

# MAT 2143 Lecture Notes

Last updated:

March 28, 2023

# Contents

<b>1</b>	<b>Equivalence Relations</b>	<b>3</b>
1.1	Review of Equivalence Relations . . . . .	3
1.2	Examples of Equivalence Relations . . . . .	3
<b>2</b>	<b>Well-defined Operations on Equivalence Classes and Number Theory</b>	<b>7</b>
2.1	Well-defined Operations on Equivalence Classes . . . . .	7
2.2	Number Theory . . . . .	9
<b>3</b>	<b>Number Theory Cont. and Integers Modulo n</b>	<b>10</b>
3.1	More Number Theory . . . . .	10
3.2	Prime Factorization . . . . .	12
3.2.1	Summary . . . . .	13
3.3	Integers Modulo n . . . . .	13
<b>4</b>	<b>Operations on <math>\mathbb{Z}_n</math>, Symmetries, and Groups</b>	<b>16</b>
4.1	Arithmetic Modulo n . . . . .	16
4.1.1	Properties of Arithmetic Modulo n . . . . .	17
4.1.2	Multiplicative Inverses . . . . .	17
4.2	Symmetries . . . . .	19
4.2.1	Properties of Symmetries . . . . .	20
4.2.2	Generating Sets . . . . .	21
4.3	Groups . . . . .	21
<b>5</b>	<b>More Examples of Groups</b>	<b>23</b>
<b>6</b>	<b>Basic Properties of Groups, Products of Groups, Isomorphisms</b>	<b>24</b>
6.1	Basic Properties of Groups . . . . .	24
6.1.1	Small Groups . . . . .	26
6.2	Products of Groups . . . . .	27
6.3	Isomorphisms . . . . .	27

<b>7 Automorphisms, Subgroups</b>	<b>29</b>
7.1 Automorphisms . . . . .	29
7.2 Quaternions . . . . .	30
7.3 Subgroups . . . . .	31
7.3.1 Subgroup Test . . . . .	32
7.3.2 Alternative Versions of Subgroup Test . . . . .	32
<b>8 Lattices and Cyclic Groups</b>	<b>34</b>
8.1 Find all subgroups of $(\mathbb{Z}, +)$ . . . . .	34
8.2 Symmetries of a Square . . . . .	35
8.2.1 Subgroups of Symmetries of a Square . . . . .	38
<b>9 Cyclic Groups</b>	<b>40</b>
9.1 Cyclic Groups . . . . .	40
<b>10 Subgroups of Cyclic Groups, Lattices, <math>\mathbb{T}</math></b>	<b>46</b>
10.0.1 Lattices . . . . .	49
10.1 Complex Numbers . . . . .	49
<b>11 Subgroups of <math>\mathbb{T}</math>, Permutations, Disjoint Cycles</b>	<b>51</b>
11.1 Subgroups of a Finite Cyclic Subgroup . . . . .	51
<b>12</b>	<b>54</b>
<b>13</b>	<b>55</b>
<b>14</b>	<b>56</b>
<b>15</b>	<b>57</b>
<b>16</b>	<b>58</b>
<b>17</b>	<b>59</b>
<b>18</b>	<b>60</b>
<b>19 Normal Subgroups, Quotient Groups</b>	<b>61</b>
19.1 Normal Subgroups . . . . .	64
19.2 Quotient Groups . . . . .	65
<b>20 Quotient Groups</b>	<b>67</b>

# Lecture 1

## Equivalence Relations

### 1.1 Review of Equivalence Relations

Set  $X$  and a notion of equivalence  $\sim$ . For all  $x, y \in X$ , either  $x \sim y$  or  $x \not\sim y$ .

**Recall:**  $X \times X = \{(x, y) : x, y \in \mathbb{R}\}$ . Define  $R = \{(x, y) : x, y \in \mathbb{R} \text{ } x \sim y\}$ .

$R$  is an **equivalence relation** if

- $x, y \in R \ \forall x \in X$
- $(x, y) \in R \iff (y, x) \in R$
- $(x, y) \in R \ (y, z) \in R \implies (x, z) \in R$

If  $R$  is an equivalence relation on  $X$ , then we define the **equivalence class** of  $x \in X$  as

$$[x] = \{y \in X : x \sim y\}$$

### 1.2 Examples of Equivalence Relations

- Take any set  $X$  and let  $x \sim y$  mean  $x = y$   
**Reflexive:**  $x \sim x$ ? Yes, because  $x = x$   
**Symmetric:**  $x \sim y \iff y \sim x$ ? Yes, because if  $x = y$ , then  $y = x$ .  
**Transitive:**  $x \sim y \text{ } y \sim z \implies x \sim z$ ? Yes, because if  $x = y$  and  $y = z$ , then  $x = z$ .
- Take  $X = \mathbb{R}^2$  and let  $(a, b) \sim (c, d)$  mean  $a^2 + b^2 = c^2 + d^2$   
**Reflexive:**  $(a, b) \sim (a, b)$ ? Yes, because  $a^2 + b^2 = a^2 + b^2$   
**Symmetric:**  $(a, b) \sim (c, d) \iff (c, d) \sim (a, b)$ ? Yes, because if  $a^2 + b^2 =$

$c^2 + d^2$ , then  $c^2 + d^2 = a^2 + b^2$ .

**Transitive:**  $(a, b) \sim (c, d) \ (c, d) \sim (e, f) \implies (a, b) \sim (e, f)$ ? Yes, because if  $a^2 + b^2 = c^2 + d^2$  and  $c^2 + d^2 = e^2 + f^2$ , then  $a^2 + b^2 = e^2 + f^2$ .

- Take  $X = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$  and let  $(a, b) \sim (c, d)$  mean  $(ad = bc)$ .

