

---

# **Math 210A Notes**

---

FALL, 2025

# Contents

<b>1 Preliminaries</b>	<b>3</b>
1.1 Groups, Permutations and Cycle Decompositions . . . . .	3
1.2 Orders of Permutations . . . . .	5
1.3 Homomorphism and Isomorphism . . . . .	6
1.4 Group Actions . . . . .	8
1.5 Permutations and Group Actions . . . . .	9
<b>2 Subgroups</b>	<b>11</b>
2.1 Subgroups . . . . .	11
2.2 Centralizers and Normalizers, Stabilizers and Kernels . . . . .	12
2.3 Cyclic Groups . . . . .	15
2.4 Subgroups Generated by Subsets of a Group . . . . .	20
2.5 Quotient Groups and Homomorphisms . . . . .	22
2.6 Cosets and Lagrange's Theorem . . . . .	26
<b>3 Quotient Groups and Homomorphisms</b>	<b>30</b>
3.1 Isomorphism Theorems . . . . .	30
3.2 The Alternating Group . . . . .	33

# Chapter 1

## Preliminaries

### 1.1 Groups, Permutations and Cycle Decompositions

#### Definition 1.1.1. (Group)

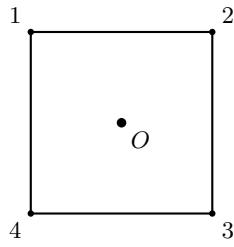
A group is an ordered pair  $(G, *)$  where  $G$  is a set and  $*$  is a mapping from  $G \times G$  to  $G$  (called a binary operation) satisfying the following:

1.  $\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$  (associativity)
2.  $\exists e \in G$  such that  $e * a = a = a * e \quad \forall a \in G$  (identity element)
3.  $\forall a \in G, \exists a^{-1} \in G$  such that  $a * a^{-1} = e = a^{-1} * a$  (inverse element)

From now on we write  $a * b = ab$ .

#### Definition 1.1.2. (Permutations)

Let  $\Omega$  be a nonempty set. The mapping  $\sigma : \Omega \rightarrow \Omega$  is a permutation of  $\Omega$  if  $\sigma$  is a bijection.



Here is a square centered at the origin. Take a copy of the square, move it around in 3-space, and lay it back down to cover the original square. This is called a rigid motion of the square, or a symmetry of the square. This creates a permutation of the vertices. How many symmetries are possible?

For the arbitrary symmetry of the square, we have 4 choices where to find 1. Once we know where vertex 1 is (say, vertex i), then vertex 2 can be one of 2 places. This gives  $4 \times 2$  symmetries. Consider the regular  $n$ -gon centered at the origin. How many symmetries do we have?  $2n$ .

#### Fact 1.1.1. (Properties of Permutations)

1. Functional composition is associative. For mappings  $\sigma, \tau, \mu$

$$\sigma \circ (\tau \circ \mu) = (\sigma \circ \tau) \circ \mu$$

2. The identity mapping on any set ( $I(x) = x$ ) is a bijection of that set.
3. If  $\sigma$  is a bijection from a set  $\Omega$  to  $\Omega$ , then there is a bijection of  $\Omega$  called  $\sigma^{-1}$  such that  $\sigma \circ \sigma^{-1} = I = \sigma^{-1} \circ \sigma$ .

#### Definition 1.1.3. (Order)

For  $a \in G$ , where  $G$  is a group, the order of  $a$ , denoted  $|a|$ , is the smallest positive integer  $k$  such that  $a^k = e$  if such a  $k$  exists. If no such  $k$  exists, then we say  $a$  has infinite order and  $|a| = \infty$ .

#### Notation . (Cycle Decomposition)

A permutation  $\sigma$  of a set  $\Omega$  can be written as a product of disjoint cycles. For example, if  $\sigma$  is a permutation of  $\{1, 2, 3, 4, 5\}$  such that  $\sigma(1) = 3, \sigma(3) = 1, \sigma(2) = 5, \sigma(5) = 2$ , and  $\sigma(4) = 4$ , then we can write

$\sigma = (1\ 3)(2\ 5)(4)$ . The order of a cycle is the number of elements in the cycle. The order of a permutation is the least common multiple of the orders of the disjoint cycles.

**Example 1.1.1.**

If  $\sigma = (1\ 2)(3\ 2)$ , then  $\sigma(3) = 1$ .

If  $\mu = (3\ 2)(1\ 2)$ , then  $\mu(3) = 2$ .

$S_n$  is not abelian for  $n \geq 3$ .

## 1.2 Orders of Permutations

$S_X$  refers to the set of all permutations on the set  $X$ . That is, the elements of  $S_X$  are bijections from  $X$  to itself.  $S_n$  refers to when  $X = \{1, 2, \dots, n\}$ .

Let  $n = 5$ . How many elements are in  $S_5$ ?  $5! = 120$ . Why? Given a  $\sigma \in S_5$ , we have 5 choices for  $\sigma(1)$ , 4 for  $\sigma(2), \dots$  so there are  $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5! = 120$  choices for  $\sigma$ . In general, there  $n!$  elements in  $S_n$ .

$S_5$  : how many cycles of length 5 are in  $S_5$ ?

$$(1 \ 2 \ 3 \ 4 \ 5) \quad (5 \ 4 \ 3 \ 2 \ 1)$$

$$(1 \ 2 \ 3 \ 5 \ 4) \quad \cancel{(2 \ 3 \ 4 \ 5 \ 1)}$$

:

There are  $5!$  ways of filling in a blank 5-cycle. However, each 5-cycle is represented 5 ways, so we divide by 5. Thus there are  $\frac{5!}{5} = 4! = 24$  distinct 5-cycles in  $S_5$ . How many

$$4 \text{ cycles? } \frac{5 \cdot 4 \cdot 3 \cdot 2}{4} = 30$$

$$3 \text{ cycles? } \frac{5 \cdot 4 \cdot 3}{3} = 20$$

$$2 \text{ cycles? } \frac{5 \cdot 4}{2} = 10$$

$$1 \text{ cycles? } \frac{5}{1} = 5$$

How many distinct  $r$ -cycles  $r \leq n$  are there in  $S_n$ ?  $\frac{n!}{r(n-r)!}$

$$\frac{n \cdot (n-1) \cdot (n-2) \cdots (n-r+1)}{r!}$$

How many distinct elements of the form  $(\dots)(\dots)$  disjoint in  $S_5$ ?

$$\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2 \cdot 1}{3} = 20$$

How many of the form  $(\dots)(\dots)$ ?

$$\frac{\frac{5 \cdot 4}{2} \cdot \frac{3 \cdot 2}{2}}{2} = \frac{30}{2} = 15$$

How many distinct elements of the form  $(\dots)(\dots)$  in  $S_n$ ?

$$\frac{n \cdot (n-1)}{2} \cdot \frac{(n-2)(n-3)(n-4)}{3}$$

How many distinct elements of the form  $(\dots)(\dots)$  in  $S_n$ ?

$$\frac{\frac{n \cdot (n-1)}{2} \cdot \frac{(n-2)(n-3)}{2}}{2}$$

**Definition 1.2.1.** (Field)

$(F, +, \cdot)$  is a field if

1.  $(F, +)$  is an abelian group with identity 0
2.  $(F \setminus \{0\}, \cdot)$  is an abelian group with identity 1
3. Left and right distributive laws hold

The following are groups:

$$GL_n(F) = \{\text{all } n \times n \text{ matrices with entries in } F \text{ and with non-zero determinants}\}$$

$$SL_n(F) = \{\text{all } n \times n \text{ matrices with entries in } F \text{ and with determinant 1}\}$$

### 1.3 Homomorphism and Isomorphism

In general, we can tell how similar groups are by the mappings we make between them where the mappings preserve the group structure of the domain.

#### Definition 1.3.1. (Homomorphism)

Let  $(G, \star)$  and  $(H, \diamond)$  be groups. A map  $\Phi : G \rightarrow H$  is a homomorphism if for all  $g_1, g_2 \in G$ ,

$$\Phi(g_1 \star g_2) = \Phi(g_1) \diamond \Phi(g_2)$$

We usually write

$$\Phi(xy) = \Phi(x)\Phi(y)$$

and we know that  $xy$  happens in  $G$  and  $\Phi(x)\Phi(y)$  happens in  $H$ .

**Example 1.3.1.**  $\pi : \mathbb{R}^2 \rightarrow \mathbb{R}$  by  $\pi(x, y) = x \forall (x, y) \in \mathbb{R}^2$  is a homomorphism. Letting  $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ , we have

$$\begin{aligned}\pi((x_1, y_1) + (x_2, y_2)) &= \pi(x_1 + x_2, y_1 + y_2) \\ &= x_1 + x_2 \\ &= \pi(x_1, y_1) + \pi(x_2, y_2)\end{aligned}$$

Showing that  $\pi$  is indeed a homomorphism.

What elements are in the set  $\{p \in \mathbb{R}^2 : \pi(p) = 0\} = K$ ?

$$K = \{(x, y) : x = 0\}$$

This is the kernel of  $\pi$ .

#### Definition 1.3.2. (Kernel)

Let  $G$  and  $H$  be groups and let  $\Phi : G \rightarrow H$  be a group homomorphism. The kernel of  $\Phi$  is

$$\ker(\Phi) = \{g \in G : \Phi(g) = e_H\} = \Phi^{-1}(e_H)$$

where  $e_H$  is the identity element in  $H$ .

#### Definition 1.3.3. (Isomorphism)

Let  $G$  and  $H$  be groups. A map  $\Psi : G \rightarrow H$  is an isomorphism if

1.  $\Psi$  is a homomorphism
2.  $\Psi$  is bijective

If there exists an isomorphism  $\Psi : G \rightarrow H$ , we say that  $G$  and  $H$  are isomorphic, denoted  $G \cong H$ .  $\cong$  is an equivalence relation on any collection of groups.

