Finite Group Theory

IKHAN CHOI

Contents

1. Special groups

1.1. Cyclic groups.

(1) A subgroup is also cyclic.
(2) The number of subgroups = the number of divisors of its order.
(3) Endomorphism ring is given by $\mathbb{Z}/n\mathbb{Z}$.
(4) Automorphism group is given by $(\mathbb{Z}/n\mathbb{Z})^\times$.
(5) The number elements of order d is $\phi(d)$.
(6)

1.2. Abelian groups.
Fundamental theorem of finitely generated abelian groups

Theorem 1.1. *Let G be a finite group. If $G/Z(G)$ is cylic, then G is abelian.*

Theorem 1.2. *Let G be a finite group. If $x \mapsto x^3$ is a surjective endomorhpism, then G is abelian.*

1.3. Symmetric groups.

1.4. Coxeter groups.

1.5. Linear groups.

First Written : December 15, 2019.
Last Updated : December 15, 2019.

2. Classification of small groups

2.1. Sylow theorem.

Definition 2.1 (Sylow p-subgroup)**.** Let G be a finite group of order $n = p^a m$ for a prime $p \nmid m$. A *Sylow p-subgroup* is a subgroup of order p^a. We are going to denote the set of Sylow p-subgroups by $\mathrm{Syl}_p(G)$ and the number of Sylow p-subgroups by $n_p(G)$.

Theorem 2.1 (Sylow)**.** *Let G be a finite group of order $n = p^a m$ for a prime $p \nmid m$. Then,*

$$p \mid n_p - 1, \qquad n_p \mid m$$

for some $k \in \mathbb{N}$.

Proof. Step 1: A Sylow p-subgroup exists. We apply mathematical induction on orders. The base step is trivial. Suppose every finite group of order less than n possesses a Sylow p-subgroup.

By applying the orbit-stabilizer theorem for the action $G \curvearrowright G$ by conjugation, build the class equation

$$n = |Z(G)| + \sum_i |G : C_G(g_i)|.$$

There are two cases: $p \mid |Z(G)|$ or $p \nmid |Z(G)|$.

Case 1: $p \mid |Z(G)|$. The group G has a normal subgroup of order p by applying Cauchy's theorem for abelian groups on the center. Then, the inverse image of a Sylow p-subgroup of the quotient group is also a Sylow p-subgroup of G.

Case 2: $p \nmid |Z(G)|$. Since $p \mid n$, we have $p \nmid |G : C_G(g)|$ for some $g \in G$. Then, a Sylow p-subgroup of the centralizer is also a Sylow p-subgroup of G.

Therefore, we are done for Step 1.

Step 2: A Sylow p-subgroups get action by conjugation. Let P be a Sylow p-subgroup of G. We construct class equations via the orbit-stabilizer theorm for various actions to extract information on n_p. Note that stabilizers in any setwise conjugation action is exactly normalizers.

(1) The action $P \curvearrowright \mathrm{Syl}_p(G)$ gives
$$n_p = 1 + \sum_i |P : N_P(P_i)|$$
since $P = N_P(P_i) \le N_G(P_i)$ and $P_i \trianglelefteq N_G(P_i)$ imply and $P = P_i$. (Pass P though $\pi : N_G(P_i) \to N_G(P_i)/P_i$.)

(2) Suppose the action $G \curvearrowright \mathrm{Syl}_p(G)$ is not transitive. Take another Sylow p-subgroup P' is not conjugate with P in G. The two actions $P \curvearrowright \mathrm{Orb}_G(P)$ and $P' \curvearrowright \mathrm{Orb}_G(P)$ gives
$$|\mathrm{Orb}_G(P)| = 1 + \sum_i |P : N_P(P_i)| = \sum_i |P' : N_{P'}(P_i)|.$$
It deduces $|\mathrm{Orb}_G(P)| \equiv 0, 1 \pmod p$ simultaneously, which leas a contradiction.

(3) The action $G \curvearrowright \mathrm{Syl}_p(G)$ gives
$$n_p = |G : N_G(P_i)|$$
for all $P_i \in \mathrm{Syl}_p(G)$ because the action is transitive.

Then, (1) proves $p \mid n_p - 1$, and (3) proves $n_p \mid m$. $\square$

Corollary 2.2. *Let G be a finite group. Then,*

(1) *every pair of two Sylow p-subgroup is conjugate.*
(2) *every p-subgroup is contained in a Sylow p-subgroup.*
(3) *a Sylow p-subgroup is normal if and only if $n_p = 1$.*

Theorem 2.3. *Alternative proof for existence of p-groups.*

Proof. Let $|G| = p^{a+b}m$. Let $\mathcal{P}_{p^a}$ be the set of all p^a-sets in G. Give $G \curvearrowright \mathcal{P}_{p^a}$ by left multiplication. Since $v_p(|\mathcal{P}_{p^a}|) = v_p(\binom{p^a(p^b m)}{p^a}) = b$, there is an orbit $\mathcal{O}$ such that $v_p(|\mathcal{O}|) \leq b$. We have transitive action $G \curvearrowright \mathcal{O}$ and the stabilizer H satisfies $p^a \mid |G|/|\mathcal{O}| = |H|$. Since $H \curvearrowright \mathcal{O}$ trivially, $H \curvearrowright A$ for $A \in \mathcal{O} \subset \mathcal{P}_{p^a}$. It is only possible when $H \subset A$, hence $|H| = p^a$. $\square$

Investigation of a group of a given order is divided into two main parts: the existence of a subgroup of particular orders and the measurement of the size of conjugate subgroups.

