

Suns

Eric Liu

CONTENTS

CHAPTER 1	GROUPS	PAGE 2
1.1	Definition of groups	2
1.2	Group Action	6
1.3	Normal Subgroups	7
1.4	Isomorphism theorems	10
1.5	Free group and presentation	14
1.6	Center and Commutator	16
1.7	Semidirect Product	21
1.8	Finitely generated abelian group	26
1.9	Sylow theorems	29
1.10	Old Numbers	33
1.11	Symmetric Groups	35
1.12	Analysis of some finite group	40
1.13	Nilpotency and Solvability	44
1.14	p -group	48
1.15	Simplicity of $\mathrm{PSL}_n(\mathbb{F})$	49
1.16	Future Direction	54
1.17	Recreational Exercises	55

Chapter 1

Groups

1.1 Definition of groups

Let M be a set equipped with a binary operation $M \times M \rightarrow M$. We say M is a **monoid** if the binary operation is associative and there exists a two-sided identity $e \in M$.

Example 1.1.1: Identity of monoids is required to be two-sided

Defining $(x, y) \mapsto y$, we see that the operation is associative and every element is a left identity, but no element is a right identity unless $|M| = 1$. This is an example why identity must be two-sided.

Because the identity of a monoid is defined to be two-sided, clearly it must be unique. Suppose every element of monoid M has a left inverse. Fix $x \in M$. Let $x^{-1} \in M$ be a left inverse of x . To see that x^{-1} is also a right inverse of x , let $(x^{-1})^{-1} \in M$ be a left inverse of x^{-1} and use

$$(x^{-1})^{-1} = (x^{-1})^{-1}e = (x^{-1})^{-1}(x^{-1}x) = ((x^{-1})^{-1}x^{-1})x = ex = x$$

to deduce

$$xx^{-1} = (x^{-1})^{-1}x^{-1} = e$$

In other words, if we require every element of a monoid M to have a left inverse, then immediately every left inverse upgrades to a right inverse. In such case, we call M a **group**. Notice that inverses of elements of a group are clearly unique.

Theorem 1.1.2. (Group criteria) If a binary operation $G \times G \rightarrow G$ is associative, has a left identity, and always has a left inverse, then G forms a group.

Proof. If $y \in G$ is **idempotent**, then it must be identity, since $y = (y^{-1}y)y = y^{-1}y = e$. Because of such, we see a left inverse is also a right inverse, since $(xx^{-1})(xx^{-1}) = xex^{-1} =$

xx^{-1} . This then shows that the left identity is also a right identity, since $xe = x(x^{-1}x) = x$. \blacksquare

Theorem 1.1.3. (Group criteria for finite set) Let $|G| \in \mathbb{N}$. If the binary operation $G \times G \rightarrow G$ is associative and both cancellation laws holds:

$$au = aw \implies u = w \quad \text{and} \quad ua = wa \implies u = w$$

then G forms a group.

Proof. Because the set is finite, for all a , we may attach it with an natural number $n(a)$ such that $a^{n(a)+1} = a$. Clearly,

$$aa^{n(a)}b = a^{n(a)+1}b = ab = ab^{n(b)+1} = ab^{n(b)}b$$

This then by cancellation laws implies $a^{n(a)} = b^{n(b)}$, which can be easily checked to be the identity. \blacksquare

Theorem 1.1.4. (Subgroup criteria for finite subset) Let G be a group and $S \subseteq G$ be finite. If S is closed under the binary operation, then S forms a group.

Proof. Because S is finite, for all $a \in S$, there exists $n(a) \in \mathbb{N}$ such that

$$a^{n(a)}a = a$$

Multiplying both side with a^{-1} , we see that $a^{n(a)} = e$ and $a^{-1} = a^{n(a)} \in S$. \blacksquare

Example 1.1.5: Euler's totient function

By [theorem 1.1.3](#), we see that the set of nonzero integer relatively prime to n and modulo n forms a group under multiplication modulo n , called the **multiplicative group of integer modulo n** , or equivalently the unit group of the ring \mathbb{Z}_n . This immediately shows that

$$a^{\phi(a)} \equiv 1 \pmod{n}$$

for all $a \in \mathbb{N}$ coprime with n , where the **totient function** $\phi(a)$ is the number of natural numbers $\leq a$ and coprime with a . We now have **Fermat's little theorem** as a special case.

Theorem 1.1.6. (Group property of totient function) Let ϕ be the Euler totient function. For all $a, n \in \mathbb{N}$, we have $n \mid \phi(a^n - 1)$.

Proof. This is a consequence of the fact that $a \in \mathbb{Z}_{a^n-1}^\times$ and that a has order n in the group. \blacksquare

Unlike the category of monoids, the category of groups behaves much better. Given two groups G, H and a function $\varphi : G \rightarrow H$, if φ respects the binary operation, then φ also respects the identity:

$$e_H = (\varphi(x)^{-1})\varphi(x) = (\varphi(x)^{-1})\varphi(xe_G) = (\varphi(x)^{-1}\varphi(x))\varphi(e_G) = \varphi(e_G)$$

which implies that φ must also respect inverse. In such case, we call φ a **group homomorphism**. In this note, by a **subgroup** H of G , we mean an injective group homomorphism $H \hookrightarrow G$. Clearly, a subset of G forms a subgroup if and only if it is closed under both the binary operation and inverse. Note that one of the key basic property of subgroup $H \subseteq G$ is that if $g \notin H$, then $hg \notin H$, since otherwise $g = h^{-1}hg \in H$.

Let S be a subset of G . The group of **words** in S :

$$\{s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \in G : n \in \mathbb{N} \cup \{0\} \text{ and } s_i \in S \text{ and } \epsilon_i = \pm 1\}$$

is clearly the smallest subgroup of G containing S . We say this subgroup is **generated** by S . If G is generated by a single element, we say G is **cyclic**. Let $x \in G$. The **order** of G is the cardinality of G , and the order of x is the cardinality of the cyclic subgroup $\langle x \rangle \subseteq G$, or equivalently the infimum of the set of natural numbers n that makes $x^n = e$. Clearly, finite cyclic groups of order n are all isomorphic to \mathbb{Z}_n .

Let G be a group and H a subgroup of G . The **right cosets** Hx are defined by $Hx \triangleq \{hx \in G : h \in H\}$. Clearly, when we define an equivalence relation in G by setting:

$$x \sim y \iff xy^{-1} \in H$$

the equivalence class $[x]$ coincides with the right coset Hx . Note that if we partition G using **left cosets**, the equivalence relation being $x \sim y \iff x^{-1}y \in H$, then the two partitions need not to be identical.

Example 1.1.7: An non-normal subgroup

Let $H \triangleq \{e, (1, 2)\} \subseteq S_3$. The right cosets are

$$H(2, 3) = \{(2, 3), (1, 2, 3)\} \quad \text{and} \quad H(1, 3) = \{(1, 3), (1, 3, 2)\}$$

while the left cosets being

$$(2, 3)H = \{(2, 3), (1, 3, 2)\} \quad \text{and} \quad (1, 3)H = \{(1, 3), (1, 2, 3)\}$$

However, as one may verify, we have a well-defined bijection $xH \mapsto Hx^{-1}$ between the sets of left cosets and right cosets of H . Therefore, we may define the **index** $[G : H]$ of H in G

to be the cardinality of the collection of left cosets of H , without falling into the discussion of left and right. Moreover, let K be a subgroup of H , by axiom of choice, clearly we have:

$$[G : K] = [G : H] \cdot [H : K]$$

which gives **Lagrange's theorem**

$$o(G) = [G : H] \cdot o(H)$$

as a corollary.

Example 1.1.8: Isomorphic subgroups can have different indices

Note that every nontrivial subgroups of \mathbb{Z} are isomorphic, yet they are of distinct index. However, subgroups $H \leq G$ isomorphic through an automorphism $\varphi \in \text{Aut}(G)$ must have the same index, since $xH \mapsto \varphi(x)\varphi(H)$ forms a well-defined bijection.

Theorem 1.1.9. (Order formula) Let $H, K \leq G$. Then

$$|HK| \cdot o(H \cap K) = o(H) \cdot o(K)$$

and

$$[G : H \cap K] \leq [G : H] \cdot [G : K]$$

If moreover that H, K both have finite index, then

$$\text{lcm}([G : H], [G : K]) \leq [G : H \cap K]$$

Proof. The first formula follows from checking that the natural map from the left coset space $K \diagup H \cap K$ to the left coset space $HK \diagup H$ forms a well-defined bijection. The second formula follows from checking that the natural map from the left coset space $G \diagup H \cap K$ to the product $G \diagup H \times G \diagup K$ of left coset spaces forms a well-defined injection. The third formula follows from

$$[G : H \cap K] = [G : H] \cdot [H : H \cap K] = [G : K] \cdot [K : H \cap K]$$



1.2 Group Action

Let G be a group and X a set. If we say G **acts on X from left**, we are defining a function $G \times X \rightarrow X$ such that

- (i) $e \cdot x = x$ for all $x \in X$.
- (ii) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$.

Note that there is a difference between left action and right action, as gh means $g \circ h$ in left action and means $h \circ g$ in right action. Because groups admit inverses, a G -action is in fact a group homomorphism $G \rightarrow \text{Bij}(X)$.

Let $x \in X$. We call the set $\Gamma \triangleq \{g \cdot x \in X : g \in G\}$ the **orbit** of x . Clearly the set $\text{Stab}(x)$ of all elements of G that fixes x forms a group, called the **stabilizer subgroup**. Consider the action left, and let $G/\text{Stab}(x)$ denote the left coset space. The fact that the obvious mapping between $G/\text{Stab}(x)$ and Γ forms a bijection is called the **orbit-stabilizer theorem**, which relates the index of $\text{Stab}(x)$ and the length of Γ :

$$[G : \text{Stab}(x)] = |\Gamma|$$

The two most important group action are **left multiplication** and **left conjugation**:

$$g \cdot A \triangleq \{ga \in G : a \in A\} \quad \text{and} \quad g \cdot A \triangleq \{gag^{-1} \in G : a \in A\}$$

on the power set of G . Clearly, orbit of a subgroup under left multiplication is its left coset space.

Theorem 1.2.1. (Cauchy's theorem for finite group) Let $p \mid o(G)$. Then the number of elements of order divided by p is a positive multiple of p .

Proof. The set X of p -tuples (x_1, \dots, x_p) that satisfies $x_1 \cdots x_p = e$ clearly has cardinality $o(G)^{p-1}$. Consider the group action $\mathbb{Z}_p \rightarrow \text{Bij}(X)$ defined by

$$g \cdot (x_1, \dots, x_p) \triangleq (x_p, x_1, \dots, x_{p-1}), \quad \text{where } \mathbb{Z}_p = \langle g \rangle$$

Notice that $x^p = e$ if and only if $(x, \dots, x) \in X$. Therefore the number of cardinality 1 orbit equals to number of solution to $x^p = e$. By **orbit-stabilizer theorem**, an orbit in X either has cardinality p or 1. Therefore, we may write

$$p \mid o(G)^{p-1} = m + kp$$

with m the number of cardinality 1 orbits and k the number of cardinality p orbits. Clearly we have $p \mid m$, as desired. ■

1.3 Normal Subgroups

Because the inverse of an injective group homomorphism forms a group homomorphism, we know $\text{Aut}(G)$ forms a group. We say $\phi \in \text{Aut}(G)$ is an **inner automorphism** if ϕ takes the form $x \mapsto gxg^{-1}$ for some fixed $g \in G$. We say two elements $x, y \in G$ are **conjugated** if there exists some inner automorphism that maps x to y . Clearly conjugacy forms an equivalence relation. We call its classes **conjugacy classes**.

From the point of view of inner automorphism, we see that it is well-defined whether an element $g \in G$ **normalize** a subset $S \subseteq G$:

$$gSg^{-1} = S$$

independent of left and right. Because of the independence, for each subset $S \subseteq G$, we see that the set of elements $g \in G$ that normalize S forms a group, called the **normalizer** of S , in fact the stabilizer subgroup $\text{Stab}(S)$ under the conjugacy action.

Example 1.3.1: Conjugation can send subgroups to proper subgroup

Consider $G \triangleq \text{GL}_2(\mathbb{R})$ and consider:

$$H \triangleq \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R}) : n \in \mathbb{Z} \right\} \quad \text{and} \quad g \triangleq \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R})$$

Note that $gHg^{-1} < H$.

Given $x, y \in G$, we often write

$$[x, y] \triangleq xyx^{-1}y^{-1} \quad \text{or} \quad [x, y] \triangleq x^{-1}y^{-1}xy$$

and call $[x, y]$ the **commutator** of x and y . The differences again lies in sides. Taking the first definition, we see that $[x, y] \in H$ if and only if $Hxy = Hyx$, while the second definition leads us to $[x, y] \in H \iff xyH = yxH$. However, because $[x, y]$ in first definition is just $[x^{-1}, y^{-1}]$ in second definition, if $H, K \leq G$, then the set $[H, K]$ is defined the same using either the first or the second definition. In general, $[H, K]$ doesn't form a group. In fact, we clearly have $[H, K] = [K, H]^{-1}$.

Equivalent Definition 1.3.2. (Normal subgroups) Let $N \leq G$. We say N is a **normal subgroup** of G if any of the followings hold true:

- (i) $\phi(N) \subseteq N$ for all $\phi \in \text{Inn}(G)$
- (ii) $\phi(N) = N$ for all $\phi \in \text{Inn}(G)$

- (iii) $xN = Nx$ for all $x \in G$.
- (iv) The set of all left cosets of N equals the set of all right cosets of N .
- (v) N is a union of conjugacy classes.
- (vi) $[N, G] \subseteq N$.
- (vii) For all $x, y \in G$, we have $xy \in N \iff yx \in N$.

Proof. (i) \implies (ii): Let $\phi \in \text{Inn}(G)$. By premise, $\phi(N) \subseteq N$ and $\phi^{-1}(N) \subseteq N$. Applying ϕ to both side of $\phi^{-1}(N) \subseteq N$, we have $\phi(N) \subseteq N \subseteq \phi(N)$, as desired.

(ii) \implies (iii): Consider the automorphisms:

$$\phi_{L,x}(g) = xg \quad \text{and} \quad \phi_{L,x^{-1}}(g) = x^{-1}g \quad \text{and} \quad \phi_{R,x}(g) = gx$$

Because $\phi_{L,x^{-1}} \circ \phi_{R,x} \in \text{Inn}(G)$, by premise we have:

$$xN = \phi_{L,x}(N) = \phi_{L,x} \circ \phi_{L,x^{-1}} \circ \phi_{R,x}(N) = \phi_{R,x}(N) = Nx$$

(iii) \implies (iv) is clear. (iv) \implies (iii): Let $x \in G$. By premise, there exists some $y \in G$ that makes $xN = Ny$. Let $x = ny$. The proof then follows from noting

$$xN = Ny = N(n^{-1}x) = Nx$$

(iii) \implies (v): Let $n \in N$ and $x \in G$. We are required to show $xnx^{-1} \in N$. Because $xN = Nx$, we know $xn = \tilde{n}x$ for some $\tilde{n} \in N$. This implies

$$xnx^{-1} = \tilde{n}xx^{-1} = \tilde{n} \in N$$

(v) \implies (vi): Fix $n \in N$ and $x \in G$. By premise, $xn^{-1}x^{-1} \in N$. Therefore, $n(xn^{-1}x^{-1}) \in N$, as desired.

(vi) \implies (vii): Let $xy \in N$. To see yx also belong to N , observe:

$$(xy)^{-1}(yx) = (xy)^{-1}x^{-1}xyx = [xy, x] \in N$$

(viii) \implies (i): Let $n \in N$ and $x \in G$. Because $(nx)x^{-1} = n \in N$, by premise we have $x^{-1}nx \in N$, as desired. \blacksquare

Notably, since given the "conjugate by left" $\varphi_g \in \text{Inn}(G)$ and $\phi \in \text{Aut}(G)$, we have $\phi \circ \varphi_g \circ \phi^{-1} = \varphi_{\phi(g)}$, we see that $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. We call $\text{Aut}(G)/\text{Inn}(G)$ the **outer automorphism group** of G .

