Suns

Eric Liu

Contents

Chapter 1

Groups

1.1 Definition of groups

Let M be a set equipped with a binary operation $M \times M \to M$. 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 has 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.

Example 1.1.2: Another group axioms

Another set of axioms for group is to require the operation to be associative, identity to be left, and the existence of left inverses. Under such condition, we see that if an element y 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 $xe = x(x^{-1}x) = x$.

Example 1.1.3: Group criteria for finite set

If the underlying set is finite, then weaker assumption can be made. For example, suppose only that the binary operation to be associative and that both cancellation holds:

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

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.

Example 1.1.4: Finite subset closed under binary operation forms a subgroup

Let $S \subseteq G$ be a finite subset closed under the binary operation. 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 $a^{-1} = a^{n(a)} \in S$.

Example 1.1.5: Euler's totient function

By example 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

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

for all $a \in \mathbb{N}$ coprime with n, where the **totient function** $\varphi(a)$ is the number of natural numbers smaller than a and coprime with a. We now have **Fermat's little**

theorem as a special case.

Unlike the category of monoids, the category of groups behaves much better. Given two groups G, H and a function $\varphi : G \to H$, 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:

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

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 1.1.6: 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 1.1.7: 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 $\varphi \in \operatorname{Aut}(G)$ must have the same index, since $xH \mapsto \varphi(x)\varphi(H)$ forms a well-defined bijection.

Theorem 1.1.8. **(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

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

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 $G \times X \to X$ 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 $G \to \text{Bij}(X)$.

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 $G \diagup \text{Stab}(x)$ denote the left coset space. The fact that the obvious mapping between $G \diagup \text{Stab}(x)$ 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**:

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

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 $\mathbb{Z}_p \to \text{Bij}(X)$ 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 and Characteristic Subgroup

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 $xn = \widetilde{n}x$ for some $\widetilde{n} \in N$. This implies

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

(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. ■

Equivalent Definition 1.3.3. (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 $\varphi \in \text{Aut}(G)$

(ii) $\varphi(K) = K$ for all $\varphi \in \text{Aut}(G)$.

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

Theorem 1.3.4. (Basic properties of characteristic subgroups)

(i) If there exists a unique subgroup $H \leq G$ of a fixed index, then $H \operatorname{char} G$.

(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. ■

Example 1.3.5: 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 Hamiltonian because every nontrivial element is of order 4.

Given $H \leq G$, clearly, $N_G(H)$ is the largest subgroups of G in which H is normal. Let $N \trianglelefteq G$. We say a group homomorphism $\pi : G \to G/N$ satisfies the **universal property of quotient group** G/N if

(i) π vanishes on N. **(Group condition)**

(ii) For all group homomorphism $f : G \to H$ that vanishes on N there exist a unique group homomorphism $\widetilde{f} : G/N \to H$ that makes the diagram:

$$\begin{tikzcd}
G \arrow[r, two heads, "\pi"] \arrow[dr, "f"'] & G/N \arrow[d, "\widetilde{f}"] \\
 & H
\end{tikzcd}$$

commute. **(Universality)**

Theorem 1.3.6. (The first isomorphism theorem for groups) The group homomorphism $\pi : G \to G/N$ is always surjective with kernel N. Let $f : G \to H$ be a group homomorphism. Then $\ker f$ is normal in G, and the induced homomorphism $\widetilde{f} : G/\ker f \to H$ is injective.

Proof. They are consequences of the construction. ■

Equivalent Definition 1.3.7. (Core) Let $H \leq G$, and let $\varphi : G \to \mathrm{Bij}(G/H)$ be the left multiplicative action on the left coset space of H. We have

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

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

Proof. Routine. ■

Theorem 1.3.8. (Properties of core) Let G be finite. Then

(i) $[G : \mathrm{Core}(H)]$ divides $[G : H]!$, for all $H \leq G$

(ii) Any subgroup of G of index p, where p is the smallest prime dividing $o(G)$, is normal in G.

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

Equivalent Definition 1.3.9. (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 $x_i \triangleq hg_1$ if $\epsilon_i = 1$ and hg_i^{-1} if $\epsilon_i = -1$. ■

1.4 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 $i : S \hookrightarrow F_S$ such that for all group G and function $f : S \to G$, there exists a unique group homomorphism $\widetilde{f} : F_S \to G$ that makes the diagram:

$$\begin{tikzcd}
S \arrow[r, hook, "\iota"] \arrow[dr, "f"'] & F_S \arrow[d, dashed, "\widetilde{f}"] \\
& G
\end{tikzcd}$$

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

$$\begin{tikzcd}
S \arrow[r, "\pi \circ \iota"] \arrow[dr, "f"'] & \langle S \mid R \rangle \arrow[d, dashed, "\widehat{f}"] \\
& G
\end{tikzcd}$$