In order to show the existence of subgroups of paricular orders:

(1) p-groups always exist,
(2) extension theory, (what can subgroups of subgroups do?)
(3) normalizers,
(4) Poincare theorem: kernel of permutation representation

In order to find the size of conjugacy classes:

(1) measure the order of normalizers, (find some groups normalize a subgroup)
(2) count elements,

2.2. **Semidirect product.**

Definition 2.2 (External semidirect product)**.** Suppose we have three data: groups $(N,+), (H,\cdot)$ and a group homomorphism $\varphi : H \to \mathrm{Aut}(N)$. The *semidirect product* $N \rtimes_\varphi H$ is a group defined on the set $N \times H$ by

$$(n,h)(n',h') = (n + \varphi(h)n', hh').$$

The motivation of the group structure of semidirect product is shown in the following theorem.

Theorem 2.4 (Internal semidirect product)**.** *Let N, H be subgroups of G such that*

$$N \trianglelefteq G, \quad N \cap H = 1, \quad NH = G.$$

Then, $G \cong N \rtimes_\varphi H$, where the action φ is given by conjugation

$$\varphi(h) : N \to N : n \mapsto hnh^{-1}.$$

2.3. **Groups of order less than 64.**

2.3.1. *Two primes.*

Example 2.1 ($|G| = p^2$)**.**

Example 2.2 ($|G| = pq$)**.**

2.3.2. *Three primes.*

Lemma 2.5. *Let N, H be groups. Let $\varphi_1, \varphi_2 : H \to \mathrm{Aut}(N)$ be group actions. If there are $\nu \in \mathrm{Aut}(N)$ and $\eta \in \mathrm{Aut}(H)$ such that a diagram*

$$\begin{tikzcd} H \arrow[r, "\varphi_1"] \arrow[d, "\eta"] & \mathrm{Aut}(N) \arrow[d, "\nu \cdot \nu^{-1}"] \\ H \arrow[r, "\varphi_2"] & \mathrm{Aut}(N) \end{tikzcd}$$

commutes, then a map

$$N \rtimes_{\varphi} H \to N \rtimes_{\varphi'} H : (n, h) \mapsto (\nu(n), \eta(h))$$

is an isomorphism.

Lemma 2.6. *Let Z, G be finite groups. If Z is cyclic, then $\varphi, \varphi' : Z \to \mathrm{Aut}(G)$ induces the isomorphic semidirect product iff their images are conjugate.*

Example 2.3 (Conjugacy classes of $\mathrm{GL}_2(\mathbb{F}_p)$)**.**

(1) $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$: $\binom{q-1}{2} = \frac{(q-1)(q-2)}{2}$ classes of size $\frac{|G|}{(q-1)^2} = q(q+1)$.
(2) $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$: $q - 1$ classes of size 1.
(3) $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$: $q - 1$ classes of size $\frac{|G|}{q(q-1)} = q^2 - 1$.
(4) otherwise, the eigenvalues are in $\mathbb{F}_{q^2}$. So, $\frac{|\mathbb{F}_{q^2}| - |\mathbb{F}_q|}{2} = \frac{q(q-1)}{2}$ classes of size $\frac{q(q-1)}{2}$.

Example 2.4 ($|G| = p^3$)**.**

Example 2.5 ($|G| = p^2 q$)**.** We divide three cases: $p + 2 \le q$, $p > q$, and $p^2 q = 12$. In each case we have a normal Sylow p-subgroup, groups are classified by semidirect products of a Sylow p-subgroup and a Sylow q-subgroup.

Case 1: $p + 2 \le q$. Sylow's theorem implies $n_q = 1$.

(1) Let $G \cong Z_q \rtimes Z_{p^2}$, and consider actions of the form
$$\varphi : Z_{p^2} \to \mathrm{Aut}(Z_q) \cong Z_{q-1}.$$
There are
$$\min\{v_p(q-1), 2\} = \begin{cases} 2 & , p^2 \mid q - 1, \\ 1 & , p \parallel q - 1, \\ 0 & , \text{otherwise} \end{cases}$$
nonabelian groups.
(2) Let $G \cong Z_q \rtimes (Z_p \times Z_p)$, and consider actions of the form
$$\varphi : Z_p \times Z_p \to \mathrm{Aut}(Z_q) \cong Z_{q-1}.$$
There are
$$\min\{v_p(q-1), 1\} = \begin{cases} 1 & , p \mid q - 1, \\ 0 & , \text{otherwise} \end{cases}$$
nonabelian groups.