**Reflexive:**  $(a, b) \sim (a, b)$ ? Yes, because multiplication of  $\mathbb{Z}$  is commutative, so  $ab = ba$ .

**Symmetric:**  $(a, b) \sim (c, d) \iff (c, d) \sim (a, b)$ ? Yes,

$$(a, b) \sim (c, d) \implies ad = bc$$

$$cb = da$$

$$(c, d) \sim (a, b)$$

**Transitive:**  $(a, b) \sim (c, d) \ (c, d) \sim (e, f) \implies (a, b) \sim (e, f)$ ? We want  $ad = bc$ ,  $cf = de \implies af = be$

**Case 1:**  $c = 0$  Then  $bc = 0 = ad$ ,  $d \in \mathbb{Z} \setminus \{0\}$ , so  $d \neq 0$ ,  $a = 0$   
 $cf = 0 = de$ , again  $d \neq 0$ , so  $e = 0$ .

$$\therefore af = be = 0$$

**Case 2:**  $c \neq 0$  Then  $\frac{ad}{c} = b$ ,  $\frac{de}{c} = f$

$$\therefore af = a \cdot \frac{de}{c} = \frac{ad}{c} \cdot e = be$$

**Theorem 1.2.1.** Let  $X$  be a set with an equivalence relation. Then

$$[x] \cap [y] \neq \emptyset \implies [x] = [y]$$

So, equivalence classes are disjoint or equal.

*Proof.* Assume  $[x] \cap [y] \neq \emptyset$ . So  $\exists z \in [x] \cap [y]$

Now let  $a \in [x]$

$$\begin{aligned}
 a &\sim z && \text{(since } z \in [x] \text{ , } z \sim x \sim a) \\
 z &\sim y && \text{(since } z \in [y]) \\
 a &\sim y && \text{(transitivity)} \\
 a &\in [y] \\
 \therefore [x] &\subseteq [y]
 \end{aligned}$$

Now take  $b \in [y]$ , using the same arguments we get

$$\begin{aligned}
 b &\sim z && \text{(since } z \in [y] \text{ , } z \sim y \sim b) \\
 z &\sim x && \text{(since } z \in [x]) \\
 b &\sim x && \text{(transitivity)} \\
 b &\in [x] \\
 \therefore [y] &\subseteq [x]
 \end{aligned}$$

□

**Observation:** If  $X$  is some set with an equivalence relation, then every  $x \in X$  is in some equivalence class.

**Definition 1.2.1** (Partitions). *Say we have some  $R_j \subseteq X$  for  $j \in \{1, 2, \dots, n\}$ , with every  $x \in X$  in exactly one  $R_j$ , then the  $R_j$  form a partition of  $X$ .*

**Theorem 1.2.2.** *Let  $X$  be a set with an equivalence relation. Then the equivalence classes form a partition of  $X$ .*

*Proof.* If  $z \in X$ , then  $z \in [z]$ , therefore  $z$  is in at least one equivalence class. If  $z \in [x]$  and  $z \in [y]$ , then  $[x] \cap [y] \neq \emptyset$  therefore  $[x] = [y]$  (as shown previously). Therefore  $z$  is in at most one equivalence class. □

**Theorem 1.2.3.** *Let  $R_j$  form a partition of  $X$ . Say that  $x \sim y$  means  $x, y \in R_j$  for some  $j$ . Then  $\sim$  is an equivalence relation on  $X$ .*

*Proof.*

- $x \in X$ , so  $x \in R_j$  for some  $j$  implies  $x, x \in R_j \implies x \sim x$
- $x \sim y \iff x, y \in R_j \iff y, x \in R_j \iff y \sim x$

•

$$\begin{aligned}
 x \sim y \quad y \sim z &\implies \begin{cases} x, y \in R_i \\ y, z \in R_j \end{cases} \implies y \in R_i, R_j \\
 &\implies i = j \\
 &\implies x, z \in R_j \\
 &\therefore x \sim z
 \end{aligned}$$

□

### Example of Finding Equivalence Classes

Take  $X = R \times R$ , and let  $(a, b) \sim (c, d)$  mean  $a^2 + b^2 = c^2 + d^2$ . Find the equivalence class of  $(0, 0)$ ,  $(3, 4)$ ,  $(a, b)$

$$\begin{aligned}
 [(0, 0)] &= \{(x, y) : (x, y) \sim (0, 0)\} \\
 &= \{(x, y) : x^2 + y^2 = 0^2 + 0^2 = 0\} \\
 &= \{(x, y) : x = y = 0\}
 \end{aligned}$$

$$\begin{aligned}
 [(3, 4)] &= \{(x, y) : (x, y) \sim (3, 4)\} \\
 &= \{(x, y) : x^2 + y^2 = 3^2 + 4^2 = 25\} \\
 &= \{(x, y) : \sqrt{x^2 + y^2} = 5\}
 \end{aligned}$$

$$\begin{aligned}
 [(a, b)] &= \{(x, y) : (x, y) \sim (a, b)\} \\
 &= \{(x, y) : x^2 + y^2 = a^2 + b^2 = r\} \\
 &= \{(x, y) : \sqrt{x^2 + y^2} = r\}
 \end{aligned}$$

## Lecture 2

# Well-defined Operations on Equivalence Classes and Number Theory

### 2.1 Well-defined Operations on Equivalence Classes

Consider a set  $X$ , an equivalence relation  $\sim$ , and an operation  $\cdot$ . This operation is [well-defined on equivalence classes](#) if

$$\left. \begin{array}{l} x \sim y \\ w \sim z \end{array} \right\} \implies x \cdot w \sim y \cdot z$$
$$\left. \begin{array}{l} [x] = [y] \\ [w] = [z] \end{array} \right\} \implies [x \cdot w] = [y \cdot z]$$

