

# MATH 541 Lecture Notes

PONGSAPHOL PONGSAWAKUL

Spring 2023

## Contents

<b>1</b>	<b>Groups</b>	<b>3</b>
1.1	Axioms of Groups . . . . .	3
1.1.1	Properties . . . . .	4
1.2	Dihedral Groups . . . . .	6
1.2.1	Triangle . . . . .	6
1.2.2	n-gon . . . . .	7
1.2.3	Definition . . . . .	7
1.3	Symmetric Group . . . . .	7
1.3.1	Cycle Decomposition . . . . .	8
1.4	Homomorphisms and Isomorphisms . . . . .	8
1.5	Group Actions . . . . .	10
<b>2</b>	<b>Subgroups</b>	<b>11</b>
2.1	Definition and Examples . . . . .	11
2.2	Centralizers and Normalizers, Stabilizers and Kernels . . . . .	11
2.3	Cyclic groups . . . . .	12
<b>3</b>	<b>Quotient Groups and Homomorphisms</b>	<b>14</b>
3.1	Definition and Examples . . . . .	14
3.2	MORE ON COSETS AND LAGRANGE's THEOREM . . . . .	16

- Book: Dujmit Foote “Modern Algebra 3rd ed”
- Midterm 3/23 in class
- Final 5/8
- Homeworks: weekly
- Honors Credit: Extra sections + homeworks

# 1 Groups

Operations often modeled:  $+$ ,  $\cdot$

composition: space of thing that you are looking at  $\leftarrow$  almost always not commutative

**Groups:** One operation  $\cdot$

**Rings:** 2 operations:  $+$ ,  $\cdot$  that play nice

## 1.1 Axioms of Groups

By “operation” on  $S$ , I mean a function  $\cdot : S \times S \rightarrow S$

Instead of  $\cdot(a, b)$ , we write  $a \cdot b$

A group is a set  $G$  with an operation  $\cdot$  satisfying:

1. Associativity:  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. There is an identity element: there is one special element  $1 \in G$  so  $1 \cdot a = a$  for any  $a \in G$  and  $a \cdot 1 = a$  for any  $a \in G$
3. Inverses: For any  $a \in G$ , there is a  $b \in G$  so  $a \cdot b = b \cdot a = 1$

**Note:**  $a \cdot b = b \cdot a$  is not an axiom.

If  $G$  satisfies this, we call it an abelian group

**Example 1.**  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$

1. 0 is the identity
2. inverses:  $-a$  is the inverse of  $a$

**Example 2.**  $(\mathbb{Q} \setminus \{0\}, \cdot)$ ,  $(\mathbb{R} \setminus \{0\}, \cdot)$ ,  $(\mathbb{C} \setminus \{0\}, \cdot)$

1. 1 is the identity
2. Inverses:  $\frac{1}{a}$  is the inverse of  $a$

**Note:**  $(\mathbb{Z} \setminus \{0\}, \cdot)$  is not a group

$(V, +)$  is a group

**Example 3.** For  $n$ , a natural number,  $(\mathbb{Z}/n\mathbb{Z}, +)$  is a group

On  $\mathbb{Z}$ , we say  $a, b$  are  $(\text{mod } n)$  equivalent (written  $a \equiv b(\text{mod } n)$ ) if  $n$  divides  $a - b$

$\mathbb{Z}/n\mathbb{Z}$  is the set of equivalence classes mod  $n$

**Example 4.**  $n = 2$ : (odds, evens) which is  $\{0_{\text{mod } 2}, 1_{\text{mod } 2}\}$

$$17_{\text{mod } 2} + 64_{\text{mod } 2} = 81_{\text{mod } 2} = 1_{\text{mod } 2}$$

**Example 5.**  $\mathbb{Z}/3\mathbb{Z} = \{0_{\text{mod } 3}, 1_{\text{mod } 3}, 2_{\text{mod } 3}\}$

**Example 6.**  $(2\mathbb{Z}, +)$  is a group (even numbers)

**Example 7.** If  $(G, \cdot_G)$  and  $(H, \cdot_H)$  are groups, then  $(G \times H, \cdot_{G \times H})$  is a group

- $(g_1, h_1) \cdot_{G \times H} (g_2, h_2) = (g_1 \cdot_G g_2, h_1 \cdot_H h_2)$
- Identity:  $1_{G \times H} = (1_G, 1_H)$
- Inverse of  $(g, h)$ :  $(g^{-1}, h^{-1})$

