

# Introduction to Group Theory

Based on the lectures of Florian Naef  
David Lawton  
22337087

20th May 2024.

## Contents

<b>1</b>	<b>Lecture 1: Definitions &amp; Examples</b>	<b>2</b>
<b>2</b>	<b>Lecture 2: Integers Modulo <math>n</math> and the Quaternion Group</b>	<b>4</b>
2.1	Integers Modulo $n$ : $\mathbb{Z}/n\mathbb{Z}$ . . . . .	4
2.2	Quaternion Group . . . . .	5
<b>3</b>	<b>Lecture 3: Generators-Relations</b>	<b>6</b>
<b>4</b>	<b>Lecture 4: Symmetric Group</b>	<b>7</b>
<b>5</b>	<b>Lecture 5: The Category of Groups.</b>	<b>8</b>
<b>6</b>	<b>Lecture 6: Group Actions</b>	<b>10</b>
<b>7</b>	<b>Lecture 7: Subgroups</b>	<b>12</b>
<b>8</b>	<b>Lecture 8: Cyclic Groups and Subgroups.</b>	<b>13</b>
8.1	Cyclic Groups . . . . .	13
8.2	Subgroups of Cyclic Groups . . . . .	15
<b>9</b>	<b>Lecture 9: Euclidean Algorithm</b>	<b>16</b>
<b>10</b>	<b>Lecture 10: Subgroups of Finite Cyclic Groups</b>	<b>18</b>

# 1 Lecture 1: Definitions & Examples

**Definition 1.1.** A **group** is pair  $(G, m)$  such that  $G$  is a **set** and  $m : G \times G \rightarrow G$  is a mapping from  $G$  to itself s.t.

- $G$  is associative under  $m$ , ie.  $m(a, (b, c)) = m((a, b), c) \forall a, b, c \in G$ .
- $G$  has a unit, ie.  $\exists e \in G$  s.t.  $m(e, g) = m(g, e) = g \forall g \in G$ .
- Each element of  $G$  has an inverse, ie.  $\forall a \in G, \exists b \in G$  s.t.  $m(a, b) = m(b, a) = e$ .

---

*Remark.* We usually write  $m(a, b)$  as  $a * b$ ,  $a \cdot b$ , or  $ab$ . Associativity becomes  $a(bc) = (ab)c$ . We also write the inverse of element  $a$  as  $a^{-1}$ .

The notation  $(G, m)$  is rewritten simply as  $G$  for convenience.

*Example.*

1.  $G = \{e\}$  (Trivial group)
  2.  $(\mathbb{Z}, +)$ ,  $e = 0$ ,  $a^{-1} = -a$  (Integers under addition)
  3.  $(\mathbb{Q}, +)$  (Rational numbers under addition)<sup>1</sup>
  4.  $(\mathbb{Q}^x = \mathbb{Q} \setminus \{0\}, *)$ ,  $e = 1$ ,  $a^{-1} = \frac{1}{a}$
  5.  $GL(n, \mathbb{R}) = \{n \times n \text{ matrix } A \text{ with entries in } \mathbb{R} | \det A \neq 0\}$ ,  $e = \mathbb{I}$ ,  $A^{-1} = A^{-1}$  (General linear group)
  6.  $S(X) = \{f : X \times X \rightarrow X | f \text{ bijective}\}$ ,  $e = Id_X$ ,  $f^{-1} = f^{-1}$
- 

**Definition 1.2.** A group is **abelian** if all elements of the set are commutative under the mapping, ie. for group  $G = (G, m)$ ,  $ab = ba \forall a, b \in G$ .<sup>2</sup> Note:  $a * b$  often written as  $a + b$  for abelian groups.

**Proposition 1.1.** For any group the following is true.

1. The unit is unique
2. For each  $a \in G$ ,  $a^{-1}$  is uniquely determined.
3.  $(a^{-1})^{-1} = a$
4.  $(ab)^{-1} = b^{-1}a^{-1}$
5. For any  $a_1, \dots, a_n$ , the value of  $a_1 \cdot \dots \cdot a_n$  is independent of bracketing.

*Proof.* Each numbered proof correspond to the respective number in the proposition.

1. Suppose  $e, e'$  are both units of group  $G$ . Then  $e = e'e = e'$ .  $\square$
2. Given  $a \in G$ , suppose  $\exists b_1, b_2 \in G$  s.t. they both satisfy the conditions of the inverse of  $a$ . Then  $b_1 = b_1e = b_1(ab_2) = (b_1a)b_2 = eb_2 = b_2$ .  $\square$

---

<sup>1</sup>For any field  $F$ ,  $(F, +)$  and  $(F \setminus \{0\}, *)$  are groups.

<sup>2</sup>1, 2, 3 abelian. 4, 5 generally non-abelian ( $n \geq 2$  in 4,  $|X| \geq 3$  in 5.)

3. Let  $b = (a^{-1})^{-1}$ , therefore  $ba^{-1} = e = a^{-1}b$ .  $a$  satisfies this, and since the inverse is uniquely determined,  $a = b = (a^{-1})^{-1}$ .
4.  $ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e$ . Similar for  $(b^{-1}a^{-1})ab$ . Therefore  $b^{-1}a^{-1}$  satisfies the conditions of the inverse of  $ab$ , and is therefore equal to  $(ab)^{-1}$  since the inverse is uniquely determined.
5. Proof by induction. Let  $f(a_1, \dots, a_n)$  be a bracketing of  $a_1, \dots, a_n$ . Define  $f(a_1, \dots, a_n) = (a_1(\dots(a_{n-1}a_n)\dots)) := m_n(a_1, \dots, a_n)$ .

Induction on  $n$ :

$n = 1, 2$ :  $m(a_1) = a_1$ ,  $m_2(a_1, a_2) = m(a_1, a_2)$ .

$n \geq 3$ :  $f = m(f_1(a_1, \dots, a_k), f_2(a_{k+1}, \dots, a_n))$ .

By ind. hyp.  $f_1 = m_k$ ,  $f_2 = m_{n-k}$ .