**Example 1.3.2.** Let  $k \in \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ . Define  $\phi_k : \mathbb{Q}^* \rightarrow \mathbb{Q}^*$  by  $\phi_k(q) = kq$ . We claim that  $\phi$  is an isomorphism. Show that  $\Phi_k$  is a homomorphism and a bijection:

1. Homomorphism:

$$\begin{aligned}\phi_k(q_1 + q_2) &= k(q_1 + q_2) \\ &= k(q_1 + q_2) \\ &= kq_1 + kq_2 \\ &= \phi_k(q_1) + \phi_k(q_2)\end{aligned}$$

2. Bijections:

- Injective: Suppose  $\phi_k(q_1) = \phi_k(q_2)$ . Then

$$\begin{aligned}\phi_k(q_1) &= \phi_k(q_2) \\ \iff kq_1 &= kq_2 \\ \iff q_1 &= q_2 \quad (k \neq 0)\end{aligned}$$

- Surjective: We want to show  $\phi_k(\mathbb{Q}) = \mathbb{Q}$ . Let  $q \in \mathbb{Q}$ . Since  $k \neq 0$ ,  $\frac{q}{k} \in \mathbb{Q}$ . Then

$$\phi_k\left(\frac{q}{k}\right) = k \cdot \frac{q}{k} = q$$

Thus  $\phi_k$  is surjective.

$$\ker \phi_k = \{0\} \text{ since } \phi_k(q) = 0 \iff kq = 0 \iff q = 0.$$

**Fact 1.3.1.** Suppose  $G \cong H$ , that is there exists  $\phi : G \rightarrow H$  which is a homomorphic bijection. Then

1.  $|G| = |H|$
2.  $G$  is abelian if and only if  $|H|$  is abelian
3.  $\forall x \in G \quad |x| = |\phi(x)|$  (Corresponding elements have the same order)

## 1.4 Group Actions

There are many examples of groups acting on sets. For instance, consider an element in  $S_5$ , call it  $\sigma$ .  $\sigma$  is a permutation of  $\{1, 2, 3, 4, 5\}$  and it is also an element of a group

$$\begin{aligned}\sigma &= (1 \ 2 \ 3 \ 4 \ 5) \\ \sigma(5) &= 4\end{aligned}$$

We say that  $\sigma$  is acting on the set  $\{1, 2, 3, 4, 5\}$ .

Consider the set of all  $2 \times 2$  matrices with elements in  $\mathbb{R}$ . Let  $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$  and let  $k \in \mathbb{R}$ . Then  $kA = \begin{bmatrix} k & 2k \\ 3k & 4k \end{bmatrix}$ . We say that  $\mathbb{R}$  is acting on the set of all  $2 \times 2$  matrices with elements in  $\mathbb{R}$ .

**Definition 1.4.1.** (Group Action)

Let  $G$  be a group and  $A$  be a set. A group action of  $G$  on  $A$  is a map from  $G \times A$  to  $A$  (written  $g.a \quad \forall g \in G, a \in A$ ) such that

1.  $g_1.(g_2.a) = (g_1g_2).a \quad \forall g_1, g_2 \in G$  (Compatibility)
2.  $1.a = a$  (or  $e.a = a$ )  $\quad \forall a \in A$  (Identity)

**Example 1.4.1.** Let  $G = S_n$ . Let's verify that  $S_n$  acts on the set  $\{1, 2, \dots, n\}$ . Define the group action

$$\sigma.a = \sigma(a) \quad \forall \sigma \in S_n, a \in \{1, 2, \dots, n\} \tag{*}$$

Then let  $\sigma_1, \sigma_2 \in S_n$  and  $a \in \{1, 2, \dots, n\}$ . We have

$$\begin{aligned}\sigma_1.(\sigma_2.a) &= \sigma_1.(\sigma_2(a)) \\ &= \sigma_1(\sigma_2(a)) \\ &= (\sigma_1 \circ \sigma_2)(a) \\ &= (\sigma_1 \circ \sigma_2).a\end{aligned}\tag{I}$$

To verify the identity property, recall that the identity map, denoted  $I$ , is the identity of  $S_n$  and

$$I(a) = a \quad \forall a \in \{1, 2, \dots, n\}$$

That is,

$$I.a = I(a) = a \quad \forall a \in \{1, 2, \dots, n\} \tag{II}$$

By (I) and (II),  $S_n$  acts on the set  $\{1, 2, \dots, n\}$  by the group action defined in (\*).

**Example 1.4.2.** A vector space over a field  $F$  is a set  $V$  with two binary operations vector addition and scalar multiplication, and other properties including

- $a(bv) = (ab)v \quad \forall a, b \in F, v \in V$  (Compatibility)
- $1v = v \quad \forall v \in V$  where 1 is the multiplicative identity in  $F$  (Identity)

Since  $F$  is not a group with respect to multiplication, we must say that  $F^* = F \setminus \{0\}$  acts on  $V$ .

## 1.5 Permutations and Group Actions

Let  $G$  be a group acting on a set  $S$ . That is, define a mapping  $G \times S \rightarrow S$  denoted by  $g.a \quad \forall g \in G$  and  $a \in S$ . Fix  $g \in G$ . Then this defines a map  $\sigma_g$  such that  $\sigma_g : S \rightarrow S$  by  $\sigma_g(a) = g.a$

**Example 1.5.1.** Take  $G = \mathbb{R} \setminus \{0\}$  with respect to multiplication. Let  $S = M_2(\mathbb{R})$ .

$$\begin{aligned}\sigma_{\sqrt{2}}(A) &= \sqrt{2}.A \\ &= \sqrt{2} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\ &= \begin{bmatrix} \sqrt{2}a & \sqrt{2}b \\ \sqrt{2}c & \sqrt{2}d \end{bmatrix}\end{aligned}$$

For  $\begin{bmatrix} 1 & \pi \\ e & \ln(2) \end{bmatrix}$ , we have

$$\sigma_{\sqrt{2}} \begin{bmatrix} 1 & \pi \\ e & \ln(2) \end{bmatrix} = \begin{bmatrix} \sqrt{2} & \sqrt{2}\pi \\ \sqrt{2}e & \sqrt{2}\ln(2) \end{bmatrix}$$

What is the range of  $\sigma_{\sqrt{2}}$ ?  $M_2(\mathbb{R})$ .

**Assertion 1.** 1.  $\sigma_g$  as defined is a permutation of the set  $S$ .

2. For the sake of notation, we change the name of our set to  $A$ . The map from  $G$  to  $S_A$  defined by  $g \mapsto \sigma_g$  is a homomorphism.

**Proof.** 1. Let  $g \in G$  be given and  $\sigma_g$  be defined as above. Clearly,  $\sigma_g$  is a mapping from  $S \rightarrow S$ . We will show that  $\sigma_g$  is a bijection by showing it has a two-sided inverse. Let  $a \in S$  and note  $g^{-1} \in G$  since  $G$  is a group. Then

$$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \\ &= \sigma_{g^{-1}}(g.a) \\ &= g^{-1}.(g.a) \\ &= (g^{-1}g).a \\ &= e.a \\ &= a.\end{aligned}$$

We see that  $\sigma_{g^{-1}} \circ \sigma_g$  is the identity mapping from  $S \rightarrow S$ . To show that  $\sigma_g \circ \sigma_{g^{-1}}$  is also the identity map from  $S \rightarrow S$  is analogous. Thus we have a two-sided inverse as desired. Hence,  $\sigma_g$  is a permutation of  $S$  as desired. That is,  $\sigma_g$  is an element of the symmetric group of  $S$ .

2. Let  $\Psi : G \rightarrow S_A$  be defined by  $\Psi(g) = \sigma_g \quad \forall g \in G$ . Let  $a \in A$  and  $g_1, g_2 \in G$ . We want to show that  $\Psi(g_1g_2) = \Psi(g_1) \circ \Psi(g_2)$ . Since these are mappings in  $S_A$ , we will show that their values agree  $\forall a \in A$ . We have

$$\begin{aligned}(\Psi(g_1) \circ \Psi(g_2))(a) &= \sigma_{g_1g_2}(a) \\ &= (g_1g_2).a \\ &= g_1.(g_2.a) \\ &= g_1.(\sigma_{g_2}(a)) \\ &= \sigma_{g_1}(\sigma_{g_2}(a)) \\ &= \sigma_{g_1} \circ \sigma_{g_2}(a) \\ &= (\Psi(g_1) \circ \Psi(g_2))(a).\end{aligned}$$

Hence,  $\Psi$  is a homomorphism as desired. □

If we have a homomorphism, then we have a kernel.

**Definition 1.5.1.** (Kernel of a Group Action)

For a group  $G$  acting on a set  $A$ , the kernel of the group action is

$$\{g \in G : g.a = a \quad \forall a \in A\}$$

# Chapter 2

## Subgroups

### 2.1 Subgroups

**Definition 2.1.1.** (Subgroup)

Let  $G$  be a group. The subset  $H$  of  $G$  is called a subgroup of  $G$  if

1.  $H$  is nonempty.
2.  $\forall x, y \in H, x^{-1} \in H$  and  $xy \in H$ .

**Notation .** IF  $H$  is a subgroup of  $G$ , we write  $H \leq G$ .

**Example 2.1.1.**

1.  $\mathbb{Z} \leq \mathbb{Q}$  with respect to  $(+)$ .
2. All groups have two subgroups:  $H = G$  and  $H = \{1\}$ .
3.  $2\mathbb{Z} \leq \mathbb{Z}$  with respect to  $(+)$ .
4. Let  $G = D_{2n}$  and let  $r$  be a  $360^\circ/n$  clockwise rotation of the n-gon about the origin. Then  $\{1, r, r^2, r^3, \dots, r^{n-1}\}$  forms a subgroup of  $D_{2n}$ .
5. Nonexample:  $H = \{1, -1\} \subseteq \mathbb{Z}$  forms a group with respect to multiplication, but  $H$  is not a subgroup of  $\mathbb{Z}$  since  $\mathbb{Z}$  is a group with respect to addition, NOT multiplication.
6.  $\mathbb{Z}/5\mathbb{Z}$  is not a subgroup of  $\mathbb{Z}/6\mathbb{Z}$  since  $\mathbb{Z}/5\mathbb{Z} \not\subseteq \mathbb{Z}/6\mathbb{Z}$ .

$\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$  is an additive group

$(\mathbb{Z}/6\mathbb{Z})^* = \{\bar{1}, \bar{5}\}$  is a multiplicative group with all elements coprime to 6

$(\mathbb{Z}/9\mathbb{Z})^{**} = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$  is a multiplicative group with all elements coprime to 9

**Proposition 2.1.1.** (Subgroup Criterion)

A subset  $H$  of a group  $G$  is a subgroup of  $G$  if and only if

1.  $H \neq \emptyset$ .
2.  $\forall x, y \in H, xy^{-1} \in H$  (in additive notation:  $\forall x, y \in H, x - y \in H$ ).

## 2.2 Centralizers and Normalizers, Stabilizers and Kernels

**Definition 2.2.1.** (Centralizers)

Let  $A$  be a nonempty subset of a group  $G$ . Define the centralizer of  $A$  in  $G$  to be the set

$$\begin{aligned} C_G(A) &= \{g \in G : gag^{-1} = g \ \forall a \in A\} \\ &= \{g \in G : ga = ag \ \forall a \in A\} \end{aligned}$$

The centralizer of  $A$  in  $G$  is the set of all elements in  $G$  which commute with every element in  $A$ .

**Theorem 2.2.1.**  $C_G(A) \leq G$ .

**Proof.** Let  $a \in A$ . Then

$$\begin{aligned} 1a1^{-1} &= (1a)1^{-1} \\ &= a1^{-1} \\ &= a1 \\ &= a \end{aligned}$$

Thus,  $1 \in C_G(A)$ .