**Example:** Let  $X = \mathbb{R} \times \mathbb{R}$ ,  $(a, b) \sim (c, d)$  means  $a^2 + b^2 = c^2 + d^2$ , is addition well-defined on equivalence classes? (*Addition meaning  $(x, y) + (z, y) = (x + z, y + w)$* )

$$\text{Let } \left\{ \begin{array}{l} (a, b) \sim (c, d) \\ (e, f) \sim (g, h) \end{array} \right\} \text{ then } \left\{ \begin{array}{l} a^2 + b^2 = c^2 + d^2 \\ e^2 + f^2 = g^2 + h^2 \end{array} \right.$$



Now,

$$\begin{cases} (a, b) + (e, f) = (a + e, b + f) \\ (c, d) + (g, h) = (c + g, d + h) \end{cases}$$

**Question:** Is  $(a + e)^2 + (b + f)^2 = (c + g)^2 + (d + h)^2$ ?

$$(a + e)^2 + (b + f)^2 = a^2 + 2ae + e^2 + b^2 + 2bf + f^2$$

$$(c + g)^2 + (d + h)^2 = c^2 + 2cg + g^2 + d^2 + 2dh + h^2$$

$a^2 + b^2 = c^2 + d^2$ , and  $e^2 + f^2 = g^2 + h^2$ , so

$$(a + e)^2 + (b + f)^2 = (c + g)^2 + (d + h)^2 \iff 2ae + 2bf = 2cg + 2dh$$

**Counterexample:** Take

$$(a, b) = (c, d) = (1, 2)$$

$$(e, f) = (3, 4) \quad (g, h) = (4, 3)$$

So no, addition is not well defined.

**Another Example:**  $X = (\mathbb{Z}, \mathbb{Z} \setminus \{0\})$ .  $(a, b) \sim (c, d)$  means  $ad = bc$ . Is multiplication well-defined on equivalence classes? (*Multiplication meaning*  $(x, y) \cdot (w, z) = (x \cdot w, y \cdot z)$ ). Let

$$\begin{cases} (a, b) \sim (c, d) \\ (e, f) \sim (g, h) \end{cases} \implies \begin{cases} ad = bc \\ ef = gh \end{cases}$$

Now,

$$\begin{cases} (a, b) \cdot (e, f) = (a \cdot e, b \cdot f) \\ (c, d) \cdot (g, h) = (c \cdot g, d \cdot h) \end{cases}$$

**Question:** Is  $(ae, bf) \sim (cg, dh)$ ?

$$(ae)(dh) = \text{ad} \cdot \text{eh}$$

$$(bf)(cg) = \text{bc} \cdot \text{fg}$$

We have  $(a, b) \sim (c, d)$ , so  $ad = bc$ , and  $(e, f) \sim (g, h)$ , so  $ek = fg$ . So yes, multiplication is well-defined on equivalence classes.

## 2.2 Number Theory

**Fact 2.2.1.** *Every non-empty set  $S \subseteq \mathbb{N}$  has a minimum element  $d$  in  $S$*

**Proposition 2.2.1.** *Let  $a, b \in \mathbb{Z}$ ,  $b > 0$ , then  $\exists! q, r \in \mathbb{Z}$  with  $a = bq + r$ ,  $0 \leq r < b$*

*Proof.* (Existence) Let  $S = \{a - bx : x \in \mathbb{Z}, a - bx \geq 0\}$ .  $\emptyset \neq S \subseteq \mathbb{N}$ , so  $S$  has a minimum element.

Let

$$\begin{cases} r = \min(S) \\ q = \frac{a-r}{b} \end{cases}$$

$r = a - bd$ ,  $d \in \mathbb{Z}$ , then  $bq + r = b\left(\frac{a-r}{b}\right) + r = a - r + r = a$ .

If  $b \leq r$ , then  $0 \leq r - b < r$ , which contradicts the minimality of  $r$ .

(Uniqueness) Say  $a = bq + r = bp + s$ ,  $0 \leq r, s < b$ . Then

$$b(q - p) = s - r$$

So  $s - r$  is a multiple of  $b$ , but  $0 \leq r, s < b$ , so it must be that  $r - s = 0$ , therefore  $r = s$ .  $\square$

## Lecture 3

# Number Theory Cont. and Integers Modulo $n$

### 3.1 More Number Theory

**Definition 3.1.1.**  $m \mid n$  means  $\exists x \in \mathbb{Z}$  with  $n = mx$

**Definition 3.1.2.** Let  $a, b \in \mathbb{Z}$ . If  $d$  is a positive integer with  $d \mid a$  and  $d \mid b$ , if  $c \mid a$  and  $c \mid b$ , then  $c \mid d$ , then  $d$  is a *gcd* of  $a$  and  $b$ .

**Theorem 3.1.1.** For every  $a, b \in \mathbb{Z}$ ,  $\exists ! \text{ gcd } d$ . Furthermore,  $\exists x, y \in \mathbb{Z}$ ,  $d = ax + by$ . Furthermore,  $d$  is the largest common divisor of  $a, b$

*Proof.* Let  $S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$ .  $S \subseteq \mathbb{N}$ , so  $\exists !$  minimum element  $d$  in  $S$ .