### 1.1.1 Properties

- $G$  has exactly 1 identity
- Each  $g \in G$ , there is exactly 1 inverse of  $g$  we write this  $g^{-1}$  (i.e.  $^{-1} : G \rightarrow G$ )
- $(g^{-1})^{-1} = g$
- $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
- $(a_1 \cdot a_2 \cdot \dots \cdot a_m)^{-1} = a_m^{-1} \cdot a_{m-1}^{-1} \cdot \dots \cdot a_1^{-1}$

*Proof.*

- Suppose  $a, b$  are both identities in  $G$ . Then  $a = a \cdot b = b$
- Suppose  $a, b$  are both inverses of  $g$ . i.e  $a \cdot g = g \cdot a = 1$  and  $b \cdot g = g \cdot b = 1$  Then  $b = 1 \cdot b = (a \cdot g) \cdot b = a \cdot (g \cdot b) = a \cdot 1 = a$

- know  $g \cdot g^{-1} = g^{-1} \cdot g = 1$  so  $(g^{-1})^{-1} = g$
- $(a \cdot b)^{-1}$  satisfies:  $x \cdot (a \cdot b) = (a \cdot b) \cdot x = 1$  we check  $b^{-1}a^{-1}$  does this
 
$$(b^{-1}a^{-1}) \cdot (a \cdot b) = b^{-1}(a^{-1} \cdot a)b = b^{-1} \cdot 1 \cdot b = b^{-1}b = 1$$

$$(ab)(b^{-1}a^{-1}) = a(b \cdot (b^{-1})) \cdot a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1$$

□

**Theorem 8.** In  $G$ , there is exactly 1 solution to the equation  $ax = b$  for a fixed  $a, b \in G$

**Corollary 9.** Cancellation laws:

$$ax = ay \implies x = y$$

$$xa = ya \implies x = y$$

*Proof.* If  $a \cdot x = b$

$$\begin{aligned} a^{-1} \cdot a \cdot x &= a^{-1} \cdot b \\ (a^{-1} \cdot a) \cdot x &= a^{-1} \cdot b \\ 1x &= x = a^{-1} \cdot b \end{aligned}$$

□

**Definition 10.** For  $x \in G$ , the order of  $x$ , written  $|x|$ , is the least  $n > 0$  so

$$x^n = \underbrace{x \cdot x \cdot \dots \cdot x}_n = 1_G$$

If there is no such  $n$ ,  $x$  has “infinite order”

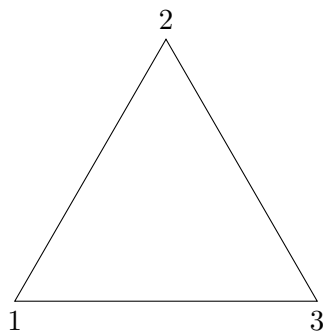
**Example 11.** In  $(\mathbb{R} \setminus \{0\}, \cdot)$ ,  $|5| = \infty$ ,  $|-1| = 2$ ,  $|1| = 1$

**Example 12.**  $(\mathbb{Z}/6\mathbb{Z}, +)$ ,  $|1_{\text{mod } 6}| = 6$ ,  $|2_{\text{mod } 6}| = 3$ ,  $|3_{\text{mod } 6}| = 2$ ,  $|4_{\text{mod } 6}| = 3$ ,  $|5_{\text{mod } 6}| = 2$

## 1.2 Dihedral Groups

### 1.2.1 Triangle

Look at the collection of symmetries of an equilateral Triangle



Rotation right

- $1 \rightarrow 2$
- $2 \rightarrow 3$
- $3 \rightarrow 1$

$r$

Rotation Left

- $1 \rightarrow 3$
- $2 \rightarrow 1$
- $3 \rightarrow 2$

$r^2$

Reflection around 2

- $1 \rightarrow 3$
- $2 \rightarrow 2$
- $3 \rightarrow 1$

$r^2 \circ s$

Reflection around 1

- $1 \rightarrow 1$
- $2 \rightarrow 3$
- $3 \rightarrow 2$

$s$

Reflection around 3

- $1 \rightarrow 2$
- $2 \rightarrow 1$
- $3 \rightarrow 3$

$r \circ s = s \circ r^2$

Identity

- $1 \rightarrow 1$
- $2 \rightarrow 2$
- $3 \rightarrow 3$

$r^3, s^2$

$$\begin{aligned}
 r^2 s &= r \cdot (r \cdot s) \\
 &= (r \cdot s) \cdot r^{-1} \\
 &= s \cdot (r^{-1} \cdot r^{-1}) \\
 &= s \cdot (r^{-1})^2
 \end{aligned}$$

