MATH 594 - Group Theory

AResseges Stery

May 21, 2024

Contents

1 Group Preliminaries

Definition 1.1 (Group). A **group** is a set G together with a binary operation $G \times G \to G$, often written $(a, b) \mapsto a \cdot b$ or simply ab, s.t. the following properties are satisfied:

1. *Associativity:* $(ab)c = a(bc)$ for all $a, b, c \in G$.
2. *Existence of Identity*: There exists $e = e_G \in G$ s.t. $\forall a \in G, ae = a = ea$.
3. *Existence of Inverse*: For all $a \in G$. there exists $b \in G$ s.t. $ab = e = ba$.

Furthermore, if the operation is commutative, i.e. for all $a, b \in G$, $ab = ba$, then the group is **commutative**, or **abelian**.

Notation. If the group G is abelian, then the operation is often represented in additive notations (with operation denoted as "$+$", and inverse of $a \in G$ being $-a$).

Remark 1.2. One implicitly presented condition is that the operation of groups need to be closed within the set predefined. This is indicated by the signature of the operation, which should land in G. This often needs to be checked when the group structure is defined in some larger structure.

Remark 1.3. From the definition of group there are some immediate facts/properties:

1) The identity in the group is unique. Suppose that there exist two identity elements e and e', then by rule 2 $e = ee' = e'$.
2) For a given element in the group, the inverse of it is unique. Let b and b' both be the inverse of some $a \in G$. Then

$$b = b(ab') = (ba)b' = b'$$

the uniqueness allows us to unambiguously denote the inverse of a as a^{-1}. This also implies $(a^{-1})^{-1} = a$, as clearly by the previous process a is the inverse of a^{-1}; and the inverse is unique.

3) $(ab)^{-1} = b^{-1}a^{-1}$. By the uniqueness of the inverse element, it suffices to check that the claimed inverse satisfies rule 2. This is indeed the case as

$$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$$

and for multiplication in the other sequence the checking is similar.

4) For $a, b, c \in G$, then $ab = ac \implies b = c$; and $ba = ca \implies b = c$. This results directly from the fact that a is invertible; and multiplying on the left/right, respectively, a, gives the desired result.

Remark 1.4. The associativity of operation in the groups gives the unambiguity of writing successive multiplications. Rigorously, when written $x_1 \dots x_n$ for $n \geq 2$, it is defined inductively on n via specifying the result to be $(x_1 \dots x_{n-1})x_n$. The convention is that for $n = 0$ this is simply the identity.

In particular one can unambiguously write out the power of an element:

$$a^n := \begin{cases} \underbrace{a \dots a}_{n} & n > 0 \\ e & n = 0 \\ \underbrace{a^{-1} \dots a^{-1}}_{n} & n < 0 \end{cases}$$

This gives $a^m \cdot a^n = a^{m+n}$ for all $m, n \in \mathbb{Z}$. The cases where m and n are of the same sign are clear; and for those of opposite sign, applying the same elimination process as Remark 1.3 3) gives the desired result.

If G is abelian, in additive notation we often denote $n \cdot a := a^n$.

Definition 1.5. If G and H are groups, a **group homomorphism** $f : G \to H$ is a map s.t. $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in G$.

Proposition 1.6. If $f : G \to H$ is a group homomorphism, then $f(e_G) = e_H$, and $f(a^{-1}) = (f(a))^{-1}$.

Proof. By Remark 1.3 4) and the property of identity, we have

$$f(e_G) \cdot e_H = f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G) \implies e_H = f(e_G)$$

For the second statement, use the above result:

$$e_H = f(e_G) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$$

By the definition $(f(a))^{-1}$ is the inverse of $f(a)$. By the uniqueness of inverse this gives $f(a^{-1}) = f(a^{-1})$. □

Remark 1.7. Given $f : G \to H$, $g : H \to K$ which are both f and g are group homomorphisms, then $f \circ g$ is also a group homomorphism. This results from the fact that

$$f(g(a \cdot b)) = f(g(a) \cdot g(b)) = f(g(a)) \cdot f(g(b))$$

The fact that morphism is closed w.r.t. composition implies that the groups form a category Grps.

Definition 1.8. If G and H are groups, then $f : G \to H$ is a **group isomorphism** if it is a bijective group homomorphism.

Proposition 1.9. $f : G \to H$ being a group homomorphism is a group isomorphism if and only if there exists a group homomorphism $g : H \to G$ s.t. $g \circ f = \mathrm{Id}_G$, and $f \circ g = \mathrm{Id}_H$.

Proof. It suffices to show implication in two directions:

$\Rightarrow$: Since f is bijective, there must admit a (pointwise) inverse of f s.t. $f^{-1} \circ f = \mathrm{Id}_G$, $f \circ f^{-1} = \mathrm{Id}_H$. Define $g = f^{-1}$. It suffices to check that g is a group homomorphism. To prove this we need to verify that for all $u, v \in H$, $g(u \cdot v) = g(u) \cdot g(v)$.

Since f is bijective, f is in particular injective, i.e. $a = b$ if and only if $f(a) = f(b)$ for all $a, b \in G$. Therefore to verify the equality above it suffices to verify the equality after applying f, i.e. $f \circ g(u \cdot v) = f \circ g(u) \cdot f \circ g(v)$. Then the equality holds as $f \circ g = \mathrm{Id}_H$.

$\Leftarrow$: Prove the contrapositive. If f is not injective, then g cannot be well-defined; and if f is not surjective, then the domain of the composition $f \circ g$ is not the whole H.

□

Remark 1.10. Recall that under the context of categories, isomorphisms are defined as in Proposition 1.9. The same proposition implies that group isomorphisms are isomorphisms in the categorical sense.

Remark 1.11. If there exists an isomorphism $f : G \to H$ between groups G and H, then G and H are considered as **isomorphic**, denoted $G \cong H$. This is an equivalence relation as compositions of isomorphisms are still isomorphisms.

Definition 1.12. Let G be a group. Then a **subgroup** of G is a subset $H \subseteq G$, which is in it self a group; and the inclusion map $i : H \hookrightarrow G$ is a group homomorphism. H being the subgroup of G is denoted as $H \leq G$.

Remark 1.13. The fact that the inclusion map is required to be a group homomorphism implies that the operation in H is simply the restriction of the operation in G.

Proposition 1.14. Let G be a group, and $H \subseteq G$ a subset. Then the followings are equivalent:

i) H is a subgroup of G.

ii) The following three conditions are satisfied:

1) For all $a, b \in H$, $a \cdot b \in H$.

2) $e_G \in H$.

3) (Under the same operation of G) $a^{-1} \in H$ for all $a \in H$.

iii) H is nonempty; and for all $x, y \in H$, $x \cdot y^{-1} \in H$.

The third condition is often used to test whether $H \subseteq G$ gives a subgroup.

Proof. Verify the following implications:

- i) $\Longrightarrow$ ii). By the definition of subgroup, H together with the same operation is a group, which by the definition of group is closed w.r.t. the group; and every element should admit an inverse. By the fact that i is an inclusion, and by Proposition 1.6 $i(e_H) = e_G$ with $e_G = e_H$.
- ii) $\Longrightarrow$ i). Check that H is a group: associativity is given by the fact that the operation is identical to that in G. and G is a group; existence of inverse and identity results directly from hypothesis 2) and 3); and the operation is defined as $H \times H \to H$ given by hypothesis 1).
- ii) $\Longrightarrow$ iii). By 2) H is nonempty. For all $x, y \in H$, by 3) $y^{-1} \in H$; and by 1) $x \cdot y^{-1} \in H$ given that both x and y^{-1} are in H.

- iii) $\implies$ ii). Since H is nonempty, there exists $a \in H$. iii) implies that $a \cdot a^{-1} = e_G \in H$, giving 2). For all $a \in H$, let $x = e_G$ and $y = a$, which gives $a^{-1} \in H$, satisfying 3). For all $a, b \in H$, letting $x = a, y = b^{-1}$ gives $a \cdot b \in H$.

□

Proposition 1.15. Let $f : G \to H$ be a group homomorphism, then if $G' \leq G$, then $f(G') \leq H$.

Proof. Apply the result of Proposition 1.14. Since $G' \leq G$, $e_G \in G'$, and by Proposition 1.6, $f(e_G) = e_H$, giving that $f(G')$ is nonempty. For all $x, y \in f(G')$, let $u, v \in G'$ s.t. $x = f(u), y = f(v)$. Since G' is a subgroup of G, $u \cdot v^{-1} \in G'$. By Proposition 1.6, this implies $f(u) \cdot f(v^{-1}) = f(u) \cdot f(v^{-1}) \in f(G')$, which gives that $f(G') \leq H$. □

Proposition 1.16. Let $f : G \to H$ be a group homomorphism. If $H' \leq H$, then $f^{-1}(H') \leq G$. In particular, $f^{-1}(e_H) = \ker f := \{u \in G \mid f(u) = e_H\}$ is a subgroup of G.

Proof. Apply the same argument as in the above proposition. $H' \leq H \implies e_H \in H' \implies e_G \in f^{-1}(H')$, i.e. $f^{-1}(H')$ is nonempty. For all $u, v \in f^{-1}(H')$, $f(u \cdot v^{-1}) = f(u)f(v)^{-1} \in H'$ since $H' \leq H$, which implies that $u \cdot v^{-1} \in f^{-1}(H')$, i.e. $f^{-1}(H')$ is a group. □

Proposition 1.17. Let $f : G \to H$ be a group homomorphism. Then f is injective if and only if $\ker f = \{e_G\}$.

Proof. Proceed by showing implication in both directions:

$\Rightarrow$: Let $u \in \ker f$. Then $f(a) = f(a) \cdot e = f(a) \cdot f(u) = f(a \cdot u)$. But f being injective implies that $a = a \cdot u$, i.e. $u = e$.

$\Leftarrow$: For $u, v \in G$ s.t. $f(u) = f(v)$, we have $e = f(u) \cdot (f(v))^{-1} = f(u) \cdot f(v^{-1}) = f(u \cdot v^{-1}) \implies thatu \cdot v^{-1} \in \ker f$. But since the only element in $\ker f$ is the identity, this gives $u \cdot v^{-1} = e \implies u = v$, i.e. f is injective.

□

2 Group of Permutations

Definition 2.1. Given a set Ω, the **permutation group** is defined to be $S_\Omega := \{f : \Omega \to \Omega \mid f \text{ bijection}\}$. Since compositions of bijective maps are still bijective, defining the operation to be composition gives this a group structure.

Remark 2.2. Notice that the permutation group structure depends only on the cardinality of the group on which permutations are considered. Explicitly, for $\alpha : \Omega \to \Omega'$ a bijection, there exists an isomorphism between the corresponding groups of permutations: $\beta : S_\Omega \to S_{\Omega'} : f \mapsto \alpha \circ f \circ \alpha^{-1}$. This is indeed an isomorphism as this is first a group homomorphism since

$$\beta(f \circ g) = \alpha \circ f \circ g \circ \alpha^{-1} = \alpha \circ f \circ (\alpha^{-1} \circ \alpha) \circ g \circ \alpha^{-1} = \beta(f) \circ \beta(g)$$

and this being an isomorphism follows from the fact that there exists an obvious inverse $\beta^{-1} : f \mapsto \alpha^{-1} \circ f \circ \alpha$. Therefore it suffices to denote such permutation group by the cardinality of Ω: for $\Omega = \{1, \ldots, n\}$ S_Ω is denoted as S_n.