Write

$$a = dq + r \quad (0 \leq r < d)$$

$$a = (ax + by)q + r \quad (\text{some } x, y \in \mathbb{Z})$$

$$r = a(1 - qx) + b(-qy)$$

$$r = ax' + by' \quad (x' = 1 - qx, y' = -qy)$$

$$0 \leq r = ax' + by' < d$$

So. either  $r = 0$  or  $r \in S$  but not both, but  $r < d$  which is the minimum of the set. Therefore  $r \notin S$ . So  $r = 0$  and  $d \mid a$ . Same argument with

$$b = dq + r \implies d \mid b.$$

Now suppose  $c \mid a$  and  $c \mid b$ , then  $a = a'c$  and  $b = b'c$ ,  $a', b' \in \mathbb{Z}$ .

$$d = ax + by = a'cx + b'cy = c(a'x + b'y)$$

So,  $c \mid d$ . □

**Corollary 3.1.1.** *If  $\gcd(a, b) = 1$ , then  $\exists x, y$  such that  $ax + by = 1$ .*

*Proof.* Same as the previous proof, in the case that  $\gcd(a, b) = 1$ . □

**Corollary 3.1.2.** *If  $\gcd(a, b) = d$ , then  $\{ax + by : x, y \in \mathbb{Z}\} = d \cdot \mathbb{Z}$ ,  $\forall n \in \mathbb{Z}$ .*

*Proof.* No proof was provided in the notes I guess. :P □

**Definition 3.1.3** (Least Common Multiple). *Let  $a, b \in \mathbb{Z}$ . If  $m$  is a positive integer with*

- $a \mid m$  and  $b \mid m$
- if  $a \mid n$  and  $b \mid n$ , then  $m \mid n$

*then  $m$  is a **lcm** of  $a, b$ .*

**Theorem 3.1.2.** *For every  $a, b$ ,  $\exists ! \text{lcm } m$ .*

**Definition 3.1.4.**  $p \in \mathbb{Z}$   $p > 1$

- $p$  is irreducible if the only positive divisors of  $p$  are 1 and  $p$
- $p$  is prime if whenever  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$

**Proposition 3.1.1.**  $p$  is prime  $\implies p$  is irreducible

*Proof.* Say  $p$  is not irreducible,  $p = ab$ , and  $1 < a, b < p$ . Then  $p \nmid a$  and  $p \nmid b$ . □

**Proposition 3.1.2.**  $p$  is irreducible  $\implies p$  is prime

*Proof.*  $p \mid ab \implies ab = mp$  for some  $m \in \mathbb{Z}$ . Say  $p \nmid a$ , since  $p$  is irreducible  $\gcd(a, p) = 1$ . So  $\exists s, t$  such that  $as + pt = 1$ .

$$b = b(as + pt) = abs + bpt = mps + bpt = (ms + bt)p$$

Therefore  $b$  is a multiple of  $p$ , so  $p \mid b$ . □

## 3.2 Prime Factorization

**Theorem 3.2.1.**  $n \in \mathbb{Z} \ n > 1$

$$\exists! \begin{cases} p_1 p_2 \dots p_s, & \text{distinct primes} \\ e_1 e_2 \dots e_s, & \text{positive integers} \end{cases}$$

With

$$n = p_1^{e_1} \cdot p_2^{e_2} \dots p_s^{e_s}$$

*Proof.* Proof was omitted. □

**Prime Factorization Gives GCD:**

**Example:**

$$a = 2 \cdot 5 \cdot 7^{10} \cdot 13 = 2^{\boxed{1}} \cdot 3^{\boxed{0}} \cdot 5^1 \cdot 7^{10} \cdot 13^1 \cdot 17^{\boxed{0}}$$

$$b = 2 \cdot 3^2 \cdot 7^2 \cdot 17 = 2^1 \cdot 3^2 \cdot 5^{\boxed{0}} \cdot 7^{\boxed{2}} \cdot 13^{\boxed{0}} \cdot 17^1$$

$$\gcd(a, b) = 2^1 \cdot 7^2$$

$$a = p_1^{e_1} \cdot p_2^{e_2} \dots p_s^{e_s}$$

$$b = q_1^{F_1} \cdot q_2^{F_2} \dots q_s^{F_s}$$

$$\forall \text{ prime } p, \text{ define } g(p) = \min \begin{cases} e_i & \text{if } p = p_i \\ f_j & \text{if } p = q_j \\ 0 \end{cases}$$

Then,

$$\gcd(a, b) = \prod_{\text{prime } p} p^{g(p)}$$

**Prime Factorization Gives LCM:**

**Example:**

$$a = 2 \cdot 5 \cdot 7^{10} \cdot 13 = 2^1 \cdot 3^0 \cdot 5^{\boxed{1}} \cdot 7^{\boxed{10}} \cdot 13^{\boxed{1}} \cdot 17^0$$

$$b = 2 \cdot 3^2 \cdot 7^2 \cdot 17 = 2^{\boxed{1}} \cdot 3^{\boxed{2}} \cdot 5^0 \cdot 7^2 \cdot 13^0 \cdot 17^{\boxed{1}}$$

$$\text{lcm}(a, b) = 2^1 \cdot 3^2 \cdot 5^1 \cdot 7^{10} \cdot 13^1 \cdot 17^1$$

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_s^{e_s}$$

$$b = q_1^{F_1} \cdot q_2^{F_2} \cdots q_s^{F_s}$$

$$\forall \text{ prime } p, \text{ define } l(p) = \min \begin{cases} e_i & \text{if } p = p_i \\ f_j & \text{if } p = q_j \\ 0 \end{cases}$$

Then,

$$\gcd(a, b) = \prod_{\text{prime } p} p^{l(p)}$$

### 3.2.1 Summary

- Definition of  $\gcd(a, b)$
- $d = \gcd(a, b)$  exists  $\implies d$  is a divisor of  $a$  and  $b$  and  $d = ax + by$  for some  $x, y \in \mathbb{Z}$
- also,  $\{ax + by : x, y \in \mathbb{Z}\} = d\mathbb{Z}$
- Definition of  $\text{lcm}(a, b)$
- $m = \text{lcm}(a, b)$  exists and is unique,  $m$  is the smallest common multiple.
- Prime Factorization exists and is unique.
- Prime factorization of  $a$  and  $b$  gives  $\gcd(a, b)$  and  $\text{lcm}(a, b)$
- $\gcd(a, b) \cdot \text{lcm}(a, b) = |ab|$

## 3.3 Integers Modulo $n$

Let  $n \in \mathbb{Z}$  with  $n \geq 2$ ,  $a \equiv b \pmod{n}$  means  $n \mid (a - b)$ . So

$$a \equiv b \pmod{n} \iff n \mid (a - b)$$

$$\iff a - b = kn, \text{ for some } k \in \mathbb{Z}$$

$$\iff \frac{a - b}{n} \in \mathbb{Z}$$

**Proposition 3.3.1.** *Congruence modulo  $n$  is an equivalence relation.*

*Proof.*

- **Reflexivity:** Show  $a \equiv a \pmod{n} \forall a \in \mathbb{Z}$ .

$$\frac{a - a}{n} = 0 \in \mathbb{Z}$$

So  $a \equiv a \pmod{n}$ .