(Symmetry of  $\triangle, \circ$ ) =  $D_6$

### 1.2.2 n-gon

Rotation right

$$\bullet k \rightarrow k + 1 \text{ (for } k < n)$$

$$\bullet n \rightarrow 1$$

$$r, |r| = n$$

Reflection around 1

$$\bullet k \rightarrow n + 2 - k$$

$$\bullet 1 \rightarrow 1$$

$$s, |r| = n$$

My Symmetry

$$\bullet 1 \rightarrow k$$

$$\bullet 2 \rightarrow k + 1$$

$$r^k$$

So,  $\{r, s\}$  generates the group of sym of regular n-gon

(Symmetry of a regular n-gon,  $\circ$ ) =  $D_{2n}$

### 1.2.3 Definition

Rules of dihedral group multiplication in  $D_{2n}$   $\{r, s\}$

$$\text{a) } r^n = 1$$

$$\text{b) } s^2 = 1$$

$$\text{c) } r \cdot s = s \cdot r^{-1}$$

When you have generators  $S$  for  $G$  and can list  $R_1, R_2, R_3$  all the rules you need to know to do multiplication in  $G$  Then  $\langle S, R_1, R_2, R_3 \rangle$  is a “presentation of the group  $G$ ”

$$D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, rs = sr^{-1} \rangle = \{1, r, \dots, r^{n-1}, s, rs, \dots, rs^{n-1}\}$$

Fact: There is a finite set of rule  $R_1, \dots, R_{2000}$  so  $\langle a, b \mid R_1, \dots, R_{2000} \rangle$  “undecidable word problem”

## 1.3 Symmetric Group

Given  $\Omega$  any set,  $S_\Omega$  = The permutations of  $\Omega$  = The bijections  $f : \Omega \rightarrow \Omega$

**Example 13.**  $\Omega = \{1, 2, 3\}$

$S_n = S_{\{1, 2, \dots, n\}}$  has  $n!$  elements

$$|S_3| = 6, |D_6| = 6, D_6 \subseteq S_3$$

$$|D_{2n}| = 2n$$

$$|S_n| = n!$$

### 1.3.1 Cycle Decomposition

$1 \rightarrow 4, 2 \rightarrow 1, 3 \rightarrow 2, 4 \rightarrow 3, 5 \rightarrow 5$  can be written as  $(1432)(5)$

$(a_1 \dots a_{m_1})(a_{m_1+1} \dots a_{m_2})$  with  $a_i$  is disjoint represents the function which satisfies

- $a_i$  to  $a_{i+1}$  unless  $i = m_j$  for some  $j$
- $a_{m_j}$  to  $a_{m_{j-1}+1}$   $j \neq 1$
- $a_{m_1}$  to  $a_1$

$$(1)(2)(3)(4)(5)(6)(7) = 1$$

$$(1442) \circ (3421) = (124)$$

$$|(123)(45)| = 6$$

Order of a product of disjoint cycles is the lcm(lengths of the cycles)

## 1.4 Homomorphisms and Isomorphisms

**Definition 14.** A homomorphism from  $(G, \cdot_G)$  to  $(H, \cdot_H)$  is a function  $f : G \rightarrow H$  such that

$$f(x \cdot_G y) = f(x) \cdot_H f(y)$$

for all  $x, y \in G$

- $f(x^{-1}) = f(x)^{-1}$

$$\begin{aligned} f(x) &= f(1_G \cdot_G x) \\ &= f(1_G) \cdot_H f(x) \\ f(x) \cdot_H (f(x))^{-1} &= f(1_G) \cdot_H f(x) \cdot_H (f(x))^{-1} \\ 1_H &= f(1_G) \end{aligned}$$