Proposition 2.3 (Cayley). Every group can be embedded into some S_Ω. Explicitly, for group G the map $\alpha : G \to S_G$ s.t. $g \mapsto \alpha_g$ where $\alpha_g(h) = gh$ (α_g is the action of G on G defined by multiplication by g.) is an injective group homomorphism.

Proof. It suffices to syntactically check that the following requirements are satisfied:

- $\alpha_g \in S_G$. It suffices to check that indeed multiplication by an element in the group gives a bijection. This is clear as the action has an inverse, namely multiplying the inverse of that element.
- *α gives a group homomorphism.* By definition $\alpha_{gh} = \alpha_g \cdot \alpha_h$.
- *α is injective.* It suffices to check that $\ker \alpha = e_G$. This is indeed the case, as for $g \in G$ s.t. $\alpha_g = \mathrm{Id}$, $\alpha_g(e_G) = g \cdot e_G = e_G \implies g = e_G$.

□

3 Groups Generated by a Subset

Remark 3.1. If $(H_i)_{i\in I}$ is a family of subgroups of G, then $\bigcap_{i\in I} H_i$ is also a subgroup of G. This can be verified by taking an element in the intersection, and check each rule of group is satisfied in each of the H_is.

Definition 3.2. If $A \subseteq G$ is a subset of G, then the **subgroup generated by** A is defined as

$$\langle A\rangle := \bigcap_{A\subseteq H\leq G} H$$

Remark 3.3. By definition $\langle A\rangle$ is well-defined as it is described by concrete elements in the group; and as in particular $A \subseteq G \leq G$. By the previous remark, $\langle A\rangle$ is a subgroup of G. It is also the smallest subgroup that contains A.

Proposition 3.4. Let $A \subseteq G$ be a subset of G, then $\langle A\rangle = \left\{x_1 \dots x_n \mid n \in \mathbb{Z}_{>0}; \forall i, x_i \in G \text{ or } x_i^{-1} \in G\right\}$. For $n = 0$, define $x_1 \dots x_n = e$.

Proof. Proceed by double inclusion:

$\subseteq$: Proceed to show that RHS satisfies the definition of the Hs above. For RHS consider $n = 1$, with $x_1 \in G$ which takes all elements in G. This gives $A \subseteq$ RHS. Further use Proposition 1.14, which for any $x_1 \dots x_m, y_1 \dots y_n \in$ RHS, each summand of $x_1 \dots x_m(y_1 \dots y_n)^{-1} = x_1 \dots x_m y_n^{-1} \dots y_1^{-1}$ is either in A or its inverse is in A implying that RHS is a group. Definition above gives the subset relation.

$\supseteq$: It suffices to verify that any element in the specified form is in $\langle A\rangle$. This is the case as for $x_1 \dots x_n$ where for all i, either $x_i \in A$ or $x_i^{-1} \in A$, $x_i \in \langle A\rangle$ by definition, and multiplication of two elements in the group is still in the group by closure of the operation.

□

Definition 3.5. The following defines some common terminology for characterization of a group:

- G is **finitely generated** if there exists a finite set $A \subseteq G$ s.t. $G = \langle A \rangle$.
- G is **finite** if it has finitely many elements.
- The **order** of G, denoted $|G|$, is the number of elements in G if it is finite; or ∞ if G is not finite (infinite).
- G is **cyclic** if it attains a generating set with a single element a. In this case G is denoted as $G = \langle a \rangle$.
- The **order** of $a \in G$, denoted $|a|$ is the order of $\langle a \rangle$.

Remark 3.6. Cyclic groups are abelian. By the alternative definition provided in Proposition 3.4, $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$.

Proposition 3.7. A group G is cyclic if and only if $G \simeq \mathbb{Z}$ for G infinite, or $G \simeq \mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}_{>0}$.

Proof. Choose $a \in G$ s.t. $G = \langle a \rangle$. Proceed via showing implication in both directions:

$\Rightarrow$: Consider $f : \mathbb{Z} \to G$ s.t. $f(1) = a$. This is a group homomorphism, Then either

- *f is injective.* By definition of cyclic groups, for any $s \in G$ there exists $m \in G$ s.t. $s = a^m$. Then $f(m) = s$ according to the definition of f, giving that f is surjective. Then this falls into the first case, giving $G \simeq \mathbb{Z}$.
- *f is not injective.* Then there are nonzero elements that are mapped to e by f. Since $\ker f \subseteq \mathbb{Z}$, there exists a smallest positive element. Define the map $f_n : \mathbb{Z}/n\mathbb{Z} \to G$ s.t. $[1] \mapsto a$. Check the followings:
  - *f_n is well-defined.* It suffices to check that if $[m_1] = [m_2]$, then $f([m_1]) = (f[m_2])$. This is indeed the case as

$$f([m_1]) = a^{m_1} \overset{!}{=} a^{m_1} \cdot a^{(m_2 - m_1)} = a^{m_2} \cdot a^{nk} = a^{m_2} \cdot (a^n)^k = a^{m_2} = f([m_2])$$

    for some $k \in \mathbb{Z}$, where $\overset{!}{=}$ holds since $[m_1] = [m_2]$ implies $n \mid (m_1 - m_2)$. This gives $a^{m_1 - m_2} = e$ since $a^n = e$.
  - *f_n is injective.* For $a \in \mathbb{Z}$ s.t. $f_n([a]) = 0$, $a = 0$ as otherwise this conflicts with the hypothesis that n is the smallest of such integers.
  - *f_n is surjective.* Follows from the same argument in the case where G is infinite.

$\Leftarrow$: Since $\mathbb{Z} = \langle 1 \rangle$ and $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$, both of which are cyclic.

□

4 The Dihedral Group

Definition 4.1. Let $n \geq 3$, and $P_n \subset \mathbb{R}^2 \simeq \mathbb{C}$ be the regular n-gon s.t. its vertices are at the n-th roots of 1. Then the **dihedral group** D_{2n} is the group of symmetry of P_n. Alternatively, one can write

$$D_{2n} = \{\varphi \in \mathrm{GL}_2(\mathbb{R}) \mid \varphi(P_n) = P_n\}$$

Remark 4.2. We have a injective map $\alpha : D_{2n} \to S_n$, where $\alpha(\varphi)$ is given by the restriction of φ to the vertices of P_n. This map is injective as $\{v_1, \dots, v_n\}$ spans $\mathbb{R}^2$. Therefore, specifying how the vertices are transformed (permuted) fixes the whole linear transformation.

Remark 4.3. Notice the following relations: by definition of rotation $\sigma^n = e$; and $\sigma\tau\sigma = \tau$, which implies $\sigma^{n-1}\tau = \tau\sigma$. This enables changing the sequence of applying σs and τs.

Proposition 4.4. For a fixed n, let σ be the operation of counter-clockwise rotation by $\frac{2\pi}{n}$ on P_n; and τ_j be the operation of symmetry w.r.t. the symmetry axis passing through the vertex j (which is a direction; invariant w.r.t. transformations on P_n). Then for every $\alpha \in D_{2n}$, it must be in the form of σ^i or $\sigma^i \cdot \tau_j$, for some $i, j \in \mathbb{Z}$.

Proof. How the operations permute the vertices is characterized by

$$\sigma : v_k \mapsto v_{k+1} \qquad \tau : v_{j+k} \mapsto v_{j-k}$$

Following the strategy of the previous remark, to fix the whole operation α it suffices to fix how vertices are transformed. Since elements of D_{2n} are linear transformations, they map line segments to line segments, and therefore adjacent vertices to adjacent vertices. Then for $v_1 \mapsto v_{i+1}$, either $v_2 \mapsto v_{i+2}$, then $\alpha = \sigma^i$; or $v_2 \mapsto v_i$, then $\alpha = \sigma^i\tau_j$. The indices are considered modulo n and then plus 1. □

Remark 4.5. Using Remark 4.3, we can check that indeed $\langle D_{2n} \rangle = D_{2n}$, by applying the remark to move all the rotations to the left of symmetries, and the reduce the expression by relations $\sigma^n = \tau^2 = e$.

5 Product of Groups

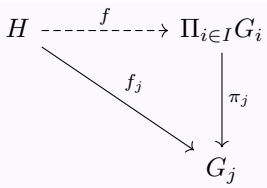
Definition 5.1 (Product of Groups). Suppose that we have a family of groups $(G_i)_{i\in I}$. The **product** of groups is defined as

$$\Pi_{i\in I} G_i := \{(x_i)_{i\in I} \mid x_i \in G_i \forall i \in I\}$$

with the operation defined component-wise i.e. $(x_i)_{i\in I} \cdot (y_i)_{i\in I} := (x_i y_i)_{i\in I}$.

Remark 5.2. By the definition of the operation, the identity in the product of groups $(G_i)_{i\in I}$ is $(e_i)_{i\in I}$ where e_i is the unique identity element in G_i; and the inverse of $(x_i)_{i\in I}$ is $(x_i^{-1})_{i\in I}$.

Proposition 5.3 (Universal Property of Product of Groups). Let group homomorphism $\pi_j : \Pi_{i\in I} G_i \to G_j, (x_i)_{i\in I} \mapsto x_j$ be the projections. Then given group homomorphisms $f_i : H \to G_i$ for all i, there exists a unique group homomorphism $f : H \to \Pi_{i\in I} G_i$ s.t. $\pi_i \circ f = f_i$ for all $i \in I$, i.e. the following diagram commute:



Proof. Since the diagram is required to commute, the homomorphism f can be only defined as $f(x) = (f_i(x))_{i\in I}$, which gives the uniqueness. Existence follows from the fact that f_is are group homomorphisms for all i, which implies that f is also a group homomorphism. □

Example 5.4 (Chinese Remainder Theorem)**.** Let $m, n \in \mathbb{Z}_{\geq 0}$ which are relatively prime. Then there exists group isomorphism $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proof. Consider group homomorphisms:

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad [x + mn\mathbb{Z}] \mapsto [x + m\mathbb{Z}]$$

$$g : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad [x + mn\mathbb{Z}] \mapsto [x + n\mathbb{Z}]$$

Check that f and g are well-defined. For f, let $a = [x + mn\mathbb{Z}] = b = [y + mn\mathbb{Z}]$. This implies that $mn \mid (x - y)$. By definition, $f(a) = [x + m\mathbb{Z}], f(b) = [y + m\mathbb{Z}]$. But this implies that $[x + m\mathbb{Z}] = [y + m\mathbb{Z}]$ as $mn \mid (x - y) \implies m \mid (x - y)$. The well-definedness of g is similar.

