (1) If G is abelian, then G is nilpotent.

(2) We have $Z_n(S_3) = \{e\}$ for any n. So S_3 is not nilpotent. So S_3 is solvable, but not nilpotent.

Remark 3.4. There are various equivalent characterizations of nilpotent groups.

Lemma 3.5. *Let G be a finite p-group for some prime p. Then G is nilpotent.*

Proof. □

Theorem 3.6. *Let G be a finite group of order $p_1^{n_1} \cdots p_k^{n_k}$ with primes p_i and $n_i > 0$. Let P_i be a Sylow p_i-subgroup of G. Then the following are equivalent:*

(1) G is nilpotent;

(2) if H is a proper subgroup of G, then H is a proper subgroup of $N_G(H)$;

(3) every Sylow p_i-subgroup is normal;
(4) $G \cong P_1 \times P_2 \times \cdots \times P_k$.

Proof. We show (1) $\implies$ (2). We proceed on induction of $|G|$. The base case is vacuous.

We know $Z(G) \neq \{e\}$. We clearly have $HZ(G) \subset N_G(H)$. We can assume $Z(G) \subset H$, otherwise, we are done. We consider the quotients $H/Z(G) \to G/Z(G)$. Then $H/Z(G)$ is a proper subgroup of $G/Z(G)$. Let $K/Z(G)$ be the normalizer of $H/Z(G)$ in $G/Z(G)$. We know $H/Z(G)$ is a proper subgroup of $K/Z(G)$ by induction hypothesis. Hence H is a proper subgroup of K. We claim $K \subset N_G(H)$. For any $h \in H$ and $k \in K$, we have $khk^{-1}Z(G) \subset HZ(G) = H$. The claim follows.

We show (2) $\implies$ (3). Let $N = N_G(P_i)$. We know P_i is a normal subgroup of N, and the unique Sylow p_i-subgroup of N. Let $H = N_G(N)$. Then we claim $H = N$. We clearly have $N \subset H$. On the other hand, for any $h \in H$, we have $hNh^{-1} = N$ by definition. This means $hP_ih^{-1} \subset N$ as well. But since hP_ih^{-1} is a Sylow p_i-subgroup of N, we must have $hP_ih^{-1} = P_i$. Therefore $h \in N = N_G(P_i)$. This proves the claim. Then by (1), we see that $N = N_G(N) = G$.

We show (3) $\implies$ (4). We have shown before that $P_1P_2 \cong P_1 \times P_2$. Now P_1P_2 and P_3 are normal subgroups of G such that $P_1P_2 \cap P_3 = \{e\}$. Then we have $P_1P_2P_3 \cong P_1 \times P_2 \times P_3$. We then proceed by induction.

Finally, we show (4) $\implies$ (1). We know P_i has nontrivial center. Therefore $P_1 \times P_2 \times \cdots \times P_k$ has non-trivial centers. We can repeat this argument for the quotient $G/Z(G)$ to show $Z_1(G) \neq Z(G)$. Since G is finite, we eventualy must have $Z_n(G) = G$ for some n. $\square$

Proposition 3.7. *Let G be a finite group. Let H be a normal subgroup of G and P be a Sylow p-subgroup of H. Then $G = HN_G(P)$.*

Proof. For any $g \in G$, since H is normal, we have $gPg^{-1} \subset H$. Then we apply the Sylow theorem to the group H, we see that $gPg^{-1} = hPh^{-1}$ for some $h \in H$. In other words, we have $h^{-1}g \in N_G(P)$. Hence $g \in HN_G(P)$. Therefore $G = HN_G(P)$. $\square$

Definition 3.8. Let G be a group. A proper subgroup M of G is called maximal if whenever $H \leq H \leq G$, then either $H = M$ or $M = G$.

Proposition 3.9. *Let G be a finite group. Then G is nilpotent if and only if all maximal subgroups of G is normal.*

Proof. Let M be a maximal subgroup of G. Then the Theorem, we know M is a proper subgroup of $N_G(M)$. We must have $N_G(M) = G$. Hence M is normal in G.

For reverse implication, we show every Sylow p-subgroup is normal (for any prime p). Let P be a Sylow p-subgroup. Assume the contrary that P is not normal in G. Then we can find a maximal subgroup M containing $N_G(P)$ (since G is finite). Then we see that M is normal in G by assumption. Then $MN_G(P) = G$ by the lemma. But $N_G(P) \subset M$, hence $M = MN_G(P) = G$. We have a contradiction. $\square$

3.1. **Inverse limits.** We consider a sequence of groups $\{G_n\}_{n=1}^{\infty}$ together with group homomorphisms $f_n : G_n \to G_{n-1}$. We define the inverse limit $\varprojlim G_i$ of of the sequence of groups as follows. As a set, we have

$$\varprojlim G_i = \{(x_i) | x_i \in G_i, f_i(x_i) = x_{i-1}\}.$$

We then define the multiplication on $\varprojlim G_i$ by

$$(x_i) \cdot (y_i) = (x_i y_i).$$

Proposition 3.10. *$\varprojlim G_i$ is a group with the multiplication defined above.*

Proof. □

Example 3.11. Let $G_n = \mathbb{Z}/p^n\mathbb{Z}$ for $n \geq 1$ and let $f_n : G_n \to G_{n-1}$ be the canonical quotient. Then the group $\varprojlim G_n$ is called p-adic integers, denoted by $\mathbb{Z}_p$. We often only consider the case when p is a prime. We will see this is actually a ring in the future semester.

An element in $\mathbb{Z}_p$ is a sequence (x_n). For example in $\mathbb{Z}_3$, we have

$$(0, 2 \times 3 + 0, 3^2 + 2 \times 3 + 0, \ldots,)$$

Equivalently, we can write $(x_n) \in \mathbb{Z}_p$ as $\sum_{i=0}^{\infty} a_i p^i$ where $0 \leq a_i < p$. Then we have $x_n = \sum_{i=0}^{n-1} a_n p^n$.

References

[1] S. Lang, *Algebra*, Revised Third Edition, Graduate Texts in Mathematics.
[2] D. Dummit and R. Foote, *Abstract Algebra*, 3rd edition, Wiley.