Let  $x, y \in C_G(A)$ . Then  $xax^{-1} = a$  and  $yay^{-1} = a$ . Note that

$$yay^{-1} = a \iff a = y^{-1} \quad (*)$$

Now

$$\begin{aligned} (xy^{-1})a(xy^{-1})^{-1} &= xy^{-1}a(y^{-1})^{-1}x^{-1} \\ &= x(y^{-1}ay)x^{-1} \\ &\stackrel{(*)}{=} xax^{-1} \\ &= a \end{aligned}$$

Hence,  $xy^{-1} \in C_G(A)$ . Furthermore,  $C_G(A) \leq G$ . □

**Notation .** If  $A = \{a\}$ , we write  $C_G(a)$  instead of  $C_G(\{a\})$ .

Why was this unnecessary? From the homework, we know that  $G$  acts on the subset  $A$  by conjugation. That is, we have a mapping  $(.) : G \times A \rightarrow A$  defined by  $g.a = gag^{-1} \ \forall g \in G, a \in A$  which satisfies both axioms of a group action.

Recall that the kernel of a group action is the kernel of the permutation representation of the group action (PRGA). The PRGA is the Homomorphism induced by the group action

$$\begin{aligned} \Psi : G &\rightarrow S_A \\ g &\mapsto \sigma_g \end{aligned}$$

**Example 2.2.1.** Find the kernel of  $G$  acting on  $A \subset G$  by conjugation.

$$\begin{aligned} \{g \in G : g.a = a \ \forall a \in A\} &= \{g \in G : gag^{-1} = a \ \forall a \in A\} \\ &= C_G(A) \end{aligned}$$

Suppose that  $A = G$ . What is  $C_G(G)$ ?

$$\{g \in G : gag^{-1} = a \ \forall a \in G\}$$

This set is called the center of  $G$  denoted  $Z(G)$ . Since  $Z(G)$  is a special case of  $C_G(A)$ , we know  $Z(G) \leq G$ .

**Definition 2.2.2.** (Normalizer)

Define  $gAg^{-1} = \{gag^{-1} : a \in A\}$ . We will define the normalizer of  $A$  in  $G$  to be the set

$$N_G(A) = \{g \in G : gAg^{-1} = A\}$$

We will prove  $N_G(A) \leq G$ , but not yet. Notice if  $gag^{-1} = a \quad \forall a \in A$  then  $gAg^{-1} = \{gag^{-1} : a \in A\} = \{a : a \in A\} = A$ . Hence

$$C_G(A) \subseteq N_G(A)$$

**Fact 2.2.1.**

- If  $G$  is abelian, then  $Z(G) = G$  since every element commutes with every other element. That is,

$$\begin{aligned} \forall a, b \in G \quad ab = ba &\iff a = bab^{-1} \quad \forall a, b \in G \\ &\implies b \in Z(G) \quad \forall b \in G \end{aligned}$$

Similarly,  $C_G(A) = N_G(A) = G$ .

- Consider  $A = \{1, (1 2)\} \subseteq S_3$ . Find  $C_{S_3}(A)$ . Notice that 1 commutes with everything in  $S_3$ , specifically 1 and  $(1 2)$ . Also,

$$(1 2)(1 2)(1 2)^{-1} = (1 2)$$

so  $(1 2) \in C_{S_3}(A)$ . Hence,  $A \leq C_{S_3}(A)$ .

**Theorem 2.2.2.** (Lagrange's Theorem)

Let  $G$  be a finite group ( $|G| \in \mathbb{N}$ ) and let  $H \leq G$ . Then

$$|H| \text{ divides } |G|$$

Since  $|A| = 2$  and  $A \leq C_{S_3}(A)$ , we know  $2 \mid |C_{S_3}(A)|$  since  $C_{S_3}(A) \leq S_3$ .

$$\left. \begin{array}{l} |C_{S_3}(A)| \mid |S_3| = 3! = 6 \\ |A| \mid |C_{S_3}(A)| \end{array} \right\} \implies |C_{S_3}(A)| \in \{2, 6\}$$

. Thus,  $C_{S_3} = A$  or  $C_{S_3}(A) = S_3$ . Well,

$$\begin{aligned} (1 2)(1 2 3) &= (2 3) \\ (1 2 3)(1 2) &= (1 3) \end{aligned}$$

so  $(1 2 3) \notin C_{S_3}(A)$ . It follows that  $|C_{S_3}(A)| = 2 \implies C_{S_3}(A) = A$ .

Let  $G$  be a group acting on a set  $S$ . That is, there is a mapping

$$(., .) : G \times S \rightarrow S$$

denoted by  $g.a \quad \forall a \in S$  with  $g_1.(g_2.a) = (g_1g_2).a$  and  $1.a = a \quad \forall a \in S, g_1, g_2 \in G$ .

**Definition 2.2.3.** (Stabilizers)

If  $G$  is a group acting on a set  $S$  and  $s \in S$ , then we define the stabilizers of  $s$  in  $G$  to be the set

$$G_s = \{g \in G : g.s = s\}$$

**Theorem 2.2.3.**  $G_s \leq G$ .

**Proof.** Since  $G$  acts on  $S$  we know that  $1.s = s$ . Hence  $1 \in G_s \implies G_s \neq \emptyset$ . Let  $x, y \in G_s$ . Then

$$\begin{aligned} s &= 1.s = (y^{-1}y).s \\ &= y^{-1}.(y.s) \\ &= y^{-1}.s \quad (\text{since } y \in G_s) \end{aligned}$$

Hence  $y^{-1} \in G_s$ . Furthermore,

$$\begin{aligned} (xy).s &= x.(y.s) \\ &= x.s \\ &= s \end{aligned}$$

Hence  $xy \in G_s$ . Thus,  $G_s \leq G$ . □

Now to show  $N_G(A)$  where  $A \subseteq G$  is a subgroup of  $G$ . To that end, let  $S = \mathcal{P}(G)$ , the power set of  $G$ , and define a map

$$G \times S \rightarrow S \text{ by } g.B = gBg^{-1} = \{gbg^{-1} : \forall g \in G, B \in \mathcal{P}(G)\}$$

Let's prove this defines a group action. Let  $g_1, g_2 \in G$  and  $B \in \mathcal{P}(G)$ . Well,

$$1.B = \{1b1^{-1} : b \in B\} = \{b : b \in B\} = B$$

so the identity axiom holds. Furthermore,

$$\begin{aligned} (g_1g_2).B &= (g_1g_2)B(g_1g_2)^{-1} \\ &= \{(g_1g_2)b(g_1g_2)^{-1} : b \in B\} \\ &= \{(g_1g_2)b(g_2^{-1}g_1^{-1}) : b \in B\} \\ &= \{g_1(g_2bg_2^{-1})g_1^{-1} : b \in B\} \\ &= \{g_1b'g_1^{-1} : b' \in g_2Bg_2^{-1}\} \\ &= g_1(g_2Bg_2^{-1})g_1^{-1} \\ &= g_1(g_2.B)g_1^{-1} \\ &= g_1.(g_2.B) \end{aligned}$$

Hence, we have defined a group action. Now, back to showing that  $N_G(A) \leq G$  ( $A \subseteq G$ ).

Recall,  $G_s = \{g \in G : g.s = s\}$ . Given our new group action  $G$  acting on  $\mathcal{P}(G)$  by conjugation, we have

$$\begin{aligned} G_a &= \{g \in G : g.A = A\} \\ &= \{g \in G : gAg^{-1} = A\} \\ &= N_G(A) \end{aligned}$$

We can then deduce that  $N_G(A) \leq G$  as  $G_A \leq G$ .

## 2.3 Cyclic Groups

**Definition 2.3.1.** (Cyclic Group)

A group  $H$  is cyclic if  $H$  is generated by a single element. That is,

$$\exists x \in H \text{ such that } H = \{x^n : n \in \mathbb{Z}\}$$

$$(\exists x \in H \text{ such that } H = \{nx : n \in \mathbb{Z}\} \text{ using additive notation})$$

We write  $\langle x \rangle = H$  ( $x$  generates  $H$ ).

**Example 2.3.1.** 1.  $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

2. The rotations in  $D_{2n}$  are generated by  $r$  (360/n clockwise rotation)
3.  $U_4 = \{1, -1, i, -i\} = \langle i \rangle$

**Note .** If  $H = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ , we define

$$\begin{aligned} x^0 &= 1 \\ x^{-n} &= (x^n)^{-1} = (x^{-1})^n \text{ for } n > 0 \end{aligned}$$

**Proposition 2.3.1.** If  $H = \langle x \rangle$ , then  $|H| = |x|$ . If one side of this equality is infinity, then so is the other. More specifically,

1. If  $|x| = n < \infty$ , then  $x^n = 1$  and  $1, x, x^2, \dots, x^{n-1}$  are all the distinct elements of  $H$ .
2. If  $|x| = \infty$ , then  $x^n \neq 1$  when  $n \neq 0$  and  $x^a \neq x^b$  for all  $a \neq b \in \mathbb{N}$ .

**Proof.** Let  $|x| = n$ .

1. Consider the case where  $n < \infty$ . Consider the elements  $1, x, x^2, \dots, x^{n-1}$  and suppose  $x^a = x^b$  where  $0 \leq a < b < n$ . Then

$$\begin{aligned} x^a = x^b &\implies 1 = x^b x^{-a} \\ &\implies 1 = x^{b-a} \end{aligned}$$

Since  $b - a > 0$ , this contradicts  $n$  being the order of  $x$ . Thus, all the  $1, x, x^2, \dots, x^{n-1}$  are distinct. Also,  $x^n = 1$  as  $n = |x|$ . Thus  $H$  contains at least  $n$  elements. It remains to show we have all of them.

Let  $t \in \mathbb{Z}$  such that  $x^t \in H$ . By the division algorithm, there exist  $q, r \in \mathbb{Z}$  such that

$$t = qn + r \text{ where } 0 \leq r < n$$

Then

$$\begin{aligned} x^t &= x^{qn+r} = x^{qn} x^r \\ &= (x^n)^q x^r \\ &= 1^q x^r \\ &= x^r \in \{1, x, x^2, \dots, x^{n-1}\} \text{ since } 0 \leq r < n \end{aligned}$$

Hence,  $H = \{1, x, x^2, \dots, x^{n-1}\}$ .

2. Next, suppose  $|x| = \infty$  (no positive powers of  $x$  is the identity). For the sake of contradiction, if  $x^a = x^b$  with  $a < b$  then  $x^{a-b} = 1$ , a contradiction. So distinct powers of  $x$  give distinct elements of  $H$ . It follows that  $|H| = \infty$ .

□

**Proposition 2.3.2.** Let  $G$  be a group and let  $x \in G$ . Let  $m, n \in \mathbb{Z}$ . If  $x^n = 1$  and  $x^m = 1$ , then  $x^d = 1$  where  $d = \gcd(m, n)$ . In particular, if  $x^m = 1$  for some  $m \in \mathbb{Z}$  then  $|x| \mid m$ .