- **Symmetric:** Show  $a \equiv b \iff b \equiv a \forall a, b \in \mathbb{Z}$

$$a \equiv b \iff \frac{a - b}{n} \in \mathbb{Z} \iff -\frac{a - b}{n} = \frac{b - a}{n} \in \mathbb{Z} \iff b \equiv a$$

- **Transitivity:** Show  $a \equiv b \wedge b \equiv c \implies a \equiv c \forall a, b, c \in \mathbb{Z}$

$$\begin{aligned} a \equiv b \equiv c &\implies \frac{a - b}{n} \in \mathbb{Z} \wedge \frac{b - c}{n} \in \mathbb{Z} \\ &\implies \frac{a - b}{n} + \frac{b - c}{n} = \frac{a - c}{n} \in \mathbb{Z} \implies a \equiv c \end{aligned}$$

□

**Example:** Define  $\mathbb{Z}_n = \{[k]_n : k \in \mathbb{Z}\}$ . Consider  $n = 5$ .

- $[2] = \{\dots, -8, -3, 2, 7, 12, 17, \dots\}$
- $[0] = \{\dots, -10, -5, 0, 5, 10, \dots\}$
- $[7] = \{\dots, -3, 2, 7, 12, 17, 22, \dots\}$

**Note:**  $\mathbb{Z}_5$  is a set containing 5 elements, and each element of  $\mathbb{Z}_5$  is a subset of  $\mathbb{Z}$ . Also, recall that equivalence classes are disjoint or equal, so  $[2] = [7]$

$$\begin{aligned} \mathbb{Z}_5 &= \{[0], [1], [2], [3], [4]\} \\ &= \{[-2], [-1], [0], [1], [2]\} \end{aligned}$$

**Examples:**

(a)  $[3]_5 = [8]_5 \quad 3 \equiv 8 \pmod{5} \quad 5 \mid (8 - 3)$

$$(b) \quad [3]_9 = [-24]_9 \quad 3 \equiv -24 \pmod{9} \quad 9|(3 - (-24))$$

All representations in an equivalence class are equivalent (modulo  $n$ ).

**Question:** Is addition and multiplication on  $\mathbb{Z}_n$  well defined? We want

$$\begin{cases} [a] + [b] = [a + b] \\ [a] \cdot [b] = [a \cdot b] \end{cases}$$

We'll see this in the lecture.



## Lecture 4

# Operations on $\mathbb{Z}_n$ , Symmetries, and Groups

### 4.1 Arithmetic Modulo $n$

**Question:** Is addition and multiplication on  $\mathbb{Z}_n$  well defined? We want

$$\begin{cases} [a] + [b] = [a + b] \\ [a] \cdot [b] = [a \cdot b] \end{cases}$$

**Proposition 4.1.1.** *Let  $n \in \mathbb{Z}$   $n \geq 2$ . Suppose*

$$\begin{aligned} a &\equiv a' \pmod{n} \\ b &\equiv b' \pmod{n} \end{aligned}$$

*then*

$$\begin{aligned} a + b &\equiv a' + b' \pmod{n} \\ ab &\equiv a'b' \pmod{n} \end{aligned}$$

*So, addition and multiplication on integers are well well defined on congruence classes.*

*Proof.*

$$a \equiv a' \pmod{n} \iff \frac{a - a'}{n} \in \mathbb{Z} \iff a' = a + sn \text{ for some } s \in \mathbb{Z}$$

$$b \equiv b' \pmod{n} \iff \frac{b - b'}{n} \in \mathbb{Z} \iff b' = b + tn \text{ for some } t \in \mathbb{Z}$$

Then,

$$\frac{(a + b) - (a' + b')}{n} = \frac{a - a'}{n} + \frac{b - b'}{n} \in \mathbb{Z}$$

So,  $a + b \equiv a' + b' \pmod{n}$ . Also,

$$\begin{aligned} \frac{ab - a'b'}{n} &= \frac{ab - a'b + a'b - a'b'}{n} \\ &= \left( \frac{a - a'}{n} \right) b + \left( \frac{b - b'}{n} \right) a' \in \mathbb{Z} \end{aligned}$$

So  $ab \equiv a'b' \pmod{n}$ . □

#### 4.1.1 Properties of Arithmetic Modulo n

- **Commutative:**  $a + b \equiv b + a \pmod{n}$
- **Commutative:**  $ab \equiv ba \pmod{n}$
- **Associative:**  $(a + b) + c \equiv a + (b + c) \pmod{n}$
- **Associative:**  $(ab)c \equiv a(bc) \pmod{n}$
- **Distributive:**  $a(b + c) \equiv ab + ac \pmod{n}$
- **Identity for +:**  $a + 0 \equiv a \pmod{n}$
- **Identity for ·:**  $a \cdot 1 \equiv a \pmod{n}$
- **Additive Inverse:**  $a + (-a) \equiv 0 \pmod{n}$
- **Multiplicative Inverse?**

#### 4.1.2 Multiplicative Inverses

**Proposition 4.1.2.** Let  $a \in \mathbb{Z}_n$ ,  $\exists b \in \mathbb{Z}_n$  with  $ab \equiv 1 \pmod{n} \iff \gcd(a, n) = 1$ .