$$1_H = f(1_G) = f(x \cdot_G x^{-1}) = f(x) \cdot_H f(x^{-1})$$

$$1_H = f(1_G) = f(x^{-1} \cdot_G x) = f(x^{-1}) \cdot_H f(x)$$

**Definition 15.** If  $f$  is a bijection and a homomorphism, then  $f$  is an isomorphism

**Example 16.**  $\cdot id : G \rightarrow G$

$$\cdot^{-1} : G \rightarrow G, x \mapsto x^{-1}$$

$$(x \cdot y)^{-1} = (x^{-1}) \cdot (y^{-1})$$



is an isomorphism if and only if  $G$  is abelian

$$xyx^{-1}y^{-1} = 1$$

**Example 17.**  $e^x : (\mathbb{R}, +) \rightarrow (\mathbb{R}, \cdot), f(x + y) = f(x) \cdot f(y)$  is an isomorphism

**Example 18.**  $f : \mathbb{Z}/6\mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z}$

- $0 \rightarrow 0$
- $1 \rightarrow 1$
- $2 \rightarrow 2$
- $3 \rightarrow 0$
- $4 \rightarrow 1$
- $5 \rightarrow 2$

is a homomorphism NOT an isomorphism

**Definition 19.**  $G$  and  $H$  is isomorphic if there is a  $f : G \rightarrow H$  which is an isomorphism (written  $G \cong H$ )

If  $G \cong H$  then

- $G$  is a belian iff  $H$  is abelian

**Abelian:** For every  $x, y$   $x \cdot_G y = y \cdot_G x$

$$f(y) \cdot_H f(x) = f(y \cdot_G x) = f(x \cdot_G y) = f(x) \cdot_H f(y)$$

So, any 2 elements

If  $f$  is a  $\cong$ ,  $f : G \rightarrow H$  and  $x \in G$  has order 2 Then  $f(x) \in H$  has order 2

$$\begin{aligned} x^2 &= 1_G \\ (f(x))^2 &= f(x) \cdot f(x) = f(x \cdot x) = f(1_G) = 1_H \end{aligned}$$

**Recall**  $D_{2n} = \langle r, s \mid r^n = 1, s^2 = 1, rs = sr^{-1} \rangle$

If  $G = \langle g_1, \dots, g_n \mid R_1, R_2, \dots \rangle$  and  $h_1, \dots, h_n \in H$  so  $R_1(h_1 \dots h_n) \dots$  Then  $f : g_i \mapsto h_i$  is a homomorphism

## 1.5 Group Actions

**Definition 20.** A group action is a function

$$\alpha : G \times A \rightarrow A$$

so

$$\alpha(g, \alpha(h, a)) = \alpha(g \cdot h, a)$$

We write  $g \cdot a$  for  $\alpha(g, a)$

$$g \cdot (h \cdot a) = (g \cdot h) \cdot a$$

- $1_G \cdot a = a$  for any  $a \in A$

For any  $g \in G$  the function  $g \cdot : A \rightarrow A$ ,  $a \mapsto g \cdot a$  is a bijection of  $A$ .

$$\begin{aligned} (g \cdot (g^{-1} \cdot_G)) : A &\rightarrow A \\ &= (g \cdot g^{-1}) \cdot a \\ &= 1_G \cdot a = a \\ g^{-1}(g \cdot a) &= a \end{aligned}$$

Since this function has an inverse (as a function) it is bijective

**Recall:**  $S_A$  is the group of all permutations of  $A$

Get a function  $\sigma : G \rightarrow S_A$  and  $\sigma(g) =$  the function  $a \mapsto g \cdot a$

**Observation:**  $\sigma$  is a homomorphism

$$\sigma(g \cdot h) = \sigma(g) \cdot \sigma(h)$$

**Example 21.**  $(\mathbb{R}, +)$  acts on  $A = \{1, 2, 3\}$

$$g \cdot a = a$$

$$\sigma : \mathbb{R} \rightarrow S_3, g \mapsto 1_{S_3}$$

## 2 Subgroups

### 2.1 Definition and Examples

**Definition 22.** Let  $G$  be a group. The subset  $H$  of  $G$  is a subgroup of  $G$  if

- $1_G \in H$
- $\forall x, y \in H, x \cdot y \in H$
- $\forall x \in H, x^{-1} \in H$

We write  $H \leq G$  to indicate that  $H$  is a subgroup of  $G$ .