**Proof.** Let  $m, n, d$  be defined as above. Then by the Euclidean algorithm

$$\exists x_0, y_0 \in \mathbb{Z} \text{ such that } d = mx_0 + ny_0$$

Then

$$\begin{aligned} x^d &= x^{mx_0+ny_0} \\ &= (x^m)^{x_0}(x^n)^{y_0} \\ &= 1^{x_0}1^{y_0} \\ &= 1 \end{aligned}$$

To prove the second assertion, let  $x^m = 1$  and  $n = |x|$ . Then  $x^n = 1$  by definition of order.

**Case 1:** If  $m = 0$  then certainly  $n|m$ .

**Case 2:** Let  $m \neq 0$ . We know  $n < \infty$  since  $x^m = 1$ . Let  $d = \gcd(m, n)$  and hence by the first assertion  $x^d = 1$ . Since  $0 < d \leq n$  and  $n$  is the smallest positive integer such that  $x^n = 1$ , we have that  $n = d$ . By definition,

$$d|m \implies n|m \text{ as desired.}$$

□

### Theorem 2.3.1. (Cyclic Groups Isomorphisms)

1. Any infinite cyclic group  $\langle x \rangle$  is isomorphic to  $\mathbb{Z}$  (with the mapping  $\phi : \mathbb{Z} \rightarrow \langle x \rangle, k \mapsto x^k$ ).
2. If  $\langle x \rangle$  and  $\langle y \rangle$  are cyclic groups both with order  $n < \infty$ , then

$$\begin{aligned} \phi : \langle x \rangle &\rightarrow \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

is a well-defined isomorphism.

We will use multiplicative notation when describing an arbitrary cyclic group of order  $n \in \mathbb{N}$ , and denote this group  $\mathbb{Z}_n$ . NOT to be confused with the additive group  $\mathbb{Z}/n\mathbb{Z}$ , which is cyclic of order  $n$ . Most times we will refer to an infinite cyclic group as  $\mathbb{Z}$ .

### Proposition 2.3.3. (The Order of $x^a$ in a Cyclic Group)

Let  $G$  be a group and let  $x \in G$ . Let  $a \in \mathbb{Z} - \{0\}$ .

1. If  $|x| = \infty$ , then  $|x^a| = \infty$ .
2. If  $|x| = n < \infty$ , then  $|x^a| = \frac{n}{\gcd(n, a)}$ .

In particular,  $|x^a| = \frac{n}{a}$  when  $a|n$  ( $a \in \mathbb{N}$ ).

**Proof.** We start with the following claim: Let  $a, n \in \mathbb{Z}$  not both zero.

$$\text{If } \gcd(a, n) = d \text{ then } \gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$$

**Proof.** Let  $a, n$  and  $d$  be as defined. Then there exists  $x_0, y_0 \in \mathbb{Z}$  such that

$$d = ax_0 + ny_0$$

It follows that

$$1 = \frac{a}{d}x_0 + \frac{n}{d}y_0$$

Since  $\gcd(\frac{a}{d}, \frac{n}{d})$  divides  $\frac{a}{d}$  and  $\frac{n}{d}$ ,  $\gcd(\frac{a}{d}, \frac{n}{d})$  divides the right-hand side, so  $\gcd(\frac{a}{d}, \frac{n}{d})|1$ . Thus,  $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$ . □

1. Suppose by way of contradiction that

$$|x| = \infty \text{ and } |x^a| = m < \infty$$

By definition of order

$$(x^a)^m = 1 \iff x^{am} = 1$$

It follows that

$$(x^{am})^{-1} = 1^{-1} \iff x^{-am} = 1$$

Since  $a \neq 0$  by assumption and  $m \neq 0$  by definition of order, then  $am \neq 0$  and one of  $-am$  or  $am$  is positive, so some positive power of  $x$  is the identity, contradicting  $|x| = \infty$ . So,  $|x^a| = \infty$ .

2. Let  $|x| = n < \infty$  and let  $y = x^a$ ,  $\gcd(a, n) = d$ . We also write  $n = db$  and  $a = dc$  for some integers  $c, b$  (not that  $b > 0$ ). From our claim,

$$\gcd(c, b) = \gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$$

We want to show that  $|y| = b$ . To this end, notice that

$$\begin{aligned} y^b &= (x^a)^b = x^{ab} \\ &= x^{(dc)b} \\ &= x^{(dc)\left(\frac{n}{d}\right)} \\ &= (x^n)^c \\ &= 1^c \\ &= 1 \end{aligned}$$

Thus,  $|y|$  divides  $b$ . Let  $k = |y|$ . Then

$$y^k = 1 = x^{ak}$$

Hence,  $|x| \mid ak$ . That is,

$$\begin{aligned} n \mid ak &\iff db \mid dck \\ &\iff b \mid ck \\ &\iff \frac{n}{d} \mid \frac{a}{d}k \end{aligned}$$

Since  $\frac{n}{d}$  and  $\frac{a}{d}$  are relatively prime, this gives  $\frac{n}{d} \mid k$ , that is  $b \mid k$ . Since  $b \mid k$  and  $k \mid b$ ,  $k = b$  as both  $k, b \in \mathbb{N}$ .  $\square$

**Proposition 2.3.4.** Let  $H = \langle x \rangle$ .

1. Assume  $|x| = \infty$ . then  $H = \langle x^a \rangle$  if and only if  $a = \pm 1$ .
2. Assume  $|x| = n\infty$ . Then  $H = \langle x^a \rangle$  if and only if  $\gcd(a, n) = 1$ . In particular, the number of generators of  $H$  is  $\phi(n)$ , where  $\phi$  is Euler's Phi function.

**Proof.** 2. If  $|x| = n < \infty$ , we know that  $|x^a| = |\langle x^a \rangle|$ . This subgroup equals all of  $H \iff |x^a| = n \iff \frac{n}{\gcd(a, n)} = n \iff \gcd(a, n) = 1$ . Since  $\phi(n)$  is the number of  $a \in \{1, 2, 3, \dots, n\}$ , which are relatively prime to  $n$ ,  $\phi(n)$  gives the number of generators of  $H$ .  $\square$

What are the generators of  $\langle x \rangle = \mathbb{Z}_{10}$ ?  $\phi(1) = \phi(2)\phi(5) = 4$

$$x^1, x^3, x^7, x^9$$

What are the generators of  $\mathbb{Z}/15\mathbb{Z} = \langle \bar{1} \rangle = \{k\bar{1} : k \in \mathbb{Z}\}$ ?

$$\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14}$$

**Theorem 2.3.2.** (Subgroups of Cyclic Groups)

Let  $H = \langle x \rangle$  be a cyclic group.

1. Every subgroup of  $H$  is cyclic. More precisely, if  $K \leq H$  then either

$$K = \{1\} \text{ or } K = \langle x^d \rangle$$

where  $d$  is the smallest positive integer such that  $x^d \in K$ .

2. If  $|H| = \infty$ , then for any distinct nonnegative integers  $a$  and  $b$

$$\langle x^a \rangle \neq \langle x^b \rangle$$

and  $\forall m \in \mathbb{Z}$

$$\langle x^m \rangle = \langle x^{|m|} \rangle$$

where  $|m|$  denotes the absolute value of  $m$ . So, the nontrivial subgroups of  $H$  correspond bijectively with the integers  $1, 2, 3, \dots$

3. If  $|H| = n < \infty$ , then for every  $a \in \mathbb{N}$  which divides  $n$ , there is a unique subgroup  $H$  with order  $a$ . This subgroup is the cyclic group  $\langle x^d \rangle$  where  $d = \frac{n}{a}$ . Furthermore, for every  $m \in \mathbb{Z}$ ,  $\langle x^m \rangle = \langle x^{\gcd(n,m)} \rangle$  so the subgroups of  $H$  correspond bijectively with the positive divisors of  $n$ .

**Proof.** 1. Let  $K \leq H$ . If  $K = \{1\}$ , then we are done. Suppose  $K \neq \{1\}$ . Thus, there exists some  $a \neq 0$  such that  $x^a \in K$ . Since  $K$  is a group,  $(x^a)^{-1} \in K$ . That is,  $x^{-a} \in K$ , and since either  $a$  or  $-a$  must be positive the set of all positive powers of  $x$  such that  $x$  to that positive power is an element of  $K$  is nonempty. That is,

$$P = \{n \in \mathbb{N} : x^n \in K\} \neq \emptyset$$

Thus, by the well-ordering principle, the set  $P$  contains a minimal element, call it  $d$ . By definition,  $x^d \in K$  and since  $K$  is a group  $\langle x^d \rangle \leq K$ . Let  $k \in K$ . Then,  $k = x^b$  for some  $b \in \mathbb{Z}$ . By the division algorithm, we have integers  $q, r$ , such that

$$b = qd + r \text{ where } 0 \leq r < d$$

Hence,

$$\begin{aligned} x^b &= x^{qd+r} \\ \implies x^b &= (x^{qd})x^r = (x^d)^qx^r \\ \implies (x^d)^{-q}x^b &= x^r \end{aligned}$$

Since  $x^d, x^b \in K$  and  $K$  is a group,

$$(x^d)^{-q} \in K \text{ and } (x^d)^{-q}x^b \in K$$

so  $x^r \in K$ . However, since  $d$  is the minimal positive power of  $x$  such that  $x^d \in K$ ,  $r$  must not be a positive power. Therefore,  $r = 0$  and it follows that

$$k = x^b = (x^d)^q \in \langle x^d \rangle$$

Therefore,  $K \leq \langle x^d \rangle$ . This gives  $\langle x^d \rangle = K$ .

2. Suppose  $|H| = n < \infty$  and  $a \mid n$  where  $a \in \mathbb{Z}$ . Let  $d = \frac{n}{a}$ . Hence

$$|\langle x^d \rangle| = \frac{n}{n/a} = a$$

**Uniqueness:** To show uniqueness, suppose  $K$  is any subgroup of  $H$  of order  $a$ . Then by part 1,  $K = \langle x^b \rangle$  where  $b$  is the smallest positive integer such that  $x^b \in K$ . We know

$$\frac{n}{d} = a = |K| = |x^b| = \frac{d}{\gcd(n,b)}$$

It follows that

$$d = \gcd(n, b)$$

Hence,  $d \mid b$  by definition and  $x^b \in \langle x^d \rangle$ . It follows that

$$K = \langle x^b \rangle \leq \langle x^d \rangle$$

and so  $K = \langle x^d \rangle$  as they have the same order. The final assertion follows from the fact that

$$\langle x^m \rangle \leq \langle x^{\gcd(m,n)} \rangle$$

and 2.5.2 (2) says

$$|<x^m>| = \frac{n}{\gcd(n, m)}$$

and

$$\left|x^{\gcd(m,n)}\right| = \frac{n}{\gcd(n, \gcd(m, n))}$$

and we know  $\gcd(n, \gcd(m, n)) = \gcd(n, m)$ . Since  $\gcd(m, n) \mid n$  this shows that every subgroup of  $H$  arises from a divisor of  $n$ .  $\square$

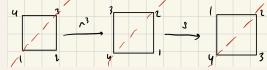
## 2.4 Subgroups Generated by Subsets of a Group

We have already examined the case of generating a subgroup with one element ( $\langle x \rangle$ ). What does it mean to generate a subgroup or a group with more than one element?