Use the universal property above (Proposition 5.3), there exists a unique $h : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ s.t. $h_1 = f, h_2 = g$ where h_i indicates the projection to i-th field after applying h. Check that this is an isomorphism:

- h is injective. Consider the kernel of h: for all $[x + mn\mathbb{Z}] \in \ker h$, $[x + m\mathbb{Z}] = 0$ and $[x + n\mathbb{Z}] = 0$ as it must be in the kernel of both h_1 and h_2. But this implies that $m \mid x$ and $n \mid x$, i.e. $mn \mid x$, which gives $[x + mn\mathbb{Z}] = 0$. That is, elements in $\ker h$ are identically zero, which gives the injectivity.
- Notice that $\mathbb{Z}/mn\mathbb{Z}$ has mn elements, while $\mathbb{Z}/m \times \mathbb{Z}/n\mathbb{Z}$ has $m \cdot n = mn$ elements. Therefore h being injective implies h being bijective.

□

6 Congruence Relations

Definition 6.1 (Left/Right Congruence)**.** Let G be a group, with $H \leq G$. Then for $x, y \in G$,

- x and y are **left congruent** mod H, denoted $x \equiv_\ell y \pmod H$ if $x^{-1}y \in H$.
- x and y are **right congruent** mod H, denoted $x \equiv_r y \pmod H$ if $xy^{-1} \in H$.

Remark 6.2. $\equiv_\ell$ and $\equiv_r$ are equivalence relations. The equivalence classes are noted as xH and Hx for $x \in G$, respectively.

Notation. If G is abelian, the operation is written additively. The congruence classes will then be denoted as $x + H$ and $H + x$ for left and right congruence classes, respectively.

Proof. The proof is similar for two equivalence relations, so we only check for left congruence:

- $\equiv_\ell$ *is Reflexive.* $x^{-1} \cdot x = e \in H$.
- $\equiv_\ell$ *is symmetric.* If $x^{-1}y \in H$, given that H is a subgroup of G, $(x^{-1}y)^{-1} \in H$. This implies that $y^{-1}x \in H$, i.e. $y \equiv_\ell x \pmod H$.
- $\equiv_\ell$ *is transitive.* Suppose that $x \equiv_\ell y \pmod H, y \equiv_\ell z \pmod H$. By the fact that subgroups are closed, $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$.

□

Remark 6.3. G is the disjoint union of equivalence classes w.r.t. $\equiv_\ell$. For $x, y \in G$ s.t. $x \equiv_\ell y \pmod H$, there exists $h \in H$ s.t. $x = yh$.

Proposition 6.4. There is a bijection between $\{xH \mid x \in G\}$ and $\{Hx \mid x \in G\}$ for all $x \in G, H \leq G$.

Proof. Define the map $\varphi : \{xH \mid x \in G\} \to \{Hx \mid x \in G\}$, $gH \mapsto Hg^{-1}$. Check that this is well-defined: for $g_1, g_2 \in G$ s.t. $g_1H = g_2H$, there exists $h \in H$ s.t. $g_1 = g_2h$. Then $\varphi(g_1H) = Hg_1^{-1} = H(g_2h)^{-1} = Hh^{-1}g_2^{-1} = Hg_2^{-1} = \varphi(g_2H)$. It has inverse $Hg \mapsto g^{-1}H$, with well-definedness similarly proved. This implies that φ is a bijection. □

Remark 6.5. In the prove above, we cannot define $\varphi : gH \mapsto Hg$ as in this case this is not well-defined. Specifically, if g_1 does not commute with h for $g_1 = g_2h$, $\varphi(g_2H) = Hg_1h$ which is not necessarily equal to Hg_1.

Since the number of congruence classes w.r.t. $x \in G$ does not change with choice of left or right congruence classes and depends only on H, the following definition is well-defined:

Definition 6.6 (Index). Let G be a group, with $H \leq G$. Then the number of distinct xH for $x \in G$ is the **index** of H in G, denoted as $(G : H)$.

Remark 6.7. For all $g_1, g_2 \in H$, there exists bijections $g_1H \mapsto g_2H$ and $Hg_1 \mapsto Hg_2$, given by multiplication on the left by $g_2g_1^{-1}$, and multiplication on the right by $g_1^{-1}g_2$, respectively.

Theorem 6.8 (Lagrange). Let G be a group. If $H \leq G$, and G is finite, then $|G| = |H| \cdot (G : H)$.

Proof. By Remark 6.3, G is the disjoint union of congruence classes. There are $(G : H)$ congruence classes (in the form of xH for $x \in G \setminus H$), with each having $|H|$ elements (given by $\{xh \mid h \in H\}$). □

Corollary 6.9. In particular, for all $H \leq G$, $|H| \mid |G|$. If G is finite, for all $g \in G$, $|\langle g \rangle| \mid |G|$, i.e. $g^{|G|} = g^{|\langle g \rangle| \cdot (G:\langle g \rangle)} = e$.

Example 6.10 (Fermat's Little Theorem). Let $G = (\mathbb{Z}/p\mathbb{Z})^\times$ with p prime. Then $|G| = p - 1$. For $a \in \mathbb{Z}$ s.t. $p \nmid a$, $|[a]| = p - 1$, which implies that $a^{p-1} \equiv 1 \pmod{p}$ (using the above Corollary).

We now seek to define a group structure on the congruence classes modulo a subgroup $H \leq G$. The issue is that the operation is not necessarily well-defined. The natural definition of the group operation is given via $(g_1 H, g_2 H) \mapsto (g_1 g_2 H)$. For $g_1 \equiv_\ell g_1' \pmod{H}, g_2 \equiv_\ell g_2' \pmod{H}$ we would like $g_1 g_2 \equiv_\ell g_1' g_2'$. In terms of the elements, we have $g_1 g_1'^{-1} g_2 g_2'^{-1} \in H$ and we want $g_1 g_2 g_2'^{-1} g_1^{-1} \in H$. This requires extra requirements on H.

Claim 6.11. The following two conditions are equivalent:

- For all $g_1^{-1} g_1' \in H, g_2^{-1} g_2' \in H$, this implies $(g_1 g_2)^{-1}(g_1 g_2)' \in H$.
- For all $x \in G, h \in H, xhx^{-1} \in H$.

Proof. Consider the following constructions in two directions:

$\Rightarrow$ Notice $g_1^{-1} g_1 \in H$ by hypothesis. Choose $g_2^{-1} = x, g_2' = x^{-1}$.

$\Leftarrow$ Notice $(g_1 g_2)^{-1}(g_1 g_2)' = g_2^{-1} g_1^{-1} g_1' g_2' \in H$. Choose $g_2 = g_2' = x$, with $g_1^{-1} g_1' = h$. Such g_1 and g_1' exists by first arbitrarily choose $g_1 \in H$ then compute $g_1' = g_1 h$.

□

This gives rise to the definition of normal subgroups, and the formulation quotient with respect to it, as follows.

7 Normal Subgroup, Quotient Group and Isomorphism Theorems

Definition 7.1 (Normal Subgroup). A subgroup $H \leq G$ is **normal** if for all $x \in G, xHx^{-1} \in H$, where

$$xHx^{-1} := \{xhx^{-1} \mid h \in H\}$$

Normal subgroups are denoted by $H \lhd G$.

Definition 7.2 (Quotient Group). Let G be a group, and $H \lhd G$. Then the **quotient group** G/H is the set of left equivalence classes w.r.t. H, together with the group operation $(g_1 H)(g_2 H) := (g_1 g_2)H$.

Remark 7.3. Explicitly check that this gives a group structure: by definition we have the identity element eH, with the inverse of $g_1 H = (g_1^{-1})H$. The well-definedness of the group follows from the fact that all the left congruence classes of H are well-defined, i.e. operations on it does not depends on the choice if representative, by Claim 6.11. This also gives a group homomorphism $\pi : G \to G/H$ with $x \mapsto xH$. This is indeed a group homomorphism as $\pi(ab) = (ab)H = aHbH = \pi(a)\pi(b)$.

Remark 7.4. The definition above is identical when formulated in terms of left or right congruence classes. Since we have the bijection between left and right congruence classes, to check that the definitions are identical it suffices to check that the bijection is compatible with the group operation specified. This indeed can be defined as such, as denoting the bijection to be $\Phi : xH \mapsto Hx^{-1}$ we have

$$\Phi(xH \cdot yH) = Hx^{-1} \cdot Hy^{-1} := Hy^{-1}x^{-1} = \Phi((xy)H)$$

Example 7.5. The followings give some examples of normal subgroups:

1. Trivially, $\{e\}$ and G are normal subgroups of G.
2. If G is abelian, for all $x \in G$, $H \leq G$, we have $xHx^{-1} = xx^{-1}H = H$ which implies that every subgroup is normal. Further the quotient G/H is abelian, as by Remark 7.3, the operation in G induces the operation in G/H.
3. Consider the nontrivial case, where $G = D_3 = \langle \sigma, \tau \rangle = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. Then
   - Consider $H_1 = \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$. Check $\tau\sigma\tau^{-1} = \tau\sigma\tau = \sigma^2\tau\tau = \sigma^2 \in H_1$; and $\tau\sigma^2\tau^{-1} = \tau\sigma^2\tau = \sigma\tau\tau = \sigma \in H_1$. Similarly for $\sigma\tau$ and $\sigma^2\tau$. This implies that H_1 is normal in G.
   - Consider $H_2 = \{e, \tau\}$. we have $\sigma\tau\sigma^{-1} = \sigma\tau\sigma^2 = \tau\sigma = \sigma^2\tau \notin H_2$ which implies that H_2 is not a normal subgroup.

Proposition 7.6. If $H \leq G$, then the following statements are equivalent:

1) H is a normal subgroup of G.
2) $gH = Hg$ for all $g \in G$, i.e. the left and right equivalence classes are equal.
3) $gHg^{-1} = H$ for all $g \in G$.

Proof. First see that statement 2) and 3) are equivalent, by right multiplying g and g^{-1}, respectively. For the rest of the equivalence, consider

- *3) $\implies$ 1).* This in particular implies that $xhx^{-1} \in H$ for all $h \in H$, which is exactly the definition of normal subgroups.
- *1) $\implies$ 3).* The definition of normal subgroups implies that $gHg^{-1} \subseteq H$ for all $g \in G$. Apply this to $g^{-1} \in G$ gives $g^{-1}Hg \subseteq H \implies H \subseteq gHg^{-1}$. Combining the two statements gives the desired equality. Alternatively, one can see that conjugating by g is an isomorphism onto its image, where inclusion in one side implies that this is bijective.

□

Corollary 7.7. Every subgroup with index 2 is normal.

Proof. Let $H \leq G$ be index 2. Then the left congruence classes are given by $\{H, gH\}$ for $g \in G \setminus H$; with the right equivalence classes $\{H, Hg\}$. This implies that $gH = Hg$ in terms of individual elements. By Proposition 7.6 this implies that H is normal in G. □

Proposition 7.8. Let $H \subseteq G$ be a subset. Then H is a normal subgroup in G if and only if there is some group homomorphism $f : G \to G'$ s.t. $\ker f = H$.