It remains to show that  $m(m_k, m_{n-k}) = m_n \forall k$ .

$$k = 1 : m(a_1, m_{n-1}(a_2, \dots, a_n)) = m_n(a_1, \dots, a_n).$$

$$\begin{aligned} k > 1 : m(m_k(a_1, \dots, a_k), m_{n-k}(a_{k+1}, \dots, a_n)) &= m(m(a_1, m_{k-1}(a_2, \dots, a_k)), m_{n-k}(a_{k+1}, \dots, a_n)). \\ &= m(a_1, m(m_{k-1}(a_2, \dots, a_k), m_{n-k}(a_{k+1}, \dots, a_n))) \text{ by associativity.} \\ &= m(a_1, m_{n-1}(a_2, \dots, a_n)) = m_n(a_1, \dots, a_n) \end{aligned}$$

□

---

*Remark.* Either of left or right inverse, uniquely characterise  $a^{-1}$ .

---

**Proposition 1.2.** *Left and right cancellation hold in any group.*

$$ax = ay \therefore x = y \tag{1}$$

$$xa = ya \therefore x = y \tag{2}$$

*Proof.* Multiply by  $a^{-1}$  from left, right respectively.

□

---

*Remark.* Let  $(G, m)$ ,  $m : G \times G \rightarrow G$  satisfy:

- $m(a, m(b, c)) = m(m(a, b), c)$  (Associativity)
- $\exists e \in G$  s.t.  $m(e, g) = g, \forall g \in G$ . (Left-unit)
- $\forall a \in G, \exists b \in G$  s.t.  $m(b, a) = e$ . (Left-inverse)

then  $(G, m)$  is a group.

*Notation.*

$$x^n = x \cdot (x, n - 2 \text{ times}) \cdot x, \quad x^{-n} = x^{-1} \cdot (x^{-1}, n - 2 \text{ times}) \cdot x^{-1} \tag{3}$$

$$n \cdot x = x + x + x + \dots + x, \quad -n \cdot x = (-x) + (-x) + (-x) + \dots + (-x) \text{ (For abelian)} \tag{4}$$

---

**Definition 1.3.** The **order** of  $x \in G$  is the smallest  $n \in \mathbb{Z}^+$  s.t.  $x^n = e$ . The order is denoted  $|x| = n$ .

---

*Example.* •  $G = \mathbb{C}^\times, x = i, |x| = 4$ .

$$\bullet G = \text{GL}(2, \mathbb{R}), x = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, |x| = 6$$

## 2 Lecture 2: Integers Modulo n and the Quaternion Group

### 2.1 Integers Modulo n: $\mathbb{Z}/n\mathbb{Z}$

**Definition 2.1.** Let  $a, b \in \mathbb{Z}$ . We say  $a, b$  have the same residue mod  $n$ , and write  $a \equiv b \pmod{n}$  if  $\exists k \in \mathbb{Z}$  s.t.  $a - b = k \cdot n$ .

Given  $a \in \mathbb{Z}$  denote by

$$\begin{aligned}\bar{a} &= \{b \in \mathbb{Z} | b \equiv a \pmod{n}\} \\ &= \{a + kn \in \mathbb{Z} | k \in \mathbb{Z}\} \subseteq \mathbb{Z}\end{aligned}$$

and define

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{a} \subseteq \mathbb{Z} | a \in \mathbb{Z}\} \quad (5)$$

**Lemma 2.1.** •  $a \equiv b \pmod{n} \Leftrightarrow \bar{a} = \bar{b}$

$$\bullet \mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

*Proof.*

$$\begin{aligned}a \equiv b \pmod{n} &\Rightarrow a = b + k \cdot n \\ &\Rightarrow b = a - k \cdot n = a + l \cdot n, \quad l \in \mathbb{Z} \\ &\Rightarrow b \equiv a \pmod{n}\end{aligned}$$

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} &= \{\bar{a} \subseteq \mathbb{Z} | a \in \mathbb{Z}\}, \quad \bar{a} = \{a + kn \in \mathbb{Z} | k \in \mathbb{Z}\} \\ &\Rightarrow \forall a < n, \quad \bar{a} = \{a + kn \in \mathbb{Z} | k \in \mathbb{Z}\}, \\ &\quad \forall a \geq n, \quad \bar{a} = \{n + b + kn \in \mathbb{Z} | k \in \mathbb{Z}, a = n + b\} \\ &\quad = \{b + (k+1)n | k \in \mathbb{Z}\} = \bar{b}\end{aligned}$$

$$\begin{aligned}&\Rightarrow \forall a \geq n, \quad \bar{a} = \overline{a-n} \\ &\Rightarrow \mathbb{Z}/n\mathbb{Z} = \{\bar{a} \subseteq \mathbb{Z} | a \in \mathbb{Z}, a < n\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}\end{aligned}$$

□

**Proposition 2.2.** The assignment  $m(\bar{a}, \bar{b}) = \overline{a+b}$  is well defined, and  $(\mathbb{Z}/n\mathbb{Z}, m)$  is an abelian group.

*Proof.* Let  $\bar{a}_1 = \bar{a}_2, \bar{b}_1 = \bar{b}_2$ , this implies that  $a_1 \equiv a_2 \pmod{n}, b_1 \equiv b_2 \pmod{n}$ . It is then necessary that  $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ . Thus  $\overline{a_1 + b_1} = \overline{a_2 + b_2}$ , and so  $m$  is well defined.

It remains to show that  $(\mathbb{Z}/n\mathbb{Z}, m)$  is a group. Therefore we must show that it is associative, and contains a left-unit, and left-inverse.

Let  $G = (\mathbb{Z}/n\mathbb{Z}, m)$ . For  $a, b, c \in G$ ,

$$\begin{aligned}m(a, b) &= a + b, \quad m(b, c) = b + c \\ &\Rightarrow m(a, m(b, c)) = a + b + c = m(m(a, b), c),\end{aligned}$$

therefore  $G$  is associative.

To show the existence of the left-unit, we must show there exists  $e \in G$  s.t.  $e + g = g \quad \forall g \in G$ . For  $m(\bar{a}, \bar{b}) = \overline{a+b} = \bar{b}$ , where  $\bar{a}, \bar{b} \in G$ , it is clear from this that  $a = k \cdot n$  for some  $k \in \mathbb{Z}$ . Therefore  $a \equiv 0 \pmod{n}$ . This implies that  $\bar{a} = \bar{0}$ . Therefore  $\bar{0}$  is the left-unit of  $G$  (and consequently right-unit as abelian).