Example 1.3.3: Dedekind and Hamiltonian group

A group is said to be **Dedekind** if all of its subgroups are normal. Clearly every abelian group is Dedekind. Non-abelian Dedekind groups are called **Hamiltonian**. The simplest Hamiltonian group is the **quaternion group** Q_8 , which is the group of the quaternions under multiplication:

$$Q_8 \triangleq \{1, i, j, k, -1, -i, -j, -k\}$$

Note that Q_8 is Dedekind because every nontrivial element is of order 4. Clearly, Q_8 has center $\{\pm 1\}$. Because $Z(Q_8)$ has index 4, we know $Q_8/Z(Q_8)$ is abelian. This then by **correspondence theorem** implies $Q'_8 \leq Z(Q_8)$. Because Q_8 is non-abelian, we now see $Q'_8 = Z(Q_8) = \{\pm 1\}$. Note that Q_8 clearly has the conjugacy classes

$$\{1\} \cup \{-1\} \cup \{\pm i\} \cup \{\pm j\} \cup \{\pm k\}$$

Interestingly, Q_8 is a group that contains a smallest non-trivial subgroup. Every non-trivial subgroup of Q_8 must contain the group $\{\pm 1\}$.

1.4 Isomorphism theorems

Let $N \trianglelefteq G$. We say a group homomorphism $\pi : G \rightarrow G/N$ satisfies the **universal property of quotient group** G/N if

- (i) π vanishes on N . (**Group condition**)
- (ii) For all group homomorphism $f : G \rightarrow H$ that vanishes on N there exist a unique group homomorphism $\tilde{f} : G/N \rightarrow H$ that makes the diagram:

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow f & \downarrow \tilde{f} \\ & & H \end{array}$$

commute. (**Universality**)

Equivalent Definition 1.4.1. (Characteristic subgroup) Given arbitrary groups G , we say $K \operatorname{char} G$ is a **characteristic subgroup** if any of the followings holds true:

- (i) $\varphi(K) \leq K$ for all $\varphi \in \operatorname{Aut}(G)$
- (ii) $\varphi(K) = K$ for all $\varphi \in \operatorname{Aut}(G)$.

Proof. (i) \implies (ii) follows from noting $\varphi^{-1}(K) \leq K \leq \varphi^{-1}(K)$. (ii) \implies (i) is clear. ■

Theorem 1.4.2. (Basic properties of characteristic subgroups)

- (i) If there exists a unique subgroup $H \leq G$ of a fixed index, then H is characteristic.
- (ii) If $K \operatorname{char} H \trianglelefteq G$, then $K \trianglelefteq G$.
- (iii) If $K \operatorname{char} H \operatorname{char} G$, then $K \operatorname{char} G$.

Proof. (i): To show that H is characteristic, we are required to prove $[G : H] = [G : \varphi(H)]$ for all $\varphi \in \operatorname{Aut}(H)$, which follows from checking that $xH \mapsto \varphi(x)\varphi(H)$ forms a well-defined bijection between the left cosets spaces of H and $\varphi(H)$.

(ii) and (iii): Because $H \trianglelefteq G$, every inner automorphism can be restricted $\operatorname{Aut}(H)$. (ii) then follows. The proof for (iii) is the same, in which every automorphism of G can be restricted automorphism of H . ■

A subgroup $H \leq G$ is said to be **strictly characteristic** if it is preserved by all surjective endomorphism. Clearly, centers are all strictly characteristic. A group is said to be **fully characteristic** if it is preserved by all endomorphism. Clearly, commutator subgroups are all fully characteristic.

Example 1.4.3: A center that isn't fully characteristic

Consider $S_3 \times \mathbb{Z}_2$. Recall that this group has center $1 \times \mathbb{Z}_2$. The function that maps $(\pi, y) \mapsto ((1, 2)^y, 0)$ for all $\pi \in S_3$ is clearly an endomorphism that doesn't preserve the center.

Notably, given a normal subgroup $N \trianglelefteq G$ and an endomorphism $f \in \text{End}(G)$, in general we can't naturally induce an endomorphism on G/N . If we were to require a subgroup to always allow us to induce endomorphism on its factor group, then we would need it to be fully characteristic. However, when we only want to induce automorphism from an automorphism $f \in \text{Aut}(G)$, a characteristic subgroup clearly suffices. In fact, given a characteristic subgroup $K \text{ char } G$, this gives us a group homomorphism $\text{Aut}(G)/\text{Aut}(G/K)$.

Example 1.4.4: A normal subgroup that isn't characteristic

Consider the additive group of \mathbb{Q} . $\mathbb{Z} \leq \mathbb{Q}$ is then normal but not characteristic, since $x \mapsto \frac{1}{2}$ is an automorphism that doesn't preserve \mathbb{Z} .

Note that even though normal subgroups need not be preserved by automorphisms, normality is: Given $N \trianglelefteq G$ and $f \in \text{Aut}(G)$, we also have $f(N) \trianglelefteq G$.

Theorem 1.4.5. (The first isomorphism theorem for groups) The group homomorphism $\pi : G \rightarrow G/N$ is always surjective with kernel N . Let $f : G \rightarrow H$ be a group homomorphism. Then $\ker f$ is normal in G , and the induced homomorphism $\tilde{f} : G/\ker f \rightarrow H$ is injective.

Proof. They are consequences of the construction. ■

Equivalent Definition 1.4.6. (Core) Let $H \leq G$, and let $\varphi : G \rightarrow \text{Bij}(G/H)$ be the left multiplicative action on the left coset space of H . We have

$$\ker \varphi = \bigcap_{g \in G} H^g, \quad \text{where } H^g \triangleq gHg^{-1}$$

and they are the largest subgroup of H normal in G , called the **core** of H .

Proof. Routine. ■

As we will see, consideration of core is in fact useful in theory of finite group.

Theorem 1.4.7. (Properties of core) Let G be finite. Then

- (i) $[G : \text{Core}(H)]$ divides $[G : H]!$, for all $H \leq G$
- (ii) Any proper subgroup of G of smallest possible index is normal.

Proof. (i) is a consequence of **first isomorphism theorem**, since we have an injective group homomorphism $G/\text{Core}(H) \hookrightarrow \text{Bij}(G/H)$. (ii) follows from one, since we would get $\text{Core}(H) = H$. ■

Equivalent Definition 1.4.8. (Normal closure) Let $S \subseteq G$. Then

$$\langle\{s^g \in G : s \in S, g \in G\}\rangle = \bigcap_{S \subseteq N \trianglelefteq G} N$$

is the smallest normal subgroup of G that contains S . This is called the **normal closure** of S in G .

Proof. The latter expression is clearly the smallest normal subgroup of G that contains S . \leq part is clear. The only part we need to prove is \geq , which requires us to prove the former expression is normal, which is a consequence of computing

$$h(g_1 s_1 g_1^{-1})^{\epsilon_1} \cdots (g_n s_n g_n^{-1})^{\epsilon_n} h^{-1} = (x_1 s_1 x_1^{-1})^{\epsilon_1} \cdots (x_n s_n x_n^{-1})^{\epsilon_n}$$

where $x_i \triangleq h g_i$ if $\epsilon_i = 1$ and $h g_i^{-1}$ if $\epsilon_i = -1$. ■

Theorem 1.4.9. (Third isomorphism theorem and correspondence theorem) Let $N \trianglelefteq G$. The canonical projection $\pi : G \rightarrow G/N$ gives rise to a bijection between the set of subgroups of G that contains N and the set of subgroups of G/N . The bijection is moreover a bijection between the set of normal subgroups of G that contains N and the set of normal subgroups of G/N . The bijection also maps normalizer of subgroups $\leq G$ that contains N to the normalizer of the image of the subgroup.

In fact, given $K \trianglelefteq G$ that contains N , if we identify K/N as a subgroup of G/N the natural way:

$$\begin{array}{ccc} K & \xrightarrow{\pi} & \frac{K}{N} \\ & \searrow & \downarrow \\ & & \frac{G}{N} \end{array}$$

then $\frac{K}{N} \trianglelefteq \frac{G}{N}$ is the normal subgroup that corresponds to $K \trianglelefteq G$, and we have a natural isomorphism $\frac{G}{K} \cong \frac{G}{\frac{K}{N}}$.

Proof. Routine. ■

Theorem 1.4.10. (Second isomorphism theorem) Let $H \leq G$. If $K \leq N_G(H)$, then their product:

$$HK \triangleq \{hk \in G : h \in H \text{ and } k \in K\}$$

forms a group (in fact, the subgroup generated by $H \cup K$) and is defined independent of left and right. Moreover, $H \trianglelefteq HK$ with $hkH = Hk$, and $H \cap K \trianglelefteq K$ with

$$HK \diagup H \cong K \diagup H \cap K \quad \text{via} \quad kH \longleftrightarrow k(H \cap K)$$

Proof. To see $HK \subseteq KH$, simply observe $hk = k(k^{-1}hk)$. The converse inclusion is proved similarly. The fact that HK forms a group now follows. The rest are clear. \blacksquare

Example 1.4.11: Product of two subgroups

In general, product of two subgroups needs not to form a group. For example, consider the product of the subgroup H generated by $(1, 2) \in S_3$ and the subgroup K generated by $(2, 3) \in S_3$. Since $(2, 3)(1, 2) \notin HK$, we see HK isn't a group.

On the other hand, given two normal subgroups $N, M \trianglelefteq G$. By the [preserved-by-conjugations definition of normal subgroups](#), clearly both NM and $N \cap M$ are normal in G .

1.5 Free group and presentation

Let S be a set. By the **free group generated by S** , we mean a group F_S together with an injective function $\iota : S \hookrightarrow F_S$ such that for all group G and function $f : S \rightarrow G$, there exists a unique group homomorphism $\tilde{f} : F_S \rightarrow G$ that makes the diagram:

$$\begin{array}{ccc} S & \xrightarrow{\iota} & F_S \\ & \searrow f & \downarrow \tilde{f} \\ & & G \end{array}$$

commutes. Given a set of **relators** $R \subseteq F_S$, by **presentation** $\langle S \mid R \rangle$, we mean the group $F_S / \text{ncl}_{F_S}(R)$. Since kernel is normal, such group clearly satisfies the universal property that for all group G and function $f : S \rightarrow G$ such that the kernel of induced group homomorphism $\tilde{f} : F_S \rightarrow G$ contains R , there exists a unique group homomorphism $\hat{f} : \langle S \mid R \rangle \rightarrow G$ that makes the diagram

$$\begin{array}{ccc} S & \xrightarrow{\pi \circ \iota} & \langle S \mid R \rangle \\ & \searrow f & \downarrow \hat{f} \\ & & G \end{array}$$

Example 1.5.1: Dihedral group

The **Dihedral group** D_n is defined by

$$D_n \triangleq \langle r, s \mid r^n = s^2 = e, srs^{-1} = r^{-1} \rangle$$

Clearly, every element can be written as $r^a s^b$ with $0 \leq a \leq n-1$ and $b \in \{0, 1\}$. This implies that D_n has at most $2n$ number of elements. To see that $o(D_n) = 2n$, one first consider the group homomorphism $D_n \rightarrow \text{GL}_2(\mathbb{C})$ induced by

$$r \mapsto \begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix} \quad \text{and} \quad s \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

where $\xi \triangleq \exp(2\pi i/n)$. Because

$$r^a = \begin{pmatrix} \xi^a & 0 \\ 0 & \xi^{-a} \end{pmatrix} \quad \text{and} \quad r^a s = \begin{pmatrix} 0 & \xi^a \\ \xi^{-a} & 0 \end{pmatrix}$$

We now see that indeed $o(D_n) = 2n$. Moreover, because from the relators, we have the formula

$$(r^a s^b)(r^c s^d) = r^{a+(-1)^b c} s^{b+d}$$

which by direct computation implies $D'_n = \langle r^2 \rangle$. Suppose $r^a s^b \in Z(D_n)$ with $0 \leq a \leq n-1$ and $b \in \{0, 1\}$. Then from the formula, we must have

$$a + (-1)^b c \equiv c + (-1)^d a \pmod{n}, \quad \text{for all } c, d \in \mathbb{Z} \quad (1.1)$$

Because d can be arbitrary, this implies

$$2a \equiv 0 \pmod{n}$$

Clearly we have $D_1 \cong \mathbb{Z}_2$ and $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Therefore, we from now on suppose $n \geq 3$.

Let n be odd. Then clearly $a = 0$. Since $rs \neq sr$ in general, we see that we also must have $b = 0$. We have shown that D_n has trivial center for odd $n \geq 3$.

Let n be even. Then we must have $a \in \{0, \frac{n}{2}\}$. If $a = 0$, then again because $rs \neq sr$ in general, we must have $b = 0$. If $a = \frac{n}{2}$, then from the **equation 1.1**, regardless of d , we see

$$(-1)^b c \equiv c \pmod{n}, \quad \text{for all } c \in \mathbb{Z}$$

which can only be true if $b = 0$. We have shown that D_n has center $\{e, r^{\frac{n}{2}}\}$ for even $n \geq 3$. Note that again by direct computation, one can check that the pattern of conjugacy classes differ according to parity of n . Regardless of parity, for fixed $k \in \mathbb{Z}$, the set $\{r^{\pm k}\}$ form a conjugacy class. If n is odd, then the rest $\{r^t s : 1 \leq t \leq n-1\}$ forms a class. If n is even, then the rest forms two classes:

$$\{r^r s \in D_n : 1 \leq t \leq n-1 \text{ is even}\} \cup \{r^t s \in D_n : 1 \leq t \leq n-1 \text{ is odd}\}$$

1.6 Center and Commutator

Let $S \subseteq G$. Clearly $N_G(S)$ is the largest subgroup in which S is preserved by inner automorphism. Consider its **centralizer** $C_G(S) \triangleq \{g \in G : gs = sg \text{ for all } s \in S\}$. To see that $C_G(S) \trianglelefteq N_G(S)$, one simply observe that $C_G(S)$ is the kernel of the conjugacy action $N_G(S) \rightarrow \text{Bij}(S)$, where $\text{Bij}(S)$ can be replaced by $\text{Aut}(S)$ if S forms a subgroup G . In such case, **first isomorphism theorem** gives us an injection

$$N_G(S)/C_G(S) \hookrightarrow \text{Aut}(S)$$

We call the centralizer of the whole group $Z(G) \triangleq C_G(G)$ **center**.

Equivalent Definition 1.6.1. (Property of center) Let $S \subseteq G$. We have

$$S \subseteq Z(G) \iff C_G(S) = G$$

Proof. Routine. ■

Clearly, regardless of G , we always have a natural surjective group homomorphism $G \twoheadrightarrow \text{Inn}(G)$, such group homomorphism is injective (and thus an isomorphism) if and only if G is centerless.

Because every element of the center form a single conjugacy classes, by **orbit-stabilizer theorem**, we have the **class equation**:

$$o(G) = o(Z(G)) + \sum [G : C_G(x)]$$

where x runs through conjugacy classes outside of $Z(G)$. From class equation, we immediately see that **finite p -groups** must have nontrivial centers.

Example 1.6.2: Infinite p -group

The **Prüfer group** $\mathbb{Z}(p^\infty)$ is defined by

$$\mathbb{Z}(p^\infty) \triangleq \{\exp(2\pi im/p^n) \in \mathbb{C} : m \in \mathbb{Z} \text{ and } n \in \mathbb{N}\}$$

It is an infinite group whose every nontrivial element has order p^n for some $n \in \mathbb{N}$.