Proof. Consider implication in two directions:

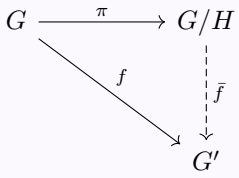
$\Rightarrow$: Consider the group homomorphism induced by the quotient structure: $\pi : G \to G/H$, $g \mapsto gH$. Then $\ker \pi = \{g \in G \mid gH = H\}$. This implies that $g \in H$.

$\Leftarrow$: By Proposition 1.16 H is a subgroup in G. Check that it is normal: for all $h \in H$, $g \in G$, we have

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)(f(g))^{-1} = e \implies ghg^{-1} \in H$$

□

Proposition 7.9 (Universal Property of Quotient Group)**.** Let G be a group, and H is normal in G. Let $\pi : G \to G/H$, and $f : G \to G'$ be group homomorphisms s.t. $H \subseteq \ker f$. Then there exists a unique group homomorphism $\bar{f} : G/H \to G'$ s.t. $\bar{f} \circ \pi = f$, i.e. the following diagram commutes:



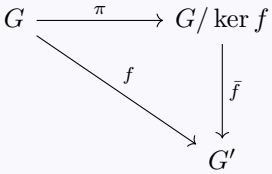
Proof. For uniqueness, notice that since the diagram is required to commute, we have $\bar{f}(gH) = f(g)$ for all $g \in G$. Since π is surjective, the behavior of $\bar{f}$ is described only on image of π, i.e. on congruence classes of form gH for $g \in G$. This gives the uniqueness of the map.

For existence, check that f is well-defined, and is indeed a group homomorphism:

- *$\bar{f}$ is well-defined.* For $gH = g'H$, we want to show that $\bar{f}(gH) = \bar{f}(g'H)$, i.e. $f(g) = f(g')$. But $gH = g'H$ implies $g^{-1}g' \in H$, i.e. $f(g) \cdot (f(g'))^{-1} = f(g \cdot g'^{-1}) \in f(H) = e$, which gives $f(g) = f(g')$.
- *$\bar{f}$ is a group homomorphism.* This is simply paraphrasing of the definition $(gH)(g'H) = (gg')H$.

□

Theorem 7.10 (First Isomorphism Theorem)**.** If $f : G \to G'$ is a surjective group homomorphism, then $G' \simeq G/\ker f$, i.e. the following diagram commutes with $\bar{f}$ an isomorphism:



Proof. Uniqueness and existence of $\bar{f}$ follows from Prop 7.9.

Check that $\bar{f}$ is an isomorphism. Surjectivity follows from the fact that f is surjective, and the diagram is required to commute. To check that $\bar{f}$ is injective, consider $\ker \bar{f}$. For, $x \in \ker \bar{f}$, $\bar{f}(x) = f(x') = e$ for $x' \in G$ s.t. $\pi(x') = x$. But this implies that $x' \in \ker f$, i.e. $\pi(x') = x = e$. □

Corollary 7.11. If $f : G \to G'$ is any group homomorphism, then $\operatorname{im} f \simeq G/\ker f$.

Remark 7.12. If $f : G \to G'$ is a group homomorphism, and H' is normal in G', then $f^{-1}(H')$ is normal in G.

Proof. Denote $p' : G' \to G'/H'$ which is the projection into the quotient. Notice that $p' \circ f(f^{-1}(H)) = e$, i.e. $f^{-1}H = \ker(p' \circ f)$. Proposition 7.8 gives that $f^{-1}(H')$ is normal. □

Remark 7.13. Let H and H' be normal in G and G', respectively. Let $f : G \to G'$, $p : G \to G/H$, $p' : G' \to G'/H'$ be group homomorphisms s.t. $f(H) \subseteq H'$. Then there exists a unique group homomorphism $\bar{f} : G/H \to G'/H'$ s.t. the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p'} \\ G/H & \xrightarrow{\bar{f}} & G'/H' \end{array}$$

Proof is by applying universal property (Proposition 7.9) on p and $p' \circ f$. It is applicable as $f(H) \subseteq H'$, i.e. $H \subseteq \ker(p' \circ f)$.

Parenthesis 7.14. Let $p : G \to G/H$ be the projection into the quotient. Then if $H \leq M$, then M is normal in G if and only if $p(M) = M/H$ is normal in G/H.

Proof. Show implications in both directions:

- $\Rightarrow$ Use Remark 7.13, with $G = G'$, $H' = M$, and f the identity map. By hypothesis that $H \leq M$, we have $f(H) \subseteq M$. The remark says that there exists a map $\bar{f} : G/H \to G/M$, with kernel $p(M)$ by the fact that the diagram commutes. Proposition 7.8 gives the fact that $p(M)$ is normal in G/H.
- $\Leftarrow$ Since M/H is normal in G/H it is valid to consider the quotient $(G/H)/(M/H)$ with the projection $p' : G/H \to (G/H)/(M/H)$, which is a group homomorphism. It is then clear that $\ker(p' \circ p) = M$, i.e. M is a normal subgroup by Proposition 7.8.

□

Theorem 7.15 (Third Isomorphism Theorem)**.** Let G a group, and H, M subgroups in G s.t. $H \leq M \leq G$. Then $(G/H)/(M/H) \simeq G/M$.

Proof. Let $p : G \to G/H$ be the projection into the quotient. Consider the group homomorphism $\alpha : G/H \to G/M$, given $xH \mapsto xM$. $\ker \alpha = \{xH \mid x \in M\} = p(M)$. By Parenthesis 7.14 we know that $p(M)$ is normal in G/H. The First Isomorphism Theorem (Theorem 7.10) gives the desired isomorphism. □

The following theorem connects the subgroups in the quotient and the subgroups in the original group:

Theorem 7.16 (Correspondence). Let G be a group, and H a normal subgroup in G. Then we have an *order-preserving* bijection:

$$\Phi : \{\text{subgroups in } G/H\} \longleftrightarrow \{\text{subgroups of } G \text{ containing } H\}$$

which maps normal subgroups to normal subgroups. Being *order-preserving* implies that $U \subseteq V$ if and only if $\Phi(U) \subseteq \Phi(V)$.

Proof. Define Φ as p^{-1} with p being the projection $G \to G/H$, as by the definition of quotient groups, we have $K \subseteq G/H \implies p^{-1}K \subseteq G$ by the fact that p^{-1} is order-preserving. Further by Parenthesis 7.14 we have $K \lhd G/H \implies p^{-1}K \lhd G$. The images are subgroups containing H, as in particular we have $p^{-1}(K) \supseteq p^{-1}(e) = H$.

Now check that the inverse of Φ exists; and the composition in two directions are both the identity. Check the followings:

- $p(p^{-1}(K)) = K$ for $K \leq G/H$. By definition $p(p^{-1})(K) \subseteq K$. The equality follows from the fact that p is surjective.
- $p^{-1}(p(M)) = M$ for $M \leq G$. $p^{-1}(p(M)) \supseteq M$ is given by definition; while $g \in p^{-1}(p(M))$ implies that $gH = xH$ for $x \in M$ as p is surjective. But this implies that $g = xh$ for some $h \in H$, i.e. $g \in M$.

□

For the formulation of the Second Isomorphism Theorem, we need to first introduce some definitions:

Definition 7.17. Let $B \leq G$. Then the **normalizer** of B in G is defined as

$$N_G(B) := \{g \in G \mid gBg^{-1} \subseteq B\}$$

Remark 7.18. By definition of normalizer, B is normal in G (the normalizer makes B a normal subgroup). This is also the largest subgroup of G in which B is normal, as suppose that there exists a larger one, it would be included in the normalizer by definition. The normalizer exists as in particular B is normal in B, implying that $B \subseteq N_G(B)$.

Notation. Let $A, B \leq G$ be subgroups. Denote

$$AB := \{ab \mid a \in A, b \in B\}$$

Remark 7.19. By definition AB is not necessarily a subgroup in G: for $a_1b_1, a_2b_2 \in AB$, $a_1b_1(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1}$ which is not in the form of AB. But if $A \subseteq N_G(B)$, this is the case as we have

$$a_1b_1b_2^{-1}a_2^{-1} = (a_1a_2^{-1})(a_2b_1b_2^{-1}a_2^{-1})$$

which gives $a_1b_1(a_2b_2)^{-1} = a'b'$ for $a' = a_1a_2^{-1}$ and $b = a_2b_1b_2^{-1}a_2^{-1} \in B$.

Theorem 7.20 (Second Isomorphism Theorem). Let A and B be subgroups of G. Further let $A \subseteq N_G(B)$. Then $A \cap B \trianglelefteq A$ and $B \trianglelefteq AB$; and we have the isomorphism $A/(A \cap B) \simeq AB/B$.

Proof. Notice $A \cap B \subseteq B$ and $A \subseteq N_G(B)$. Therefore, for all $b \in A \cap B$, $a \in A$, $aba^{-1} \in A \cap B$ by closure of operation in A and B is normal in A. Further $B \lhd AB$ as $(ab)b'(ab)^{-1} = abb'b^{-1}a^{-1} \in B$ since $a \in N_G(B)$. Consider $f : A \to AB$, $a \mapsto ab$

for some fixed $b \in B$. $\operatorname{im} f \in B$ as B is a group, and in particular $A \cap B \subseteq B$. Use the result in Remark 7.13 to get the following commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{f} & AB \\ \downarrow & & \downarrow \\ A/(A \cap B) & \xrightarrow{\bar{f}} & AB/B \end{array}$$

f is an isomorphism by definition, which implies that the induced homomorphism $\bar{f}$ is an isomorphism. □

8 The Symmetric and Alternating Group

Recall that the Symmetric group S_n is defined as

$$S_n := \{f : \{1, \dots, n\} \to \{1, \dots, n\} \mid f \text{ bijective}\}$$

with operation given by composition of maps.

Notation. For $\sigma \in S_n$, it is often denoted by the one-to-one mappings:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Example 8.1. The composition of maps can be simply read off from the relations: for example

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{Id}$$

Definition 8.2 (Cycle). In S_n, for $k \geq 2$, a k-**cycle** in S_n is a permutation $\sigma = (a_1, \dots, a_k)$ for $a_1, \dots, a_k \in \{1, \dots, n\}$ where $\sigma(a_i) = a_{i+1}$ for $i < k$; and $\sigma(a_k) = a_1$; and $\sigma(i) = i$ for $i \notin \{a_1, \dots, a_k\}$.

Example 8.3. Adopting the notation for cycles, Example 8.1 can be written as $(321)(231) = e = \mathrm{Id}$.

Definition 8.4 (Transposition). **Transposition**s in Symmetric groups are 2-cycles (ij) for $i < j$.

Remark 8.5. The following gives some basic properties of the Symmetric group:

1. Let $\sigma = (a_1 \dots, a_k)$ be a k-cycle. Then $|\sigma| = k$.
2. If σ and τ are disjoint cycles, i.e. the sets of elements that they act nontrivially on are disjoint, then $\sigma\tau = \tau\sigma$.
3. For all $\sigma \in S_n$, it can be written as a product of disjoint cycles, unique up to reordering. This can be constructed by chasing the image of any element x in σ, which decomposes σ into the product of a cycle and something else. The rest

part of σ acts trivially on x, which implies that they are disjoint.