Example 1.4.1: Dihedral group

The **Dihedral group** D_n is defined by

$$D_n \triangleq \langle x, y \mid x^n = y^2 = e, yxy^{-1} = x^{-1} \rangle$$

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

1.5 Second and third isomorphism theorem

Theorem 1.5.1. (Third isomorphism theorem and correspondence theorem) Let $N \trianglelefteq G$. The canonical projection $\pi : G \to G/N$ 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. In fact, given $K \trianglelefteq G$ that contains N, if we identify K/N as a subgroup of G/N the natural way:

$$\begin{tikzcd}
K \arrow[r, two heads, "\pi"] \arrow[dr] & \frac{K}{N} \arrow[d, hook] \\
 & \frac{G}{N}
\end{tikzcd}$$

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

Proof. Routine. ■

Theorem 1.5.2. (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

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

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. ■

Example 1.5.3: 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.

1.6 Semidirect Product

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

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

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** $\text{Hol}(G) \triangleq G \rtimes_{\mathbf{id}} \text{Aut}(G)$.

Theorem 1.6.1. (Universal property of semidirect product) Let N, H be two groups and $\varphi : H \to \text{Aut}(N)$ be a group homomorphism. If group homomorphisms $f : N \to G, g : H \to G$ satisfy

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

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

$$\begin{tikzcd}
N \rtimes_\varphi H \arrow[dr, dashed, "k"] & H \arrow[l, hook'] \arrow[d, "g"] \\
N \arrow[u, hook] \arrow[r, "f"'] & G
\end{tikzcd}$$

commutes.

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

Theorem 1.6.2. (Presentation of semidirect product) Let $N \triangleq \langle X \mid R \rangle, H \triangleq \langle Y \mid S \rangle$ and $\varphi : H \to \text{Aut}(N)$ be a group homomorphism. We have

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

Proof. ■

Example 1.6.3: Classification of semidirect product of $\mathbb{Z}_8 \rtimes \mathbb{Z}_2$

Write $\text{Aut}(\mathbb{Z}_8) \triangleq \{1,3,5,7\}$, so there are four distinct action $\mathbb{Z}_2 \longrightarrow \text{Aut}(\mathbb{Z}_8)$. In particular, 3 of them are non-trivial, giving three possibly distinct semidirect product of $\mathbb{Z}_8 \rtimes \mathbb{Z}_2$:

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

Clearly, every element can be written as $x^a y^b$ with $a \in \{0, \dots, 7\}$ and $b \in \{0, 1\}$.
$n = 3$, Quasidihedral

$$x \mapsto \begin{pmatrix} \xi & 0 \\ 0 & -\overline{\xi} \end{pmatrix} \quad \text{and} \quad y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$n = 5$, M-group or **Iwasawa** group

$$x \mapsto \begin{pmatrix} \xi & 0 \\ 0 & -\xi \end{pmatrix} \quad \text{and} \quad y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Equivalent Definition 1.6.4. (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 $H \to G/N$.

(iv) There exists a homomorphism $r : G \to H$, called the **retraction**, that is identity on H and has kernel N. Such retraction then give us a right split short exact 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 $H \longrightarrow G/N$ 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 $r(gr(g^{-1})) = r(g)r(r(g^{-1})) = r(g)r(g^{-1}) = e$. ■

Suppose $N \trianglelefteq G$ and $H \leq G$ satisfies the conditions in the recognition theorem for inner semidirect product. Defining $\varphi : H \to \text{Aut}(N)$ by $\varphi_h(n) \triangleq hnh^{-1}$, we see that the natural map $N \rtimes_\varphi H \to G$ indeed forms a well-defined group isomorphism.

Example 1.6.5: Inner semidirect product

$$\begin{tikzcd} 1 \arrow[r] & A_n \arrow[r] & S_n \arrow[r, "\text{sgn}"] & \mathbb{Z}_2 \arrow[r] & 1 \end{tikzcd}$$

Equivalent Definition 1.6.6. (Recognition theorem) Let $N_1, \dots, N_k \trianglelefteq G$. We say G is an **internal direct products of** N_i if any of the followings hold true:

(i) The natural map $N_1 \times \cdots \times N_k \to G$ forms a group isomorphism.

(ii) $N_1 \cdots N_k = G$ and $N_i \cap \prod_{j \neq i} N_j = \{e\}$ 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 $n_2 = \cdots = n_k = e$.

(ii) $\implies$ (i): We first need to show that the map forms a homomorphism, which boils down to showing that for $i \neq j$, we have $[N_i, N_j] = 1$, which follows from the premise and the fact that $[N_i, N_j] \leq N_i \cap N_j$. Surjectivity is clear. For injectivity, if $n_1 \cdots n_k = e$, then because $n_2 \cdots n_k = n_1^{-1} \in N_1$, we know $n_2 \cdots n_k = e$ and $n_1 = e$. Continuing the process, we see $n_1 = \cdots = n_k = e$. ■

Example 1.6.7: The requirement in definitions of internal direct products for groups

Let $G \triangleq \mathbb{Z}_4 \times \mathbb{Z}_2$. 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.