To show the existence of the left-inverse, we must show that  $\forall a \in G, \exists b \in G$  s.t.  $m(a, b) = e$ . If

$m(\bar{a}', \bar{b}') = \bar{0}$ , then  $a' = -b' \pmod{n}$ . Therefore,  $a' = n - b' \pmod{n}$ , which implies that  $\bar{a} = \overline{n - b'}$ . Hence,  $\forall \bar{g} \in G, \bar{g}^{-1} = \overline{n - g}$ .

$G = (\mathbb{Z}/n\mathbb{Z}, m)$  then satisfies all the required conditions of a group. To show that  $G$  is abelian, one must only note that  $a + b = b + a \forall a, b \in \mathbb{Z}$  which implies that  $\overline{a + b} = \overline{b + a}$ , and consequently  $m(\bar{a}, \bar{b}) = m(\bar{b}, \bar{a}) \forall \bar{a}, \bar{b} \in G$ .

□

*Notation.* We write  $a = \bar{a}$ , for example, in  $\mathbb{Z}/5\mathbb{Z}$ , we write  $2 + 3 = 0$ .

**Lemma 2.3.**  $1 \in \mathbb{Z}/n\mathbb{Z}$  has order  $n$ .

*Proof.*

$$n \cdot 1 = n = 0$$

$$k \cdot 1 = k \neq 0, \text{ for } 0 < k < n$$

□

## 2.2 Quaternion Group

Let  $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ , with  $m : Q_8 \times Q_8 \rightarrow Q_8$  given by:

$$i^2 = j^2 = k^2 = -1$$

$$ij = k, ki = j, jk = i$$

$$ji = -k, ik = -j, kj = -i$$

where signs manipulate as expected.

**Proposition 2.4.**  $(Q_8, m)$  is a group.

*Proof.* Simple to show associativity, left-unit, left-inverse. Not done here.

□

### 3 Lecture 3: Generators-Relations

Given a set  $r_1, r_2, r_3, \dots, r_l$  of words (relations) in  $g_1^\pm, g_2^\pm, \dots, g_k^\pm$  (generators). We can define a group

$$G = \langle g_1, \dots, g_k | r_1, \dots, r_l \rangle \quad (6)$$

This is called the presentation of a group. We will define the group more precisely later.

Elements of  $G$  are words (combinations) of  $g_1^\pm, g_2^\pm, \dots, g_l^\pm$  under the equivalence relation given by

- removing/adding  $g_i g_i^{-1}, g_i^{-1} g_i, e$ ,
- replacing an occurrence of  $r_i$  with  $e$ .

*Example.* Dihedral Group

$$D_{2n} = \langle r, s | r^n = s^2 = (sr)^2 = e \rangle \quad (7)$$

Let  $w$  try to enumerate all the elements of  $D_{2n}$ : If  $f$  is any word in  $r^\pm, s^\pm$ , use  $r^{-1} = r^{n-1}$  and  $s^{-1} = s$  to get a word in  $r, s$ . Since  $s^2 = e$ , we can assume

$$f = r^{i_1} s r^{i_2} s \dots s r^{i_l}, \quad i_j > 0 \quad (8)$$

and then use  $sr = (sr)^{-1} = r^{-1} s^{-1} = r^{n-1} s$  to move the terms around and reach the form  $f = sr^i$  or  $f = r^i$ .

$$\Rightarrow D_{2n} = \{e, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\} \quad (9)$$

These elements are not necessarily distinct.

$D_{2n}$  is the group of symmetries on a regular  $n$ -gon.  $D_{2n}$  can be realised as

$$r = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}, \quad \theta = \frac{2\pi}{n}, \quad s = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \quad (10)$$

*Remark.*

- $G = \langle \text{gen.} | \text{rel.} \rangle$  is always a group.
- Generally, it is difficult to decide for  $x \in G$ , if  $x = e$ .

## 4 Lecture 4: Symmetric Group

The symmetric group is the group of bijective maps from a set of  $n$  elements to the its These map between permutations of these  $n$  elements.

$$S_n = \{\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\} | \sigma \text{ bij.}\} \quad (11)$$

Each element of  $S_n$  can be written in the form of the permutation it maps the original set to, ie.  $(\sigma(1), \dots, \sigma(n))$ .

$$\sigma = (2 \ 1 \ 3) \in S_3 \text{ or } \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \in S_3. \quad (12)$$

as well as this these maps can be decomposed into cycles. For example,

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} \in S_5 \\ 1 &\rightarrow 3 \rightarrow 5 \rightarrow 1, \ 2 \rightarrow 4 \rightarrow 2 \\ \Rightarrow \sigma &= (1 \ 3 \ 5) (2 \ 4) \end{aligned}$$

this is called cycle decomposition.

**Definition 4.1.** Given  $a_1, a_2, \dots, a_l \in \{1, \dots, n\}$ , all distinct, we define an ‘**l-cycle**’:  $S_n \ni \sigma := (a_1 \ \dots \ a_l)^3$  by the formula

$$\sigma(x) = \begin{cases} a_{j+1} & , \text{ if } x = a_j \\ x & , \text{ else} \end{cases} \quad (13)$$

**Lemma 4.1.** Let  $\sigma = (a_1 \ a_2 \ \dots \ a_l)$  and  $\tau = (b_1 \ b_2 \ \dots \ b_k)$  be such that  $\{a_1, a_2, \dots, a_l\} \cap \{b_1, b_2, \dots, b_k\} = \emptyset$ . Then  $\sigma \cdot \tau = \tau \cdot \sigma$ .