4. Cycle $(a_1 \dots a_k) = (a_1 a_k) \dots (a_1 a_3)(a_1 a_2)$. This implies that every $\sigma \in S_n$ can be decomposed into transpositions.

Parenthesis 8.6. All groups with 2 elements are isomorphic. $G = \{e, a\}$ gives $a \cdot a = e$, which implies that $G \simeq \mathbb{Z}/2\mathbb{Z}$.

Example 8.7. Consider symmetric groups with small n:

1. $S_1 = \{e\}$.
2. $S_2 = \{e, (12)\}$. By Parenthesis 8.6, this is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.
3. S_3 is not abelian: Let $\sigma = (123)$, $\tau = (12)$, we have $|\sigma| = 3$, $|\tau| = 2$, and further $S_3 = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. This implies that $S_3 \simeq D_3$.

Definition 8.8 (Inversion). **Inversion**s in σ are elements in the set $\{(i, j) \mid 1 \le i < j \le n, \sigma(i) > \sigma(j)\}$.

Definition 8.9 (Signature). Consider group homomorphism $\varepsilon : S_n \to \{\pm 1\}$ where the operation in $\{\pm 1\}$ is integer multiplication, defined as $\sigma \mapsto (-1)^{(\#\text{ inversions in } \sigma)}$. σ is even if $\varepsilon(\sigma) = 1$; and odd if $\varepsilon(\sigma) = -1$.

Example 8.10. Transpositions are odd. For $\sigma = (ij)$ with $i < j$, written out explicitly it is given by the map

$$\begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & n \\ 1 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$$

The inversions are given by $\{(i, k), (k, j) \mid i < k < j\} \cup \{(i, j)\}$. The first part has even elements which implies that $\varepsilon(\sigma) = (-1)^1 = -1$.

Example 8.11. If σ is a product of k transpositions, then $\varepsilon(\sigma) = (-1)^k$. By Remark 8.5 4., any k-cycle can be decomposed into $(k-1)$ transpositions, which implies that its signature is $(-1)^{k-1}$.

Proposition 8.12. ε is a group homomorphism.

Proof. Consider $R = \mathbb{Q}[x_1, \dots, x_n]$ the polynomial ring, where $\mathbb{Q}$ is a field. This gives a domain as every nonzero element in a field is invertible.

Define $\Delta := \Pi_{i<j}(x_i - x_j)$. R being a domain implies that this is nonzero. Given $\sigma \in S_n$, we can construct a map $\varphi_\sigma : R \to R$ which is a morphism of $\mathbb{Q}$-algebra (homomorphism that is $\mathbb{Q}$-linear). By the universal property of multivariate polynomial ring, to specify φ_σ, it suffices to specify the image of x_is. Define $\varphi_\sigma(x_i) = x_{\sigma(i)}$ for all i.

Notice that $\varphi_\sigma(\Delta) = \Pi_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}) = \varepsilon(\sigma) \cdot \Delta$. Now consider the map $\varphi : \sigma \mapsto \varphi_\sigma$. Notice that this is a group homomorphism: in particular $\varphi_\sigma \circ \varphi_\tau = \varphi_{\sigma\tau}$ as maps are associative. Apply to Δ gives $\varepsilon(\sigma)\varepsilon(\tau) = \varepsilon(\sigma\tau)\Delta$, i.e. $(\varepsilon(\sigma)\varepsilon(\tau) - \varepsilon(\sigma\tau))\Delta = 0$. Since R is a domain, and $\Delta \neq 0$, this implies that $\varepsilon(\sigma)\varepsilon(\tau) = \varepsilon(\sigma\tau)$ which gives the desired group homomorphism. □

Definition 8.13 (Alternating Group). The **Alternating Group** A_n is defined as $A_n := \ker \varepsilon_n$ for $\varepsilon_n : S_n \to \{\pm 1\} \simeq S_2$

Remark 8.14. For $n \geq 2$, transpositions exist, which implies that ε is surjective, with $e \mapsto 1, \tau \mapsto -1$ for τ some transposition. The First Isomorphism Theorem (Theorem 7.10) gives that $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$.

9 Classification of Groups of Small Order

Proposition 9.1. If G is a finite group, and $|G| = p$ which is prime, then $G \simeq Z/p\mathbb{Z}$.

Proof. Choose $x \in G$ s.t. $x \neq e$. Denote $H = \langle x \rangle$. Clearly $|H| \geq 2$, as in particular both x and e are in H. By Lagrange, $|H| \mid p$, which implies that $H = G$, i.e. G is cyclic. Proposition 3.7 gives the desired isomorphism. □

The proposition above gives that for $p = 2, 3, 5, 7$, the group of order p is isomorphic to the corresponding $\mathbb{Z}/p\mathbb{Z}$. The following classifies group of order 4 and 6:

Proposition 9.2. For group G with order 4, either $G \simeq \mathbb{Z}/4\mathbb{Z}$, or $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Consider the following two cases:

- There exists some $x \in G$ s.t. $|x| = 4$, i.e. G is cyclic. Then by Proposition 1.9, $G \simeq \mathbb{Z}/4\mathbb{Z}$.
- G is not cyclic. Lagrange's Theorem gives that for all $x \in G$, $|x| \mid 4$, where the only nontrivial case is $|x| = 2$. Then $G = \{e, a, b, c\}$ with $a^2 = b^2 = c^2 = e$. Notice $ab \neq a, b, e$, which implies that $c = ab$. This characterization gives the isomorphism to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ given by $a \mapsto (1, 0)$ and $b \mapsto (0, 1)$

□

Remark 9.3. In the proof above, notice $ba \neq e, a, b$, i.e. $c = ab = ba$. Therefore it is abelian. This is often referred to as the Klein 4-gruop.

Now consider the case where G has 6 elements:

Proposition 9.4. If $|G| = 6$, then either $G \simeq \mathbb{Z}/6\mathbb{Z}$, or $G \simeq D_3$.

Proof. Consider the two cases separately:

- G is abelian. By Proposition 3.7, $G \simeq \mathbb{Z}/6\mathbb{Z}$.
- G is not abelian. Lagrange gives that for all $x \in G$ s.t. $x \neq e$, $|x| = 2$ or 3.

  Lemma 9.5. If $|G|$ is even, there exists an element of order 2 in G.

  Proof. Suppose not. Then in particular there cannot exist any element of even order, i.e. for all $x \in G$, $x^{-1} \neq x$. Then consider pairs (x, x^{-1}) for all x. Together with e, this gives odd number of elements, which is a contradiction. □

Claim that there exists $x \in G$ s.t. $|x| = 3$. Suppose not. Then for all $x \in G, x^2 = e$. By proof for the case where there are 4 elements in the group, this gives that G is abelian, i.e. it has a subgroup $\{e, x, y, xy\}$ for $x, y \neq e$. But this gives a contradiction with Lagrange's Theorem.

Let $|\sigma| = 3$. This gives the explicit expression of elements in G: $G = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. Notice that $\tau\sigma \neq e, \tau, \sigma, \sigma^2$ by the fact that they are nontrivial and have different order. Then either

- $\tau\sigma = \sigma\tau$. But then $(\sigma\tau)^2 = \sigma^2 \neq e$, $(\sigma\tau)^3 = \tau$, which implies that $(\sigma\tau)$ generates G. This is a contradiction.
- $\tau\sigma = \sigma^2\tau$. Then this characterize that $G \simeq D_3$.

□

Theorem 9.6 (Structural Theorem for Finitely Generated Abelian Groups)**.** Let G be a finitely generated abelan group. Then

$$G \simeq \mathbb{Z}^r \times \Pi_{i \in I}(\mathbb{Z}/p_i^{m_i}\mathbb{Z})$$

for $r \in \mathbb{Z}_{\geq 0}$, p_i prime, $m_i \in \mathbb{Z}_{>0}$; and pairs (p_i, m_i) are unique up to reordering.

The proof quite resembles that of Structural Theorem for finitely generated modules over PIDs, and is not repeated here.

Remark 9.7. Since $\mathbb{Z}$ has infinitely many elements, this implies that if G being a finitely generated abelian group is finite, then $r = 0$, and $G \simeq \Pi_{i \in I}\mathbb{Z}/p_i^{m_i}\mathbb{Z}$.

Example 9.8. Structural theorem directly gives the classification of isomorphism classes of abelian groups with 8 elements: $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

10 Group Action on Sets

Definition 10.1 (Group Action)**.** Let G be a group, and X a set. A **(left) action** of G on X is a map $G \times X \to X$, written $(g, x) \mapsto gx$, satisfying

- $ex = x$ for all $x \in X$.
- $g_1(g_2x) = (g_1g_2)x$ for all $g_1, g_2 \in G$, $x \in X$.

Proposition 10.2. Left (and therefore right) group actions correspond to group homomorphisms $\varphi : G \to S_X$, where $S_X := \{f : X \to X \mid f \text{ bijection}\}$ is the set of bijective maps from X to itself.

Proof. Notice that $\varphi_e = \mathrm{Id}$; and for all $g, h \in G$, $\varphi_g \circ \varphi_h = \varphi_{gh}$ for all $g, h \in G$, which gives $\varphi_g \circ \varphi_{g^{-1}} = \varphi_e = \mathrm{Id}$. Therefore, taking S_X as a group, with the identity being the identity map, and operation the composition of maps, φ gives a group homomorphism between g and S_X.

For the other direction, given a group homomorphism $\varphi : G \to S_X$, we get a left action on X given by $(g, x) \mapsto \varphi(g)(x)$. □

Example 10.3. The following gives some examples of group actions:

1. Recall that S_X attains a group structure. Therefore, for all X, S_X acts on X by $(f, x) \mapsto fx$ with the corresponding homomorphism $S_X \to S_X$.
2. Consider geometrically, D_n acts on the vertices of a regular n-gon.
3. Let G be a group, and $H \leq G$. Then we have an action of G on the left congruence classes of G modulo H, given by $(g, aH) \mapsto (ga)H$. Check that this is well-defined: if $aH = bH$, want to show that $(ga)H = (gb)H$. Hypothesis gives that $aH = bH$, i.e. $a^{-1}b \in H$. But $(ga)^{-1}(gb) = a^{-1}g^{-1}gb = a^{-1}b \in H$, which gives the equality $(ga)H = (gb)H$.
4. A group acts on itself via the action of conjugation, given by $(g, x) \mapsto gxg^{-1}$. Clearly, $(e, x) \mapsto exe^{-1} = x$; and $(gh, x) \mapsto (ghxh^{-1}g^{-1}) = (g, (h, x))$.

Definition 10.4. Let $x, y \in X$. Then for a group action of G on X, $x \sim y$ if there exists $g \in G$ s.t. $gx = y$.

Remark 10.5. This is an equivalence relation:

- *Reflexive.* let $g = e$.
- *Symmetric.* Suppose that there exists g s.t. $gx = y$. Then multiplying g^{-1} on th left gives $g^{-1}(gx) = g^{-1}y$, i.e. $x = g^{-1}y$.
- *Transitive.* Suppose that there exists $g, h \in G$ s.t. $y = gx, z = hy$, then $z = (hg)x$.