*Proof.* Suppose such  $b$  exists, then

$$\begin{aligned} ab - 1 &= rn \text{ for some } r \in \mathbb{Z} \\ ab + (-r)n &= 1 \\ \therefore \gcd(a, n) &= 1 \end{aligned}$$

Suppose  $\gcd(a, n) = 1$ , then

$$\begin{aligned} as + nt &= 1 \text{ for some } s, t \in \mathbb{Z} \\ as - 1 &= (-t)n \\ as &\equiv 1 \pmod{n} \end{aligned}$$

So we can choose  $b = s$ . □

**Example:** Addition and multiplication in  $\mathbb{Z}_6$ .

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

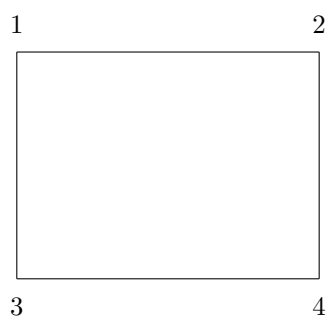
The table being symmetric implies that addition is commutative, 0-row and 0-column implies that 0 is the identity for addition, every row has a 0 implies that the additive inverse exists for every element.

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The table being symmetric implies that multiplication is commutative, 1-row and 1-column is the header implies that 1 is the identity for multiplication, some rows not having 1 implies that some elements have no multiplicative inverse.

## 4.2 Symmetries

Consider the symmetries of a rectangle.



The notation for functions is

$$F = \begin{pmatrix} 1 & 2 & 3 & 4 \\ f(1) & f(2) & f(3) & f(4) \end{pmatrix}$$

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

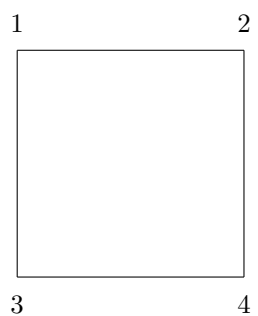
$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

**Claim:**  $\{\epsilon, \rho, \alpha, \beta\}$  are *all* the symmetries of a rectangle.

*Proof.* DGD Question - Will add later.

□

Consider the symmetries of a square.



$$\begin{array}{ccc}
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} & \epsilon & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} & 90^\circ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} & 180^\circ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \\
\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} & 270^\circ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}
\end{array}$$

#### 4.2.1 Properties of Symmetries

$S = \{\alpha, \beta, \dots\}$  symmetries of some object, with the operation composition.

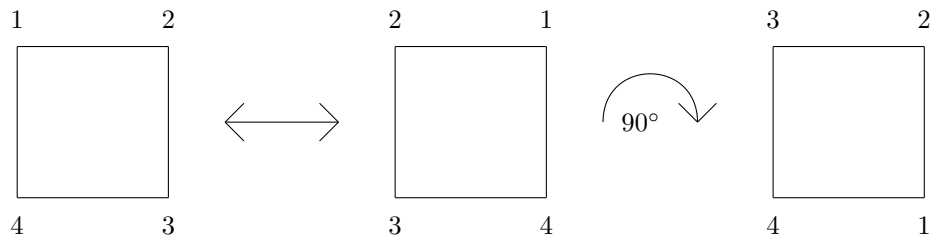
**Properties:**

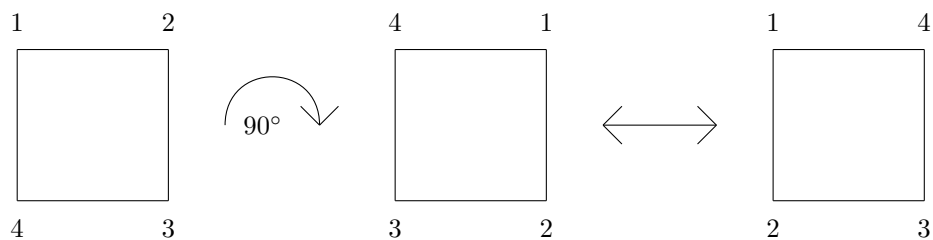
- $\alpha \circ \beta$  is a symmetry  $\forall \alpha, \beta \in S$
- $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma) \quad \forall \alpha, \beta, \gamma \in S$
- $\exists \epsilon \in S$  such that  $\epsilon \circ \alpha = \alpha \circ \epsilon = \alpha \quad \forall \alpha \in S$
- $\forall \alpha \in S, \exists \beta \in S$ , such that  $\alpha \circ \beta = \beta \circ \alpha = \epsilon \quad \forall \alpha, \beta \in S$

*Note: we often write  $\alpha\beta$  instead of  $\alpha \circ \beta$*

**Example:**  $S =$  symmetries of some object, is  $gh = hg \quad \forall g, h \in S$ ? **Answer:**

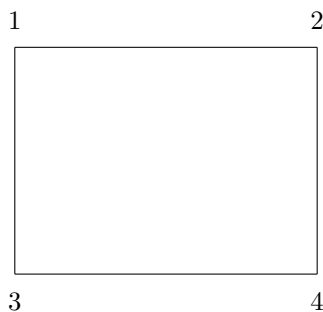
For a rectangle, yes. But for a square, no.





These symmetries do not commute, so  $gh \neq hg$ .

### 4.2.2 Generating Sets



$$\epsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

**Check:**  $\alpha\beta = \rho$ ,  $\alpha^2 = \epsilon$ . So  $\forall g \in S$ ,  $g$  can be written in terms of  $\alpha, \beta$ .