Let $N \trianglelefteq G$. Because $xy \in N$ if and only if $yx \in N$, regardless of the definition, we see that

$$[g, h] \in N \iff gN, hN \in G/N \text{ commutes}$$

Therefore, the factor group G/N is abelian if and only if $[G, G] \subseteq N$. In this note, we use G' to denote the **commutator subgroup** of G , the subgroup generated by $[G, G]$.

From our observation, clearly G' is the smallest normal subgroup that makes the quotient abelian. In fact, any subgroup H containing G' is normal, since if $ghg^{-1}h^{-1} \in H$, then we clearly have $ghg^{-1} \in H$. We call G/G' the **abelianization** of G .

Theorem 1.6.3. (Property of commutator subgroup) Given normal subgroup $N \trianglelefteq G$, if $G' \cap N = 1$, then $N \leq Z(G)$.

Proof. Fix $n \in N$ and $g \in G$. Because N is normal, we know $gng^{-1}n^{-1} \in N$. It then follows from $N \cap G' = 1$ that $gng^{-1}n^{-1} = e$, which implies $gn = ng$. \blacksquare

Example 1.6.4: Commutator subgroup of $\mathrm{GL}_2(\mathbb{R})$ is $\mathrm{SL}_2(\mathbb{R})$

Clearly we have $(\mathrm{GL}_2(\mathbb{R}))' \leq \mathrm{SL}_2(\mathbb{R})$. The opposite relation requires computation. We offer a fast way. Write $[g, h] \triangleq ghg^{-1}h^{-1}$. Compute that

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \left[\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right], \quad \text{for all } x \in \mathbb{R}$$

Compute that

$$\begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} = \left[\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right], \quad \text{for all } x \in \mathbb{R}^\times$$

We now see that for $a \neq 0$, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} 1 & ab \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \in (\mathrm{GL}_2(\mathbb{R}))'$$

Compute that

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \left[\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 2 \end{pmatrix} \right]$$

We now see that for $a = 0$, we have

$$\begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -\frac{d}{b} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{b} & 0 \\ 0 & b \end{pmatrix} \in (\mathrm{GL}_2(\mathbb{R}))'$$

Theorem 1.6.5. (Schur's upper bound for order of commutator subgroup) Let $C \subseteq G$ be the set of commutators. If $[G : Z(G)] \triangleq n$, then

$$|C| \leq n^2 \quad \text{and} \quad o(G^{(1)}) \leq n^{2n^3}$$

Proof. To prove $|C| \leq n^2$, we show that

$$\begin{cases} aZ(G) = cZ(G) \\ bZ(G) = dZ(G) \end{cases} \implies [a, b] = [c, d]$$

The premise gives us $ac^{-1} \in Z(G)$ and $bd^{-1} \in Z(G)$. We then can compute

$$aba^{-1}b^{-1} = aba^{-1}(cc^{-1})b^{-1} = cbc^{-1}b^{-1} = cbc^{-1}b^{-1}(dd^{-1}) = cdc^{-1}d^{-1} \quad (\text{done})$$

Before proving the second part, we first prove a necessary lemma:

$$[a, b]^{n+1} = [a, b^2] \cdot [bab^{-1}, b]^{n-1}, \quad \text{for all } a, b \in G$$

The premise $[G : Z(G)] = n$ implies $g^n \in Z(G)$ for all $g \in G$. Therefore, we may compute

$$\begin{aligned} [a, b]^{n+1} &= aba^{-1}[a, b]^n b^{-1} = ab^2 a^{-1} b^{-1} [a, b]^{n-1} b^{-1} = [a, b^2] b [a, b]^{n-1} b^{-1} \\ &= [a, b^2] (b[a, b]b^{-1})^{n-1} = [a, b^2] \cdot [bab^{-1}, b]^{n-1} \quad (\text{done}) \end{aligned}$$

Recall that $C = \{c^{-1} \in G : c \in C\}$. Since $|C| \leq n^2$, to prove $o(G^{(1)}) \leq n^{2n^3}$, we only have to show that

For all $g \in G^{(1)}$, when written in the form $g \triangleq c_1 \cdots c_m$, where $c_i \in C$, we may require $m \leq n^3$.

Fix g . Let $g \triangleq c_1 \cdots c_m$ with smallest m . We prove such by showing that each c_i can occurs at most n times in the expression $c_1 \cdots c_m$. Assume some c_j occurs $> n$ times in the expression. Because in general, we have

$$z[x, y] = [zxz^{-1}, zyz^{-1}]z^{-1}$$

in groups, we may pull the c_j to the most left in the expression. Then our lemma $[a, b]^{n+1} = [a, b^2] \cdot [bab^{-1}, b]^{n-1}$ gives a contradiction, to the minimality of m . (done) ■

Theorem 1.6.6. (Schur's upper bound for index of center) Let $G \triangleq \langle g_1, \dots, g_m \rangle$ be finitely generated. If $o(G^{(1)}) \triangleq n$, then

$$[G : Z(G)] \leq n^m$$

Proof. Clearly we have

$$Z(G) = \bigcap_{i=1}^m C_G(g_i)$$

Orbit-stabilizer theorem says that

$$[G : C_G(g_i)] = |\Gamma|$$

where Γ is the orbit of g_i under the conjugacy action $G \longrightarrow \text{Inn}(G)$. Since $xg_i x^{-1} = [x, g_i]g_i$, for all $x \in G$, we see $|\Gamma| \leq n$. The proof then follows from [order formula](#):

$$[G : Z(G)] = [G : \bigcap_{i=1}^m C_G(g_i)] \leq \prod_{i=1}^m [G : C_G(g_i)] \leq n^m$$

■

Equivalent Definition 1.6.7. (Abelian) We call a group G **abelian** if any of the followings hold true

- (i) $Z(G) = G$
- (ii) $G' = 1$
- (iii) $g \mapsto g^{-1}$ forms an automorphism.
- (iv) $\text{Inn}(G)$ is trivial.

Proof. Routine. ■

Interestingly, our equivalence definition for Abelian immediately gives a corollary on automorphism groups:

Corollary 1.6.8. (Finite group with order ≥ 3 has a nontrivial automorphism) If $o(G) \geq 3$, then $\text{Aut}(G)$ is nontrivial.

Proof. If G is non-abelian, then $\text{Inn}(G)$ is non-trivial. If G is abelian, then we have the inversion automorphism. Such inversion automorphism is non-trivial unless all nontrivial elements of G has order 2. In such case, G forms a finite-dimensional \mathbb{F}_2 -vector space, which allow us to easily find an inversion automorphism. ■

Theorem 1.6.9. (Abelian criteria for finite group) Let G be a finite group and $\varphi \in \text{Aut}(G)$ be an automorphism that satisfies

$$|\{g \in G : \varphi(g) = g^{-1}\}| > \frac{3}{4} \cdot o(G)$$

Then G is abelian.

Proof. Denote $S \triangleq \{x \in G : \varphi(x) = x^{-1}\}$. Because of consideration of order, we only have to prove $S \subseteq Z(G)$. Fix $x \in S$. We prove that $C_G(x) = G$. Now, since

$$y^{-1}x^{-1} = \varphi(xy) = \varphi(x)\varphi(y) = x^{-1}y^{-1}, \quad \text{for all } y \in S \cap x^{-1}S$$

we see that $S \cap x^{-1}S \subseteq C_G(x)$. The proof then follows from computing

$$\begin{aligned}|S \cap x^{-1}S| &= |S| + |x^{-1}S| - |S \cup x^{-1}S| \\ &\geq \frac{3}{2} \cdot o(G) + 2\epsilon - o(G) > \frac{1}{2} \cdot o(G)\end{aligned}$$

and consideration of the order. ■

Example 1.6.10: Lower bound in **our abelian criteria for finite group is necessary**

Consider

$$D_4 \triangleq \langle r, s \mid r^4 = s^2 = e, srs^{-1} = r^{-1} \rangle$$

There are exactly three quarters of elements of order dividing 2, i.e., $\{e, r^2, rs, r^2s, r^3s\}$. The identity automorphism send them to their inverse, but the group is not abelian.

1.7 Semidirect Product

Let N, H be two groups and $\varphi : H \rightarrow \text{Aut}(N)$ be a group homomorphism. Clearly, when we define a binary operation on $N \times H$ by

$$(n_1, h_1) \cdot (n_2, h_2) \triangleq (n_1\varphi_{h_1}(n_2), h_1h_2)$$

We have the **external semidirect product group** $N \rtimes_\varphi H$ in which the inverse of (n, h) is $(\varphi_{h^{-1}}(n^{-1}), h^{-1})$. Remarkably, the automorphism $\varphi_h \in \text{Aut}(N)$ is always the restriction of the inner automorphism $n \mapsto hnh^{-1}$ in the parent group $N \rtimes_\varphi H$. In particular, given a group G , indeed, every automorphism $\psi \in \text{Aut}(G)$ of G is a restriction of the inner automorphism

$$(g, \varphi) \mapsto (e, \psi) \cdot (g, \varphi) \cdot (e, \psi)^{-1}$$

of the **holomorph group** $\text{Hol}(G) \triangleq G \rtimes_{\text{id}} \text{Aut}(G)$.

Theorem 1.7.1. (Universal property of semidirect product) Let N, H be two groups and $\varphi : H \rightarrow \text{Aut}(N)$ be a group homomorphism. If group homomorphisms $f : N \rightarrow G, g : H \rightarrow G$ satisfy

$$f(\varphi_h(n)) = g(h)f(n)g(h^{-1}), \quad \text{for all } n \in N, h \in H$$

then there exists a unique $k : N \rtimes_\varphi H \rightarrow G$ that makes the diagram:

$$\begin{array}{ccc} N \rtimes_\varphi H & \xleftarrow{\quad} & H \\ \uparrow & \searrow k & \downarrow g \\ N & \xrightarrow{f} & G \end{array}$$

commutes.

Proof. It is routine to check that $k(n, h) \triangleq f(n)\varphi_h(g(h))$ suffices. The uniqueness follows from noting $(n, e) \cdot (e, h) = (n, h)$ for all $n \in N$ and $h \in H$. ■

It is worth mentioning here that direct product is a special case of semidirect product. If $\varphi : H \rightarrow \text{Aut}(N)$ is trivial, then $N \rtimes_\varphi H \cong N \times H$. Also, it is not true that every two distinct group homomorphism $\psi, \varphi : H \rightarrow \text{Aut}(N)$ must induce distinct semidirect product. For example, given $f \in \text{Aut}(H)$, we have

$$N \rtimes_{\varphi \circ f} H \cong N \rtimes_\varphi H \quad \text{via} \quad (n, f^{-1}(h)) \mapsto (n, h) \tag{1.2}$$

Theorem 1.7.2. (Presentation of semidirect product) Let $N \triangleq \langle X \mid R \rangle$, $H \triangleq \langle Y \mid S \rangle$ and $\varphi : H \rightarrow \text{Aut}(N)$ be a group homomorphism. We have

$$N \rtimes_{\varphi} H = \langle X \cup Y \mid R, S, yxy^{-1} = w_y(x) \text{ for all } x \in X, y \in Y \rangle$$

where $w_y(x)$ is a fixed word in X that stands for $\varphi_y(x) \in N$.

Proof. See Chapter 10, Section 1, Corollary 1 of the book Presentations of Groups (2nd ed.) by D.L. Johnson. The proof is not difficult, but without his approach, can be rather lengthy and tedious. ■

Example 1.7.3: Classification of semidirect product of $C_8 \rtimes C_2$

Write $\text{Aut}(C_8) \triangleq \{1, 3, 5, 7\}$, so there are four distinct action $C_2 \longrightarrow \text{Aut}(C_8)$ giving us possibly four distinct semidirect product of $C_8 \rtimes C_2$:

$$\langle x, y \mid x^8 = y^2 = e, yxy^{-1} = x^n \rangle, \quad n \in \{1, 3, 5, -1\}$$

Because every word clearly can be written as $x^a y^b$ with $0 \leq a \leq 7$ and $b \in \{0, 1\}$, regardless of n , and because as a priori, we are already aware that $C_8 \rtimes C_2$ has order 16, we know that indeed the elements $x^a y^b$ are nontrivial unless $a = b = 0$. To see that the four groups are non-isomorphic, one can first use the formula:

$$(x^a y)^2 = x^{a(n+1)}$$

to count the number of elements of order 2, and therefore confirm that the only possible isomorphism is between $n = 1$ and $n = 5$, which is also impossible, since $n = 5$ is clearly non-abelian.

Equivalent Definition 1.7.4. (Recognition theorem for inner semidirect product) Let $N \trianglelefteq G$ and $H \leq G$. The followings are equivalent

- (i) $G = NH$ and $N \cap H = 1$.
- (ii) Every g can be uniquely written as $g = nh$.
- (iii) The composition of $\pi : G \twoheadrightarrow G/N$ and $i : H \hookrightarrow G$ forms an isomorphism $H \rightarrow G/N$.
- (iv) There exists a homomorphism $r : G \rightarrow H$, called the **retraction**, that is identity on H and has kernel N . Such retraction then give us a right split sequence

$$1 \longrightarrow N \longrightarrow G \xrightarrow{r} H \longrightarrow 1$$

since $r \circ i = \mathbf{id}_H$.

Proof. (i) \implies (ii) is clear. (ii) \implies (iii): Let $h \in N$. To prove that $H \rightarrow G/N$ is injective, we are required to show $h = e$. Because $h \in N$, we know $h = eh = he$ implies that $h = e$. Surjectivity is clear.

(iii) \implies (iv): Clearly $r \triangleq (\pi \circ i)^{-1} \circ \pi$ suffices.

(iv) \implies (i): $N \cap H = 1$ is clear. To see that $G = NH$, just observe that $g = gr(g^{-1})r(g)$, where $gr(g^{-1}) \in N$, since $r(gr(g^{-1})) = r(g)r(r(g^{-1})) = r(g)r(g^{-1}) = e$. \blacksquare

Suppose $N \trianglelefteq G$ and $H \leq G$ satisfies the conditions in the **recognition theorem for inner semidirect product**. Defining $\varphi : H \rightarrow \text{Aut}(N)$ by $\varphi_h(n) \triangleq hnh^{-1}$, we see that the natural map $N \rtimes_{\varphi} H \rightarrow G$ indeed forms a well-defined group isomorphism. Note that if H is also normal in G , then the action $\varphi_h(n) = hnh^{-1}$ become trivial, since we would have $[H, N] \subseteq H \cap N = 1$. This agrees with the **recognition theorem for direct product**.

Example 1.7.5: Inner semidirect product

View \mathbb{Z}_2 as a subgroup of S_n by sending $1 \mapsto (1, 2)$. We see that we have a right split sequence:

$$1 \longrightarrow A_n \longrightarrow S_n \xrightarrow{\text{sgn}} C_2 \longrightarrow 1$$

Therefore, we may write

$$S_n \cong A_n \rtimes_{\varphi} C_2, \quad \text{with } \varphi_1(g) = (1, 2)g(1, 2)^{-1}$$

Let \mathbb{F} be a field, and view \mathbb{F}^{\times} as a subgroup of $\text{GL}_n(\mathbb{F})$ by sending c to $\text{diag}(c, 1, \dots, 1)$. We see that we have a right split sequence:

$$1 \longrightarrow \text{SL}_n(\mathbb{F}) \longrightarrow \text{GL}_n(\mathbb{F}) \xrightarrow{\det} \mathbb{F}^{\times} \longrightarrow 1$$

Equivalent Definition 1.7.6. (Recognition theorem for direct product) Let N_1, \dots, N_k be normal subgroups of G . We say G is an **internal direct products** of N_i if any of the followings hold true:

- (i) The natural map $N_1 \times \dots \times N_k \rightarrow G$ forms a group isomorphism.
- (ii) $N_1 \cdots N_k = G$ and $N_i \cap \prod_{j \neq i} N_j = 1$ for all i .
- (iii) $N_1 \cdots N_k = G$ and $N_i \cap \prod_{j < i} N_j = 1$ for all i .