Definition 10.6 (Orbit). Let there be an action of G on X. the **orbit** of $x \in X$ is defined as

$$\mathcal{O}(x) = \{g(x) \mid g \in G\}$$

Definition 10.7 (Stabilizer). For all $x \in X$, the **stabilizer** of x is

$$\mathrm{Stab}_G(x) := \{g \in G \mid gx = x\}$$

Remark 10.8. The stabilizer $\mathrm{Stab}_G(x)$ is a subgroup of G. Use the characterization of subgroups:

- By definition of group action, $e \in \mathrm{Stab}_G(x)$, which is the unit element.
- If $g, h \in G$, then $gx = x \implies x = g^{-1}x$, i.e. $g^{-1} \in G$. Therefore $g^{-1}h \in G$.

Lemma 10.9. For all $x \in X$, there is a bijection

$$(G/\mathrm{Stab}_G(x))_\ell \longleftrightarrow \mathcal{O}(x)$$

where $(G/\mathrm{Stab}_G(x))_\ell$ denotes the left congruence classes of $\mathrm{Stab}_G(x)$. In particular, $|\mathcal{O}(x)| = (G : \mathrm{Stab}_G(x))$, i.e. if G is finite, then $|\mathcal{O}(x)| \mid |G|$.

Proof. Notice that $gx = hx$ implies that $(g^{-1}h)x = x$, i.e. $g^{-1}h \in \mathrm{Stab}_G(X) \implies g\mathrm{Stab}_G(x) = h\mathrm{Stab}_G(x)$; and the implication in the inverse direction is similar. This gives a bijection $\{gx \mid x \in G\} \to (G/\mathrm{Stab}_G(x))_\ell$ given by $gx \mapsto g\mathrm{Stab}_G(x)$. □

Definition 10.10 (Transitive). The action of G on X is **transitive** if there is only one orbit, i.e. for all $x, y \in X$, there exists some $g \in G$ s.t. $x = gy$.

Corollary 10.11. If the action of G on X is transitive, then for all $x \in X$, $\mathcal{O}(x) = X$. Let $H = \mathrm{Stab}_G(x)$, then there exists a bijection $(G/H)_\ell \to X$ given by $gH \mapsto gx$. This corresponds to the action of G on $(G/H)_\ell$: $(g, aH) \mapsto (ga)H$.

Remark 10.12. If G acts on X, then $X = \amalg_{i \in I} \mathcal{O}(x_i)$, where x_is are representatives in each orbit. In particular this can be split as

$$|x| = \sum_{x_i} |\mathcal{O}(x_i)| = |\mathrm{Fix}(x)| + \sum_{|\mathcal{O}(x_i)| \geq 2} |\mathcal{O}(x_i)|$$

where $\mathrm{Fix}(x) := \{x \in X \mid gx = x,\ \forall g\}$, i.e. points that are stabilized by the whole group.

Definition 10.13 (Center). Let G be a group. The **center** of g is defined as

$$Z(G) := \{x \in G \mid xg = gx,\ \forall g \in G\}$$

Definition 10.14 (Centralizer). Given $x \in G$, the **centralizer** of x in G is defined as

$$C_G(x) := \{g \in G \mid xg = gx, \text{i.e. } gxg^{-1} = x\}$$

i.e. in which x is in the center. One can also consider the centralizer of a subgroup in a similar manner.

Example 10.15. Fix G a group, and consider the action of G on itself by conjugation. x and y are conjugate if $\mathcal{O}(x) = \mathcal{O}(y)$, i.e. there exists $g \in G$ s.t. $x = gyg^{-1}$. In particular, in this case the stabilizers are the same as the centralizers.

Notice that with the action defined as conjugation, $|\mathcal{O}(x)| = 1$ if and only if $x \in Z(G)$. This gives the class equation

$$|G| = |Z(G)| + \sum_i (G : C_G(x_i)) \tag{1}$$

where x_i vary over the set of conjugate classes with more than 1 element.

Definition 10.16 (p-group). If p is a prime integer, a **p-group** is a group of order p^m for some $m \geq 1$.

Proposition 10.17. If G is a p-group, then $Z(G) \neq \{e\}$. Further by the class equation, $p \mid Z(G)$.

Proof. Consider divisibility by p on both sides of the class equation. For the second term on RHS, for all i s.t. $G \neq C_G(x_i)$, since $C_G(x_i)$ is a subgroup by Lagrange $(G : C_G(x)) \mid |G| = p^m$. Further as $G \neq C_G(x_i)$, $p \mid (G : C_G(x))$, $|G| = p^m$ gives $p \mid |G|$, which implies that $p \mid |Z(G)|$. □

Corollary 10.18. If p is prime, then every group with p^2 elements is abelian:

Proof. By structrual theorem, either $G \simeq \mathbb{Z}/p^2\mathbb{Z}$, or $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Since G is a p-group, by Proposition 10.17, $p \mid |Z(G)|$. Lagrange gives $|Z(G)| \mid p^2$. Then either:

- $|Z(G)| = p^2$. Then G is by definition abelian.
- $|Z(G)| = p$. Notice that $Z(G) \trianglelefteq G$. Consider the group $G/Z(G)$. This has p elements, and is therefore cyclic. Let $xZ(G)$ be a generator of $G/Z(G)$. Then for all $a, b \in G$, there exists $i, j \in \mathbb{Z}$ and $a', b' \in Z(G)$ s.t. $a = x^i a'$, $b = x^j b'$. But notice that $ab = ba$, i.e. G is abelian, which is a contradiction.

□

Remark 10.19. The above result cannot be generalized. That is, for $H \lhd G$, H abelian and G cyclic, G is not necessarily abelian. Consider the counterexample where $G = S_3$, $H = \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$.

Remark 10.20. If G acts on X, G also acts on $\mathcal{P}(X)$, the power set of X. Explicitly, for $A \in \mathcal{P}(X)$, $gA = \{gx \mid x \in A\}$. This also extends to the conjugacy of a subset in a similar manner.

If X is a group (e.g. G itself) then this gives a group automorphism, which sends subgroups by subgroups, via left-composing with a group element.

11 Sylow Theorems

Lagrange gives that for a finite group G and $H \leq G$, $|H| \mid |G|$, and $|x| \mid |G|$ for all $x \in G$. It is then of our interest to see how much we can get in the other direction: given a group G, can we get any information the order of its subgroups, and the number of them?

It is impossible that we have the followings:

- For all $m \mid |G|$, there exists $x \in G$ s.t. $|x| = m$. For example, it is impossible to have such x for $m = |G|$ in G non-cyclic.
- For all $m \mid |G|$, there exists a subgroup of G of order m. In particular, in a subsequent theorem (Theorem 13.3) we will show that A_5 has non nontrivial normal (e.g. index-2) subgroups, i.e. no subgroup of order 30.

Theorem 11.1 (Cauchy). For G a finite group, and p prime s.t. $p \mid |G|$, there exists $x \in G$ s.t. $|x| = p$.

Proof. First consider the simple case where G is abelian, and then reduce the general case to the abelian one.

Case 1. G is abelian. Follows from the structural theorem for finite abelian groups: G is isomorphic to a product of groups where one of them is $\mathbb{Z}/p^m\mathbb{Z}$ for $m \in \mathbb{Z}_{>0}$. This gives an element with order p.

Alternatively, prove by contradiction. Suppose that for all $x \in G$, $|x| \neq p$. Then for all $x \in G$, $p \nmid |x|$. (Otherwise for $|x| = m$ and $p \mid m$, $\left|x^{m/p}\right| = p$.) Let N be the largest common multiple of all order of elements in G, then $(p, N) = 1$. Let $x_1, \ldots, x_n$ be the elements of G. Consider the group homomorphism

$$f : \mathbb{Z}^n \to G, \qquad f(a_1, \ldots, a_n) = x_1^{a_1} \cdots x_n^{a_n}$$

Notice that if $(a_1, \ldots, a_n) \in H := \{(b_1, \ldots, b_n) \mid N \mid b_i, \forall i\}$, then $f(a_1, \ldots, a_n) = e$ since $|x_i| = a_i \mid N \implies x_i^N = e$. This implies that $H \subseteq \ker f$. Using the universal property of quotient groups, we have a group homomorphism

$$\bar{f} : \mathbb{Z}^n/H \simeq (\mathbb{Z}/N\mathbb{Z})^n \to G, \qquad \overline{(a_1, \ldots, a_n)} \mapsto x_1^{a_1} \cdots x_n^{a_n}$$

Since taking $a_i = 1$ and $a_{j(j\neq i)} = 0$ gives x_i, $\bar{f}$ is surjective. the first isomorphism theorem gives $G \simeq (\mathbb{Z}/N\mathbb{Z})^n / \ker(\bar{f})$. Lagrange gives $|G| \mid |\mathbb{Z}/N\mathbb{Z}|^n = N^n$, which gives a contradiction as $p \mid |G| \mid N^n$, but $(p, N) = 1$ by hypothesis.

Case 2. G is not necessarily abelian. Argue by induction on the order of the group:

- *Base case.* $|G| = 1$. The statement is vacuous as the hypothesis is not satisfied.
- *Inductive step.* Suppose that the theorem is true for all groups G' with $|G'| < |G|$. Use the class equation

$$|G| = |Z(G)| + \sum_i (G : C_G(x_i)) \qquad \text{where } x_i \text{ runs over set of representatives of conjugacy classes}$$

If we can find a subgroup $H < G$ s.t. $p \mid |H|$, then we can find $x \in H < G$ of order p by induction hypothesis, which by definition also has order p in G.

Now assume that $p \nmid |H|$ for all $H < G$. Lagrange gives $p \mid (G : H)$ for all H as $p \mid |G|$. In particular, for all representative of conjugacy classes x_i, $p \mid (G : C_G(x_i))$, and by class equation we have $p \mid Z(G)$. Since $Z(G) \lhd G$, this gives a contradiction.

□

Corollary 11.2. If G is a finite group and p is a prime, then G is a p-group if and only if the order of any element in G is a power of p.

Proof. $\Rightarrow$: Lagrange. $\Leftarrow$: Cauchy, via considering the quotient by subgroup generated by any element recursively. □

Definition 11.3 (p-Sylow Subgroup)**.** Let G be a finite group with order $|G| = p^m n$ for p prime, and $(n, p) = 1$. A p-**Sylow subgroup** is a subgroup $H \leq G$ satisfying $|H| = p^m$.

Theorem 11.4 (Sylow I)**.** Let G be a finite group and p a prime. If $p \mid |G|$, then G has a p-Sylow subgroup

Proof. Apply induction on $|G|$. The theorem is vacuous for $|G| = 1$. Now assume that for all G' s.t. $|G'| < |G|$ the theorem holds.