*Proof.* Since the two sets,  $A = \{a_1, a_2, \dots, a_l\}, B = \{b_1, b_2, \dots, b_k\}$  are disjoint,  $\sigma(b_i) = b_i, \tau(a_i) = a_i$  and  $\sigma(x) = \tau(x) = x \ \forall x$  not in  $A, B$ . Therefore it follows that  $\sigma \cdot \tau(b_i) = \tau \cdot \sigma(b_i) = b_{i+1}, \sigma \cdot \tau(a_i) = \tau \cdot \sigma(a_i) = a_{i+1}$ , and  $\sigma \cdot \tau(x) = \tau \cdot \sigma(x) = x \ \forall x$  not in  $A, B$ . Therefore  $\forall g \in \{1, \dots, n\}, \tau \cdot \sigma = \sigma \cdot \tau$ . □

**Proposition 4.2.** Every  $\sigma \in S_n$  admits a decomposition into disjoint cycles.

*Proof.* For some  $\sigma \in S_n$ , and  $i \in \{1, \dots, n\}$  be s.t.  $i = \min\{j \in \{1, \dots, n\} | \sigma(j) \neq j\}$ . For some  $l_1, l_2$ , we have  $\sigma^{l_1}(i) = \sigma^{l_2}(i)$ . Therefore,  $\sigma^{l_1-l_2}(i) = i$ , and w.l.o.g.  $l = l_1 - l_2 > 0$ . Set  $\sigma = (i \ f(i) \ \dots \ f^{l-1}(i))$ .

The proof is continued by replacing  $\sigma$  with  $\sigma_1^{-1} \cdot \sigma$ , and  $i = \min\{j \in \{1, \dots, n\} | \sigma(j) \neq j\}$  with  $i = \min\{j \in \{1, \dots, n\} | \sigma_1^{-1} \cdot \sigma(j) \neq j\}$  and repeating. □

---

*Remark.* Not every product of cycles is a cycles decomposition. ie. If the cycles are not disjoint.

---

---


$$^3(a_1 \ a_2 \ \dots \ a_l) = (a_2 \ \dots \ a_l \ a_1)$$

## 5 Lecture 5: The Category of Groups.

Consider  $G = \{e, a, b, c\}$  with multiplication.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

(14)

Note that if we assign  $a = 2, b = 1, c = 3$  this 'is' (isomorphic to, this will be defined later)  $\mathbb{Z}/4\mathbb{Z}$ .

**Definition 5.1.** Let  $G, H$  be groups. A group **homomorphism** is a map  $\varphi : G \rightarrow H$  s.t.

$$\varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b) \quad (15)$$

( $\cdot_G, \cdot_H$  denote the binary maps of  $G, H$  respectively.)

**Definition 5.2.** If group homomorphism  $\varphi$  is a bijection, then it is called a **group isomorphism**. In this case  $G, H$  are **isomorphic**.

**Proposition 5.1.** Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then

1.  $\varphi(e_G) = e_H$
2.  $\varphi(a^{-1}) = \varphi(a)^{-1}$

*Proof.* From the definition of a group homomorphism:

$$\begin{aligned} \varphi(e_G \cdot_G b) &= \varphi(e_G) \cdot_H \varphi(b) \\ &= \varphi(b) \end{aligned}$$

This implies

$$\varphi(b) = \varphi(e_G) \cdot_H \varphi(b)$$

which can only be true if

$$\varphi(e_G) = e_H \quad (16)$$

proving the first condition. The second condition begins in a similar way, from the definition of a group homomorphism we know

$$\varphi(a \cdot_G a^{-1}) = \varphi(a) \cdot_H \varphi(a^{-1})$$

but

$$\begin{aligned} \varphi(a \cdot_G a^{-1}) &= \varphi(e_G) = e_H \\ \Rightarrow \varphi(a) \cdot_H \varphi(a^{-1}) &= e_H \\ \Rightarrow \varphi(a^{-1}) &= \varphi(a)^{-1} \end{aligned}$$

□

**Definition 5.3.**  $|G|$  is called the **order** of  $G$ . This is defined as the number of elements in the group for a finite group (group in which the underlying set is finite) or infinity for a non-finite group.



**Proposition 5.2.** *Let  $G$  be a group of order 2. Then  $G \cong \mathbb{Z}/2\mathbb{Z}$  (Isomorphic)*

*Proof.*  $G$  group  $\Rightarrow \exists e \in G$ , and  $a \in G$  s.t  $a \neq e$ . Define map  $\varphi : \mathbb{Z}/n\mathbb{Z} \rightarrow G$ .

$$0 \mapsto e$$

$$1 \mapsto a$$

We must then check that  $\varphi(x + y) = \varphi(x)\varphi(y) \forall x, y \in \mathbb{Z}/n\mathbb{Z}$ :

$x$	$y$	
0	0	Trivially true
1	1	$\varphi(1 + 1) = \varphi(0) = e$ $\varphi(1)\varphi(1) = a^2$ Only true if $a^2 = e$ , which must be true since $a^2 = a$ implies $a = e$ .
0	1	True since $\varphi(1) = a, e\varphi(1) = a$
1	0	True since $\varphi(1) = a, e\varphi(1) = a$

□

**Proposition 5.3.**

1. Let  $f : H \rightarrow K, g : G \rightarrow H$  be group homomorphisms, then so is  $f \circ g$ .
2. Let  $f : H \rightarrow K$  be a group isomorphism, then so is  $f^{-1}$ .

*Proof.*

1.  $(f \circ g)(ab) = f(g(ab)) = f(g(a)g(b)) = f(g(a))f(g(b)) = (f \circ g)(a)(f \circ g)(b)$   
Therefore  $f \circ g$  satisfies the condition of a group homomorphism.
2.  $f(f^{-1}(ab)) = ab = f(f^{-1}(a))f(f^{-1}(b))$ , then since  $f$  is injective,  $f(p) = f(q)$  implies  $p = q$ . Therefore  $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$ , and  $f^{-1}$  is then a group homomorphism.

□

## 6 Lecture 6: Group Actions

**Definition 6.1.** A **group action** of a group  $G$  on a set  $X$  is a map  $G \times X \rightarrow X$  written as  $(g, x) \mapsto g.x$  s.t.

- $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$
- $e \cdot x = x$

We sometimes write  $G \curvearrowright X$ .

A map of sets  $G \times X \rightarrow X$  can be equivalently given by

$$\begin{aligned} G &\rightarrow^\rho \{f : X \rightarrow X\} \\ g &\mapsto \rho(g) \end{aligned}$$

where  $\rho(g)(x) = g \cdot x$ .