**Proposition 23.** A subset  $H$  of a group  $G$  is a subgroup of  $G$  if and only if

- $H \neq \emptyset$
- $\forall x, y \in H, xy^{-1} \in H$

### 2.2 Centralizers and Normalizers, Stabilizers and Kernels

**Definition 24** (Centralizer). Let  $G$  be a group and  $A$  be a subset of  $G$ . The centralizer of  $A$  in  $G$  is

$$C_G(A) = \{g \in G \mid gag^{-1} = a \text{ for all } a \in A\}$$

Moreover,  $C_G(A)$  is a subgroup of  $G$ .

**Definition 25** (Center). Let  $G$  be a group. The center of  $G$  is

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$$

**Definition 26** (Normalizer). Let  $G$  be a group and  $A$  be a subset of  $G$ . Let

$$gAg^{-1} = \{gag^{-1} \mid a \in A\}$$

The Normalizer of  $A$  in  $G$  is

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

**Definition 27** (Stabilizer). If  $G$  is a group acting on a set  $S$  and  $s$  is some fixed element of  $S$  the stabilizer of  $s$  is

$$G_s = \{g \in G \mid g \cdot s = s\}$$

## 2.3 Cyclic groups

**Definition 28.** A group  $H$  is a cyclic if  $H$  can be generated by a single element. i.e.,  $H = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$  for some  $x \in H$ .

**Proposition 29.** If  $H = \langle x \rangle$ , then  $|x| = n$ .

*Proof.* Let  $|x| = n$  then  $1, x, x^2, \dots, x^{n-1}$  are distinct

If  $x^a = x^b$  for  $0 \leq a < b < n$  then  $x^{b-a} = 1$  but  $b - a < n$  contradict  $\square$

**Proposition 30.** Let  $G$  be an arbitrary group,  $x \in G$  and let  $m, n \in \mathbb{Z}$ . If  $x^n = 1$  and  $x^m = 1$ , then  $x^d = 1$ , where  $d = (m, n)$ .

*Proof.* By the Euclidean Algorithm, there exists  $q, r \in \mathbb{Z}$  such that  $d = mr + ns$  where  $d = (m, n)$ . Thus

$$x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1$$

$\square$

**Theorem 31.** For any two cyclic groups of the same order are isomorphic.

*Proof.* Suppose  $\langle x \rangle$  and  $\langle y \rangle$  are both cyclic groups of order  $n$ . Let  $\varphi : \langle x \rangle \rightarrow \langle y \rangle$  be defined by  $\varphi(x^k) = y^k$

- $\varphi$  is well defined, if  $x^r = x^s$  then  $\varphi(x^r) = \varphi(x^s)$ . Because  $x^r = x^s$  then from proposition 30,  $n \mid r - s$ ,  $r = tn + s$  then

$$\begin{aligned} \varphi(x^r) &= \varphi(x^{tn+s}) \\ &= y^{tn+s} \\ &= (y^n)^t y^s \\ &= y^s \\ &= \varphi(x^s) \end{aligned}$$

- $\varphi$  is injective
- $\varphi$  is surjective

□

**Theorem 32.** If  $H_1, H_2$  is cyclic groups and  $|H_1| = |H_2|$  then  $H_1 \cong H_2$ .

**Proposition 33.** Let  $G$  be a group, let  $x \in G$  and let  $a \in \mathbb{Z} - \{0\}$ .

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

*Proof.*

1. Proof by contradiction, Suppose  $|x| = \infty$  and  $|x^a| = m < \infty$  then,  $1 = (x^a)^m = x^{am}$  and  $x^{-am} = (x^{am})^{-1} = 1^{-1} = 1$ . Since either  $am$  or  $-am$  is greater than 0, then it is contradicts  $|x| = \infty$
2. Since  $x^n = 1$  so  $(x^n)^{\frac{a}{(n,a)}} = (x^a)^{\frac{n}{(n,a)}}$  then  $|x^a| = \frac{n}{(n,a)}$ .
3. Just a special case of 2.

□

**Theorem 34.** If  $H = \langle x \rangle$  and  $|x| = n$  then  $x^a = 1$  if and only if  $n \mid a$ .

**Theorem 35.** If  $H = \langle x \rangle$  and  $K \leq H$ . Then  $K$  is cyclic

*Proof.* Let  $a$  be the least positive integer such that  $x^a \in K$ , let  $y = x^a$

Then we want to show  $\langle y \rangle = K$ .