Case 1. $p \mid Z(G)$. By the result from the abelian case of Cauchy, there exists $g \in Z(G)$ s.t. $|g| = p$. Let $k = \langle g \rangle$. Then $K \trianglelefteq G$ as in particular $K \leq Z(G)$. Consider $G' = G/K$, and apply the inductive hypothesis. Since $|G| = p^m n$, either $m = 1$, where K gives the desired p-Sylow group; or for $m > 1$ since $|K| = p$, $|G'| = p^{m-1} n < |G|$. Inductive Hypothesis gives that there exists a p-Sylow subgroup $H' \leq G'$ with $|H'| = p^{m-1}$. Use this in the quotient to construct a p-Sylow subgroup in G: Let $\pi : G \to G/K$ be the quotient, and consider $H = \pi^{-1}(H')$. Notice that $K = \pi^{-1}(e) < \pi^{-1}(H') = H$, and $H' \simeq H/K$. Lagrange gives $|H| = |H'| \cdot p = p^m$, which implies that H is a p-Sylow subgroup.

Case 2. $p \nmid |Z(G)|$. Consider again the class equation

$$|G| = |Z(G)| + \sum_i (G : C_G(x_i)) \qquad \text{where } x_i \text{ runs over set of representatives of conjugacy classes}$$

Since $|G| = p^m n$, in particular $p \mid |G|$. By divisibility, there exists x_i s.t. $p \nmid (G : C_G(x))$. Since $C_G(x_i) \leq G$, hyperref[thm: Lagrange]Lagrange gives $p \mid C_G(x_i)$, i.e. $|C_G(x_i)| = p^m q$ for $q < n$ (otherwise $x_i \in Z(G)$, which falls back to the first case). In particular, $|C_G(x_i)| < |G|$. Apply the inductive hypothesis gives that there exists a p-Sylow subgroup in $C_G(x_i)$, which by counting the order is also a p-Sylow subgroup in G.

□

Remark 11.5. Sylow I implies Cauchy, as by the existence pf a p-Sylow subgroup using Corollary 11.2 the order of any element must be a power of p; and there is only one element of order 1 (the unit). We present the prove in such sequence as we have used Cauchy in the proof of Sylow I.

Theorem 11.6 (Sylow II)**.** For G a finite group, and p a prime s.t. $p \mid |G|$. For $K \leq G$ any p-subgroup and $H \leq G$ any p-Sylow subgroup, then there exists $a \in G$ s.t. $K \subseteq aHa^{-1}$.

Corollary 11.7. For H and H' p-Sylow subgroups of G, there exists $a \in G$ s.t. $H' = aHa^{-1}$ (by argument on order). That is, p-Sylow subgroups conjugate into each other.

Theorem 11.8 (Sylow III)**.** Let n_p be the number of p-Sylow subgroups in G. Then

1) $n_p \equiv 1 \pmod{p}$.
2) $n_p = (G : N_G(H))$ for any H that is a p-Sylow subgroup. Since $H \leq N_G(H) \leq G$, in particular by Lagrange we have $n_p \mid \frac{|G|}{|H|}$.

Remark 11.9. More generally, for all $H \leq K \leq G$ we have $(G : H) = (G : K) \cdot (K : H)$ for G finite, via counting the elements.

Proof of Theorem 11.6 and 11.8. We first prove a general result, and then use it to show both Sylow II and Sylow III.

Consider the action of G on subgroups of G by conjugation. Given $H' \leq G$, by definition we have $\mathrm{Stab}_G(H') = N_G(H')$. Fix a p-Sylow subgroup H of G. Let $\mathcal{H} = \{H = H_1, \dots, H_r\}$ be the orbit of H under conjugation of elements in G. Let $A \leq G$ a p-subgroup, and consider the inclusion

$$L = A \cap N_G(H)/A \cap H \hookrightarrow N_G(H)/H = R$$

Since A is a p-subgroup, L can be identified as a subgroup of A, whose order is a power of p. On the other hand, $|R| = \frac{|N_G(H)|}{|H|} \mid \frac{|G|}{|H|} \nmid p$. Further Lagrange gives $|L| \mid |R|$, i.e. $L = \{e\} \implies A \cap N_G(H) = A \cap H$.

Conjugation induces an action of A on $\mathcal{H}$. After reordering, let $H_1, \dots, H_s \in \mathcal{H}$ be the representatives of the orbits of the action. Then

$$r = \sum_{i=1}^{s} |\mathcal{O}(H_i)| = \sum_{i=1}^{s} (A : \mathrm{Stab}(H_i)) = \sum_{i=1}^{s} (A : A \cap N_G(H_i)) = \sum_{[} i = 1]^{s} (A : A \cap H_i)$$

Now use the equality above to prove the theorems:

1) Take $A = H$. Since for all i, $|H_i| = |H|$, $H \subseteq H_i$ if and only if $i = 1$. Further since A is a p-group, $(A : A \cap H_i)$ is a power of p for all i. This gives $r \equiv 1 \pmod{p}$ (Sylow III 1)).
2) Take $A = K$ in Sylow II. By the construction in 1), there exists $i \leq s$ s.t. $A \subseteq H_i$. This proves Sylow II.
3) By Sylow II any two p-Sylow subgroups are conjugate, which implies that $r = n_p$ and that there is only one orbit for such H_i. Then

$$r = |\mathcal{O}(H)| = \frac{|G|}{|\mathrm{Stab}_G(H)|} = (G : \mathrm{Stab}_G(H)) = (G : N_G(H))$$

□

Definition 11.10 (Characteristic Subgroup). A subgroup $H \leq G$ is a **characteristic subgroup** of G if it is preserved by any $\sigma \in \mathrm{Aut}(G)$.

Remark 11.11. In Sylow III, suppose that $n_p = 1$, and let H be the unique p-Sylow subgroup. Since $\sigma \in \mathrm{Aut}(G)$ maps subgroups to subgroups, $|\sigma(H)|$ is also a p-Sylow subgroup (as p-Sylow subgroups are constrained by only cardinality). This implies that $\sigma(H) = H$, i.e. H is a characteristic subgroup of G.

Example 11.12. Let G be a finite group, with $H \trianglelefteq G$. Suppose that $p \mid |H|$. Let K be the unique p-Sylow subgroup of H. Then $K \trianglelefteq G$ as $g \in G$ gives $\sigma \in \mathrm{Aut}(H)$ which preserves K. However, in general from $K \trianglelefteq H$ and $H \trianglelefteq G$ we cannot necessarily get $K \trianglelefteq G$.

12 Application of Sylow Theorems

Sylow theorems, especially Sylow III, gives constraints on the number of p-Sylow subgroups. This, together with the constraint of the order of the group, could reveal the group structure with little extra information.

The first application involves classifying groups with order a product of two primes.

Proposition 12.1. Let G be a group of order pq, with p and q distinct primes, and $p < q$. If $n_p = 1$, then G is abelian and cyclic.

Proof. Notice first that $n_q = 1$ as by Sylow III $n_q \mid \frac{|G|}{q} = p$, and $n_q \not\equiv 1 \pmod q$. Since $p < q$, $n_q = 1$.

Therefore in G we have a unique p- and q-Sylow subgroup. Let them be P and Q, with p and q elements, respectively. Since $n_p = 1$, by Corollary 11.7 $P \trianglelefteq G$. Consider the map

$$\varphi : Q \to \mathrm{Aut}(P) \qquad y \mapsto (x \mapsto (yxy^{-1}))$$

This is indeed an automorphism on P as P is normal in G. Since both P and Q has prime order, they are both cyclic. Then $\varphi \simeq (\mathrm{Hom}(\mathbb{Z}/q\mathbb{Z}, \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})))$ where LHS has q elements and RHS has $(p-1)$ elements. Lagrange implies that $|\mathrm{im}\ \varphi| \mid (p-1)$ and $|\mathrm{im}\ \varphi| \mid (q)$ as $\mathrm{im}\ \varphi$ is a subgroup of Q and $\mathrm{Aut}(P)$. Since q is prime, and $q > p > p-1$, $|\mathrm{im}\ \varphi| = 1$, i.e. for all $x \in P, y \in Q$, $yxy^{-1} = x \implies yx = xy$, that is elements in P and Q commute.

Since both P and Q are cyclic, there exists $x \in P$ and $y \in Q$ s.t. $P = \langle x \rangle, Q = \langle y \rangle$. Consider the order of pq: let it be m, i.e. $(xy)^m = e$. This gives $x^m = y^{-m} = (y^m)^{-1}$. Lagrange gives $|P \cap Q| \mid p, q$, which implies that $|P \cap Q| = 1$, $P \cap Q = \{e\}$. Further notice that $x^m, (y^m)^{-1} \in P \cap Q$, which gives $p \mid m, q \mid m \implies pq \mid m$, i.e. $pq \mid |xy|$. Using the fact that $|xy| \mid |G| = pq$ we get $|xy| = pq$. Therefore, $G = \langle pq \rangle$, which is cyclic. □

Proposition 12.2. Let G be a group of order pq, with p and q distinct primes, and $p < q$. If $q \equiv 1 \pmod p$ (i.e. n_p is not necessarily 1), then there exists non-abelian group G with order pq.

Proof. Construction of non-abelian groups often results from maps as they generally do not commute.

Consider $(\mathbb{Z}/q\mathbb{Z})^\times$ with order $(q-1)$. Since $p \mid (q-1)$, Cauchy gives that there exists $r \in \mathbb{Z}$ s.t. $r \not\equiv 1 \pmod q$, and $r^p \equiv 1 \pmod q$ (i.e. r is a nontrivial element in $\mathbb{Z}/q\mathbb{Z}$ with order p). Consider

$$\alpha, \beta : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \qquad \alpha : x \mapsto (x+1) \qquad \beta : x \mapsto \bar{r}x$$

Since q is prime, $\bar{r}$ has an inverse for all r, which implies that α and β are bijections. Further notice that $|\alpha| = q$, $|\beta| = |\bar{r}| = p$. Notice

$$\beta\alpha\beta^{-1}(x) = \bar{r}(\bar{r}^{-1}x + 1) = x + \bar{r} \implies \beta\alpha = \alpha^r\beta$$

which does not necessarily commute. This gives a non-abelian group with order pq:

$$\langle \alpha, \beta \rangle = \{\alpha^i\beta^j \mid i \in [\![0, q-1]\!], j \in [\![0, p-1]\!]\}$$

□

> **Remark 12.3.** Up to isomorphism, this is the only non-abelian group of order pq. The only adjustment that we can make is to vary r; but to maintain its order p, it can only vary through the primitive p-th roots in $\mathbb{Z}/q\mathbb{Z}$; and we have the isomorphism via varying r.

The second application uses Sylow Theorems to count elements, which narrows down the possibilities of the structure of a particular group.

> **Proposition 12.4.** Suppose that G is a group, with $|G| = 30 = 2 \cdot 3 \cdot 5$. Then there is an index-2 subgroup H.

Proof. Let P and Q be the p-Sylow subgroups with 3 and 5 elements, respectively. They exist by Sylow I.