**Proposition 6.1.** A map  $G \times X \rightarrow X$  defines a group action iff<sup>4</sup> the corresponding map  $G \rightarrow^\rho \{f : X \rightarrow X\}$  is s.t.  $\rho(g) \in S_X \ \forall \ g \in G$  and  $\rho : G \rightarrow S_X$  is a group homomorphism.<sup>5</sup>

*Proof.*

$$\begin{aligned} \rho(g_1)(\rho(g_2)(x)) = \rho(g_1 g_2)(x) &\Leftrightarrow \rho(g_1) \circ \rho(g_2) = \rho(g_1 g_2) \\ &\Leftrightarrow \rho(e) = \text{id}_X \end{aligned}$$

$$\begin{aligned} \text{"} \Rightarrow \text{"} : \rho(g) \circ \rho(g^{-1}) = \rho(gg^{-1}) = \rho(e) = \text{id}_X &\Rightarrow \rho(g) \text{ surj.}^6 \\ \rho(g^{-1}) \circ \rho(g) = \rho(g^{-1}g) = \text{id}_X &\Rightarrow \rho(g) \text{ inj.}^7 \end{aligned}$$

This implies that  $\rho(g) \in S_X$ , as the requirement is that the map is bijective. Since the first line, at the start of the proof, is true for any for any group action, this implies that  $\rho : G \rightarrow S_X$  is a group homomorphism. Then, since all steps taken are reversible, the same process can be taken in reverse to show the bijectivity of  $\rho(g)$ , and  $\rho$  being a group homomorphism, implies that the map  $G \times X \rightarrow X$  is a group action, proving “ $\Leftarrow$ ”.

□

*Example.*

1. Trivial action: For any  $X$ , we define  $G \times X \rightarrow X$  s.t.  $(g, x) \mapsto x$ .

2. Defining action of  $S_X$  on  $X$ :  $S_X \times X \rightarrow X$ ,  $(\sigma, x) \mapsto \sigma(x)$ .

We can claim that the map  $\rho$  from above is in this scenario  $\text{id} : S_X \rightarrow S_X$ .

3.  $G$  acting on itself by

$\rho_l : G \times G \rightarrow G$	$(g, x) \mapsto gx$	Called <b>left regular action</b> .
$\rho_r : G \times G \rightarrow G$	$(g, x) \mapsto xg^{-1}$	Called <b>right regular action</b> .
$\rho_{\text{adj.}} : G \times G \rightarrow G$	$(g, x) \mapsto gxg^{-1}$	Called <b>adjoint action</b> .

<sup>4</sup>If and only if

<sup>5</sup> $S_X$  is the symmetric group on set  $X$

<sup>7</sup>Maps are surjective if and only if a right inverse exists for each element. Maps are injective if and only if a left inverse exists for each element.

action:

$\rho_l :$

We can let the map corresponding to  $\rho_l, \phi : G \rightarrow \{f : X \rightarrow X\}$  be s.t.  $\phi(g)(x) = gx$ .

Then  $\phi(g_1)(\phi(g_2)(x)) = \phi(g_1)(g_2x) = g_1g_2x = \phi(g_1g_2)(x)$ .

$\Rightarrow \phi(g_1) \circ \phi(g_2) = \phi(g_1g_2), \phi(e) = e$

As in the above proof, this implies both left and right inverses therefore  $\rho_l \in S_X$

$\rho_r :$

Analagous to  $\rho_l$

$\rho_{adj} :$

Similar to  $\rho_l$ , define  $\phi(g)(x) = gxg^{-1}$ . Then  $\phi(g_1)(\phi(g_2)(x)) = \phi(g_1)(g_2xg_2^{-1})$

$= g_1g_2xg_2^{-1}g_1^{-1} = (g_1g_2)x(g_1g_2)^{-1} = \phi(g_1g_2)(x)$ .

$\Rightarrow \phi(g_1) \circ \phi(g_2) = \phi(g_1g_2), \phi(e) = e$

Same conclusion can be drawn as in the case of  $\rho_l$ .

4.  $D_{2n} \times \{1, \dots, n\} \rightarrow \{1, \dots, n\} :$

$$(r^i, j) \mapsto i + j \bmod n$$

$$(r^i s, j) \mapsto i - j \bmod n$$

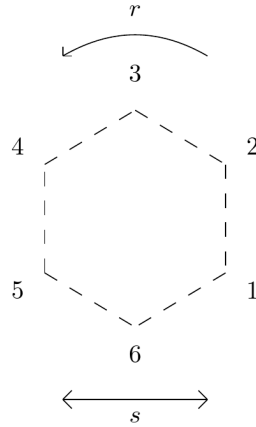


Figure 1: Illustration of the action of the  $D_{12}$  group on the set  $\{1, \dots, n\}$ . The element  $s$  of  $D_{2n}$  reflects across the vertical, and the element  $r$  rotates by  $\frac{2\pi}{n}$  in the anti-clockwise direction.

## 7 Lecture 7: Subgroups

**Definition 7.1.** A subset  $H \leq G$  of a group  $(G, m)$  is a **subgroup** if the restriction of  $m$  to  $H \times H$  turns  $H$  into a group. We write  $H \leq G$  in that case.

---

*Remark.* To specify,  $H$  is required to have contain the unit, inverses and be associative, it is also required to have closure under  $m$ . That is to say  $\forall a, b \in H, m(a, b) \in H$ .

---

**Proposition 7.1.**  $H \subseteq G$  is a subgroup iff

- $H$  is non-empty.
- if  $a, b \in H$ ,  $ab^{-1} \in H$ .

*Proof.*

" $\Rightarrow$ " :  $H \leq G \Rightarrow \exists e \in H$  s.t.  $ea = a \forall a \in H$ .  
 $\therefore H$  non-empty.  
 $H \leq G \Rightarrow \forall b \in H, \exists c \in H$  s.t.  $bc = e$  ( $c = b^{-1}$ )  
 $\therefore \forall a, b \in H, m(a, b^{-1}) = ab^{-1} \in H$  due to closure under  $m$

" $\Leftarrow$ " : As a subset of  $G$ , associativity implied.  
 $H$  non-empty  $\therefore \exists h \in H$ . Second condition implies  $aa^{-1} \in H \Rightarrow e \in H$ . (unit exists)  
w.l.o.g. we can impose that the subset  $H$  is not the trivial group, ie.  $H \neq (\{h = e\}, m)$ ,  
 $\Rightarrow \exists h \in H$  s.t.  $h \neq e \Rightarrow eh^{-1} = h^{-1} \in H$ . (inverses exist)  
for any 2 elements  $a, b \in H, ab^{-1} \in H$  and  $b^{-1} \Rightarrow a, b^{-1} \in H$  so  $ab \in H$ . (closure)  
 $\therefore H \leq G$ .