- $\langle y \rangle \subseteq K$ : Obvious
- $\langle y \rangle \supseteq K$ : Given  $x^b \in K$  we can write  $b = am + r$  with  $0 \leq r < a$

$$\begin{aligned} x^b &= x^{am+r} = (x^a)^m x^r \\ &= y^m x^r \quad (x^r \in K) \\ x^r &= y^{-m} x^b \quad (y^{-m}, x^b \in K) \end{aligned}$$

So,  $x^r \in K$  so  $r = 0$ ,  $x^b = y^m$

Therefore  $\langle y \rangle = K$

□

## 3 Quotient Groups and Homomorphisms

### 3.1 Definition and Examples

**Definition 36.** If  $\varphi : G \rightarrow H$  is a homomorphism then  $\ker(\varphi) = \{x \in G \mid \varphi(x) = 1_H\}$

**Lemma 37.**  $\ker(\varphi) \leq G$

*Proof.* Proof each properties of subgroup

- Closed identity, Since  $\varphi(1_G) = 1_H$

$$\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G) \cdot \varphi(1_G) = 1_H$$

So,  $1_G \in \ker(\varphi)$

- Closed under inverses, if  $x \in \ker(\varphi)$

$$\begin{aligned}\varphi(x^{-1}) &= (\varphi(x))^{-1} = (1_H)^{-1} = 1_H \\ 1_H &= \varphi(1_G) = \varphi(x^{-1}x) = \varphi(x) \cdot \varphi(x^{-1})\end{aligned}$$

So,  $x^{-1} \in \ker(\varphi)$

- Closed under multiplication, if  $x, y \in \ker(\varphi)$

$$\begin{aligned}\varphi(xy) &= \varphi(x) \cdot \varphi(y) \\ &= 1_H \cdot 1_H = 1_H\end{aligned}$$

So,  $xy \in \ker(\varphi)$

□

**Definition 38.** Given  $\varphi : G \rightarrow H$  a homomorphism and  $K = \ker(\varphi)$  For any  $a \in H$ , let

$$X_a = \{x \in G \mid \varphi(x) = a\}$$

then

$$G/K = (\{X_a \mid a \in H\}, \circ)$$

where

$$X_a \circ X_b = X_{ab}$$

**Lemma 39.** If  $\varphi : G \rightarrow H$  is a homomorphism,  $K = \ker(\varphi)$ , and  $\varphi(b) = a$  then  $X_a = bK$  where  $bK = \{bz \mid z \in K\}$

*Proof.* The goal is to show  $X_a = bK$

- $X_a \supseteq bK$ , Given  $y \in bK, y = bz$  for some  $z \in K$

$$\varphi(y) = \varphi(b \cdot z) = \varphi(b) \cdot \varphi(z) = a \cdot 1_H = a$$

- $X_a \subseteq bK$ , Given  $\varphi(y) = a$

$$\varphi(b^{-1}y) = \varphi(b^{-1})\varphi(y) = (\varphi(b))^{-1} \cdot \varphi(y) = a^{-1} \cdot a = 1$$

Therefore  $X_a = bK$  □

**Definition 40.** For any  $N \leq G$  and for any  $g \in G$  let

$$gN = \{gn \mid n \in N\}$$

and

$$Ng = \{ng \mid n \in N\}$$

**Theorem 41.** Let  $G$  be a group and  $K$  be the kernel of some homomorphism. Then the set whose elements are the left cosets of  $K$  in  $G$  with operation defined by

$$uK \circ vK = (uv)K$$

forms a group  $G/K$ .

*Proof.* Let  $X, Y \in G/K$  and let  $Z = XY$  in  $G/K$ . Since  $K$  is the kernel of some homomorphism,  $\varphi : G \rightarrow H$ , so  $X = \varphi^{-1}(a)$  and  $Y = \varphi^{-1}(b)$  for some  $a, b \in H$ . By definition of the operation in  $G/K$ ,  $Z = \varphi^{-1}(ab)$ .