**Example 2.4.1.**  $D_{2n}$  = symmetries of a regular n-gon centered around the origin. Let  $r$  be a  $360/n$  clockwise rotation of the n-gon about the origin. Let  $s$  be a reflection of the n-gon about the line from vertex 1 to the origin.



Notice:  $1, r, r^2, r^3$  are all distinct. Now consider  $s, sr, sr^2, sr^3$  (we read these right-to-left).  $sr^3$  is the  $270^\circ$  rotation clockwise, then the reflection about the line where vertex 1 was to the origin.



Is  $s \in \{1, r, r^2, r^3\}$ ? No,  $s$  fixes vertex 1 and the only element that fixes vertex 1 is the identity. But  $s \neq 1$ , so  $s$  is not a rotation. From here, we can deduce that

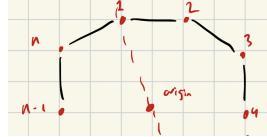
$$sr^j \neq r^i$$

for any  $0 \leq j \leq 3$  or  $0 \leq i \leq 3$  (if it were true that  $sr^j = r^i$  for some  $i$  and  $j$ , then  $s = r^{i-j}$ ). Hence  $D_{24} = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} = \langle r, s \rangle$

In  $D_{2n}, n \geq 3$ , we want to show that

$$D_{2n} = \{e, r, r^2, r^3, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$$

where  $s$  is a reflection over the line passing through vertex 1 and the origin.



1. Why are all  $e, r, r^2, \dots, r^{n-1}$  distinct?

$$\begin{aligned} r^i(1) &= i + 1 \text{ for } 0 \leq i \leq n - 1 \\ r^i(1) &= r^j(1) \\ \implies i + 1 &= j + 1 \\ \implies i &= j \end{aligned}$$

so the  $r^i$ 's are distinct.

2.  $s \neq r^i$  for any  $i \in \{0, \dots, n - 1\}$ .  $s(1) = 1$  if  $r^i(1) = 1$ , we know from part 1 that  $i = 0$ . That is,  $r^i = e$ . But  $s(2) = n \neq 2 = e(2) \implies s \neq e, s \neq r^i \forall 0 \leq i \leq n$
3. Let's show that  $r^i \neq sr^j$  for any  $i, j \in \{0, \dots, n - 1\} = A$ . Suppose there exists  $i, j \in A$  such that  $r^i = sr^j$ . We define  $r^{-1}$  as a counter-clockwise rotation;  $r^{-1} = r^{n-1}$ . This gives

$$\begin{aligned} r^i &= sr^j \\ \implies r^{i-j} &= s \\ \implies r^{i+n-j} &= s \end{aligned}$$

where we adjust  $(i + n - j) \bmod n$  as needed. This contradicts  $s \notin \{e, r, r^2, \dots, r^{n-1}\}$ . Hence  $r^i \neq sr^j$  for any  $i, j \in A$ .

4. Show that  $sr^i \neq sr^j$  for any  $i \neq j$  in  $A$ . For the sake of contradiction, suppose there exists  $i, j \in A$  such that  $sr^i = sr^j$ . Then

$$\begin{aligned} s^2r^i &= s^2r^j \\ \implies er^i &= er^j \\ \implies r^i &= r^j \end{aligned}$$

This contradicts  $i \neq j$ .

$$\begin{aligned} D_{2n} &= \{e, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\} \\ sr &\neq rs \\ (s \circ r)(1) &= s(r(1)) & (r \circ s)(1) &= r(s(1)) \\ &= s(2) & &= r(1) \\ &= n & &= 2 \end{aligned}$$

But  $sr = r^{-1}s$ . If  $sr(1) = r^{-1}s(1)$  and  $sr(2) = r^{-1}s(2)$ , then  $sr = r^{-1}s$ . It can be shown inductively that  $sr^i = r^{-i}s \forall i \in \mathbb{Z}$ .

Let  $x \in G$  and  $H \leq G$ . If  $x \in H$ , then  $\langle x \rangle \leq H$ . In some sense,  $\langle x \rangle$  is the smallest subgroup of  $G$  which contains  $x$ . "Smallest" refers to containment.

**Proposition 2.4.1.** If  $\mathcal{A}$  is any collection of subgroups of a group  $G$ , then  $\bigcap_{H \in \mathcal{A}} H \leq G$ .

**Proof.** HW

**Definition 2.4.1.** (Generating Sets)

If  $A$  is any subset of the group  $G$ , define

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

This is called the subgroup of  $G$  generated by  $A$ .  $A$  is called the generating set.

Notice that in the notation of prop 2.4.1

$$\mathcal{A} = \{H \leq G : A \subseteq H\} \text{ (nonempty as } G \in \mathcal{A} \text{ since } G \leq G \text{ and } A \subseteq G\}$$

We will show that  $\langle A \rangle$  is the unique minimal element of  $\mathcal{A}$ .

We know that  $A \subseteq H \forall H \in \mathcal{A}$ . Thus  $A \subseteq \langle A \rangle$ , so  $\langle A \rangle \in \mathcal{A}$ . Let  $K \in \mathcal{A}$ . We know that

$$\bigcap_{H \in \mathcal{A}} H \leq K$$

That is,  $\langle A \rangle \leq K$ . Hence,  $\langle A \rangle$  is minimal with respect to inclusion. When  $A$  is finite, that is

$$A = \{a_1, \dots, a_n\} \text{ for } n \in \mathbb{N}$$

then we write

$$\langle A \rangle = \langle a_1, a_2, \dots, a_n \rangle$$

This is a more concrete version of the previous set  $\langle A \rangle = \bigcap_{H \leq G, A \subseteq H} H$ . Denote

$$\overline{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \dots a_n^{\epsilon_n} : n \in \mathbb{N}, \epsilon_i = \pm 1, a_i \in A\}$$

In  $D_{2n}$ ,  $x \in \langle r, s \rangle$  could look like

$$rssssssr^{-1}s^{-1}srrs^{-1}rr^{-1}s = r^2$$

**Proposition 2.4.2.**  $\langle A \rangle = \overline{A}$ .

## 2.5 Quotient Groups and Homomorphisms

Let  $G$  be a group and  $N \leq G$ . Define a relation on  $G$  by

$$a \sim b \iff a^{-1}b \in N$$

It is straightforward to verify that this is an equivalence relation on  $G$ . For  $a \in G$ , the equivalence class of  $a$  is

$$\begin{aligned} \{b \in G : a \sim b\} &= \{b \in G : a^{-1}b \in N\} \\ &= \{b \in G : a^{-1}b = n \text{ for } n \in N\} \\ &= \{b \in G : b = an \text{ for } n \in N\} \\ &= \{an : n \in \mathbb{N}\} \\ aN &:= \{an : n \in N\} \end{aligned}$$

**Definition 2.5.1.** (Coset)

For a subgroup  $N$  of  $G$  and  $g \in G$ , let

$$\begin{aligned} gN &= \{gn : n \in N\} \\ Ng &= \{ng : n \in N\} \end{aligned}$$

be called the left coset and right coset of  $N$  in  $G$ , respectively. Any element of a coset is called a representative of that coset. We will denote the set of all left cosets of  $N$  in  $G$  by  $G/N$  (read  $G$  modulo  $N$  or  $G$  mod  $N$ ).

**Proposition 2.5.1.** Let  $N \leq G$ .  $G/N$  forms a partition of  $G$ . For all  $a, b \in G$ ,

$$aN = bN \iff a \text{ and } b \text{ are representatives of the same coset.}$$

**Proof.** Since we have recognized left cosets as the equivalence classes induced by an equivalence relation, they form a partition. That is,

$$G = \bigcup_{g \in G} gN$$

$$\forall g_1, g_2 \in G \quad g_1N = g_2N \iff g_1N \cap g_2N \neq \emptyset$$

Suppose  $a^{-1}b \in N$ . Then  $a^{-1}b = n$  for some  $n \in N$ . It follows that  $b = an \in aN$  so  $b \in aN$ . Since  $N$  is a subgroup,  $1 \in N$  hence  $b \cdot 1 \in bN$ . It follows that  $aN \cap bN \neq \emptyset \implies aN = bN$ .

Now assume  $aN = bN$ . Then  $an = b$  for some  $n \in N$ . It follows that  $n = ba^{-1} \in N$ . Finally, we have

$$\begin{aligned} aN = bN &\iff a^{-1}b \in N \\ &\iff b \in aN \\ &\iff b \in aN \text{ and } a \in aN \\ &\iff a \text{ and } b \text{ are representatives of } aN(\text{or } bN) \end{aligned}$$

□

**Proposition 2.5.2.** Let  $N \leq G$ .

1. The operation on  $G/N$  described by  $aN \cdot bN = (ab)N \quad \forall a, b \in G$  is well-defined if and only if  $gng^{-1} \in N \quad \forall g \in G, n \in N$
2. If the operation above is well-defined, then  $G/N$  defines a group, where

$$\begin{aligned} 1 \cdot N &\text{ is the identity} \\ (gN)^{-1} &= g^{-1}N \quad \forall g \in G \end{aligned}$$

**Proof.** 1. ( $\Leftarrow$ ) Suppose  $gng^{-1} \in N \quad \forall g \in G, n \in N$ . Let  $a, a_1 \in aN$  and  $b, b_1 \in bN$ . We want to show that

$$abN = a_1b_1N$$

$a_1 = an$  and  $b_1 = bm$  for some  $n, m \in N$ . Note that  $a_1b_1 \in abN \iff a_1b_1N = abN$ , so we will prove the

former.

$$\begin{aligned} a_1 b_1 &= (an)(bm) = a(bb^{-1})nbm \\ &= ab(b^{-1}nb)m \end{aligned}$$

by assumption,  $b^{-1}n(b^{-1})^{-1} \in N$  so it follows that  $a_1 b_1 = abn_1 m$  where  $n_1 \in N$ . Since  $N$  is a subgroup of  $G$ ,  $n_1 m \in N$ , call it  $n_2$ . Thus  $a_1 b_1 = abn_2$  where  $n_2 \in N$ . That is,  $a_1 b_1 \in abN$ , proving our result ( $a_1 b_1 N = abN$ ).