□

---

*Example.*

1. Every group  $G$  has a trivial subgroup,  $(\{e\}, m) \leq G$ , and an improper subgroup,  $G \leq G$ .
2.  $n\mathbb{Z} = \{nk | k \in \mathbb{Z}\} \subseteq \mathbb{Z}$  is a subgroup of  $(\mathbb{Z}, +)$ .
3. Given  $x \in G$ ,  $\langle x \rangle = \{x^n | n \in \mathbb{Z}\} \subseteq G$  is the subgroup of  $G$  generated by  $x$ .
4. Let  $G \times X \rightarrow X$  be a group action, and  $s \in X$ . The **stabilizer of  $s$** ,  $G_s := \{g \in G | g \cdot s = s\}$ , forms a subgroup of  $G$ .
5. Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then
  - $\ker \varphi := \{g \in G | \varphi(g) = e\}$
  - $\text{im } \varphi := \varphi(G) = \{\varphi(g) \in H | g \in G\}$
are both subgroups, of  $G$  and  $H$  respectively.

## 8 Lecture 8: Cyclic Groups and Subgroups.

### 8.1 Cyclic Groups

**Definition 8.1.** A group  $H$  is **cyclic** if it can be generated by a single element. That is to say  $\exists x \in H$  s.t.  $H = \langle x \rangle = \{x^n | n \in \mathbb{Z}\}$ .

**Proposition 8.1.** If  $H = \langle x \rangle$ , then  $|H| = |x|$ <sup>8</sup>. Also

1. if  $|H| = n < \infty$ , then the elements  $e, x, x^2, \dots, x^{n-1}$  are all distinct and  $H = \{e, x, \dots, x^{n-1}\}$ .
2. if  $|H| = \infty$  then  $H = \{\dots, x^{-2}, x^{-1}, e, x, x^2, \dots\}$  and  $x^a \neq x^b$  if  $a \neq b$ .

*Proof.*

$$|x| = n :$$

We first show  $H = \langle x \rangle \subseteq \{e, x, \dots, x^{n-1}\}$ .

Let  $x^m \in H$ ,  $m = kn + r$ ,  $0 \leq r \leq n - 1$

$$x^m = x^{kn+r} = x^n \cdot x^n \cdot \dots \cdot x^n \cdot x^r = e \cdot x^r = x^r$$

$$\Rightarrow H = \langle x \rangle = \{x^r | 0 \leq r \leq n - 1\} = \{e, x, \dots, x^{n-1}\}.$$

To show  $x^i \neq x^j \forall i, j$  s.t.  $0 \leq i, j \leq n - 1$ ,

assume  $x^i = x^j$ ,  $\Rightarrow x^{i-j} = e$ . But,  $0 \leq i - j \leq n - 1$ , contradicting  $|x| = n$

$$|x| = \infty :$$

$x^i \neq x^j \forall i \neq j$  shown as in the first case.

□

**Proposition 8.2.** Let  $H = \langle x \rangle$ , then

- if  $|H| = n$ , there exists a group isomorphism defined by

$$\varphi : \mathbb{Z}/n\mathbb{Z} \rightarrow H \tag{17}$$

$$k \mapsto x^k \tag{18}$$

- and if  $|H| = \infty$ , there exists group isomorphism defined by

$$\varphi : \mathbb{Z} \rightarrow H$$

$$k \mapsto x^k$$

*Proof.*

- $\varphi$  well defined:

Finite order:  $k \equiv l \pmod{n} \Rightarrow k = l + mn$ ,  $m \in \mathbb{Z}$ .

Then  $x^k = x^{l+mn} = x^l(x^n)^m = x^l$ . No equivalent terms in  $\mathbb{Z}$  for non-finite order.

- $\varphi$  group homomorphism:

$$\varphi(k_1 + k_2) = x^{k_1+k_2} = x^{k_1} \cdot x^{k_2} = \varphi(k_1) \cdot \varphi(k_2)$$

---

<sup>8</sup>The order of element  $x \in G$  can also be defined as the order of the subgroup which it generates.

- $\varphi$  bijective:

Follows from previous proposition. Also provable through existence of left, right inverses.

□

## 8.2 Subgroups of Cyclic Groups

**Proposition 8.3.** *Let  $G = \langle x \rangle$  be cyclic and  $H \leq G$  be a subgroup. Then  $H$  is also cyclic.*

*Proof.* Trivial if  $H = \{e\}$ . Assume not the case, and let  $l = \min\{m \in \mathbb{Z}^{>0} \mid x^m \in H\}$ . Then it is obvious that  $\langle x^l \rangle \subseteq H$  (closure of subgroup). We then let  $x^k \in H$  be an arbitrary element of  $H$ . We can write  $k = l \cdot k' + r$ ,  $0 \leq r < l$ , then  $x^r = x^{k-lk'} = x^k(x^l)^{k'} \in H$  (closure of  $H$ ). But  $r < l$ , and  $l$  is the minimum greater than 0. Hence,  $r = 0$ ,  $x^r = e$ , and  $x^k = (x^l)^{k'} \in \langle x^l \rangle$ . Thus,  $H \subseteq \langle x^l \rangle$ , but  $\langle x^l \rangle \subseteq H$ , and so  $H = \langle x^l \rangle$ .  $\square$

**Proposition 8.4.** *Let  $G = \langle x \rangle$  be an infinite cyclic group ( $|G| = \infty$ ). Then the assignment  $n \mapsto \langle x^n \rangle$  defines a bijection from  $\mathbb{N}$  and subgroups of  $G$ .*