1.7 Centralizer

Let $S \subseteq G$, and 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 $N_G(S) \longrightarrow \text{Bij}(S)$. Clearly centralizers are always abelian. We call the centralizer of the whole group $Z(G) \triangleq C_G(G)$ **center**. 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 1.7.1: 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 1.7.2. (Normal subgroup that intersects with commutator subgroup must be contained by the center) 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 $gn = ng$. ■

Example 1.7.3: Dihedral group

Fix $n \geq 3$. We write the **Dihedral group** D_n as

$$\{r_0, \dots, r_{n-1}, s_0, \dots, s_{n-1}\}$$

where

$$r_k \triangleq \begin{pmatrix} \cos \frac{2\pi k}{n} & -\sin \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} & \cos \frac{2\pi k}{n} \end{pmatrix} \quad \text{and} \quad s_k \triangleq \begin{pmatrix} \cos \frac{2\pi k}{n} & \sin \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} & -\cos \frac{2\pi k}{n} \end{pmatrix}$$

stand for rotation and symmetries. Easily, one then can check that if n is even, then $Z(D_n) = \left\{r_0, r_{\frac{n}{2}}\right\}$, and if n is odd, then $Z(D_n) = \{r_0\}$

Example 1.7.4: Criterion for abelianess

If $G \diagup Z(G)$ 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 $G \diagup Z(G)$ cyclic. For example, consider D_4. Because $o(Z(D_4)) = 2$, we know $D_4 \diagup Z(D_4)$ is abelian, but D_4 isn't.

1.8 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.

Theorem 1.8.1. (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 1.8.2. (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 1.8.3. (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 1.8.4. (Simplicity of A_n)

(i) A_3 is simple.

(ii) A_4 is not simple.

(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 1.8.5. (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 intersects with commutator subgroup must be contained by the center. ■

1.9 Finitely generated abelian group

Theorem 1.9.1. (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 $y_1 = c_1 x_1 + \cdots + c_k x_k$.

Proof. Such is proved via induction on $s \triangleq c_1 + \cdots + c_k$. 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

$$\begin{aligned} y_1 &= (c_1 - c_2)x_1 + c_2(x_2 + x_1) + \cdots + c_k x_k \\ &= c_1 x_1 + \cdots + c_k x_k \end{aligned}$$

as desired. ■

Theorem 1.9.2. (Fundamental theorem for finitely generated abelian group, invariant factor form) Let G be a finitely generated abelian group. Then we may write:

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s} \times \mathbb{Z}^r$$

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 $m_1 x_1 + m_2 x_2 + \cdots + m_k x_k = 0$. 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 $m_{t+1} = \cdots = m_k = 0$.

Let $c_i \triangleq \frac{m_i}{\gcd(m_1,\dots,m_t)}$ for all $i \in \{1,\dots,t\}$. By theorem 1.9.1, 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 $y_1 = c_1x_1 + \cdots + c_tx_t$. Clearly, we have $G = \langle y_1,\dots,y_t,x_{t+1},\dots,x_k\rangle$. Compute

$$\gcd(m_1,\dots,m_t)y_1 = m_1x_1 + \cdots + m_tx_t = 0$$

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 $G/pG \cong \mathbb{Z}_p^s$.

(ii): The existence follows from noting that

$$\gcd(m,n) = 1 \implies \mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

The uniqueness follows from noting that given a primary decomposition form whose p-part has the form $\mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_k}}$, 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

$$G_{T_p} \cong \mathbb{Z}_{p^{n_1}} \times \cdots \times \mathbb{Z}_{p^{n_k}}$$

and that

$$\frac{p^{d-1}\mathbb{Z}_{p^{n_i}}}{p^d\mathbb{Z}_{p^{n_i}}} \cong \begin{cases} \mathbb{Z}_p & \text{if } d-1 < n_i \\ 0 & \text{if } d-1 \geq n_i \end{cases}$$

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

1.10 Sylow theorems

Theorem 1.10.1. (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.,

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

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

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

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

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

where $\mathrm{Fix}(G)$ 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 $\mathrm{Fix}(G)$ are exactly those subsets of X that contains n_i cycles of length p^i. The proof now follows from directly computing that $|\mathrm{Fix}(G)| = \prod_{i=0}^{k} \binom{m_i}{n_i}$. ■

Theorem 1.10.2. (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 be 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:

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

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

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

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

Theorem 1.10.3. (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. ■

Corollary 1.10.4. (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

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

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

Theorem 1.10.5. (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 $hgP = gP$. ■

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

Theorem 1.10.6. (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 $\text{Stab}(P) = N_G(P)$. ■

1.11 Application of Sylow theorems

Before we go into detail, we first mention that normal Sylow subgroups are clearly characteristic, so we will use the word "characteristic Sylow subgroup" instead.