2. Suppose the operation is well-defined. We want to show  $G/N$  is a group.

**Associativity:** Let  $aN < bN < cN \in G/N$  ( $a, b, c \in G$ ). Then

$$\begin{aligned} aN(bNcN) &= aN((bc)N) \\ &= a(bc)N \\ &= (ab)cN \\ &= ((ab)N)cN \\ &= (aNbN)cN \end{aligned}$$

**Identity, Closure, and Inverses:** Let  $aN \in G/N$  be given. Since  $B$  is a group,  $1 \in G$  and thus

$$1N \in G/N$$

and

$$(aN)(1N) = (a1)N = aN$$

Also,

$$\left. \begin{array}{l} a \in G \\ G \text{ is a group} \end{array} \right\} \implies a^{-1} \in G \implies a^{-1}N \in G/N$$

and so

$$\begin{aligned} (aN)(a^{-1}N) &= (aa^{-1})N \\ &= 1N \\ &= (a^{-1}a)N \\ &= (a^{-1}N)(aN) \end{aligned}$$

□

$G/N$  will be a group when  $N$  has that nice property, detailed in the following definition.

**Definition 2.5.2.** (Normal Subgroup)

A subgroup  $N$  of  $G$  is called normal in  $G$  if every element of  $g$  normalizes  $N$ . That is,  $N$  is normal in  $G$  if

$$gNg^{-1} = N \quad \forall g \in G$$

If  $N$  is a normal subgroup of  $G$ , then we write  $N \trianglelefteq G$ .

**Theorem 2.5.1.** (Characterizations of Normal Subgroups)

The  $N \leq G$ . The following are equivalent:

1.  $N \trianglelefteq G$
2.  $N_G(N) = G$
3.  $gN = NG \quad \forall g \in G$
4. The operation "coset multiplication" is well-defined
5.  $gNg^{-1} \subseteq N \quad \forall g \in G$

**Example 2.5.1.** Checking that a subgroup is normal is not practical using the definition. We would need to check that  $gng^{-1} \in N \quad \forall g \in G, n \in N$ . If a subgroup is finitely generated, it suffices to check that the generators map back to the subgroup by conjugating.

Let  $G = D_{16}$ . Is  $\langle s \rangle$  normal in  $D_{16}$ ? We need to examine  $gsg^{-1}$  for an arbitrary  $g \in D_{16}$ . Letting  $g = s^i r^j$  where  $i \in \{0, 1\}$  and  $j \in \{0, \dots, 7\}$ . Then

$$\begin{aligned} gsg^{-1} &= (s^i r^j) s (s^i r^j)^{-1} \\ &= s^i r^j s r^{-j} s^{-i} \\ &= r^j s r^{-j} \text{ (when } i = 0) \\ &= r^j r^{-j} s \text{ (} sr^{-j} = r^{-(j)} s = r^j s\text{)} \\ &= r^{2j} s \end{aligned}$$

When  $j = 1$ , this gives that  $gsg^{-1} = r^2 s \notin \langle s \rangle$  since this would imply that  $r^2$  is either the identity or  $s$  ( $r^2 s = 1 \implies r^2 = s$ ,  $r^2 s = s \implies r^2 = 1$ ) which is a contradiction.

**Theorem 2.5.2.** (Big Theorem)

A subgroup  $N \leq G$  is normal in  $G$  if and only if it is the kernel of some homomorphism.

**Proof.** ( $\Leftarrow$ ) HW

( $\Rightarrow$ ) Suppose  $N \trianglelefteq G$ . Let's define

$$\begin{aligned} \pi : G &\rightarrow G/N \\ \pi(g) &= gN \quad \forall g \in G \end{aligned}$$

Let  $g_1, g_2 \in G$ . Then

$$\begin{aligned} \pi(g_1 g_2) &= (g_1 g_2)N \\ &= (g_1 N)(g_2 N) \\ &= \pi(g_1) \pi(g_2) \end{aligned}$$

Hence,  $\pi$  is a homomorphism. It remains to show that  $\ker \pi = N$ . Note that

$$\begin{aligned} \ker \pi &= \{g \in G : \pi(g) = 1N\} \\ &= \{g \in G : gN = 1N\} \\ &= \{g \in G : g \in 1N\} \\ &= \{g \in G : g \in N\} \\ &= N \end{aligned}$$

completing the proof. □

**Definition 2.5.3.** (Natural Projection Homomorphism)

Let  $N \trianglelefteq G$ . The homomorphism

$$\begin{aligned} \pi : G &\rightarrow G/N \\ \pi(g) &= gN \end{aligned}$$

is called the natural projection (homomorphism) of  $G$  onto  $G/N$ .

If  $\overline{H} \leq G/N$ , the complete preimage of  $\overline{H}$  is  $\pi^{-1}(\overline{H})$ .

**Note .** If  $\overline{H} \leq G/N$ , then

$$N \leq \pi^{-1}(\overline{H})$$

Since  $1N \in \overline{H}$ , we have  $N = \ker \pi = \pi^{-1}(1N) \subseteq \pi^{-1}(\overline{H})$ .

$Q_8$ : we have that  $\langle -1 \rangle$  is a normal subgroup, so  $Q_8 / \langle -1 \rangle$  is a group consisting of  $1 \langle -1 \rangle, i \langle -1 \rangle, j \langle -1 \rangle, k \langle -1 \rangle$

$$(i \langle -1 \rangle)^2 = i^2 \langle -1 \rangle = -1 \langle -1 \rangle = 1 \langle -1 \rangle$$

so,  $Q_8 / \langle -1 \rangle \cong V_4$ .

$$\begin{aligned}\langle i \langle -1 \rangle \rangle &\cong Q_8 / \langle -1 \rangle \\ \langle i \langle -1 \rangle \rangle &= \{i \langle -1 \rangle, 1 \langle -1 \rangle\} = \overline{H} \\ \pi^{-1}(\overline{H}) &= \{g \in Q_8 : \pi(g) \in \overline{H}\}\end{aligned}$$

$$\begin{aligned}\pi(1) &= 1 \langle -1 \rangle \in \overline{h} & \pi^{-1}(\overline{H}) &= \{1, i, -1, -i\} \\ \pi(i) &= i \langle -1 \rangle \in \overline{H} \\ \pi(-1) &= -1 \langle -1 \rangle = 1 \langle -1 \rangle \in \overline{H} \\ \pi(-i) &= -i \langle -1 \rangle = i \langle -1 \rangle \in \overline{H}\end{aligned}$$

## 2.6 Cosets and Lagrange's Theorem

There are a lot of ways to see if a subgroup is normal.

Some things to know about normal subgroups: Let  $G$  be a group.

1.  $\{1\} \trianglelefteq G$  and  $G \trianglelefteq G$  and  $G/\{1\} \cong G, G/G \cong \{1\}$
2. When  $G$  is clearly an additive group we denote left and right cosets  $g + N$  and  $N + g$ , respectively, where  $N \leq G$  and

$$\begin{aligned} g + N &= \{g + n : n \in N\} \\ N + g &= \{n + g : n \in N\} \end{aligned}$$

3. When  $G$  is abelian, every subgroup is normal

We move away from normal subgroups and just analyze subgroups.

**Theorem 2.6.1.** (Lagrange's Theorem)

If  $G$  is a finite group and  $H \leq G$ , then  $|H| \mid |G|$  and the number of left cosets of  $H$  in  $G$  is  $|G|/|H|$ .

**Proof.** Here is a proof idea (problems 18, 19 from section 1.7): the left cosets form a partition of  $G$

$$G = \bigcup_{g \in G} gH$$

There is a bijection from  $H$  to  $gH$  ( $h \mapsto gh$ ) so  $|H| = |gH|$ . Then,

$$|G| = k|H|$$

where  $k$  is the number of distinct left cosets of  $H$  in  $G$ . Rearranging gives

$$k = \frac{|G|}{|H|}$$

□

**Definition 2.6.1.** (Index of a Subgroup)

If  $G$  is a group (possibly finite) and  $H \leq G$ , then the number of distinct left cosets of  $H$  in  $G$  is called the index of  $H$  in  $G$ , denoted  $|G : H|$ .

**Corollary 2.6.1.** If  $G$  is a finite group and  $x \in G$ , then  $|x| \mid |G|$ .

**Proof.** We proved that  $|x| = |\langle x \rangle|$  and  $\langle x \rangle \leq G$ . The claim follows immediately from Lagrange's theorem. □

**Example 2.6.1.** For a finite group with  $H \leq G$

$$|G : H| = |G|/|H|$$

**Example 2.6.2.** Consider  $G = \mathbb{Z}$  and  $H = 3\mathbb{Z}$ .

$$|\mathbb{Z} : 3\mathbb{Z}| = 3 = |\mathbb{Z}/3\mathbb{Z}|$$

$$\begin{aligned} 3\mathbb{Z} &= \{3x : x \in \mathbb{Z}\} \\ 1 + 3\mathbb{Z} &= \{1 + 3x : x \in \mathbb{Z}\} \\ 2 + 3\mathbb{Z} &= \{2 + 3x : x \in \mathbb{Z}\} \\ 3 + 3\mathbb{Z} &= \{3 + 3x : x \in \mathbb{Z}\} = 0 + 3\mathbb{Z} \end{aligned}$$

**Corollary 2.6.2.** If  $G$  is a group of prime order  $p$ , then  $G$  is cyclic.

**Proof.** Let  $x \in G$  where  $x \neq 1_G$ . Then  $|x| \mid |G|$ . Since  $|G| = p$ , a prime, then  $|x| \in \{1, p\}$ . Since  $x \neq 1_G$ ,  $|x| \neq 1$ . Thus  $|x| = p$  and hence  $\langle x \rangle = G$ .  $\square$

**Example 2.6.3.** A subgroup  $H$  of a group  $G$  with index 2 is normal ( $|G : H| = 2$ ). Let  $g \in G - H$ . Then  $gH \neq 1H$ . Since  $|G : H| = 2$ , there are two distinct cosets of  $H$  in  $G$  and since one of them is  $1H$ , the other must be  $gH$ . Similarly, there are only two distinct right cosets of  $H$  in  $G$ , namely  $H1$  and  $Hg$ . Since  $1H = H1$  and cosets form a partition of  $G$ , we have

$$gH = G - H = Hg$$

Hence the left and right cosets of  $H$  are the same and  $H$  is normal in  $G$ .

**Example 2.6.4.** A subgroup  $H$  is a normal subgroup of  $G$  is not a transitive statement. Let  $G = D_8$ . Then  $|D_8| = 8$ ,  $|\langle s \rangle| = 2$ ,  $|\langle s, r^2 \rangle| = 4$ . Clearly,

$$\langle s \rangle \leq \langle s, r^2 \rangle \leq D_8$$

We have

$$|D_8 : \langle s, r^2 \rangle| = 2$$

and

$$|\langle s, r^2 \rangle : \langle s \rangle| = 2$$

so

$$\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$$

but  $\langle s \rangle$  is not normal in  $D_8$  since  $rsr^{-1} = r^2s \notin \langle s \rangle$ .