Proof. (i) \implies (ii): Clearly we have $N_1 \cdots N_k = G$. Let $n_2 \cdots n_k \in N_1$. Because $n_2 \cdots n_k$ is both the image of $(n_2 \cdots n_k, e, \dots, e)$ and (e, n_2, \dots, n_k) , by injectivity of the natural map,

we know $n_2 = \dots = n_k = e$.

(ii) \implies (iii) is clear. It remains to show (iii) \implies (i). The proof relies on induction on k . We first prove the base case $k = 2$. Because $[N_1, N_2] \leq N_1 \cap N_2 = 1$, we know the natural map forms homomorphism. Surjectivity is clear. For injectivity, if $n_1 n_2 = e$, then since $n_1 = n_2^{-1} \in N_2$, we know $n_1 = n_2 = e$.

We now prove the inductive case. By the base case, the natural map:

$$(N_1 \cdots N_k) \times N_{k+1} \longrightarrow N_1 \cdots N_k N_{k+1} = G$$

forms a group isomorphism. By inductive hypothesis, the natural map:

$$N_1 \times \cdots \times N_k \longrightarrow N_1 \cdots N_k$$

also forms a group isomorphism. Composing the two together, we get the desired isomorphism. \blacksquare

It should be noted that we didn't define internal direct products for infinite index, since the original statement can not be naively generalized to the infinite case. The ill behavior can be seen from multiple aspect. For example, we have

$$\prod_{i \in I} N_i \trianglelefteq \prod_{i \in I} G_i \quad \text{and} \quad \frac{\prod G_i}{\prod N_i} \cong \prod_{i \in I} \frac{G_i}{N_i} \quad \text{and} \quad Z\left(\prod_{i \in I} G_i\right) = \prod_{i \in I} Z(G_i)$$

even if the index set I is infinite, but we only have

$$\left(\prod_{i \in I} G_i\right)' \leq \prod_{i \in I} (G'_i)$$

where the equality holds if I is finite.

Equivalent Definition 1.7.7. (Recognition theorem for direct product for finite group) Let G be a finite group, and let $N_1, \dots, N_k \trianglelefteq G$ satisfy $G = N_1 \cdots N_k$ and $o(G) = o(N_1) \cdots o(N_k)$. Then G is the internal direct product of N_i .

Proof. The proof is done by induction on k . The base case $k = 1$ is trivial. For the inductive case, one first use **the order formula** to compute

$$o(N_1) \cdots o(N_k) o(N_1 \cap (N_2 \cdots N_k)) = o(G) o(N_1 \cap (N_2 \cdots N_k)) = o(N_1) o(N_2 \cdots N_k)$$

which gives

$$o(N_1 \cap (N_2 \cdots N_k)) = \frac{o(N_2 \cdots N_k)}{o(N_2) \cdots o(N_k)} \leq 1$$

which by **recognition theorem** implies G is the internal direct product $N_1 \times (N_2 \cdots N_k)$. The rest then follows from the inductive hypothesis. \blacksquare

Example 1.7.8: The requirement in definitions of internal direct products for groups

Let $G \triangleq C_4 \times C_2$. Clearly the direct product of $\langle(1, 0)\rangle$ and $\langle(2, 0)\rangle$ is isomorphic to G , but they do not form an internal direct product of G . It is because of such, we must require $N_1 \times \cdots \times N_k$ not only isomorphic to G , but moreover the natural way in **definition of internal direct products for groups**.

Example 1.7.9: The requirement in definitions of internal direct products for groups

Let $G = \mathbb{Z} \times \mathbb{Z}$. Clearly $N_1 \triangleq \mathbb{Z} \times 1, N_2 \triangleq 1 \times \mathbb{Z}, N_3 \triangleq \{(x, x) \in G : x \in \mathbb{Z}\}$ satisfies

$$G = N_1 N_2 N_3 \quad \text{and} \quad N_1 \cap N_2 = N_1 \cap N_3 = N_2 \cap N_3 = 1$$

Yet, later we will see that **we can never have the isomorphism $\mathbb{Z} \times \mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$** . This is why we must require $N_i \cap \prod_{j \neq i} N_j = 1$ in the definition internal direct product.

Example 1.7.10: Subgroups are not products of intersections

In general, we don't have

$$H \leq G_1 \times \cdots \times G_k \implies H = (G_1 \cap H) \times \cdots \times (G_k \cap H)$$

even in the category of abelian group. For example, consider $H \triangleq \{(x, x) \in \mathbb{Z}^2 : x \in \mathbb{Z}\}$.

1.8 Finitely generated abelian group

Theorem 1.8.1. (Change of basis for finitely generated abelian group) Let $k \in \mathbb{N}$, $G = \langle x_1, \dots, x_k \rangle$ be abelian and $c_1, \dots, c_k \in \mathbb{N}$ satisfies $\gcd(c_1, \dots, c_k) = 1$. Then there exists $y_1, \dots, y_k \in G$ such that $G = \langle y_1, \dots, y_k \rangle$ and $y_1 = c_1x_1 + \dots + c_kx_k$.

Proof. Such is proved via induction on $s \triangleq c_1 + \dots + c_k$. The base case $s = k$ is clear. We now prove the inductive case. Because $\gcd(c_1, \dots, c_k) = 1$, by changing the order if necessary, we may write $c_1 > c_2$. Now, because $\gcd(c_1 - c_2, c_2, \dots, c_k) = 1$ and $G = \langle x_1, x_2 - x_1, x_3, \dots, x_k \rangle$, we see by inductive hypothesis that there exists y_1, \dots, y_k such that $G = \langle y_1, \dots, y_k \rangle$ and

$$\begin{aligned} y_1 &= (c_1 - c_2)x_1 + c_2(x_2 + x_1) + \dots + c_kx_k \\ &= c_1x_1 + \dots + c_kx_k \end{aligned}$$

as desired. ■

Theorem 1.8.2. (Structure theorem for finitely generated abelian group) Let G be a finitely generated abelian group. Then we may write:

$$G \cong C_{n_1} \times \dots \times C_{n_s} \times \mathbb{Z}^r$$

for $n_i \geq 2$. Moreover, we know that

- (i) Such r is unique, called the **rank** of G .
- (ii) Under the assumption that n_i each is a power of some prime, the expression exists and is unique, called the **primary decomposition form**.
- (iii) Under the assumption that $n_i \mid n_{i+1}$ for all i , the expression exists and is unique, called the **invariant factor form**.

Proof. We first show the **existence** via induction on the number of generators. The base case is clear. Suppose that the existence holds true for any abelian group that has a generating set of cardinality $k - 1$, and suppose that G has a generating set $\{x_1, \dots, x_k\}$ where x_1 has order smaller than any elements of any generating sets of cardinality k .

By inductive hypothesis, we only have to show that G is an internal direct product of $\langle x_1 \rangle$ and $\langle x_2, \dots, x_k \rangle$. Assume not for a contradiction. Then there exists $m_1 \neq 0$ such that $m_1x_1 + m_2x_2 + \dots + m_kx_k = 0$. By possibly changing sign of some of the x_i and exchanging the order, we may suppose $m_1 < o(x_1)$ and $m_1, \dots, m_t \in \mathbb{N}$ and $m_{t+1} = \dots = m_k = 0$.

Let $c_i \triangleq \frac{m_i}{\gcd(m_1, \dots, m_t)}$ for all $i \in \{1, \dots, t\}$. By theorem 1.8.1, we know there exists $y_1, \dots, y_t \in G$ such that $\langle y_1, \dots, y_t \rangle = \langle x_1, \dots, x_t \rangle$ with $y_1 = c_1 x_1 + \dots + c_t x_t$. Clearly, we have $G = \langle y_1, \dots, y_t, x_{t+1}, \dots, x_k \rangle$. Compute

$$\gcd(m_1, \dots, m_t) y_1 = m_1 x_1 + \dots + m_t x_t = 0$$

We now see $o(y_1) \leq m_1 < o(x_1)$, a contradiction to the choice that x_1 has the smallest order. (done)

(i): Fix an expression of G , and let p be a prime that satisfies $p \nmid n_i$ for all i . The rest then follows from checking that $G/pG \cong C_p^r$.

(ii): The existence follows from noting that

$$\gcd(m, n) = 1 \implies C_{mn} \cong C_m \times C_n$$

The uniqueness follows from noting that given a primary decomposition form whose p -part has the form $C_{p^{n_1}} \times \dots \times C_{p^{n_k}}$, then the **torsion p -subgroup** G_{T_p} of G

$$G_{T_p} \triangleq \{x \in G : o(x) = p^n \text{ for some } n \geq 0\}$$

is

$$G_{T_p} \cong C_{p^{n_1}} \times \dots \times C_{p^{n_k}}$$

and that

$$\frac{p^{d-1}C_{p^{n_i}}}{p^d C_{p^{n_i}}} \cong \begin{cases} C_p & \text{if } d-1 < n_i \\ 1 & \text{if } d-1 \geq n_i \end{cases}$$

(iii): Both the existence and uniqueness of invariant factor form follows from that of primary decomposition form: Just consider that C_{n_s} can only be $C_{p_1}^{d_1} \times \dots \times C_{p_m}^{d_m}$, where p_i non-repeatedly running through all the occurring prime with d_i being the highest exponential. ■

Structure theorem for finitely generated abelian group in fact also gives a structure theorem for automorphism group of finite abelian group. See [this paper](#). A particular case is that $\text{Aut}(C_p^n) \cong \text{GL}_n(\mathbb{F}_p)$.

Corollary 1.8.3. (Finite abelian group has subgroups of all possible order) Let G be a finite abelian group with $m \mid o(G)$. Then there exists subgroup of G of order m .

Proof. The proof follows from the primary decomposition form and the fact that for all $e < d \in \mathbb{N} \cup \{0\}$,

$$\{0, p^{d-e}, \dots, (p^e - 1)p^{d-e}\} \subseteq C_{p^d}$$

is a subgroup of C_{p^d} of order p^e . ■

Theorem 1.8.4. (Subgroup of finitely generated abelian group) Let G be a finitely generated abelian group that has rank r whose p -part is

$$G_{T_p} \cong C_{p^{n_1}} \times \cdots \times C_{p^{n_k}}, \quad \text{with } n_1 \geq \cdots \geq n_k$$

Then for any subgroup $H \leq G$, if we write

$$H_{T_p} \cong C_{p^{d_1}} \times \cdots \times C_{p^{d_s}}, \quad \text{with } d_1 \geq \cdots \geq d_s$$

then the rank of H is $\leq r$, and we have $s \leq k$ and $n_i \geq d_i$ for all i .

Proof. Clearly we have $H_{T_p} \leq G_{T_p}$. Consider $\Omega_1(H_{T_p}) \triangleq \{h \in H_{T_p} : h^p = e\}$. Clearly, we have

$$C_p^s \cong \Omega_1(H_{T_p}) \leq \Omega_1(G_{T_p}) \cong C_p^k$$

Therefore, by counting order, we see that indeed $s \leq k$. The rest is

$$C_p^{\text{card}\{\geq d_i\}} \cong \Omega_1(p^{d_i-1}H_{T_p}) \leq \Omega_1(p^{d_i-1}G_{T_p}) \cong C_p^{\text{card}\{\geq d_i\}}$$

We now prove that H has rank $\leq r$. Let q be a prime not in the decomposition. Since

$$\mathbb{Z}^s \cong qH \leq qG \cong \mathbb{Z}^r$$

We have an injective group homomorphism $f : \mathbb{Z}^s \rightarrow \mathbb{Z}^r$. Denote the group homomorphism by a r -by- s matrix $A \in M_{r \times s}(\mathbb{Z})$. The injectivity of f then means $Av = 0 \implies v = 0$ for all $v \in \mathbb{Z}^s$. Let $w \in \mathbb{Q}^s$ and $m \gg 0$ be a natural number large enough so that $mw \in \mathbb{Z}^s$. We then see

$$Aw = 0 \implies Amw = mA w = 0 \implies mw = 0 \implies w = 0$$

In other words, the matrix $A \in M_{r \times s}(\mathbb{Q})$ has rank s , which is only possible given that $s \leq r$. ■

1.9 Sylow theorems

Theorem 1.9.1. (Combinatorial facts) Let p be prime. Then:

- (i) Given $m \geq r \in \mathbb{N} \cup \{0\}$ with $t \in \mathbb{N}$ coprime with p , the natural number $\binom{p^m t}{p^r}$ has p -part p^{m-r} .
- (ii) We have

$$\binom{m}{n} \equiv \prod_{i=0}^k \binom{m_i}{n_i} \pmod{p}$$

when we write $m = m_k p^k + \cdots + m_0 p^0$ and $n = n_k p^k + \cdots + n_0 p^0$. This is called **Lucas modulo binomial formula**.

Proof. (i) follows from noting that

$$\binom{p^m t}{p^r} = \frac{p^m t (p^m t - 1) \cdots (p^m t - (p^r - 1))}{p^r (p^r - 1) \cdots (p^r - (p^r - 1))}$$

and that for all $i \in \{1, \dots, p^r - 1\}$, the three natural number $\{i, p^m t - i, p^r - i\}$ share the same p -part.

(ii): Let M be a set of m elements. Partition M into m_i cycles of length p^i , i.e.,

$$M \triangleq \bigcup_{i=0}^k \bigcup_{j=1}^{m_i} \Gamma_{i,j}, \quad \text{where } |\Gamma_{i,j}| = p^i$$

Because of such, we see that M can be acted on by the group

$$G \triangleq \prod_{i=0}^k \overbrace{C_{p^i} \times \cdots \times C_{p^i}}^{m_i}$$

Clearly, G also acts on the set X of the set of subsets of M that has n elements. Because G is a p -group, **orbit-stabilizer theorem** tell us that

$$\binom{m}{n} = |X| \equiv |\text{Fix}(G)| \pmod{p}$$

where $\text{Fix}(G)$ is the set of elements of X fixed by all $g \in G$. Because of uniqueness of representation in base p , we know that elements of $\text{Fix}(G)$ are exactly those subsets of X that contains n_i cycles of length p^i . The proof now follows from directly computing that $|\text{Fix}(G)| = \prod_{i=0}^k \binom{m_i}{n_i}$. ■

Theorem 1.9.2. (First and Third Sylow theorem, Wielandt's proof) Let G be a finite group of order $p^m t$ with $\gcd(p, t) = 1$. Let $1 \leq r \leq m$. Then the number n_p of p -subgroup with order p^r satisfies

$$n_p \equiv 1 \pmod{p}$$

Proof. Let X be the set of subset of G with cardinality p^r . Our goal is to find all elements of X that forms a group. Clearly we may define a left G -action on X by setting

$$g \cdot \{x_1, \dots, x_{p^r}\} \triangleq \{gx_1, \dots, gx_{p^r}\}$$

Let Γ be an orbit. If Γ contains a group, then we see that Γ is the left coset space of that group, containing exactly one group and satisfying $|\Gamma| = p^{m-r}t$. If Γ doesn't contain any group, there still exists some $S \in \Gamma$ such that $e \in S$, and clearly we will have $\text{Stab}(S) \subseteq S$. Because S isn't a group, we see $p^r = |S| > o(\text{Stab}(S))$, which by **orbit-stabilizer theorem** implies that $|\Gamma| = [G : \text{Stab}(S)] = p^{m-r+c}t$ for some $c \geq 1$.