Let  $u, v$  be arbitrary representatives of  $X, Y$  ( $\varphi(u) = a, \varphi(v) = b$  and  $X = uK, Y = vK$ )

GOAL: show  $uv \in Z$

$$\begin{aligned} uv \in Z &\iff uv \in \varphi^{-1}(a, b) \\ &\iff \varphi(uv) = ab \\ &\iff \varphi(u)\varphi(v) = ab \end{aligned}$$

Therefore  $Z$  is the (left) coset  $(uv)K$ . □

**Proposition 42.** If  $N \leq G$  then for all  $u, v \in G, uN = vN$  if and only if  $v^{-1}u \in N$

*Proof.* Since  $N$  is a subgroup of  $G$ , since  $1_G \in N$  then

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

If  $x \in uN \cap vN$  then for some  $n_1, n_2 \in N$

$$\begin{aligned} x &= un_1 = vn_2 \\ v^{-1}u &= n_2n_1^{-1} \in N \end{aligned}$$

For any  $n \in N$

$$un = (vv^{-1})un = v(v^{-1}un) \in vN$$

So  $uN \subseteq vN$ , wlog,  $vN \subseteq uN$ . Therefore  $uN = vN$ .  $\square$

**Definition 43.** The element  $gng^{-1}$  is called the *conjugate* of  $n \in N$  by  $g$ . The set  $gNg^{-1}$  is called the *conjugate* of  $N$  by  $g$ . if  $gNg^{-1} = N$  then  $g$  is said to *normalize*  $N$ .

If  $N \leq G$  called *normal* if for any  $g \in G$  normalizes  $N$ . In another word,  $gNg^{-1} = N$  for all  $g \in G$ , written

$$N \trianglelefteq G$$

**Theorem 44.** For  $N \leq G$ , the following are equivalent

- $N \trianglelefteq G$
- $N_G(N) = G$
- $gN = Ng$  for all  $g \in G$
- $gNg^{-1} \subseteq N$  for all  $g \in G$

## 3.2 More on Cosets and Lagrange's Theorem

**Theorem 45** (Lagrange's Theorem). Let  $G$  be a finite group and  $H \leq G$ , then

$$|H| \mid |G|$$

and

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

is the number of  $H$ -cosets in  $G$ .

**Definition 46.** If  $H \leq G$ . then the “index of  $H$  in  $G$ ” is the number of left  $H$  cosets in  $G$



**Corollary 47.** If  $G$  is a finite group and  $x \in G$  then  $|x| \mid |G|$ , So,  $x^{|G|} = 1$

*Proof.* let  $H = \langle x \rangle \leq G$  So  $|x| \mid |G|$  Since for  $x^a = 1$  if and only if  $|x| \mid a$ , So  $x^{|G|} = 1$   $\square$

**Corollary 48.** If  $|G| = p$  is prime, then  $G \cong \mathbb{Z}/p\mathbb{Z}$

*Proof.* Take any  $x \in G \setminus \{1\}$ ,  $|x| \mid |G|$ , So,  $|x| = p$  Since  $\langle x \rangle = H \leq G$  and  $p = |x| = |H|$  therefore  $H = G$   $\square$

**Theorem 49.** For any  $n \in \mathbb{N}$  either  $p \mid n$  or  $p \mid n^{p-1} - 1$

**Theorem 50 (Sylow).** If  $G$  is finite of order  $p^\alpha \cdot m$  where  $p \nmid m$  where  $p$  is prime. Then  $G$  has a subgroup of size  $p^\alpha$ .

**Definition 51.** If  $H, K \leq G$  then

$$HK = \{hk \mid h \in H, k \in K\} = \bigcup_{h \in H} hK$$

**Lemma 52.** If  $cK$  intersects  $H$  then  $|cK \cap H| = |K \cap H|$

*Proof.* Let  $a \in cK \cap H$  let  $f : K \cap H \rightarrow cK \cap H$ ,  $x \mapsto ax$

Claim:  $x \in K \cap H \implies ax \in cK \cap H$   $ax \in H$  because  $a, x \in H \leq G$

$a = cl$  for some  $l \in K$  because  $a \in cK$   $ax = c \underbrace{(lx)}_{\in K} \in cK$  So,  $f$  is now injective

Claim: If  $y \in cK \cap H$  then  $a^{-1}y \in K \cap H$   $y \in cK$ ,  $y = cl$ ,  $a^{-1}y = (a^{-1}cl \in K$