*Proof.* By Prop. 8.2.1, each subgroup of  $G$  is of the form  $\langle x^n \rangle$ ,  $n \in \mathbb{Z}$ . Since  $\langle x^{-n} \rangle = \langle x^n \rangle$ , we can assume  $n \in \mathbb{N}$  (hence, map is surjective). Suppose  $\langle x^n \rangle = \langle x^m \rangle$ , then

$$\begin{aligned} x^n &= x^{km} \\ \Rightarrow n &= km \end{aligned}$$

Similarly  $m = k'n$ . Then  $n = kk'n$ , but  $k, k' \in \mathbb{N}$ , so  $k = k' = 1$  and  $m = n$  (map is then injective). Then since the outlined map is both injective and surjective, it is bijective.  $\square$

---

*Remark.* From Thm. 8.1.1,  $G = \langle x \rangle$  s.t.  $|G| = \infty$  is isomorphic to  $\mathbb{Z}$ . Since each element  $x^n$  is mapped to  $n$ , each subgroup  $\langle x^n \rangle$  is mapped to the corresponding subgroup generated by  $n$ ,  $\{\dots, -n, 0, n, 2n, \dots\}$  which is written as  $n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}$ .

---

## 9 Lecture 9: Euclidean Algorithm

**Definition 9.1.** We say  $m$  is a divisor of  $n$  if  $\exists k \in \mathbb{Z}$  s.t.  $n = km$  and write  $m|n$  in that case.

---

*Example.*

- $1|n \ \forall n \in \mathbb{Z}$
- $d|m, d|n \Rightarrow d|m \pm n$
- $n|0, \ \forall n$
- $d|n \Rightarrow |d| \leq |n|, \text{ if } n \neq 0$
- $n|n, \ \forall n$

---

**Definition 9.2.** For  $m, n \in \mathbb{Z}$  we define the greatest common divisor,  $\gcd(m, n) := (m, n) := \max\{d \in \mathbb{Z}^{>0} \mid d|m, d|n\}$ , we set  $(0, 0) = 0$ .

**Lemma 9.1.**

1.  $(m, n) = (n, m)$
2.  $(m, n) = (m, n + am) \ \forall a \in \mathbb{Z}$
3.  $(m, n) = (r, n), \ \forall r \equiv m \pmod{n}$
4.  $(m, 0) = |m|$

*Proof.* 1. Trivial, from definition of g.c.d., changing order does not change set of common denominators.

2. It is sufficient for this proof to show that the sets  $A = \{d \in \mathbb{Z}^{>0} \mid d|m, d|n\}$  and  $B = \{d \in \mathbb{Z}^{>0} \mid d|m, d|n + am\}$ , for any  $n \in \mathbb{Z}$ , are equal.

For any  $d \in A$ ,  $d|m, d|n$ . We can then write  $m = dp, n = dq$ . It follows that  $m + an = d(p + aq)$ , and so  $d|m + an$ . Thus,  $A \subseteq B$ .

For any  $d \in B$ , an analogous argument shows that  $B \subseteq A$ . Therefore  $A = B$ , and so  $\max\{d \in \mathbb{Z}^{>0} \mid d|m, d|n\} = \max\{d \in \mathbb{Z}^{>0} \mid d|m, d|n + am\}$ , and so  $(m, n) = (m, n + am) \ \forall n \in \mathbb{Z}$ .

3. Since  $r \equiv m \pmod{n}$ ,  $(r, n) = (m + an, n) = (m, n)$  by the 2nd part of Lemma 9.1.
4. For  $d \in \mathbb{Z}$  s.t.  $d|m$ , it must be that  $d|0$  also (0 divisible by all integers). Therefore,  $\{d \in \mathbb{Z} \mid d|m\} \subseteq \{d \in \mathbb{Z} \mid d|0\}$  and so  $(m, 0) = \max\{d \in \mathbb{Z} \mid d|m, d|0\} = \max\{d \in \mathbb{Z} \mid d|m\} = |m|$ .

□

**Proposition 9.2** (Euclidean Algorithm). *Let  $m, n \in \mathbb{Z}$ , then  $\exists a, b$  s.t*

$$(m, n) = am + bn \tag{19}$$

---

The procedure of Euclid's algorithm to find  $(m, n)$  for  $m, n \in \mathbb{Z}$ , where we can presume  $m > n$  w.l.o.g. (swapping), involves subtracting the maximum multiples of  $n$  from  $m$  s.t the remainder is non negative . This makes use of the second part of Lemma 9.1. The procedure is repeated until one of the remainders is zero, in which case the g.c.d. is  $(m, n) = (r_{n-1}, 0) = |r_{n-1}|$ .  $r_{n-1}$  is the remainder produced after  $n - 1$  iterations of the procedure.

---



*Proof.* For  $m, n \in \mathbb{Z}$ , to find  $(m, n)$ , we use Lemma 9.1. First we can assume  $m \geq n$ , then  $(m, n) = (n, r_1)$  where  $r_1 \equiv m \pmod{n}$ . Since  $0 \leq r_1 \leq |n|$ , we can replace  $n$  with  $r_2 \equiv n \pmod{|r_1|}$ . This is repeated until  $r_{l+1} = 0 = r_{l-1} \pmod{r_l}$ . Then

$$(m, n) = (r_l, r_{l+1}) = (r_l, 0) = |r_l|$$

Since  $r_{i+1} + k_{i+1}r_i = r_{i-1}$ ,

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & k_{i+1} \end{pmatrix}}_{A_i} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}$$

Thus

$$\begin{aligned} \begin{pmatrix} r_l \\ 0 \end{pmatrix} &= A_l \cdot A_{l-1} \cdot \dots \cdot A_1 \cdot A_0 \cdot \begin{pmatrix} m \\ n \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} m \\ n \end{pmatrix} \end{aligned}$$

□

## 10 Lecture 10: Subgroups of Finite Cyclic Groups

**Proposition 10.1.** *Let  $G = \langle x \rangle$  be a cyclic group of order  $|G| = n$ . Then*

1.  $\langle x^l \rangle = \langle x^{(l,n)} \rangle$
2.  $|\langle x^l \rangle| = \frac{n}{(l,n)}$