In summary, by counting orbit, we have shown that:

$$\binom{p^m t}{p^r} = |X| = n_p p^{m-r} t + l p^{m-r+1} t, \quad \text{for some } l \in \mathbb{N}$$

Let $ut \equiv 1 \pmod{p}$. Recalling that $\binom{p^m t}{p^r}$ has p -power p^{m-r} , it remains to show

$$u \cdot \frac{\binom{p^m t}{p^r}}{p^{m-r}} \equiv 1 \pmod{p}$$

which follows from noting:

$$u \cdot \frac{\binom{p^m t}{p^r}}{p^{m-r}} = ut \cdot \binom{p^m t - 1}{p^r - 1} \equiv \binom{p^m t - 1}{p^r - 1} \equiv 1 \pmod{p}$$

where the last equality follows from **Lucas modulo binomial formula** and the observation that

$$p^m t - 1 = t_k p^{m+k} + \dots + (t_0 - 1)p^m + (p - 1)p^{m-1} + \dots + (p - 1)p^0$$

where $t = t_k p^k + \dots + t_0 p^0$ with $t_0 > 0$. ■

Corollary 1.9.3. (Every p -subgroup is contained by some Sylow p -subgroup) Let G be a finite group and $H \leq G$ a p -group. Then H must be contained by some Sylow p -subgroup of G .

Proof. Consider the conjugacy action $H \longrightarrow \text{Bij}(\text{Syl}_p(G))$. First Sylow theorem and orbit-stabilizer theorem shows that there must be a singleton orbit. Let that singleton be P .

We claim $H \leq P$. Because $\{P\}$ is a singleton orbit of the conjugacy action, we know $H \leq N_G(P)$. Then by second isomorphism theorem, we see that HP is a group such that $HP/P \cong H/H \cap P$. This implies that HP is a p -group. The fact HP contains P forces $P = HP$, which implies $H \leq P$. ■

Theorem 1.9.4. (Counting lemma for p -group) Let G be a p -group acting on a finite set X . Then

$$|X| \equiv |\text{Fix}(G)| \pmod{p}$$

where $\text{Fix}(G) \triangleq \{x \in X : gx = x \text{ for all } g \in G\}$.

Proof. This is a consequence of orbit-stabilizer theorem. ■

Theorem 1.9.5. (Second Sylow theorem) Sylow p -subgroups are conjugated to each other.

Proof. Let H and P be two Sylow p -subgroups of G , and let H acts on left coset space of P by left multiplication. Because P is Sylow, by counting lemma for p -group, we know the number of fixed points gP is nonzero. Let gP be a fixed point. We then see that, as desired, $g^{-1}hg \in P$ for all $h \in H$, since $hgP = gP$. ■

Corollary 1.9.6. (Normalizers of Sylow subgroups Don't satisfy normalizer condition) Let G be a finite group and $P \in \text{Syl}_p(G)$. Then

$$N_G(P) = N_G(N_G(P))$$

Proof. Let $x \in N_G(N_G(P))$. We are required to show $x \in N_G(P)$. By definition, we have

$$xPx^{-1} \leq xN_G(P)x^{-1} = N_G(P)$$

In other words, both P and xPx^{-1} are Sylow p -subgroup of $N_G(P)$. Therefore, by second Sylow theorem, there exists some $y \in N_G(P)$ such that

$$xPx^{-1} = yPy^{-1} = P$$

This then implies $x \in N_G(P)$. ■

Corollary 1.9.7. (Restriction of conjugacy classes onto normalizer of Sylow subgroups, on element of center of Sylow subgroups) Let G be a finite group, $P \in \text{Syl}_p(G)$, and $a, b \in Z(P)$. If a, b are conjugate in G , then they are conjugate in $N_G(P)$.

Proof. Write $b = xax^{-1}$ with $x \in G$. By definition, we have

$$(x^{-1}gx)a(x^{-1}gx)^{-1} = x^{-1}gbg^{-1}x = x^{-1}bx = a, \quad \text{for all } g \in P$$

In other words, $x^{-1}Px \leq C_G(a)$. Then since both P and $x^{-1}Px$ are Sylow p -subgroup of $C_G(a)$, by **second Sylow theorem**, we know there exists $y \in C_G(a)$ such that $P = y^{-1}x^{-1}Pxy$. We now see that $xy \in N_G(P)$ and $(xy)a(xy)^{-1} = b$, as desired. ■

Second Sylow theorem moreover stated that given $n_p > 1$, the conjugacy action $G \rightarrow \text{Sym}(\text{Syl}_p(G)) \cong S_{n_p}$ is nontrivial, and thus injective when G is simple. This is a trick particularly useful to classify finite simple group.

Theorem 1.9.8. (Remaining part of third Sylow theorem) Let G be a finite group, and let n_p be the number of Sylow p -subgroup of G . For all Sylow p -subgroup P of G , we have

$$n_p = [G : N_G(P)]$$

Proof. This is a consequence of **second Sylow theorem** and **orbit stabilizer theorem**, where we note that when G acts on $\text{Syl}_p(G)$ by conjugation we have $\text{Stab}(P) = N_G(P)$. ■

1.10 Old Numbers

Before the first application, we first show that:

Theorem 1.10.1. (\mathbb{Z}_p^\times is cyclic) Let p be prime. Then the unit group \mathbb{Z}_p^\times is cyclic.

Proof. We are required to show the existence of elements of order $p - 1$. Let l be the least common multiple of orders of all elements, so $x^l - 1 \in \mathbb{Z}_p[x]$ has $p - 1$ distinct roots in \mathbb{Z}_p . This implies $l \geq p - 1$. Because the group is abelian, we now see from its primary decomposition form that indeed it is cyclic. \blacksquare

The slickest application of Sylow theorem is without a doubt **Wilson's theorem**.

Theorem 1.10.2. ($a^n \equiv 1 \pmod{p}$ has at most n solution for all n)

Proof. Because $\mathbb{Z}_p^\times \cong C_{p-1}$ is cyclic, we may write $a = x^c$ with $C_{p-1} = \langle x \rangle$, and the proof reduce to finding number of solution to

$$p \mid nc$$

We then see that the solution set is

$$c \in \left\{ \frac{p}{\gcd(p, n)}, \dots, \frac{p(\gcd(p, n) - 1)}{\gcd(p, n)} \right\}$$

Theorem 1.10.3. (Group theoretic side of Wilson's theorem) Let p be prime. Then

$$(p - 1)! \equiv -1 \pmod{p}$$

Proof. Consider the symmetric group S_p . The proof follows from $n_p \equiv 1 \pmod{p}$ and directly counting that $n_p = (p - 2)!$. This is easy to count, since the Sylow p -group of S_p are those generated by a single p -cycle. \blacksquare

Theorem 1.10.4. (Wolstenholme's theorem) Let p be an odd prime, and write

$$H(p - 1) \triangleq 1 + \frac{1}{2} + \dots + \frac{1}{p-1} \in \mathbb{Q}$$

Then

$$H(p - 1) \equiv 0 \pmod{p^2}$$

Proof. Because p is odd, we can group the terms of $H(p - 1)$ by pairs:

$$H(p - 1) = \left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \dots + \left(\frac{1}{\frac{p-1}{2}} + \frac{1}{p-\frac{p-1}{2}}\right)$$

Reduce each pair to a common denominator:

$$H(p-1) = \frac{p}{p-1} + \frac{p}{2(p-2)} + \cdots + \frac{p}{\frac{p-1}{2} \cdot (p - \frac{p-1}{2})}$$

We then can write

$$H(p-1) \triangleq p \cdot \frac{A}{(p-1)!} \quad (1.3)$$

where

$$A \triangleq \frac{(p-1)!}{p-1} + \frac{(p-1)!}{2(p-2)} + \cdots + \frac{(p-1)!}{\frac{p-1}{2} \cdot (p - \frac{p-1}{2})}$$

Since $p \nmid (p-1)!$, equation 1.3 reduce the proof into proving $p \mid A$. We first show that

$\frac{(p-1)!}{a(p-a)} \equiv a^{-2} \pmod{p}$, for $a \in \{1, \dots, p-1\}$, where the power a^{-2} occurs in the cyclic group $\mathbb{Z}_p^\times \cong C_{p-1}$.

Denote $x \triangleq \frac{(p-1)!}{a(p-a)} \in \mathbb{Z}$, so by Wilson's theorem, we have

$$a(p-a)x = (p-1)! \equiv -1 \pmod{p}$$

which gives us

$$a^2x \equiv 1 \pmod{p} \quad (\text{done})$$

We may now write

$$A \equiv 1^{-2} + \cdots + \left(\frac{p-1}{2}\right)^{-2} \pmod{p}$$

Because p is odd, we only have to prove $2A \equiv 0 \pmod{p}$:

$$\begin{aligned} 2A &\equiv 1^{-2} + \cdots + \left(\frac{p-1}{2}\right)^{-2} + 1^{-2} + \cdots + \left(\frac{p-1}{2}\right)^{-2} \\ &\equiv 1^{-2} + \cdots + \left(\frac{p-1}{2}\right)^{-2} + (-1)^{-2} + \cdots + \left(-\frac{p-1}{2}\right)^{-2} \\ &\equiv 1^{-2} + \cdots + \left(\frac{p-1}{2}\right)^{-2} + \left(\frac{p+1}{2}\right)^{-2} + \cdots + (p-1)^{-2} \end{aligned}$$

Because $\mathbb{Z}_p^\times \cong C_{p-1}$ is cyclic, we know the inversion $x \mapsto x^{-1}$ forms a bijection on its non-trivial elements. Therefore, we have

$$\begin{aligned} 2A &\equiv 1^2 + \cdots + (p-1)^2 \\ &= \frac{p(p-1)(2p-1)}{6} \equiv 0 \pmod{p} \end{aligned}$$

■

1.11 Symmetric Groups

Given the **symmetric group** S_n , to define parity, the fastest way is to realize it as the **group of permutation matrix**, and then call those that have determinant 1 **even**, while those that have determinant -1 **odd**. Clearly we have the **alternating group**

$$A_n \triangleq \{g \in S_n : \det(g) = 1\}$$

To see that $[S_n : A_n] = 2$ for all $n \geq 2$, just consider that for any $g \in S_n - A_n$, we have a bijection between A_n and $S_n - A_n$ defined by

$$a \mapsto ag$$

By direct observation, we see that every permutation has a fixed **cycle type**. Because

$$\sigma \circ (a_1, \dots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k))$$

we see that the conjugacy classes of S_n coincides with cycle type classes.

At this point, it is worth mentioning that, given $g \in S_n$, even though we are definitely aware of what its centralizer is, in the sense that given any $h \in S_n$, we can immediately tell whether $h \in C_{S_n}(g)$, but to actually describe $C_{S_n}(g)$ may be annoying. See this [MSE post](#).

Example 1.11.1: Conjugacy classes of A_n are either half a cycle type or all.

Recall that conjugacy classes is just the orbit of conjugacy action, and **orbit-stabilizer theorem** links the orbit Γ of an element x with its stabilizer group by

$$|\Gamma| = [G : \text{Stab}(x)]$$

Now, since we clearly have

$$\text{Stab}_{A_n}(x) = A_n \cap \text{Stab}_{S_n}(x)$$

if $\text{Stab}_{A_n}(x) \leq A_n$, then the conjugacy class of x in A_n is the half of its conjugacy class in S_n . On the other hand, if $\text{Stab}_{A_n}(x) \not\leq A_n$, then since $A_n \text{Stab}_{A_n}(x) = S_n$, by **order formula**, we know $[A_n : \text{Stab}_{A_n}(x)] = [S_n : \text{Stab}_{S_n}(x)]$, which implies that the conjugacy class of x in A_n is the same as in S_n .

Theorem 1.11.2. (generator of S_n) Let $n \geq 2$. Then S_n is generated by transpositions or $\{(1, 2), (1, \dots, n)\}$ or $\{(1, k) \in S_n : 2 \leq k \leq n\}$

Proof. Since in general, we have

$$(1, \dots, k) = (2, 3)(3, 4) \cdots (k-2, k-1)(k-1, k)(1, k)$$

and that in general, we have

$$(i, j) = (1, i)(1, j)(1, i)^{-1}$$

We only have to show $(1, i)$ can be generated by $\{(1, 2), (1, \dots, n)\}$, which is proved via two inductions, with one of them being

$$(k, k+1)(1, k)(k, k+1)^{-1} = (1, k+1)$$

while the other being

$$g(i, i+1)g^{-1} = (i+1, i+2), \quad \text{for all } i \leq n-2$$

where we denote $g \triangleq (1, \dots, n)$. ■

Theorem 1.11.3. (S_n has trivial center for $n \geq 3$) $Z(S_n) = 1$ for all $n \geq 3$.

Proof. Let $\tau \neq e \in S_n$. Because τ is nontrivial, we know $\tau(i) = j$ for some $i \neq j$. Let $\sigma(i) = i$ and $\sigma(j) \neq j$. We now see $\sigma \circ \tau \circ \sigma^{-1} \neq \tau$, as desired. ■

Theorem 1.11.4. (A_n are generated by 3-cycles for $n \geq 3$) Given $n \geq 3$, A_n is generated by 3-cycles.

Proof. Such is proved via induction on n . The base case is clear. We now prove the inductive case. Let $\sigma \in A_n$. By inductive hypothesis, if σ doesn't move n , then σ can be generated by 3-cycles. If σ move n , then because inverse of a 3-cycle is a 3-cycle, and because there exists a 3-cycle τ such that $\tau \circ \sigma$ fix n , we see σ can also be generated by 3-cycles. ■

Theorem 1.11.5. (Commutator subgroup of S_n is A_n for $n \geq 3$) $S'_n = A_n$ for all $n \geq 3$.

Proof. $S'_n \leq A_n$ follows from computation. Because A_n is generated by 3-cycles, to show $S'_n = A_n$, we only have to show S'_n contains all 3-cycles, which follows from computing

$$(a, b, c) = [(a, b), (a, c)]$$

■

Theorem 1.11.6. (Simplicity of A_n)

- (i) A_3 is simple.
- (ii) A_4 is not simple. It contains a characteristic 2-Sylow subgroup, i.e., the set of product of two disjoint transposition.
- (iii) A_n is simple for $n \geq 5$.

Proof. (i): Simplicity of A_3 follows from $o(A_3) = 3$.

(ii): There are three ways to partition $\{1, 2, 3, 4\}$ into 2 disjoint subsets, each of cardinality 2, i.e.,

$$\Pi_1 \triangleq \{\{1, 2\}, \{3, 4\}\} \quad \text{and} \quad \Pi_2 \triangleq \{\{1, 3\}, \{2, 4\}\} \quad \text{and} \quad \Pi_3 \triangleq \{\{1, 4\}, \{2, 3\}\}$$

Clearly, S_4 acts on $\{\Pi_1, \Pi_2, \Pi_3\}$, that is, $S_4 \longrightarrow \text{Sym}(\{\Pi_1, \Pi_2, \Pi_3\}) \cong S_3$. Direct computation now shows that we have a surjective group homomorphism $A_4 \twoheadrightarrow A_3$ with kernel $\{e, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$.

(iii): We first prove A_5 is simple. Because $A_5 \trianglelefteq S_5$ is normal, we know A_5 is the union of the classes of cycle types

$$(1, 2, 3) \quad \text{and} \quad (1, 2)(3, 4) \quad \text{and} \quad (1, 2, 3, 4, 5)$$

Direct computation shows that the first cycle type class has 20 elements, that the second cycle type class has 15 elements, and that the third cycle type class has 24 elements. It now follows from [Lagrange's theorem](#) and from [normal subgroups are unions of conjugacy classes](#) that A_5 has no proper nontrivial subgroups. [\(done\)](#)

Let $N \trianglelefteq A_n$, with $\tau \neq e \in N$ and $n > 5$. We are required to show $N = A_n$. Because $n \geq 5$, clearly for any pair of 3-cycles $\{(a_1, a_2, a_3), (b_1, b_2, b_3)\}$, there exists some $\sigma \in A_n$ such that $(b_1, b_2, b_3) = \sigma \circ (a_1, a_2, a_3) \circ \sigma^{-1}$. In other words, the class of 3-cycles forms a conjugacy class of A_n . This together with normality $N \trianglelefteq A_n$ and the fact that A_n is generated by set of 3-cycles reduce the problem into proving N contains a 3-cycle.