Corollary 1.11.1. (Classification of finite group of fixed prime structure) Let p, q, r be three distinct prime.

(i) Groups of order pq has a characteristic q-Sylow subgroup, where $p < q$. If $p \nmid q - 1$, then there is only one group of order pq, i.e., $\mathbb{Z}_p \times \mathbb{Z}_q$. If $p \mid q - 1$, then there are only two groups of order pq, i.e., $\mathbb{Z}_p \times \mathbb{Z}_q$ and $\mathbb{Z}_q \rtimes \mathbb{Z}_p$.

(ii) Groups of order $p^2 q$ has a characteristic Sylow subgroup.

(iii) Groups of order $p^3 q$ 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): Clear. The isomorphism part follows from recognition theorem.

(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 $P \in \mathrm{Syl}_3(G)$, we have $N_G(P) = P$, since $3 = n_3 = [G : N_G(P)]$. Clearly, the conjugacy action $G \longrightarrow \mathrm{Sym}(\mathrm{Syl}_3(G))$ has kernel contained by $N_G(P) = P$. This by non-normality of P implies the conjugacy action $G \hookrightarrow \mathrm{Sym}(\mathrm{Syl}_3(G)) \cong S_4$ is injective. Because both A_4 and G contains 8 elements of order 3, it now follows that $G \cong A_4$.[1]

Direct computation shows that A_4 indeed has a normal 2-Sylow subgroup, i.e., the kernel $\{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ of the surjective group homomorphism $A_4 \twoheadrightarrow A_3$.

(iii): Let $P \in \mathrm{Syl}_p(G)$. Because G is simple, by second Sylow theorem, conjugacy action $G \longrightarrow \mathrm{Sym}(\mathrm{Syl}_p(G)) \cong S_{n_p}$ is nontrivial. Simplicity of G then forces the action to be

[1] One may argue that the original assertion that groups of order $p^2 q$ 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 $n_3 = 4$.

injective, as desired.

(v): By counting, we know $1 \in \{n_p, n_q, n_r\}$. If $n_p \neq 1 \neq n_q$, then we are done. If $n_p = 1$, then denoting P the normal Sylow p-subgroup, by (i), there is a group H of order pr containing P such that $\frac{H}{P}$ is the normal Sylow r-subgroup of $\frac{G}{P}$. Again by (i), there exists a characteristic $K \in \text{Syl}_r(H)$. By correspondence theorem, we now have $K \operatorname{char} H \trianglelefteq G$, which implies that K is characteristic in G.

■

Corollary 1.11.2. (Application of Sylow theorems, given the order)

(i) No group of order 132 is simple.

(ii) Simple groups of order 60 must be A_5.

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

(ii): 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 $G/\operatorname{Core}(H) \cong \text{Sym}(G/H)$, 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 $n_2(A_5) = 5$.

■

1.12 Nilpotency and Solvability

More than often, we care about the existence of **central series**

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

where we requires the successive quotient to be **central**, i.e., $[G, A_{n+1}] \leq A_n$, or equivalently, $A_{n+1}/A_n \leq Z(G/A_n)$, or equivalently, $xyA_n = yxA_n \in G/A_n$ if one of x, y is in A_{n+1}.

To construct one, one can consider the **upper central series**, defining $G_{(n)} \triangleq [G, G_{(n-1)}]$ with $G_{(0)} \triangleq G$. This gives us

$$\cdots \trianglelefteq G_{(2)} \trianglelefteq G_{(1)} \trianglelefteq G$$

Note that

Theorem 1.12.1. (Every subgroup of a nilpotent group is subnormal) Let G be a nilpotent group with $H \leq G$. Then H is a subnormal subgroup of G.

Proof. Let

$$1 \triangleleft A_1 \triangleleft \cdots \triangleleft A_n = G$$

■

Corollary 1.12.2. (Nilpotent group satisfies normalizer condition) Let G be a nilpotent group. If $H < G$, then $H < N_G(H)$.

A group is said to be nilpotent if it admits a central series.

Equivalent Definition 1.12.3. (Nilpotency for finite group) Let G be a finite group. The followings are equivalent:

(i) G is nilpotent.

(ii) Sylow subgroups of G are all normal.

(iii) Sylow subgroups of G are all normal and they form an inner direct product equal to G.

(iv)

Proof. ■

1.13 p-group

Theorem 1.13.1. (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 $G' = Z(G)$. ■

1.14 Remarkable 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 $o(b) = 7$. ■