Case 1. $P \trianglelefteq G$ (or $Q \trianglelefteq G$, respectively). By the Second Isomorphism Theorem we have $P/P \cap Q \simeq PQ/Q$. This is applicable as we have $Q \leq N_G(P) = G$. Use with the corresponding result for Q we get $|P \cap Q| \mid 3, 5 \implies |P \cap Q| = 1$. Then $|PQ| = |P| \cdot |Q| = 3 \cdot 5 = 15$ which gives a valid H,

Case 2. Neither P or Q is normal in G. Sylow II gives $n_3(G) > 1$, and $n_5(G) > 1$. Since $|G| = 30$, we have $n_5(G) \mid \frac{30}{5} = 6 \implies n_5(G) = 6$ since $n_5(G) \equiv 1 \pmod 5$. Similarly we get $n_3(G) = 10$. Since any two 5-Sylow subgroups have intersection $\{e\}$, G has $6 \times (5-1) = 24$ elements of order 5. Similarly G has $10 \times (3-1) = 20$ elements of order 3. But then G has at least $20 + 24 = 44 > 30$ elements, which is a contradiction.

□

13 Finite Simple Groups

Consider G a finite group, with $H \lhd G$. We would like to build G with H and G/H. In the opposite direction, we would like to know when the group cannot be further decomposed in this manner.

Definition 13.1 (Simple). A group G is **simple** if $G \neq \{e\}$, and there does not exist a normal subgroup H s.t. $H \neq G$ and $H \neq \{e\}$.

Proposition 13.2. An abelian group G is simple if and only if $G \simeq \mathbb{Z}/p\mathbb{Z}$ for p prime.

Proof. Since G is abelian, every subgroup is normal. Therefore, G is simple if and only if it has non nontrivial subgroups. $G \neq \{e\}$ implies that for all $x \in G$, $x \neq e$, $\langle x \rangle = G$, then $G \simeq \mathbb{Z}/n\mathbb{Z}$. Suppose that $n = pq$ for $p, q \neq 1$, then $|x^p| = \frac{n}{p} < n$.

Converse is clear: $\mathbb{Z}/p\mathbb{Z}$ only has trivial proper subgroups for p prime, by divisibility. □

Theorem 13.3. If $n \geq 5$, then A_n is simple.

Remark 13.4. For $n = 1, 2$, $A_n = \{e\}$, which is trivial. For $n = 3$, $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ which is simple since 3 is a prime.

For $n = 4$, we have $\{e\} \lhd K_4 \lhd A_4$, where K_4 embeds into A_4 via

$$H = \{e, (12)(34), (13)(24), (14)(23)\} = \{\sigma \in A_4 \mid \sigma^2 = e\}$$

which is a subgroup preserved by conjugation.

Proof of Theorem 13.3. Proceed via induction:

- *Base case.* $n = 5$. $|A_5| = 3 \cdot 4 \cdot 5 = 60$. Argue by contradiction: suppose that there exists $H \trianglelefteq A_5$, with $H \neq A_5$, $H \neq \{e\}$.

Case 1. $5 \mid |H|$. First notice that $n_5(A_5) > 1$, as we have two distinct 5-cycles $\langle (12345) \rangle, \langle (13425) \rangle$. By divisibility there exists a 5-Sylow subgroup in H, which is also a 5-Sylow subgroup in A_5. Since $H \trianglelefteq A_5$, and by Sylow II all p-Sylow subgroups conjugate into each other, all 5-Sylow subgroups in A_5 are also in H. In particular, this implies that $n_5(H) = n_5(A_5) > 1$, and Sylow III gives

$$n_5(A_5) \mid \frac{60}{5} = 12, n_5(A_5) \equiv 1 \pmod 5 \implies n_5(A_5) = 6$$

which gives that H has $6 \times (5-1) = 24$ elements of order 5. Further by Lagrange $5 \mid |H| \mid 60$, giving $|H| = 30$. By the intermediate result in Proposition 12.4 any group of order 30 can only have one subgroup of 5 elements, which is a contradiction.

Case 2. $5 \nmid |H|$. Then by Lagrange $|H| \nmid 12$. Since H is nontrivial, $|H| \in \{2, 3, 4, 6, 12\}$. First reduce to the case where there exists $H \lhd A_5$ with $|H| \in \{2, 3, 4\}$:

- If $|H| = 12$, then $n_3(H) \mid \frac{12}{3} = 4$, $n_3(H) \equiv 1 \pmod 3$. Either
  - $n_3(H) = 1$. By Sylow II $n_3(A_5) = 1$, i.e. there exists a normal subgroup of A_5 of order 3.
  - $n_3(H) = 4$. Then there are $4 \times (3-1) = 8$ elements of order 3. Furthermore, $n_2(H) \mid \frac{12}{2} = 6$, $n_2(H) \equiv 1 \pmod 2$. Then $n_2(H) = 1$ or 3. Suppose that $n_2(H) = 3$, then there are $3 \times (2-1) = 3$ elements of order 2. Consider the subgroup generated by the product of an element of order 2 and an element of order 3. The order of the product is divisible by 2 and 3, i.e. we have an element of order 6, which is a contradiction as we have too many elements in H. Therefore there exists a unique 2-Sylow subgroup; and similarly by Sylow II $n_2(A_5) = 1$.

Now for the case where $|H| \in \{2,3,4\}$, Consider the group G/H where $G = A_5$, with order $|G/H| \in \{15,20,30\}$. Seek to get a contradiction with the hypothesis:

> **Claim 13.5.** There exists $K \trianglelefteq G/H$ nontrivial with $5 \mid |K|$.

Proof. Consider the cases separately:

- $|G/H| = 30$. By Proposition 12.4 there exists $K \trianglelefteq G/H$ with $|K| = 15$.
- $|G/H| = 15$. Using Sylow III we have

$$n_5(G/H) \mid \frac{15}{5} = 3, n_5(G/H) \equiv 1 \pmod 5 \implies n_5(G/H) = 1$$

  By Corollary 11.7 the 5-Sylow subgroup is a normal subgroup in G/H.
- $|G/H| = 20$. Same as above we have

$$n_5(G/H) \mid \frac{20}{5} = 4, n_5(G/H) \equiv 1 \pmod 5 \implies n_5(G/H) = 1$$

  which gives a normal subgroup of order 5.x

□

Now use the claim. By Correspondence, there exists $K' \leq G$ s.t. $K \simeq K'/H \trianglelefteq G/H$ which is nontrivial. This gives $K' \trianglelefteq G$ and $5 \mid |K| \implies 5 \mid |K'| = |K| \cdot |H|$, i.e. K' is a normal subgroup in G with order divisible by 5, which is a contradiction.

- *Inductive step.* For $n \geq 6$, we know that A_{n-1} is simple; and we want to show that A_n is simple.

  Argue by contradiction. Suppose that we have $H \triangleleft A_n$ with $H \neq \{e\}$. Let $G_i = \{\sigma \in A_n \mid \sigma(i) = i\} \leq G = A_n$. $G_i \simeq A_{n-1}$, which by inductive hypothesis is simple. For each $1 \leq i \leq n$, consider $H \cap G_i \trianglelefteq G_i$ (this is normal since $H \triangleleft G$). This is a subgroup, which can be only either G_i or $\{e\}$, as G_i is simple.

Case 1. There exists i s.t. $H \cap G_i = G_i$, i.e. $G_i \subseteq H$. This implies that $G_j \subseteq H$ for all j: Consider $\tau \in A_n$, then

$$\tau G_i \tau^{-1} = \{\sigma \in A_n \mid \tau^{-1}\sigma\tau \in G_i \Leftrightarrow \sigma\tau(i) = \tau(i)\}$$

i.e. $\tau G_i \tau^{-1} = G_{\tau(i)}$. But since $G_i \subseteq H \trianglelefteq G$, $\tau G_i \tau^{-1} \subseteq H$ which gives $G_j \subseteq H$ for all j. On the other hand, $\langle G_1, \dots, G_n \rangle = A_n$; and for $\sigma \in A_n$, we can write $\sigma = \sigma_1 \dots \sigma_n$ where each σ_i is the product of two transpositions. Since $n \geq 5$, any such product of two transpositions lies in some G_i. Then $\sigma \in \langle G_1, \dots, G_n \rangle = A_n \subseteq H$ which implies that $A_n \subseteq H$. Contradiction.

Case 2. $H \cap G_i = \{e\}$ for all i. This gives that for $\sigma_1, \sigma_2 \in H$ satisfying $\sigma_1(i) = \sigma_2(i) = j$, then $\sigma_1 \sigma_2^{-1} \in G_j$; and since $H \cap G_j = \{e\}$, $\sigma_1 = \sigma_2$.

Let $\sigma \in H \setminus \{e\}$. Write that as a product of disjoint cycles. Then either

* There exists a cycle of length at least 3, i.e. there exists a_1, a_2, a_3 s.t. $\sigma = (a_1 a_2 a_3) \cdots$. Take $\tau \in A_n$ s.t. τ fixes a_1, a_2 but not a_3. This indeed exists as $n \geq 5$, so after fixing two elements there can still exist cycle of length 3. Then

$$\tau\sigma\tau^{-1} = (a_1 a_2 \sigma(a_3)) \quad \text{as product of disjoint cycles}$$

  Since H is normal, $\tau\sigma\tau^{-1} \in H$; but we have $\tau\sigma\tau^{-1}(a_1) = \sigma(a_1)$ with $\tau\sigma\tau^{-1} \neq \tau$ as they do not agree on a_3, which is a contradiction.

* σ is a product of disjoint transpositions. Since $n \geq 6$, we can write

$$\sigma = (a_1 a_2)(a_3 a_4)(a_5 a_6)$$

Let $\tau = (a_1 a_2)(a_3 a_5)$, and by the same reasoning as above $\sigma' = \tau\sigma\tau^{-1} \in H$. σ and σ' agrees on a_1 but disagrees on a_3, which gives a contradiction.

□

We then give a statement of the famous theorem classifying finite simple groups. The proof is far beyond the scope of this course and is omitted.

Theorem 13.6 (Classification of Finite Simple Groups)**.** Every finite simple group is isomorphic to one of the followings:

1. $\mathbb{Z}/p\mathbb{Z}$ with p prime, $p \in \mathbb{Z}_{>0}$.
2. A_n, $n \geq 3$.
3. Finite groups of Lie type: these occur in several series given by taking $\mathbb{F}_q$-points of certain algebraic groups, where $\mathbb{F}_q$ is the finite field of q elements.

   Example 13.7. Consider the projective special linear group $\mathrm{PSL}_n(\mathbb{F}_q)$ for $n \neq 2, q \neq 2, 3$. This is defined as:

   $$\mathrm{SL}_n(\mathbb{F}_q) = \{A \in M_n(\mathbb{F}_q) \mid \det A = 1\} \qquad \mathrm{PSL}_n(\mathbb{F}_q) = \mathrm{SL}_n(\mathbb{F}_q)/\{A = \lambda\mathrm{Id} \mid \lambda^n = 1\}$$

   where the group in the quotient $\{A = \lambda\mathrm{Id} \mid \lambda^n = 1\}$ is the center of $\mathrm{SL}_n(\mathbb{F}_q)$.
4. 26 sporadic (isolated) groups, considered via embedding in $\mathrm{GL}_n(K)$ for some field K.

14 Composition Series and the Jordan Hölder Theorem

15 Solvable Groups

16 Nilpotent Groups

17 Free Groups*

18 Presentation of Groups*