Consider A_5 as a subgroup of A_n that fixes a particular set of $n - 5$ numbers. Then clearly we have $N \cap A_5 \trianglelefteq A_5$. Because A_5 is simple and contains a 3-cycle, we now only have to show $N \cap A_5 > 1$, that is, to show N contains an element that fixes at least $n - 5$ elements.

Let (a_1, a_2, a_3) be a 3-cycle such that $\{\tau(a_1), \tau(a_2), \tau(a_3)\}, \{a_1, a_2, a_3\}$ overlap. We now see $\tau \circ (a_1, a_2, a_3) \circ \tau^{-1} \circ (a_1, a_2, a_3)^{-1} \in N$ is an element that fixes at least $n - 5$ elements. ■

Theorem 1.11.7. (The only proper nontrivial normal subgroup of S_n) For $n \geq 5$, A_n is the only proper nontrivial subgroup of S_n .

Proof. Let N be a proper nontrivial subgroup of S_n . We are required to show $N = A_n$. Because $[S_n : A_n] = 2$, we only have to show $A_n \leq N$. This boils down to showing $N \cap A_n > 1$, since A_n is simple. Assume for a contradiction that $N \cap A_n = 1$. The contradiction $N = 1$ then follows from $A_n = S'_n$ and $Z(S_n) = 1$, since [normal subgroup that disjoint with the commutator subgroup must be contained by the center](#). ■

A group is said to be **complete** if the group has no outer automorphism and centerless. In other words, the natural map $G \rightarrow \text{Inn}(G)$ forms an isomorphism between G and $\text{Aut}(G)$.

Theorem 1.11.8. (Symmetric group is complete for $n \neq 2$ or 6) Let $n \geq 3$. Then S_n is complete for $n \neq 6$.

Proof. Clearly, automorphism group $\text{Aut}(G)$ in general acts on conjugacy classes of G . That is, we have a group homomorphism $\text{Aut}(G) \rightarrow \text{Bij}(\text{cl}(G))$.

Let $\alpha \in \text{Aut}(S_n)$. We first show that $\alpha \in \text{Stab}(\text{cl}((1, 2))) \implies \alpha \in \text{Inn}(S_n)$. Because S_n is generated by $\{(1, k) \in S_n : 2 \leq k \leq n\}$, we only have to show the existence of some $\sigma \in S_n$ such that

$$\alpha((1, k)) = \sigma(1, k)\sigma^{-1} = (\sigma(1), \sigma(k)), \quad \text{for all } k \geq 2$$

Because of the premise, we already know that $\alpha((1, k))$ is a 2-cycle. Our first task is to show that the intersection of the 2-cycles $\{\alpha((1, k)) : k \geq 2\}$ is nonempty. Write

$$\alpha((1, 2)) \triangleq (a, b_2)$$

Because $(1, 2)(1, 3)$ is a 3-cycle, we know $\alpha((1, 2))\alpha((1, 3)) = \alpha((1, 2)(1, 3))$ is of order 3, which is only possible if the 2-cycle $\alpha((1, 3))$ share exactly one element with the 2-cycle (a, b_2) . WLOG, let that element be a , and write

$$\alpha((1, 3)) = (a, b_3), \quad \text{where } b_3 \notin \{a, b_2\}$$

Applying the same logic to $\alpha((1, 4))$, we see that the 2-cycle $\alpha((1, 4))$ must share exactly one element with (a, b_2) and must share exactly one element with (a, b_3) . Therefore, we know $\alpha((1, 4))$ either is of the form

$$(a, b_4), \quad \text{with } b_4 \notin \{a, b_2, b_3\}$$

or is of the form (b_2, b_3) . To see that the latter is impossible, simply compute the order of $(1, 2)(1, 3)(1, 4)$ and $(a, b_2)(a, b_3)(b_2, b_3)$. Now, we apply the same logic to $\alpha((1, 5))$, and this time we can conclude that $\alpha((1, 5))$ must be of the form (a, b_5) with $b_5 \notin \{a, b_2, b_3, b_4\}$. Repeating the process, we then see

$$\sigma(1) \triangleq a \quad \text{and} \quad \sigma(k) \triangleq b_k$$

suffices. (done)

It remains to show every $\alpha \in \text{Aut}(S_n)$ fix the class of transposition. Since α must maps a transposition to an element of order 2. We only have to prove

For $n \neq 6$, the class of transposition has unique cardinality, which is $\binom{n}{2}$, among the conjugacy classes whose elements are of order 2.

Clearly, the conjugacy classes whose elements have order 2 are the classes of products of disjoint 2-cycles. Assume for a contradiction that there really is such a class that has the same cardinality of the class of transposition, says, this class is the class of k product of disjoint 2-cycles. We then would have

$$\binom{n}{2} = \frac{1}{k!} \binom{n}{2} \binom{n-2}{2} \cdots \binom{n-2(k-1)}{2}$$

Noticing the RHS is telescoping, we compute

$$\binom{n-2}{2k-2} = \frac{k!(2^{k-1})}{(2k-2)!} \quad (1.4)$$

Because the RHS now is not an integer for $k \geq 4$, we now have $k \in \{1, 2, 3\}$. Direct computation now shows that for [equation 1.4](#) to hold, we must have $k = 3$ and $n = 6$. [\(done\)](#) ■

We say a group action $G \rightarrow \text{Bij}(X)$ is **transitive** if for each $x, y \in X$, there exists some $g \in G$ such that $g \cdot x = y$. We say a subset $S \subseteq S_n$ is **transitive** if for each $i, j \in \{1, \dots, n\}$ there exists some $s \in S$ such that $s(i) = j$

Theorem 1.11.9. (S_6 is incomplete) S_6 is not complete.

Proof. [Sylow theorems](#) shows that S_5 has 6 Sylow 5-subgroups, and the conjugacy action $\phi : S_5 \rightarrow \text{Bij}(\text{Syl}_5(S_5)) \cong S_6$ is transitive. In particular, the 6 Sylow 5-subgroups are the cyclic subgroups generated by the 6 distinct 5-cycles. Because [A₅ is the only proper nontrivial normal subgroup of S₅](#), we know $\ker(\phi) \in \{1, A_5, S_5\}$. Clearly it isn't S_5 . To see it isn't A_5 , just note that if it is, then its images would have all have order 2, which just isn't the case, as one can observe that

$$(1, 2, 3)^2 \langle (2, 3, 4, 5, 6) \rangle (1, 2, 3)^{-2} \neq \langle (2, 3, 4, 5, 6) \rangle$$

Therefore, the only possibility is that ϕ is injective. Denote $H \triangleq \phi(S_5) \leq S_6$. The fact that ϕ is transitive now means that $H \leq S_6$ is transitive.

Now, consider the left multiplication action $\sigma : S_6 \rightarrow \text{Bij}(S_6 \diagup H)$ on the left coset spaces of H . Because [A₆ is the only proper nontrivial normal subgroup of S₆](#) and $\text{Core}(H) \leq H$, we know σ must be injective. In other words, σ is an automorphism.

Note that all elements of $\sigma(H) \leq S_6$ fix a point, i.e., $H \in S_6 \diagup H$ itself, while $H \leq S_6$, since being transitive, fix no points. If σ is inner, this is clearly impossible, thus the proof. ■

1.12 Analysis of some finite group

Corollary 1.12.1. (Classification of semidirect product of $C_q \rtimes C_p$ with $p \mid q - 1$)

Let p, q be two primes. If $p \nmid q - 1$, then the semidirect product $C_q \rtimes C_p$ must be a direct product. If $p \mid q - 1$, then the semidirect product $C_q \rtimes C_p$ has exactly two non-isomorphic meanings.

Proof. Clearly, we have

$$\text{Aut}(C_q) \cong \mathbb{Z}_q^\times \cong C_{q-1}$$

Let x and y each be the generators of C_p and C_{q-1} . Let $x \mapsto y^c$ defines a group homomorphism. Because $x^p = e$, we must have $q - 1 \mid pc$. Therefore, if $p \nmid q - 1$, the only action $\varphi \in \text{Hom}(C_p, \text{Aut}(C_q))$ is trivial.

Suppose $p \mid q - 1$. By the [universal property of presentation](#), we now see that the possible group homomorphism $\text{Hom}(C_p, C_{q-1})$ are exactly $x \mapsto y^{\frac{q-1}{p}d}$ for $d \in \mathbb{Z}$. Let φ_d and $\varphi : \mathbb{Z}_p \rightarrow \mathbb{Z}_{q-1}$ denote $x \mapsto y^{\frac{q-1}{p}d}$ and $x \mapsto y^{\frac{q-1}{p}}$ with $d \neq 0$. Clearly we have

$$\varphi_d = \varphi \circ \psi$$

where $\psi \in \text{Aut}(C_p)$ is defined by $\psi(x) \triangleq x^d$. Because [two actions differs by a automorphism in front induces the same semidirect product](#), we have shown that there can be at most two distinct semidirect product $C_q \rtimes C_p$.

To see that they are distinct, we claim that the nontrivial one is not abelian, which follows from noting that

$$(n, e) \cdot (e, h) = (n, h) \quad \text{and} \quad (e, h) \cdot (n, e) = (\varphi_h(n), h)$$

in general. ■

We now have enough tools to state and prove our result. Note that [normal Sylow subgroups are clearly characteristic](#), so we will use the word "characteristic Sylow subgroup" instead.

Corollary 1.12.2. (Analysis of finite group of fixed prime structure) Let p, q, r be three distinct prime.

- (i) Groups of order pq , where $p < q$, is always a semidirect product $C_q \rtimes C_p$, [and we know there are at most 2 of them](#), depending on whether $p \mid q - 1$.
- (ii) Groups of order p^2q has a characteristic Sylow subgroup.
- (iii) Groups of order p^3q has a characteristic Sylow subgroup, given that $(p, q) \neq (2, 3)$.

- (iv) Groups of order pqr has a characteristic r -Sylow subgroup and a normal subgroup of order qr , where $p < q < r$. If $q \nmid r - 1$, then groups of order pqr moreover has a characteristic q -Sylow subgroup.
- (v) Simple groups of order $p^a m$, where $a, m \in \mathbb{N}$ satisfies $p \nmid m > 1$, must satisfies $o(G) \mid n_p!$.

Proof. (i): Clearly $n_q = 1$. Let $P \in \text{Syl}_p(G)$. Clearly $P \cap Q = 1$. This by **order formula** implies $PQ = G$. The rest then follows from **recognition theorem for inner semidirect product**.

(ii): If $p > q$, then clearly n_p can only be 1. If $p < q$, then we must have $n_q \in \{1, p^2\}$. If $n_q = 1$, then we are done. If not, then from $n_q \equiv 1 \pmod{q}$, we see $q = p + 1$, which can only happens if $q = 3$ and $p = 2$. We claim that in such case, i.e., $o(G) = 12$, then either $n_3 = 1$ or $G \cong A_4$, which contains a characteristic 2-Sylow subgroup.

If $n_3 = 4$, then for any $P \in \text{Syl}_3(G)$, we have $N_G(P) = P$, since $4 = n_3 = [G : N_G(P)]$. Clearly, the conjugacy action $G \rightarrow \text{Bij}(\text{Syl}_3(G))$ has kernel contained by $N_G(P) = P$. This by non-normality of P and $o(P) = 3$ implies the conjugacy action $G \hookrightarrow \text{Bij}(\text{Syl}_3(G)) \cong S_4$ is injective. Note that G has 8 elements of order 3. Since A_4 is the only subgroup of S_4 with order 12 and 8 elements of order 3, we now see $G \cong A_4$.¹ The proof then follows from recalling that **A_4 has a characteristic 2-Sylow subgroup**.

(iii): Suppose G has no characteristic Sylow subgroup. We are required to show $(p, q) = (2, 3)$, which will follows from showing $q = p + 1$.

Now, since G has no characteristic Sylow subgroup, we know $n_p = q$, which by $n_p \equiv 1 \pmod{p}$ implies $p < q$, which further implies $n_q \in \{p^2, p^3\}$. Counting now give us $n_q = p^2$, which by $n_q \equiv 1 \pmod{p}$ and $p < q$ implies $q = p + 1$.

(iv): We first show $n_r = 1$. By counting, we know $1 \in \{n_p, n_q, n_r\}$. If n_p and n_q are both > 1 , then we are done. We now show that $n_p = 1 \implies n_r = 1$, and the proof for $n_q = 1 \implies n_r = 1$ is similar.

Denote P the characteristic Sylow p -subgroup of G . Applying (i) on $\frac{G}{P}$, we see the existence of $H \trianglelefteq G$ with order pr containing P . Applying (i) on H , we see the existence of $K \text{ char } H$ with $o(K) = r$. It then follows from **transitive property of characteristic subgroup** that K is the characteristic r -Sylow subgroup of G we are looking for.

¹One may argue that the original assertion that groups of order p^2q all have a normal Sylow subgroup holds true, but we don't know whether it is possible $n_3 = 4$. Such is possible, since A_4 really makes $n_3 = 4$.

To see G has a normal subgroup of order qr , just apply (i) on G/K . Denote that normal subgroup by $T \trianglelefteq G$. If $q \nmid r - 1$, then again by (i), there exists $L \text{char } T$ with $o(L) = r$. Because of the **transitive property of characteristic subgroup**, we now see that L is the characteristic r -Sylow subgroup of G we are looking for.

(v): Let $P \in \text{Syl}_p(G)$. Non-normality of P together with **second Sylow theorem** implies that the conjugacy action $G \longrightarrow \text{Bij}(\text{Syl}_p(G)) \cong S_{n_p}$ is nontrivial. Simplicity of G then forces the action to be injective, as desired. \blacksquare

Corollary 1.12.3. (i) There are exactly four groups of order 30. Precisely, they are the four possible semidirect product of $C_{15} \rtimes C_2$:

$$\langle x, y \mid x^{15} = y^2 = e, yxy^{-1} = x^n \rangle \quad \text{where } n \in \{1, 4, 11, -1\}$$

- (ii) The 11-sylow subgroup of groups of order $231 = 3 \cdot 7 \cdot 11$ lies in the centers.
- (iii) The 7-sylow subgroup of groups of order $385 = 5 \cdot 7 \cdot 11$ lies in the centers.
- (iv) No group of order $132 = 2^2 \cdot 3 \cdot 11$ is simple.
- (v) Groups of order $108 = 2^2 \cdot 3^3$ either has a normal subgroup of order 9, or has a normal subgroup of order 27.
- (vi) Simple groups of order 60 must be A_5 .

Proof. (i): Since $30 = 2 \cdot 3 \cdot 5$, we know G has a normal subgroup N of order 15. This allows us to write $G \cong N \rtimes C_2$. Since the only group of order 15 is C_{15} , we now see G must be of the form:

$$G \cong C_{15} \rtimes C_2$$

To classify the possible semidirect product, one first compute $\text{Aut}(C_{15}) \cong C_4 \times C_2$,² which show us that $\text{Hom}(C_2, \text{Aut}(C_{15}))$ has only 4 elements, which can be easily checked to be $y \mapsto (x \mapsto x^n)$, where $C_2 = \langle y \rangle$, $C_{15} = \langle x \rangle$ and $n \in \{1, 4, 11, 14\}$. To see that these four possibly distinct groups are really pairwise distinct, one can use **their presentation** to easily compute that the number of elements of order 2 they contain are indeed pairwise different.

(ii): Let R be the characteristic 11-sylow subgroup of G . We are required to prove $C_G(R) = G$. Because $C_G(R)$ is exactly the kernel of the conjugacy action $G = N_G(R) \longrightarrow \text{Aut}(R)$, by **first isomorphism theorem**, we have an injection $G/C_G(R) \hookrightarrow \text{Aut}(R) \cong C_{10}$. The

²This can proved by noting $\text{Aut}(C_{15}) \cong \mathbb{Z}_{15}^\times \cong (\mathbb{Z}_5 \times \mathbb{Z}_3)^\times \cong \mathbb{Z}_5^\times \times \mathbb{Z}_3^\times \cong C_4 \times C_2$. Of course, one can also just brute force the computation.

proof then follows from counting order.