**Definition 2.6.2.** (Product of Subgroups)

Let  $H, K \leq G$ . Define

$$HK = \{hk : h \in H, k \in K\}$$

**Theorem 2.6.2.** (Order of Products of Subgroups)

If  $H$  and  $K$  are finite subgroups of a group, then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Note that  $HK$  need not be a group for this to hold.

**Proof.** Notice that  $HK$  is the union of left cosets of  $K$ . That is,

$$HK = \bigcup_{h \in H} hK$$

Since each coset of  $K$  has  $|K|$  elements, we will count the number of distinct cosets in the above union. We know  $h_1K = h_2K$  for  $h_1, h_2 \in H$  if and only if  $h_2^{-1}h_1 \in K$ . It follows that

$$\begin{aligned} h_1K = h_2K &\iff h_2^{-1}h_1 \in K \cap H \\ &\iff h_1(K \cap H) = h_2(K \cap H) \end{aligned}$$

Thus the number of distinct cosets of the form  $hK$ ,  $h \in H$  is the same as the number of distinct cosets of  $K \cap H$  in  $H$ . Since  $H \cap K \leq H$ , this is  $|H|/|H \cap K|$ . Therefore,  $HK$  consists of  $|H|/|H \cap K|$  distinct cosets of  $K$ , each of which contains  $|K|$  elements. It follows that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

$\square$

$HK$  is not always a subgroup of  $G$ .

**Example 2.6.5.** Let  $G = S_3$ ,  $H = \langle (1\ 2) \rangle$ , and  $K = \langle (2\ 3) \rangle$ . Then  $H \cap K = \{1\}$  and

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{2 \cdot 2}{1} = 4$$

Lagrange says that if  $HK \leq G$ , then  $4 \mid 3! = 6$ , a contradiction.

We can further deduce

$$\langle (1\ 2), (2\ 3) \rangle = S_3$$

since

$$4 \leq |\langle (1\ 2), (2\ 3) \rangle| \leq 6$$

and  $|\langle (1\ 2), (2\ 3) \rangle|$  must also divide 6, so  $\langle (1\ 2), (2\ 3) \rangle$  generates all of  $S_3$ .

**Proposition 2.6.1.** If  $H, K \leq G$ , then  $HK \leq G$  if and only if  $HK = KH$ . (Note:  $HK = KH$  does NOT indicate the elements of  $H$  and  $K$  commute with each other, only that for  $hk \in HK$  we have  $hk = k_1 h_1$  for some  $k_1 \in K, h_1 \in H$ .)

**Proof.** ( $\implies$ ) Assume  $HK = KH$ . Since  $H$  and  $J$  are nonempty,  $HK$  is nonempty. It remains to show that if  $a, b \in HK$ , then  $ab^{-1} \in HK$ . Let  $a, b \in HK$ . Then  $a = h_1 k_1$  and  $b = h_2 k_2$ . Then

$$\begin{aligned} ab^{-1} &= (h_1 k_1)(h_2 k_2)^{-1} \\ &= h_1 k_1 k_2^{-1} h_2^{-1} \end{aligned}$$

Since  $K \leq G$ , we have

$$k_1 k_2^{-1} = k_3 \in K$$

and since  $H \leq G$  we have

$$h_2^{-1} = h_3 \in H$$

This gives

$$ab^{-1} = h_1 k_3 h_3$$

Since  $HK = KH$ , we know that  $k_3 h_3 \in HK$ . That is,

$$k_3 h_3 = h_4 k_4 \text{ for some } h_4 \in H, k_4 \in K$$

so,

$$ab^{-1} = h_1 h_4 k_4$$

and letting  $h_1 h_4 = h_5 \in H$  we have

$$ab^{-1} = h_5 k_4 \in HK$$

Thus  $HK \leq G$ .

( $\Leftarrow$ ) Conversely, suppose  $HK \leq G$ . Our goal is to show  $HK = KH$ . That is, we want to show  $HK \subseteq KH$  and  $KH \subseteq HK$ . Since  $K \leq HK$  and  $H \leq HK$ ,

$$KH \subseteq HK \text{ by closure of } HK$$

To show  $HK \subseteq KH$ , let  $hk \in HK$ . Since  $HK$  is a subgroup,  $hk$  is the inverse to some  $a \in HK$ . That is

$$hk = a^{-1} = (hk)^{-1} = (h_a k_a)^{-1} = k_a^{-1} h_a^{-1} \in KH$$

It follows that  $HK \subseteq KH$ . Thus,  $HK = KH$ . □

**Example 2.6.6.** Let  $G = D_8$ ,  $H = \langle r \rangle$ ,  $K = \langle s \rangle$ . Notice  $rs \in HK$  and  $rs = sr^{-1} \in KH$ . Also,

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{4 \cdot 2}{1} = 8$$

So,  $HK = D_8 = KH$ .

**Corollary 2.6.3.** If  $H, K \leq G$  and  $H \leq N_G(K)$ , then  $HK \leq G$ . In particular, if  $K \trianglelefteq G$ , then  $HK \leq G \ \forall H \leq G$ .

**Proof.** We will prove  $HK = KH$ . Let  $h \in H$  and  $k \in K$ . By assumption,

$$H \leq N_G(K) \implies hkh^{-1} \in K$$

Then

$$hk = hkh^{-1}h \in KH$$

Thus  $HK \subseteq KH$ . Similarly,

$$kh = hh^{-1}kh \in HK$$

It follows that  $KH \subseteq HK$ . Hence,  $HK = KH$ . □

**Theorem 2.6.3.** (Subgroup Index Theorem)

Let  $H, K$  be subgroups of a group  $G$  with  $H \leq K \leq G$ . Then

$$|G : H| = |G : K| \cdot |K : H|$$

**Proof.** Let  $g_i$  be a distinct representation for a left coset of  $H$  in  $G$ ,  $\forall i \in I$  where  $I$  is an indexing set. So

$$\{g_iH : i \in I\} = G/H = \{gH : g \in G\}$$

and  $g_iH = Hg_j$  if and only if  $g_i = g_j$ . Let  $\psi : I \times K/H \rightarrow G/H$  be defined by

$$\psi(i, kH) = g_i k H$$

We will show  $\psi$  is a well-defined bijection.

**Well-defined:** Suppose that  $k_1H = k_2H$  for some  $k_1, k_2 \in K$ . That is,  $k_1^{-1}k_2 \in H$ . Then

$$\begin{aligned} \psi(i, k_1H) &= g_i k_1 H \psi(i, k_2H) \\ &= g_i k_2 H \end{aligned}$$

So,

$$\begin{aligned} (g_i k_1)^{-1}(g_i k_2) &= k_1^{-1} g_i^{-1} g_i k_2 \\ &= k_1^{-1} 1_G k_2 \\ &= k_1^{-1} k_2 \in H \text{ by assumption.} \end{aligned}$$

Hence,  $\psi$  is well-defined.

**Bijection:** Suppose  $\psi(i, k_1H) = \psi(j, k_2H)$ . Then

$$\begin{aligned} g_i k_1 H &= g_j k_2 H \\ \implies (g_i k_1)^{-1}(g_j k_2) &\in H \\ \implies k_1^{-1} g_i^{-1} g_j k_2 &= h \text{ for some } h \in H \\ \implies g_i^{-1} g_j &= k_1 h k_2^{-1} \text{ for some } h \in H \\ \implies g_i^{-1} g_j &\in K \text{ since } H \subseteq K \\ \implies g_i K &= g_j K \\ \implies g_i &= g_j \\ \implies i &= j \end{aligned} \tag{*}$$

Using this in (\*) gives

$$\begin{aligned} k_1^{-1} g_i^{-1} g_i k_2 &= h \text{ for some } h \in H \\ \implies k_1^{-1} k_2 &= h \in H \\ \implies k_1 H &= k_2 H \end{aligned}$$

Hence  $\psi$  is one-to-one.

Let  $gH \in G/H$ . Since the left cosets of  $K$  partition the group  $G$  we have that  $g \in g_i K$ . That is,  $g = g_i k$  for some  $k \in K$ . Hence

$$\psi(i, kH) = g_i k H = gH$$

Thus,  $\psi$  is onto.

We have that  $\psi$  is a well-defined bijection. Hence,

$$\begin{aligned} I \times K/H &\rightarrow G/H \\ |G : K| \cdot |K : H| &= |G : H| \end{aligned}$$

## Chapter 3

# Quotient Groups and Homomorphisms

### 3.1 Isomorphism Theorems

**Theorem 3.1.1.** (The First Isomorphism Theorem)

If  $\phi : G \rightarrow H$  is a group homomorphism, then  $\ker \phi \trianglelefteq G$  and

$$G/\ker \phi \cong \phi(G) \leq H$$

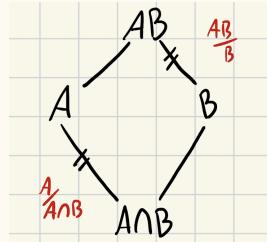
**Corollary 3.1.1.** Let  $\phi : G \rightarrow H$  be a group homomorphism.

1.  $\phi$  is injective if and only if  $\ker \phi = \{1\}$
2.  $|G : \ker \phi| = |\phi(G)|$

**Theorem 3.1.2.** (The Second Isomorphism Theorem; The Diamond Theorem)

Let  $G$  be a group and let  $A, B \leq G$ . Assume  $A \leq N_G(B)$ . Then

$$\begin{aligned} AB &\leq G \\ B &\trianglelefteq AB \\ A \cap B &\trianglelefteq A \\ AB/B &\cong A/A \cap B \end{aligned}$$



**Proof.** Since  $A \leq N_G(B)$ , it follows that

$$AB \leq N_G(B)$$

and since  $B \leq AB$ , we have  $B \trianglelefteq AB$ .

Since  $B \trianglelefteq AB$ , then  $AB/B$  is a group. Define

$$\begin{aligned} \phi : A &\rightarrow AB/B \\ \phi(a) &= aB \quad \forall a \in A \end{aligned}$$

By the First Isomorphism Theorem, if  $\phi$  is a homomorphism then

$$A/\ker \phi \cong \phi(A)$$

We need to show

1.  $\phi$  is a homomorphism

2.  $\phi(A) = AB/B$
3.  $\ker \phi = A \cap B$
1. Let  $a_1, a_2 \in A$ . Then

$$\begin{aligned}\phi(a_1 a_2) &= a_1 a_2 B \\ &= (a_1 B)(a_2 B) \\ &= \phi(a_1)\phi(a_2)\end{aligned}$$

2. Notice that  $abB = aB$  since  $b \in B$ . That is,  $\forall abB \in AB/B \ abB = aB$ . Thus our mapping is surjective. Hence  $\phi(A) = AB/B$ .