We say that  $\{\alpha, \beta\}$  **generates**  $S$

## 4.3 Groups

Let  $S$  be some set with some operation  $\cdot$ . Then  $(S, \cdot)$  is a **group** if

- **Closure:**  $ab \in S \forall a, b \in S$
- **Associativity:**  $(ab)c = a(bc) \forall a, b, c \in S$
- **Identity:**  $\exists \epsilon \in S$  such that  $x\epsilon = \epsilon x = x \forall x \in S$

- **Inverses:**  $\forall x \in S, \exists y \in S$  such that  $xy = yx = \epsilon$

**Examples:**

- Symmetries of an object form a group.
- $(\mathbb{R}, +)$  forms a group.
- $(\mathbb{R} \setminus \{0\}, \cdot)$  forms a group.
- $(\mathbb{Z}, +)$  forms a group.
- $(\mathbb{Z}, \cdot)$  does not form a group since inverses are typically not integers.
- $(\mathbb{Z}_n, +)$  forms a group.
- $(\mathbb{Z}_n \setminus \{0\}, \cdot)$  forms a group.

## Lecture 5

# More Examples of Groups

This lecture was not well organizing so I am not gonna type it out.



## Lecture 6

# Basic Properties of Groups, Products of Groups, Isomorphisms

Examples were left out I may come back to finish

### 6.1 Basic Properties of Groups

**Proposition 6.1.1.** *In every group, the identity is unique.*

*Proof.* Suppose  $a, b$  are identities, so

$$\left. \begin{array}{l} ax = xa = x \\ bx = xb = x \end{array} \right\} \forall x$$

Because  $b$  is an identity, we have  $a = ab$ , and since  $a$  is an identity, we have  $ab = b$ . So

$$a = ab = b$$

$$\therefore a = b$$

□

**Proposition 6.1.2.** *In every group, the equation  $ax = b$  has a unique solution  $x$  for all  $a, b$*

*Proof.* There was no proof :(

□

**Proposition 6.1.3.** *In every group,  $ab = ac \implies b = c$*

*Proof.* Again, no proof :(

□

*Note: For matrices it is not the same,  $AB = AC \not\Rightarrow B = C$*

**Proposition 6.1.4.** *In every group,  $(ab)^{-1} = b^{-1}a^{-1}$*

*Proof.*

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} & (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b \\ &= a\epsilon a^{-1} & &= b^{-1}\epsilon b \\ &= aa^{-1} & &= b^{-1}b \\ &= \epsilon & &= \epsilon \end{aligned}$$

□

**Proposition 6.1.5.** *In every group,  $(a^{-1})^{-1} = a$*

*Proof.* Since  $a^{-1}$  is the inverse of  $a$ , we have

$$aa^{-1} = a^{-1}a = \epsilon$$

but then,

$$a^{-1}a = aa^{-1} = \epsilon$$

So  $a$  is the inverse of  $a^{-1}$

□

**Proposition 6.1.6.** *In every group, if  $xy = x$ , for some  $x, y$ , then  $y = \epsilon$ . So if  $y$  behaves as the identity just once, then  $y$  is the identity.*

*Proof.* No proof again :P.

□

**Proposition 6.1.7.** *In every group, if  $xy = \epsilon$ , for some  $x, y$ , then  $y = x^{-1}$ . So if  $y$  behaves like  $x^{-1}$  on one side, then  $y$  is  $x^{-1}$*

*Proof.* No proof D:

□

**Proposition 6.1.8.** *In every group, the Cayley table has exactly one row and column that matches the headers, and no other row or column matches the header even once.*

*Proof.* Start by taking  $G$  to be some group, then let  $x, y \in G$ . And let  $H$  be a subgroup of  $G$ .

just kidding no proof. □

**Proposition 6.1.9.** *In every group, every row and column of the Cayley table contains each element exactly once.*

*Proof.* Why does the prof include a spot for the proof. □

### 6.1.1 Small Groups

- Say  $G$  has one element  $G = \{x\}$

**Closure:**  $x \cdot x = x$

**Identity:**  $x = \epsilon$

**Inverse:**  $x^{-1} = x$

$\cdot$	$x$
$x$	$x$

- Say  $G$  has two elements, it must have an identity so  $G = \{\epsilon, x\}$  If  $xx = x$ ,  $x = \epsilon$ , this is a contradiction, So  $xx = \epsilon$

$\cdot$	$\epsilon$	$x$
$\epsilon$	$\epsilon$	$x$
$x$	$x$	$\epsilon$

- Say  $G$  has three elements.  $G = \{\epsilon, x, y\}$

$\cdot$	$\epsilon$	$x$	$y$
$\epsilon$	$\epsilon$	$x$	$y$
$x$	$x$	$y$	$\epsilon$
$y$	$y$	$\epsilon$	$x$

$$x\epsilon = x \implies xy \neq x$$

$$\epsilon y = y \implies xy \neq y$$

So  $xy = \epsilon$

$$x\epsilon = x \implies xx \neq x$$

$$xy = \epsilon \implies xx \neq \epsilon$$

So  $xx = y$

- Say  $G$  has 4 elements. Assignment Question!

## 6.2 Products of Groups

$G, H$  are groups, define

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

$$(x, a) \cdot (y, b) = (x \cdot y, a \cdot b)$$

$$G_1 \times G_2 \times \cdots \times G_k = \{(g_1, g_2, \dots, g_k) : g_j \in G_j\}$$

**To reiterate**, operations are done by component according to the operations of the group. i.e Suppose we have a group  $G = (A, +)$  and  $H = (B, \cdot)$  and  $g, a \in G, h, b \in H$ .

$$(g, h) \times (a, b) = (g + a, h \cdot b)$$

**Proposition 6.2.1.** *The product of groups is a group.*

*Proof.* Exercise. □

## 6.3 Isomorphisms

Suppose  $\phi : G \rightarrow H$  is a bijection between two groups with the property

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

Then  $\phi$  is an [isomorphism](#) of  $G \cong H$ . So

$$G : x \cdot y = z \implies H : \phi(x) \cdot \phi(y) = \phi(z)$$

$\cdot$	$y$
$x$	$z$

$\cdot$	$y'$
$x'$	$z'$

$$x' = \phi(x) \qquad y' = \phi(y) \qquad z' = x'y' = \phi(z)$$

Start with  $G$ 's Cayley table, change the names (symbols, consistently) and permute the rows and columns. This gives  $H$ 's Cayley table.