*In particular there is a one-to-one correspondence*

$$A = \{d \in \mathbb{Z}^{>0} \mid d|n\} \leftrightarrow B = \{H \subseteq G \mid H \leq G\}$$

$$d \in A \mapsto \langle x^d \rangle$$

*Proof.*

1. It is required to show that the two groups are subsets of each other and so are equivalent.

$$\text{"} \subseteq \text{" } d = (l, n) \Rightarrow \exists k \in \mathbb{Z}^{>0} \text{ s.t. } l = kd.$$

$$x^l = x^{kd} = (x^d)^k \in \langle x^d \rangle.$$

$$\Rightarrow \langle x^l \rangle \subseteq \langle x^d \rangle.$$

$$\text{"} \supseteq \text{" } \text{By proposition 9.2, } d = al + bn.$$

$$x^d = (x^l)^a \cdot (x^n)^b = (x^l)^a \in \langle x^l \rangle$$

$$\Rightarrow \langle x^d \rangle \subseteq \langle x^l \rangle$$

$$\Rightarrow \langle x^d \rangle = \langle x^l \rangle$$

2. For some  $\langle x^l \rangle$ , we can assume  $l = d \cdot k$ , where  $d = (l, n)$ , by 1. The order of the group generated by  $\langle x^d \rangle$  is the smallest  $k \in \mathbb{N}$  s.t.  $(x^d)^k = e$  or  $dk = mn$ , for  $m \in \mathbb{Z}$ . Since  $d|n$ , we can let  $m = 1$  w.l.o.g., and so  $k = \frac{n}{d} = \frac{n}{(l,n)}$ .

Define

$$\varphi : \{d \in \mathbb{Z}^{>0} \mid d|n\} \rightarrow \{H \subseteq G \mid H \leq G\} d \mapsto \langle x^d \rangle$$

Each subgroup of  $G$  is cyclic, ie.  $\forall H \leq G, H = \langle x^l \rangle, l \in \mathbb{Z}$ . By proposition 10.1, 1.,  $\langle x^l \rangle = \langle x^{(l,n)} \rangle$ . Since  $(l, n)|n$ ,  $(l, n) \in \{d \in \mathbb{Z}^{>0} \mid d|n\}$  and so  $\varphi$  is surjective.

Suppose  $\varphi(d_1) = \varphi(d_2)$ , then by proposition 10.1, 2.,  $\frac{n}{d_1} = \frac{n}{d_2}$ . Therefore  $d_1 = d_2$ . Thus,  $\varphi$  is injective.  $\square$

*Remark.* It is also shown that group  $G$  has a unique subgroup of order  $\frac{|G|}{d}$  for each pos. divisor  $d$  of  $|G|$ .

**Corollary 10.1.1.** *For  $x \in G$ ,  $\langle x^k \rangle = \langle x \rangle$ , then  $(k, |x|) = 1$ .*

*Proof.*

$$|\langle x^k \rangle| = |\langle x \rangle| = |x|$$

$$= \frac{|x|}{(k, |x|)} \text{ by Prop. 10.1}$$

It follows that  $(k, |x|) = 1$ .  $\square$

**Definition 10.1.** Let  $G$  be a group. We define the **group of automorphisms** of  $G$  to be

$$\text{Aut}(G) = \{\varphi : G \rightarrow G \mid \varphi \text{ a group isomorphism}\} \quad (20)$$

**Lemma 10.2.**  $\text{Aut}(G) \leq S_G$ , in particular,  $\text{Aut}(G)$  is a group under composition.

*Proof.* The symmetric group is defined in Eq. 11. The symmetric group on  $G$  is thereby the group of bijective maps from  $G$  to itself. This does not require the maps to be homomorphisms, which is the requirement which the group of automorphisms of  $G$  places on these maps.

Let  $\varphi \in \text{Aut}(G)$ , then  $\varphi$  is a group isomorphism,  $\varphi : G \rightarrow G$ . Then  $\varphi$  is bijective, and thus,  $\varphi \in S_G$ . Hence,  $\text{Aut}(G) \subseteq S_G$ .

It is then required to show  $\text{Aut}(G)$  is a group under composition. The unit of  $S_G$  is  $\text{id}$ , since  $\text{id}_G(g_1)\text{id}_G(g_2) = g_1g_2$  and  $\text{id}_G$  is bijective,  $\text{id}_G$  is a group isomorphism. Thus  $\text{id}_G \in \text{Aut}(G)$ .

Since each  $\varphi \in \text{Aut}(G)$  is bijective we can assume the existence of  $\varphi \in S_G$  (bijective). Then since  $\varphi$ ,  $\varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) \forall g_1, g_2 \in G$  we can say  $\varphi^{-1}(\varphi(g_1)\varphi(g_2)) = g_1g_2 = \varphi^{-1}(\varphi(g_1))\varphi^{-1}(\varphi(g_2))$ . Since  $\varphi(g) \in G$ , it follows that  $\varphi^{-1}$  is a group isomorphism, and so  $\varphi \in \text{Aut}(G)$ .

For  $\varphi_1, \varphi_2 \in \text{Aut}(G)$ ,  $\varphi_1(g_1g_2) = \varphi_1(g_1)\varphi_1(g_2)$  and so  $\varphi_2(\varphi_1(g_1g_2)) = \varphi_2(\varphi_1(g_1))\varphi_2(\varphi_1(g_2))$ , then  $\varphi_2 \circ \varphi_1 \in \text{Aut}(G)$ .

Therefore  $\text{Aut}(G)$  is a group under composition. □

**Proposition 10.3.** The group  $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$  is isomorphic to the multiplicative group of integers modulo  $n$ .

$$\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}^\times := \{k \in \mathbb{Z}/n\mathbb{Z} \mid (k, n) = 1\} \quad (21)$$

Where  $\mathbb{Z}/n\mathbb{Z}^\times$  has group multiplication defined by  $\overline{k_1} \cdot \overline{k_2} = \overline{k_1 \cdot k_2}$ , and unit  $\overline{1}$ .

*Proof.* Define map

$$\begin{aligned} \Psi : \text{Aut}(\mathbb{Z}/n\mathbb{Z}) &\rightarrow \mathbb{Z}/n\mathbb{Z}^\times \\ \varphi &\mapsto \varphi(1) \end{aligned}$$

- $\Psi$  is well defined:

$$\langle 1 \rangle = \mathbb{Z}/n\mathbb{Z} \Rightarrow$$

□