(iii): The proof is similar to that of (ii).

(iv): If G is simple, then $n_2 \geq 3, n_3 \geq 4$, and $n_{11} \geq 12$, which is impossible by counting.

(v): Let $n_3 = 4$. We are required to prove the existence of a normal subgroup of order 9. Let $P \in \text{Syl}_3(G)$. Consider the left multiplicative action $G \rightarrow \text{Bij}(G/P) \cong S_4$ on the left cosets space G/P . The proof then follows from comparing orders and the observation that the kernel must lies in P .

(vi): Because **the only proper nontrivial normal subgroup of S_5 is A_5** and because $o(G) = 60$, to show $G \cong A_5$, we only have to establish an injective group homomorphism $G \hookrightarrow S_5$.

Let $P \in \text{Syl}_2(G)$. By simplicity of G , we always have an injective group homomorphism $G \hookrightarrow \text{Sym}(G/N_G(P)) \cong S_{[G:N_G(P)]}$, the left multiplicative action on the left coset space of $N_G(P)$. Since **$[G : N_G(P)] = n_2$** , it remains to show $n_2 = 5$.

Because G is simple and $60 \nmid 4!$, from $G/\text{Core}(H) \hookrightarrow \text{Bij}(G/H)$, where G/H is the left coset space of H , we know that G can not have proper subgroup with index < 5 . This with **$[G : N_G(P)] = n_2$** in particular implies $n_2 \geq 5$. Because G is simple, we now have $n_2 \in \{5, 15\}$.

Assume $n_2 = 15$ for a contradiction. Because $n_5 = 6$, by counting, we see that there must be a pair of distinct 2-Sylow subgroup $Q, R \in \text{Syl}_2(G)$ such that $o(Q \cap R) = 2$. Let $M \triangleq N_G(Q \cap R)$. Since Q and R , of order 4, is abelian, we know $Q, R \leq M$, which implies $4 \mid o(M)$, that is, $o(M) \in \{4, 12, 20, 60\}$. Simplicity of G forces $o(M) \neq 60$, $Q \neq R$ forces $o(M) \neq 4$, and the fact that G has no proper subgroup of index < 5 forces $o(M) \neq 20$. Therefore, we must have $o(M) = 12$.

By simplicity of G , we have an injective group homomorphism $G \hookrightarrow \text{Sym}(G/M) \cong S_5$, the left multiplicative action on the left coset space of M . Again, because **the only proper nontrivial normal subgroup of S_5 is A_5** and because $o(G) = 60$, this implies $G \cong A_5$, a contradiction, since $n_2(A_5) = 5$. ■

1.13 Nilpotency and Solvability

A **normal series** of a group G is a finite chain of subgroups

$$1 \trianglelefteq \cdots \trianglelefteq A_{n-1} \trianglelefteq A_n \trianglelefteq A_{n+1} \trianglelefteq \cdots \trianglelefteq G$$

A **composition series** is a maximal normal series.

Example 1.13.1: Subgroups in normal series need not all be normal

Consider

$$\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_4 \triangleq \langle r, s \mid r^4 = s^2 = e, srs^{-1} = r^{-1} \rangle$$

Clearly $\langle s \rangle$ is not normal in D_4 .

Equivalent Definition 1.13.2. (Solvable groups) We say a group G is **solvable** if any of the followings holds true:

- (i) G admits a finite normal series whose factor groups are all abelian.
- (ii) The **derived series**

$$\cdots \trianglelefteq G^{(2)} \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} \triangleq G, \quad \text{where } G^{(k+1)} \triangleq (G^{(k)})'$$

reach to 1.

Proof. Routine. Note that if $1 = G_n \trianglelefteq \cdots \trianglelefteq G_0 = G$ is a normal series whose factor groups are all abelian, then clearly we have $G^{(k)} \leq G_k$ ■

Clearly, solvable groups are closed under **group extension**. Given a short exact sequence of groups

$$1 \longrightarrow A \longrightarrow G \longrightarrow B \longrightarrow 1$$

If A and B are both solvable, then G is solvable. Conversely, let G be solvable and $H \leq G$. Then clearly

$$1 = G^{(n)} \cap H \trianglelefteq \cdots \trianglelefteq G^{(1)} \cap H \trianglelefteq H$$

is normal series whose factor groups are all abelian. Because of such, we say solvable groups are **subgroup-closed**. Let $N \trianglelefteq G$ and $\pi : G \rightarrow G/N$ be the natural projection. Since $\pi(G^{(k)})$ is the derived series of G/N , we see that solvable groups are also **quotient-closed**. Since taking direct product and taking commutator subgroup commutes, we moreover have

$$\left(\prod_{i=1}^n G_i \right)^{(k)} = \prod_{i=1}^n G_i^{(k)}$$

Therefore, solvable groups are also **finite direct product-closed**.

Equivalent Definition 1.13.3. (Finite solvable groups) A finite group G is solvable if and only if it admits a composition series whose factor group are all cyclic of prime order.

Proof. Routine. ■

Equivalent Definition 1.13.4. (Nilpotent groups) We call a group G **nilpotent** if G admits a **central series**, a normal series:

$$1 = G_0 \trianglelefteq \cdots \trianglelefteq G_n = G$$

such that

$$[G, G_k] \leq G_{k-1}, \quad \text{for all } k \in \{1, \dots, n\}$$

Clearly, all G_k are normal in G . Given a series of normal subgroups, we then clearly see that it is central if and only if

$$\frac{G_k}{G_{k-1}} \leq Z\left(\frac{G}{G_{k-1}}\right), \quad \text{for all } k \in \{1, \dots, n\}$$

A group is nilpotent if and only if its **lower central series**:

$$\cdots \trianglelefteq G_{(2)} \trianglelefteq G_{(1)} \trianglelefteq G_{(0)} \triangleq G, \quad \text{where } G_{(k)} \triangleq [G, G_{(k-1)}] \text{ for all } k \in \mathbb{N}$$

reach to 1. A group is nilpotent if and only if its **upper central series**:

$$1 \triangleq Z_{(0)} \trianglelefteq Z_{(1)} \trianglelefteq Z_{(2)} \trianglelefteq \cdots, \quad \text{where } \frac{Z_{(k+1)}}{Z_{(k)}} \triangleq Z\left(\frac{G}{Z_{(k)}}\right) \text{ for all } k \in \mathbb{N}$$

reach to G . The central series $1 = G_0 \triangleleft \cdots \triangleleft G_n = G$ is said to have **length** n . The **nilpotency class** of a nilpotent group is the smallest length of its central series. If a group is nilpotent, then both its lower and upper central series has length of its nilpotent class.

Proof. Clearly both lower and upper central series are central by definition. Suppose a central series

$$1 = G_0 \trianglelefteq \cdots \trianglelefteq G_n = G$$

exists. To see the lower central series reach to 1 with smallest length, use induction to show $G_{(k)} \leq G_{n-k}$ for all k . (thus the name **fastest descending series**). To see the upper central series reach to G with smallest length, use induction to show $G_k \leq Z_{(k)}$ for all k . (thus the name **fastest ascending series**) ■

Again, one can check that central series are closed under taking intersection with a subgroup, under taking finite direct product and under surjective group homomorphism, so nilpotency is also subgroup-closed, quotient-closed and finite-direct-product-closed.

Theorem 1.13.5. (Proper subgroups of nilpotent groups satisfy normalizer condition) If G is nilpotent, then any $H < G$ satisfies normalizer condition.

Proof. Note that if H doesn't contain $Z(G)$, then the elements of $Z(G)$ that lies outside H complete the proof, so we only have to consider the case $Z(G) \leq H$. ■

This is proved by induction on nilpotency class n of G . The base case $n = 1$ is clear. The inductive case follows from [third isomorphism theorem for groups](#) and the observation $G/Z(G)$ has the nilpotent class one smaller than that of G . ■

Theorem 1.13.6. (Properties of p -groups)

(i) p -groups are nilpotent, and thus solvable.

Let G be a finite p -group. Since [\$p\$ -groups has nontrivial centers](#), we see that the upper central series of G must reach to G . Therefore p -groups are nilpotent.

Equivalent Definition 1.13.7. (Finite nilpotent group) Let G be a finite group. The followings are equivalent:

(i) G is nilpotent.

(ii) Proper subgroups of G satisfies normalizer condition.

(iii) Sylow subgroups of G are all normal.

(iv) G is the internal direct product of its Sylow subgroups.

Proof. (i) \implies (ii): This is done via induction on $o(G)$. Let $H < G$. If $Z(G)$ isn't contained by H , then since $H \cdot Z(G)$ normalize H , we see H satisfies normalizer condition. Let $Z(G) \leq H$. If G is abelian, then the proof is trivial, so suppose G isn't abelian, and therefore $o(G/Z(G)) < o(G)$. Then by inductive hypothesis, $\frac{H}{Z(G)} \leq \frac{G}{Z(G)}$ satisfies normalizer condition. The proof then follows from pullback.

(ii) \implies (iii): If G is a p -group, then the proof is trivial. Let G not be a p -group and let $P \in \text{Syl}_p(G)$. To see P is normal, just observe that since [normalizers of Sylow subgroups don't satisfy normalizer condition](#), the normalizer of P must be G .

(iii) \implies (iv): This follows from [the definition of finite internal direct product](#).

(iv) \implies (i): This follows from the fact that [\$p\$ -groups and nilpotent](#) and that nilpotency is closed under taking finite direct product. ■

Example 1.13.8: A solvable group that isn't nilpotent

Consider S_3 . Because S_3 is the extension of C_3 and C_2 :

$$1 \longrightarrow A_3 \longrightarrow S_3 \longrightarrow C_2 \longrightarrow 1$$

We know S_3 is solvable. However, it clearly has 3 Sylow 2-subgroups, so we know S_3 isn't nilpotent.

1.14 p -group

Example 1.14.1: Criterion for abelianess

If $G/Z(G)$ is cyclic, then for all $a, b \in G$, we may write $a = g^n z_1$ and $b = g^m z_2$ to see that

$$ab = g^n z_1 g^m z_2 = g^{n+m} z_1 z_2 = ba$$

and concludes that G is abelian. Such criteria can not be weaken to the case $G/Z(G)$ cyclic. For example, consider D_4 . Because $o(Z(D_4)) = 2$, we know $D_4/Z(D_4)$ is abelian, but D_4 isn't.

Theorem 1.14.2. (Property of p -groups)

- (i) Groups of order p^2 are all abelian.
- (ii) Groups of order p^3 , if not abelian, satisfies $o(Z(G)) = p$ and $Z(G) = G'$

Proof. (i): This follows from our criteria for abelianess and the fact that finite p -groups have nontrivial centers.

(ii): $o(Z(G)) = p$ also follows from our criteria for abelianess and the fact that finite p -groups have nontrivial centers. Now, because G is non-abelian and because $G/Z(G)$ is abelian, we see that we must have $G' = Z(G)$. ■

Corollary 1.14.3. (Normal subgroups of finite p -groups intersect with centers)
Let $1 < N \trianglelefteq P$ where P is a finite p -group. Then $N \cap Z(P) > 1$.

Proof. Let P acts on N by conjugation. By our counting lemma for p -group, we have

$$0 \equiv o(N) \equiv |\{n \in N : gng^{-1} = n \text{ for all } g \in P\}| \pmod{p}$$

Noting that the latter set $= N \cap Z(P)$, we now see $N \cap Z(P) > 1$. ■

1.15 Simplicity of $\mathrm{PSL}_n(\mathbb{F})$

Abstract

This section shows that for $n \geq 3$, $\mathrm{PSL}_n(\mathbb{F})$ is simple, and for $n = 2$, $\mathrm{PSL}_n(\mathbb{F})$ is simple if \mathbb{F} has ≥ 4 elements.

An action $\varphi : G \rightarrow \mathrm{Bij}(X)$ is called **transitive** if for all $x, y \in X$, there exist some g that takes x to y . We say φ is **doubly transitive** if the naturally induced action on $G \rightarrow \mathrm{Bij}(X^2 - D)$, where $D \triangleq \{(x, x) \in X^2 : x \in X\}$ is the diagonal, is transitive.

Theorem 1.15.1. (Property of doubly transitive action) Let $\varphi : G \rightarrow \mathrm{Bij}(X)$ be a doubly transitive action and $|X| \geq 2$. Then

- (i) $\mathrm{Stab}(x) < G$ is maximal for all $x \in X$.
- (ii) For all $N \trianglelefteq G$, the action $\varphi|_N : N \rightarrow \mathrm{Bij}(X)$ is either trivial or transitive.

Proof. (i): Denote $H \triangleq \mathrm{Stab}(x)$. We first show that:

$$G = H \cup HgH, \quad \text{for all } g \in G - H, \text{ where } HgH \triangleq \{hg\tilde{h} \in G : h, \tilde{h} \in H\}$$

Fix $g \in G - H$. Let $\tilde{g} \in G - H$. We are required to show $\tilde{g} \in HgH$. Because $g, \tilde{g} \notin H$, doubly transitivity of φ implies the existence of some element in G that takes (x, gx) to $(x, \tilde{g}x)$. Such element is clearly in H . One then can check $\tilde{g} \in hgH$, where h is the element that takes gx to $\tilde{g}x$. (done)

$H < G$ is clear. To see that H is maximal, just observe that if a subgroup K of G properly contains H , then the subgroup contains $H \cup HgH = G$, where $g \in K - H$.

(ii): Suppose the action $N \rightarrow \mathrm{Bij}(X)$ is nontrivial. We are required to show it is transitive. Fix $x \neq y \in X$. Because N is nontrivial, we know there exists some $z \in X$ and $n \in N$ such that $nz \neq z$. Doubly transitivity of φ then implies the existence of some $g \in G$ such that $g(z, nz) = (x, y)$. The proof then follows from checking that gng^{-1} takes x to y . ■

Theorem 1.15.2. (Iwasawa criterion) Let $\varphi : G \rightarrow \mathrm{Bij}(X)$ be a doubly transitive action. If

- (i) G is **perfect**, i.e., $G^{(1)} = G$.
- (ii) There exists some $x \in X$ whose stabilizer subgroup has an abelian normal subgroup U such that $\bigcup_{g \in G} gUg^{-1}$ generates G .

then $G/\ker \varphi$ is simple.

Proof. Denote $K \triangleq \ker \varphi$ and $H \triangleq \text{Stab}(x)$. Let N be a normal subgroup of G that contains K . We are required to prove $N = K$ or G . **Maximality of H** splits the proof into two cases $NH = H$ or $NH = G$. We will prove that the case $NH = H$ leads to $N = K$, and the case $NH = G$ leads to $N = G$.

Case ($NH = H$): In such case, clearly $N \leq H$, and therefore N acts trivially on X , which implies $N \leq K$, as desired.

Case ($NH = G$): In such case, normality $U \trianglelefteq H$ implies $NU \trianglelefteq G$. This then implies that $gUg^{-1} \leq g(NU)g^{-1} = NU$ for all $g \in G$. Therefore by premise, $NU = G$. Second isomorphism theorem then shows that $G/N \cong NU/N \cong U/N \cap U$ is abelian, which by perfectness of G implies that $N = G$. ■

Let \mathbb{F} be a field. The **general linear group** $\text{GL}_n(\mathbb{F})$ is the group of n -by- n \mathbb{F} -valued matrices that has nonzero determinant. Clearly, $\text{GL}_n(\mathbb{F})$ acts naturally on the affine space $\mathbb{A}^n(\mathbb{F})$, and moreover on the projective space $\mathbb{P}^{n-1}(\mathbb{F})$.