3. Notice

$$\begin{aligned}\ker \phi &= \{a \in A : \phi(a) = 1B\} \\ &= \{a \in A : aB = 1B\} \\ &= \{a \in A : a \in B\} \\ &= A \cap B\end{aligned}$$

By the First Isomorphism Theorem on 1, 2, and 3, we have  $A/\ker \phi \cong \phi(A)$ . That is,

$$A/A \cap B \cong AB/B$$

where  $A \cap B \trianglelefteq A$ . □

**Theorem 3.1.3.** (The Third Isomorphism Theorem)

Let  $G$  be a group and let  $H$  and  $K$  be normal subgroups of  $G$  with  $H \leq K$ . Then

$$\frac{G/H}{K/H} \cong G/K$$

**Proof.** We proceed to define a homomorphism from  $G/H \rightarrow G/K$  that is surjective such that  $\ker \phi = K/H$ . Then the claim follows from the First Isomorphism Theorem.

Since  $K \trianglelefteq G$ ,  $\pi_H(K) = \{kH : k \in K\}$ . We know that the

$$\pi_H(K) \trianglelefteq \pi_H(G) = G/H$$

Notice  $\{kH : k \in K\} = K/H$ . Define

$$\begin{aligned}\phi : G/H &\rightarrow G/K \\ gH &\mapsto gK \quad \forall g \in G\end{aligned}$$

We proceed to show  $\phi$  is a well-defined, epimorphism (surjective homomorphism).

**$\phi$  is well-defined:** Suppose  $g_1H = g_2H$ . Then  $g_1 = g_2h$  for some  $h \in H$ . Since  $H \leq K$ ,  $h \in K$ . That is

$$\begin{aligned}g_1 &= g_2h \text{ where } h \in K \\ \implies g_1K &= g_2K\end{aligned}$$

Hence  $\phi(g_1H) = \phi(g_2H)$  and our function is well-defined.

**$\phi$  is a homomorphism:** Let  $g_1H, g_2H \in G/H$ . Then

$$\begin{aligned}\phi(g_1Hg_2H) &= \phi(g_1g_2H) \\ &= g_1g_2K \\ &= (g_1K)(g_2K) \\ &= \phi(g_1H)\phi(g_2H)\end{aligned}$$

Hence,  $\phi$  is a homomorphism.

**$\phi$  is surjective:**  $\phi$  is clearly surjective by construction.

$\ker \phi = K/H$ :

$$\begin{aligned}\ker \phi &= \{gH \in G/H : \phi(gH) = 1K\} \\ &= \{gH \in G/H : gK = 1K\} \\ &= \{gH \in G/H : g \in K\} \\ &= K/H\end{aligned}$$

By the First Isomorphism Theorem,

$$\frac{G/H}{K/H} \cong G/K$$

□

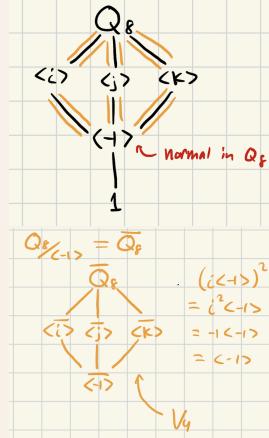
**Theorem 3.1.4.** (The Fourth Isomorphism Theorem; The Lattice Isomorphism Theorem)

Let  $G$  be a group with  $N \trianglelefteq G$ . Then there is a bijection from  $\{A \leq G : N \leq A\}$  to the set of subgroups of  $G/N$ . In particular, every subgroup of  $\bar{G} = G/N$  is of the form  $\bar{A} = A/N$  for some subgroup  $A$  of  $G$ , containing  $N$  (Namely, the complete preimage of the subgroup of  $G/N$ , under the natural projection from  $G$  to  $G/N$ ).

This bijection has the following properties:

1.  $A \leq B \iff \bar{A} \leq \bar{B}$  ( $A/N \leq B/N$ )
2. If  $A \leq B$  then  $|A : B| = |B/N : A/N| = |\bar{B} : \bar{A}|$
3.  $\langle \bar{A}, \bar{B} \rangle = \langle \bar{A}, \bar{B} \rangle$
4.  $\bar{A} \cap \bar{B} = \bar{A} \cap \bar{B}$
5.  $A \trianglelefteq G \iff \bar{A} \trianglelefteq \bar{G}$

**Example 3.1.1.** The group  $Q_8$ :



## 3.2 The Alternating Group

The following are important theorems that we will come later. We do not prove these yet, but we will soon.

**Theorem 3.2.1.** (Cauchy's Theorem)

If  $G$  is a finite group and  $p$  is a prime dividing  $|G|$ , then  $G$  has an element of order  $p$ .

**Theorem 3.2.2.** (Sylow Theorem)

If  $G$  is a finite group of order  $p^\alpha \cdot m$ , where  $p$  is prime and  $p \nmid m$ , then  $G$  has a subgroup of order  $p^\alpha$ .

**Proposition 3.2.1.**

If  $G$  is a finite abelian group and  $p$  is a prime dividing  $|G|$ , then  $G$  contains an element of order  $p$ .

**Proof.** We will use strong induction to prove this result. We will assume the result holds for all groups with order  $< |G|$  and show this implies the result for  $G$ .

Since  $|G| > 1$  there is an element  $x \in G$  such that  $x \neq 1_G$ . If  $|G| = p$ , then we are done (by Lagrange's theorem, we know  $\langle x \rangle = G$  hence  $|x| = p$ ). Suppose  $|G| > p$ , and suppose  $p \mid |x|$  for some  $x \in G$ . Then

$$|x| = pn \text{ for some } n \in \mathbb{Z}$$

We know

$$|x^n| = \frac{|x|}{\gcd(|x|, n)} = \frac{|x|}{n} = \frac{pn}{n} = p$$

We now assume  $p \nmid |x|$ . Let  $\langle x \rangle = N$ . Since  $G$  is abelian,  $N \trianglelefteq G$  and by Lagrange's theorem,

$$|G : N| = |G/N| = |G|/|N|$$

and since  $N \neq 1_G$ ,  $|G|/|N| < |G|$ . Since  $p \nmid |N|$  we have that  $p \mid |G/N|$ . By our inductive assumption, we can conclude there exists  $yN \in G/N$  such that  $|yN| = p$ . Since  $yN \neq 1N$  we have that  $y \notin N$ . But  $y^p \in N$  since

$$(yN)^p = y^p N$$

Since  $\langle y^p \rangle \leq N$  we have  $\langle y \rangle \neq \langle y^p \rangle$ . That is,  $\langle y^p \rangle < \langle y \rangle$  and further  $|y^p| < |y|$ . We know

$$|y^p| = \frac{|y|}{\gcd(|y|, p)} = \frac{|y|}{p}$$

Thus  $p \mid |y|$ . By our first case, we are done.

This completes the induction and every abelian group with  $p \mid |G|$  has one element of order  $p$ . □

Central to this proof was finding  $N \trianglelefteq G$ . What if we can't?

**Definition 3.2.1.** (Simple Group)

A (finite or infinite) group  $G$  is called simple if  $|G| > 1$  and the only normal subgroups of  $G$  are  $1$  and  $G$ .

**Example 3.2.1.**  $\mathbb{Z}_p$  where  $p$  is prime is the most important simple group (for us) ((to be proved later)).

We shift our attention back to permutations. Consider  $\sigma \in S_3$ .

$$\begin{aligned} \sigma &= (1 \ 2 \ 3) \\ \sigma &= (1 \ 3)(1 \ 2) \\ &= (1 \ 2)(1 \ 3)(1 \ 2)(1 \ 3) \end{aligned}$$

Notice that in general for any  $m$ -cycle in  $S_n$  we have

$$(a_1 \ a_2 \ a_3 \ \dots \ a_m) = (a_1 \ a_m)(a_1 \ a_{m-1}) \dots (a_1 \ a_3)(a_1 \ a_2)$$

That is, every  $m$ -cycle in  $S_n$  can be written as a product of 2-cycles (transpositions) since every permutation in  $S_n$  can be written as a product of disjoint cycles. Hence, every permutation in  $S_n$  can be written as a product of transpositions. That is,

$$\langle T \rangle = S_n \text{ where } T = \{(i \ j) : 1 \leq i < j \leq n\}$$

**Example 3.2.2.**  $S_4$ ,  $T$  has the elements

$$(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$$

**Definition 3.2.2.** (Even Permutation)

A permutation  $\alpha \in S_n$  is called even if it can be written as a product of an even number of transpositions. Otherwise,  $\alpha$  is called odd.

**Remark 3.2.1.**  $(1\ 2\ 3) = (1\ 3)(1\ 2)$ , so  $(1\ 2\ 3)$  is even. However,  $(1\ 2\ 3) = (1\ 3)(1\ 2)(1\ 3)(1\ 2)$ . Is this a well-defined definition? Can a permutation be both even and odd? **NO:** Permutations in  $S_n$  are either even or odd but not both.

**Definition 3.2.3.** (The  $\varepsilon$  Homomorphism)

For each  $\sigma \in S_n$ , define

$$\varepsilon(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even} \\ -1 & \text{if } \sigma \text{ is odd} \end{cases}$$

$\varepsilon$  defines a mapping from  $S_n$  to the multiplicative group  $G = \{-1, 1\}$ .

Let  $\sigma, \tau \in S_n$ . Assume  $\sigma, \tau$  are both even or both odd. Then  $\sigma\tau$  is an even permutation, so

$$\varepsilon(\sigma\tau) = -1 \text{ and } \varepsilon(\sigma) \cdot \varepsilon(\tau) = 1$$

If one of  $\sigma, \tau$  is odd and the other is even, then  $\sigma\tau$  is odd and

$$\varepsilon(\sigma\tau) = -1 \text{ and } \varepsilon(\sigma) \cdot \varepsilon(\tau) = -1$$

so  $\varepsilon$  is a homomorphism. By the First Isomorphism theorem, we have

$$\frac{S_n}{\ker \varepsilon} \cong \varepsilon(S_n) = \{-1, 1\}$$

By Lagrange's Theorem,

$$\begin{aligned} \frac{|S_n|}{|\ker \varepsilon|} &= |\{-1, 1\}| = 2 \\ \implies \frac{n!}{|\ker \varepsilon|} &= 2 \\ \implies |\ker \varepsilon| &= \frac{n!}{2} \end{aligned}$$

Notice that

$$\ker \varepsilon = \{\sigma \in S_n : \varepsilon(\sigma) = 1\} = \{\sigma \in S_n : \sigma \text{ is even}\}$$

**Definition 3.2.4.** (The Alternating Group)

The alternating group of degree  $n$ , denoted by  $A_n$ , is the kernel of the Homomorphism  $\varepsilon$ . It is more commonly referred to as the set of all even permutations in  $S_n$ .