$\square$

**Theorem 53.** If  $H, K$  are finite subgroups of  $G$  then

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

*Proof.*  $|HK| = \left| \bigcup_{h \in H} hK \right| = |K| \cdot \text{number of } K\text{-cosets of the form } hK \text{ for } h \in H$  Each  $h \in H$  define a coset  $hK$   $\square$

**Proposition 54.**  $HK \leq G$  if and only if  $HK = KH$

*Proof.*  $\Leftarrow$

- $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$

- 

$$\Rightarrow, H, K \leq HK, H = H \cdot 1 \subseteq HK, K = 1 \cdot K \subseteq HK$$

So,  $KH \subseteq HK$

Let  $y \in HK, y = hk, y^{-1} = k^{-1}h^{-1} \in KH$

So  $HK \subseteq KH$  □

**Theorem 55** (First Isomorphism Theorem). If  $\varphi : G \rightarrow H$  is a homomorphism then

- $\ker(\varphi) \trianglelefteq G$
- $G/\ker(\varphi) \cong \varphi(G)$

**Definition 56.**  $\varphi(G) = \text{im}(\varphi) = \{y \in H \mid \exists x \in G, \varphi(x) = y\}$

*Proof.* Build  $f : G \rightarrow G/\ker(\varphi), a \cdot K \mapsto \varphi(a)$  ( $K = \ker(\varphi)$ )

$$aK = bK \iff b^{-1}a \in K$$

If  $aK = bK$  want  $\varphi(a) = \varphi(b)$

$$\begin{aligned} \varphi(a) &= \varphi(b \cdot b^{-1}a) \\ &= \varphi(b) \cdot \varphi(b^{-1}a) \\ &= \varphi(b) \cdot 1 \\ &= \varphi(b) \end{aligned}$$

$$f(aK \cdot bK) = f(ab \cdot K) =$$

□

**Corollary 57.** Let  $\varphi : G \rightarrow H$  be a homomorphism

1.  $\varphi$  is 1-to-1 iff  $\ker(\varphi) = \{1_G\}$
2.  $|G/\ker(\varphi)| = |\varphi(G)|$

**Theorem 58** (2nd or “Diamond” isomorphism theorem). Given  $G$ , a group,  $A, B \leq G$  and  $A \leq N_G(B)$  (i.e.,  $aBa^{-1} = B$  for every  $a \in A$ ) then

- $AB \leq G$
- $B \trianglelefteq AB$
- $A \cap B \trianglelefteq A$
- $AB/B \cong A/(A \cap B)$

*Proof.*

- For  $B \trianglelefteq AB$ . For any  $a \in A, b \in B$

$$abB(ab)^{-1} = B$$

$$abB(ab)^{-1} = a(bBb^{-1})a^{-1} = aBa^{-1} = B$$

- For  $A \cap B \trianglelefteq A$

we want for any  $a \in A$ ,  $a(A \cap B)a^{-1} = A \cap B$

$$a(A \cap B)a^{-1} \subseteq aAa^{-1} = A$$

$$a(A \cap B)a^{-1} \subseteq aBa^{-1} = B$$

Given  $y \in A \cap B$ , for any  $a \in A$ , WANT  $y \in a(A \cap B)a^{-1}$

$$a^{-1}ya \in a^{-1}(A \cap B)a \subseteq A \cap B$$

$$y = a(a^{-1}ya)a^{-1} \in a(A \cap B)a^{-1}$$

Therefore  $a(A \cap B)a^{-1} = A \cap B$ , so  $A \cap B \trianglelefteq A$

- WANT  $\varphi : A \rightarrow AB/B$

$$x \in ab \cdot B = aB$$

$$x = ab \cdot b' \text{ (for some } b' \in B)$$

$$= a \cdot (bb') \text{ (for some } b' \in B)$$

$$\varphi(a) = aB$$

$$A \rightarrow AB \rightarrow AB/B$$

$$a \mapsto a \mapsto aB$$

$$\varphi(a \cdot a') = a \cdot a'B$$

$$\varphi(a) \cdot \varphi(a') = aB \cdot a'B = aa'B$$

$\varphi$  is onto. For any  $ab \in AB$

□

**Theorem 59** (The 3rd theorem). Given  $G$ , a group,  $H, K \trianglelefteq G$  with  $H \trianglelefteq K$  Then  $K/H \trianglelefteq G/H$  and  $(G/H)/(K/H) \cong (G/K)$