Theorem 1.15.3. (Kernel of general linear group acting on projective space) The kernel of the group action $\text{GL}_n(\mathbb{F}) \rightarrow \text{Bij}(\mathbb{P}^{n-1})$ is exactly the group of scalar diagonal:

$$\{cI \in \text{GL}_n(\mathbb{F}) : c \in \mathbb{F}^\times\}$$

coinciding with its center $Z(\text{GL}_n(\mathbb{F}))$.

Proof. We first show that the group of the scalar diagonal = the kernel. Clearly the group of scalar transformations lies in the kernel. To see the converse inclusion holds, let A maps

$$v \mapsto \lambda v \quad \text{and} \quad w \mapsto \mu w$$

and observes that if $\lambda \neq \mu$, then A doesn't fix $[v + w]$.

It remains to show the center = the group of scalar diagonal. Again, clearly the group of scalar diagonal lies in the center. Let $A \in Z(\text{GL}_n(\mathbb{F}))$. To prove that A is scalar diagonal, one simply consider $E_{i,j} \triangleq I_n + e_{i,j}$, where $e_{i,j} \in M_n(\mathbb{F})$ is the **matrix unit**. ■

Because the group action $\text{GL}_n(\mathbb{F}) \rightarrow \text{Bij}(\mathbb{P}^{n-1})$ has such kernel, we define the **projective general linear group** $\text{PGL}_n(\mathbb{F})$ to be the quotient group

$$\text{PGL}_n(\mathbb{F}) \triangleq \text{GL}_n(\mathbb{F}) / \{cI_n \in \text{GL}_n(\mathbb{F}) : c \in \mathbb{F}^\times\}$$

The **special linear group** $\text{SL}_n(\mathbb{F}) \leq \text{GL}_n(\mathbb{F})$ is the subgroup whose elements has determinant 1, and the kernel of its action on \mathbb{P}^{n-1} is clearly $\{cI_n \in \text{SL}_n(\mathbb{F}) : c^n = 1\}$, so we define the **projective special linear group** $\text{PSL}_n(\mathbb{F})$ to be

$$\text{PSL}_n(\mathbb{F}) \triangleq \text{SL}_n(\mathbb{F}) / \{cI_n \in \text{SL}_n(\mathbb{F}) : c^n = 1\}$$

Theorem 1.15.4. (Basic properties of special linear group) Let \mathbb{F} be an arbitrary field and $n \geq 2$. Then,

- (i) $\mathrm{SL}_n(\mathbb{F})$ acts doubly transitive on \mathbb{P}^{n-1} .
- (ii) $\mathrm{SL}_n(\mathbb{F})$ has center $\{cI_n \in \mathrm{SL}_n(\mathbb{F}) : c^n = 1\}$, thus equal to the kernel of its action on \mathbb{P}^{n-1} .

Proof. (i): Let $([v_1], [v_2]), ([w_1], [w_2]) \in (\mathbb{P}^{n-1})^2$ be two pairs off the diagonal. We are required to show the existence of some $\widehat{L} \in \mathrm{SL}_n(\mathbb{F})$ that send $[v_1]$ to $[w_1]$ and $[w_1]$ to $[w_2]$. The proof then follows from extending them to two bases $\{v_1, \dots, v_n\}, \{w_1, \dots, w_n\}$ for \mathbb{F}^n and setting $\widehat{L}(v_i) \triangleq c_i w_i$ with

$$\det(PQ^{-1}) \cdot \left(\prod_{i=1}^n c_i \right) = 1$$

where $Q, P \in \mathrm{GL}_n(\mathbb{F})$ are respectively the matrix whose i -th column is v_i, w_i . (ii): The proof that computes $Z(\mathrm{GL}_n(\mathbb{F}))$ applies here, since $E_{i,j} \in \mathrm{SL}_n(\mathbb{F})$. ■

To apply Iwasawa criterion on the projective special linear groups $\mathrm{PSL}_n(\mathbb{F})$, it remains to show

- (I) $\mathrm{SL}_n(\mathbb{F})$ is perfect.
- (II) There exists some $x \in \mathbb{P}^{n-1}$ whose stabilizer subgroup $H \leq \mathrm{SL}_n(\mathbb{F})$ has an abelian normal subgroup U such that $\bigcup_{g \in G} gUg^{-1}$ generates G .

The reasons why simplicity of $\mathrm{SL}_2(\mathbb{F})$ requires \mathbb{F} to have ≥ 4 elements lies in the fact (I) may fails to be true if \mathbb{F} has ≤ 3 elements.

Example 1.15.5: $\mathrm{SL}_2(\mathbb{F}_2)$ and $\mathrm{SL}_2(\mathbb{F}_3)$ are not perfect

By counting, we know

$$o(\mathrm{GL}_n(\mathbb{F}_p)) = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$$

Since determinant function is a surjective group homomorphism from $\mathrm{GL}_n(\mathbb{F}_p)$ to \mathbb{F}_p^\times with kernel $\mathrm{SL}_n(\mathbb{F}_p)$, we know

$$o(\mathrm{SL}_n(\mathbb{F}_p)) = \frac{1}{p-1} \cdot (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$$

In particular, $\mathrm{SL}_2(\mathbb{F}_2)$ and $\mathrm{SL}_2(\mathbb{F}_3)$ has order 6 and 24. Now, clearly $\mathrm{SL}_2(\mathbb{F}_2)$ has a faithful action on:

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

So by comparing order, we know $\mathrm{SL}_2(\mathbb{F}_2) \cong S_3$. Therefore non-perfectness of $\mathrm{SL}_2(\mathbb{F}_2)$ then follows from $S_3^{(1)} = A_3$. In fact, since $\mathrm{PSL}_2(\mathbb{F}_2) \cong \mathrm{SL}_2(\mathbb{F}_2)$, we have shown that $\mathrm{PSL}_2(\mathbb{F}_2)$ is non-simple.

Now, recall that $\mathrm{PSL}_2(\mathbb{F}_3)$ acts faithfully on $\mathbb{P}^1(\mathbb{F}_3)$, which has $\frac{3^2-1}{3-1} = 4$ points, so we have an injective group homomorphism $\mathrm{PSL}_2(\mathbb{F}_3) \hookrightarrow S_4$. Computing that $o(\mathrm{PSL}_2(\mathbb{F}_3)) = 12$, we see that since the only index 2 subgroup of S_4 is A_4 , we have the isomorphism $\mathrm{PSL}_2(\mathbb{F}_3) \cong A_4$, which is non-simple.

Regardless of whether $n > 2$, the second condition is proved using the same H and U . We pick $x \triangleq [1 : 0 : \dots : 0]$, and therefore

$$H = \left\{ \begin{pmatrix} a & * \\ \mathbf{0} & M \end{pmatrix} : a \in \mathbb{F}^\times \text{ and } M \in \mathrm{GL}_{n-1}(\mathbb{F}) \right\}$$

and since:

$$\begin{pmatrix} a & * \\ \mathbf{0} & M \end{pmatrix} \begin{pmatrix} b & * \\ \mathbf{0} & J \end{pmatrix} = \begin{pmatrix} ab & * \\ \mathbf{0} & MJ \end{pmatrix}$$

We know

$$U \triangleq \left\{ \begin{pmatrix} 1 & * \\ \mathbf{0} & I_{n-1} \end{pmatrix} \right\} \text{ is normal in } H.$$

U is abelian since

$$\begin{pmatrix} 1 & \mathbf{v} \\ \mathbf{0} & I_{n-1} \end{pmatrix} \begin{pmatrix} 1 & \mathbf{w} \\ \mathbf{0} & I_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{v} + \mathbf{w} \\ \mathbf{0} & I_{n-1} \end{pmatrix}$$

Interestingly, both (I) and (II) requires boring computations within $\mathrm{SL}_n(\mathbb{F})$.

Theorem 1.15.6. (One dimensional projective special linear group is simple over field that has ≥ 4 elements) If \mathbb{F} has ≥ 4 elements, then $\mathrm{PSL}_2(\mathbb{F})$ is simple.

Proof. (II): Since

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ -\lambda & 1 \end{pmatrix}$$

We know the group of the lower triangular matrices:

$$\left\{ \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \right\}$$

52

is a conjugate of U . We prove that $\mathrm{SL}_2(\mathbb{F})$ is generated by U and the lower triangular matrices. To see such, just observe that if any of b, c is nonzero, then by transposing the matrix if necessary, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (d-1)b^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (a-1)b^{-1} & 1 \end{pmatrix}, \quad \text{where } b \neq 0$$

and if both of them are zero, then $d = a^{-1}$ and we have

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ (1-a)a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix}$$

(I): Compute

$$\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & b(a^2 - 1) \\ 0 & 1 \end{pmatrix}$$

Because \mathbb{F} has ≥ 4 elements, we know that there exists some $a \in \mathbb{F}^\times$ such that $a^2 \neq 1$ (Consider $x^2 - 1 \in \mathbb{F}[x]$). Fix such a . We then see that $U \leq \mathrm{SL}_2(\mathbb{F})^{(1)}$ by letting b run through \mathbb{F} . Normality of $\mathrm{SL}_2(\mathbb{F})^{(1)}$ and (II) then implies $\mathrm{SL}_2(\mathbb{F})^{(1)} = \mathrm{SL}_2(\mathbb{F})$ ■

Theorem 1.15.7. (≥ 2 dimensional projective special linear groups are all simple) Let $n \geq 3$. Then we have:

- (i) $I_n + \lambda E_{ij}$ is conjugate to $I_n + E_{12}$ in $\mathrm{SL}_n(\mathbb{F})$, for all $\lambda \in \mathbb{F}^\times$.
- (ii) $\{I_n + \lambda E_{ij}\}$ generates $\mathrm{SL}_n(\mathbb{F})$.

Since $I_n + E_{12} \in U$, together they implies (II), and using them we may prove (I).

Proof. (i): ■

1.16 Future Direction

A subgroup $H \leq G$ of a finite group G is called a **Hall subgroup** if its order is coprime to its index.

Theorem 1.16.1. (Burnside's $p^a q^b$ theorem) If $o(G) = p^a q^b$ for some primes p, q , then G is solvable.

Theorem 1.16.2. (Schur-Zassenhaus theorem) Let G be a finite group and $N \trianglelefteq G$ be Hall. Then the short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

right splits, and thus G must be a semidirect product of $N \rtimes (G/N)$.

Theorem 1.16.3. (Thompson's fixed-point-free theorem) Let G be a finite group that admits a fixed-point-free automorphism of prime order. Then G is nilpotent.

Theorem 1.16.4. (Schreier theorem) Outer automorphism group of finite simple groups are solvable.

Theorem 1.16.5. (Feit-Thompson theorem) Finite groups of odd order are solvable.

1.17 Recreational Exercises

Question 1: Wording problem

Let $n \in \mathbb{Z}$ satisfies

$$(ab)^n = a^n b^n \quad \text{and} \quad (ab)^{n-1} = a^{n-1} b^{n-1} \quad \text{and} \quad (ab)^{n+1} = a^{n+1} b^{n+1}$$

for all $a, b \in G$. Show that G is abelian.

Proof.

$$\begin{aligned} a^n b^n ab &= (ab)^n(ab) = (ab)^{n+1} = a^{n+1} b^{n+1} \\ \implies b^n a &= ab^n \\ \implies (a^{n-1} b^{n-1})ba &= a^n b^n = (a^{n-1} b^{n-1})ab \\ \implies ba &= ab \end{aligned}$$

■

Question 2: Wording problem with finite group

Let G be a finite group whose order is not divisible by 3. Suppose

$$(ab)^3 = a^3 b^3, \quad \text{for all } a, b \in G$$

Show that G is abelian.

Proof. Because $3 \nmid o(G)$, we know if $g^3 = e$, then $g = e$. In other words, the endomorphism $x \mapsto x^3$ is an automorphism. Because of such, we only have to prove $a^3 b^3 = b^3 a^3$ for all $a, b \in G$. This then follows from

$$\begin{aligned} (ab)^3 &= a^3 b^3, \quad \text{for all } a, b \in G \\ \implies baba &= a^2 b^2, \quad \text{for all } a, b \in G \\ \implies (ba)^2 &= a^2 b^2, \quad \text{for all } a, b \in G \\ \implies (ab)^4 &= [(ab)^2]^2 = [b^2 a^2]^2 = a^4 b^4, \quad \text{for all } a, b \in G \\ \implies (ab)^4 &= a(ba)^3 b = ab^3 a^3 b, \quad \text{for all } a, b \in G \\ \implies a^3 b^3 &= b^3 a^3, \quad \text{for all } a, b \in G \end{aligned}$$

■

Question 3: Wording problem

Let $a, b \in G$ satisfies

$$o(a) = 5 \quad \text{and} \quad aba^{-1} = b^2$$

Find $o(b)$.

Proof.

$$\begin{aligned} aba^{-1} &= b^2 \\ \implies a^2ba^{-2} &= ab^2a^{-1} = (aba^{-1})^2 = b^4 \\ \implies b &= a^5a^{-5} = a^4b^2a^{-4} = (a^2ba^{-2})^2 = b^8 \end{aligned}$$

Therefore $o(b) = 7$. ■

Question 4: Structure theorem for finitely generated abelian group

Let G be an abelian group, and $x, y \in G$ has order m, n . Show that G has an element of order $\text{lcm}(m, n)$.

Proof. The proof follows from noting that the fact that in general, given $(a_1, \dots, a_n) \in G_1 \times \dots \times G_n$, we have

$$o((a_1, \dots, a_n)) = \text{lcm}(o(a_1), \dots, o(a_n))$$

and the fact that since $x, y \in \langle x \rangle + \langle y \rangle$, in the primary decomposition form of $\langle x \rangle + \langle y \rangle$, there must be a component of high enough power. ■

Question 5: Structure theorem for finitely generated abelian group

Let G be an abelian groups that has subgroups of order m and n . Show that it has a subgroup of order $\text{lcm}(m, n)$.

Proof. Let the subgroups be M, N . The proof then follows from noting that $\text{lcm}(m, n) \mid o(MN)$ and the fact that for every divisor d of the order of a finite abelian group H , there always exists a subgroup $\leq H$ of order d . ■

Question 6: Structure theorem for finitely generated abelian group

Let G be a finite abelian group in which the number of solution of the equation $x^n = e$ is $\leq n$ for all $n \in \mathbb{N}$. Show that G is cyclic.

Proof. Write G in its **primary decomposition form**. We are required to show that its p -torsion subgroup has at most one component. This follows from noting that for $d, e \geq 1$, the group $\mathbb{Z}_{p^d} \times \mathbb{Z}_{p^e}$ has p^2 number of solution to the equation $x^n = e$. ■

Question 7

Let $a \in G$. Show that the equation

$$x^2ax = a^{-1}$$

is solvable for $x \in G$ if and only if a is the cube of some element.

Proof. Suppose $x^2ax = a^{-1}$ for some $x \in G$. One can show that $a = (xa)^3$. If $a = y^3$, then $x \triangleq y^{-2}$ is a solution. ■

Question 8

Let $a \in G$ lies in a conjugacy class of finite cardinality and has finite order. Show that the normal closure of a is of finite order.

Proof. Recall that

$$\text{ncl}_G(\{a\}) = \{g_1 a^{\epsilon_1} g_1^{-1} \cdots g_n a^{\epsilon_n} g_n^{-1} : n \in \mathbb{N} \cup \{0\} \text{ and } \epsilon_i \in \{\pm 1\}\}$$

Question 9

Show that a group can not be written as the union of two proper subgroup.

Proof. Let $G = H \cup K$. We are required to prove $G \in \{H, K\}$. We prove such by showing that one is contained by the other. Assume not for a contradiction. Letting $h \in H - K$ and $k \in K - H$, we see that $hk \in G - H \cup K$, a contradiction. For more on this kind theorems, see the survey article [Groups as unions of proper subgroups](#), by Bhargava, M. (2009) ■