Case 2: $p > q$. Sylow's theorem implies $n_p = 1$.

(1) Let $G \cong Z_{p^2} \rtimes Z_q$, and consider actions of the form
$$\varphi : Z_q \to \mathrm{Aut}(Z_{p^2}) \cong Z_{p(p-1)}.$$
There are
$$\min\{v_q(p-1), 1\} = \begin{cases} 1 & , q \mid p-1, \\ 0 & , \text{otherwise} \end{cases}$$
nonabelian groups.

(2) Let $G \cong (Z_p \times Z_p) \rtimes Z_q$, and consider actions of the form
$$\varphi : Z_q \to \mathrm{Aut}(Z_p \times Z_p) \cong \mathrm{GL}_2(\mathbb{F}_p).$$
Note that $|\mathrm{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p) = (p-1)^2 p(p+1)$. The conjugacy class of subgroups are classified by the Jordan normal forms.

If $q = 2$, then the possible conjugacy classes are represented by
$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
There are
$$\begin{cases} 2 & , q = 2 \\ 1 & , 2 \nmid q \mid p+1, \\ \frac{q+3}{2} & , 2 \nmid q \mid p-1, \\ 0 & , \text{otherwise} \end{cases}$$
nonabelian groups. Since the number of one-dimensional linear subspaces is $q+1$ and the number of symmetric subspaces is 2 in $\mathbb{F}_q^2$, we have $\frac{(q+1)-2}{2} + 2 = \frac{q+3}{2}$ conjugacy classes of subgroups of order q in $\mathrm{GL}_2(\mathbb{F}_p)$.

Case 3: $p = 2$, $q = 3$.

Example 2.6 ($|G| = pqr$)**.**

$\lvert G\rvert = p^2q$ $(p < q)$	12	20	28	44	45	52	63
# of groups	5	5	4	4	2	5	4

$\lvert G\rvert = p^2q$ $(p > q)$	18	50	(75)
# of groups	5	5	3

$\lvert G\rvert = pqr$	30	42
# of groups	4	6

2.3.3. *More than four primes.* Under 64, there are some exceptions whose orders are formed by product of more than four primes.

$\lvert G\rvert = \prod^4 p$	16	24	40	54	56	36	60
# of groups	14	15	14	15	13	14	13

$\lvert G\rvert = \prod^{5 \text{ or } 6} p$	32	48	64
# of groups	51	52	267

3. Extension theory

Proposition 3.1. *Let N and H be groups. Then, the following objects have one-to-one correspondences among each other.*

(1) *isomorphic types of groups G such that a sequence*
$$0 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 0$$
is exact and right split,
(2) *isomorphic types of groups G such that $N \trianglelefteq G \geq H$ with $G = NH$ and $N \cap H = 1$,*
(3) *group actions $H \curvearrowright N$ preserving the group structure of N.*

Definition 3.1. The group G in the previous proposition is called the *semidirect product* of N and H.

$$0 \longrightarrow F \longrightarrow E \longrightarrow G \longrightarrow 0.$$
Four data $G, F, \varphi : G \to \mathrm{Aut}(F), c : G \times G \to F$ completely determine the extension E.

Suppose we have an extension $F \to E \to G$. There is a *set-theoretic section* $s : G \to E$. The number of s is $|G||F|$.

Definition of *action* φ: For two sections s and s', $s(g)$ and $s'(g)$ acts on F equivalently. Thus, we can define a *group homomorphism* $\varphi : G \to \mathrm{Aut}(F)$ independently on sections.

Definition of *2-cocycle* c: It is a *set-theoretic function* $c : G \times G \to F$ defined by $c(g, g') = s(g)s(g')s(gg')^{-1}$ for a section s. Actually, c depends on the section s, and c measures how much s fails to be a group homomorphism. It requires the cocycle condition for the associativity of group operation, i.e.
$$c(g, h)c(gh, k) = \varphi_g(c(h, k))c(g, hk)$$
should be satisfied. Conversely, a map $G \times G \to F$ satisfying the condition the cocycle condition gives a associative group operation on G.

If F is abelian, then the set of cocycles forms an abelian group, and is denoted by $Z^2(G, F)$. The boundaries are also defined in abelian F case.

(1) φ, c is trivial $\Leftrightarrow$ direct product,
(2) c is trivial $\Leftrightarrow$ s is a homomorphism $\Leftrightarrow$ semidirect product,
(3) φ is trivial $\Leftrightarrow$ central extension.

Group cohomology is defined for a group G and G-module A (three data: G, A, φ. What is important is that the cohomology depends on the action of G on A.

If φ is trivial so that A is just an abelian group, then the universal coefficient theorem can be applied.