**Example:**

$$\begin{array}{c|cc} & 0 & 1 \\ \hline + & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} & 1 & -1 \\ \hline \cdot & 1 & -1 \\ 1 & 1 & -1 \\ -1 & -1 & 1 \end{array} \qquad G = (\{\mathbb{Z}^+, \mathbb{Z}^-\}, \cdot)$$

$$\begin{array}{c|cc} & + & - \\ \hline \cdot & + & - \\ + & + & - \\ - & - & + \end{array}$$

$$\mathbb{Z}_2 \cong \mathbb{Z}^\times \cong G$$

**Proposition 6.3.1.** *All groups with two elements are isomorphic*

*Proof.* If  $G$  has two elements, then its Cayley table looks like

$\cdot$	$\epsilon$	$x$
$\epsilon$	$\epsilon$	$x$
$x$	$x$	$\epsilon$

Except they may use different symbols and have reordered rows/columns, so they are all isomorphic.  $\square$

# Lecture 7

## Automorphisms, Subgroups

### 7.1 Automorphisms

**Example:** Let  $H = \text{symmetries of a rectangle}$  and  $K = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(x, y) : x \in \mathbb{Z}_2, y \in \mathbb{Z}_2\}$

$$H = \{\epsilon, \alpha, \beta, \rho\} \text{ with composition}$$

$$K = \{00, 01, 10, 11\} \text{ with addition in } \mathbb{Z}_2$$

$H$	$\epsilon$	$\alpha$	$\beta$	$\rho$	$G$	00	01	10	11
$\epsilon$	$\epsilon$	$\alpha$	$\beta$	$\rho$	00	00	01	10	11
$\alpha$	$\alpha$	$\epsilon$	$\rho$	$\beta$	01	01	00	11	10
$\beta$	$\beta$	$\rho$	$\epsilon$	$\alpha$	10	10	11	00	01
$\rho$	$\rho$	$\beta$	$\alpha$	$\epsilon$	11	11	10	01	00

$$\phi \left\{ \begin{array}{l} \epsilon \rightarrow 00 \\ \alpha \rightarrow 01 \\ \beta \rightarrow 10 \\ \rho \rightarrow 11 \end{array} \right. \quad \text{or} \quad \phi \left\{ \begin{array}{l} \epsilon \rightarrow 00 \\ \alpha \rightarrow 01 \\ \beta \rightarrow 11 \\ \rho \rightarrow 10 \end{array} \right.$$

In fact, all we need for the isomorphism is  $\epsilon \rightarrow 00$ , we can have  $\alpha, \beta, \rho \rightarrow 01, 10, 11$  in any order.

An **automorphism** of  $G$  is an isomorphism  $G \rightarrow G$ , this is a symmetry group of  $G$ . The set of all automorphisms of  $G$  is a group we call  $\text{aut}(G)$ , the **automorphism group** of  $G$ .

$H$	$\epsilon$	$\alpha$	$\beta$	$\rho$
$\epsilon$	$\epsilon$	$\alpha$	$\beta$	$\rho$
$\alpha$	$\alpha$	$\epsilon$	$\rho$	$\beta$
$\beta$	$\beta$	$\rho$	$\epsilon$	$\alpha$
$\rho$	$\rho$	$\beta$	$\alpha$	$\epsilon$

$H$	$\epsilon$	$\alpha$	$\rho$	$\beta$
$\epsilon$	$\epsilon$	$\alpha$	$\rho$	$\beta$
$\alpha$	$\alpha$	$\epsilon$	$\beta$	$\rho$
$\rho$	$\rho$	$\beta$	$\epsilon$	$\alpha$
$\beta$	$\beta$	$\rho$	$\alpha$	$\epsilon$

Let  $\phi$  be any bijection  $\{\epsilon, \alpha, \beta, \rho\} \rightarrow \{\epsilon, \alpha, \rho, \beta\}$  with  $\phi(\epsilon) = \epsilon$ . Then  $\phi$  is an automorphism of  $H$ .

**Exercise:** Let  $G = \text{the symmetries of an equilateral triangle}$ . Show that

$$\text{aut}(H) \cong G$$

## 7.2 Quaternions

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

$\pm$  and 1 operate as expected. And

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

$Q_8$	1	-1	$i$	$-i$	$j$	$-j$	$k$	$-k$
1	1	-1	$i$	$-i$	$j$	$-j$	$k$	$-k$
-1	-1	1	$-i$	$i$	$-j$	$j$	$-k$	$k$
$i$	$i$	$-i$	-1	1	$k$	$-k$	$j$	$-j$
$-i$	$-i$	$i$	1	-1	$-k$	$k$	$-j$	$j$
$j$	$j$	$-j$	$-k$	$k$	-1	1	$-i$	$i$
$-j$	$-j$	$j$	$k$	$-k$	1	-1	$i$	$-i$
$k$	$k$	$-k$	$j$	$-j$	$-i$	$i$	-1	1
$-k$	$-k$	$k$	$-j$	$j$	$i$	$-i$	1	-1

- **Closure:** Yes,  $Q_8$  is closed.

- **Identity:** 1 is the identity for  $Q_8$ .
- **Inverse:** Every column has the identity (1), so an inverse exists for every element in  $Q_8$ .
- **Associativity:** Consider the set of matrices  $M_8$  with entries in  $\mathbb{C}$

$$M_8 = \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \pm \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \right\}$$

And the function  $\phi : M_8 \rightarrow Q_8$

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

$\phi : M_8 \rightarrow Q_8$  is a bijection

$$\phi(ab) = \phi(a)\phi(b)$$

Because  $M_8$  is a set of matrices, it is closed, associative, has an identity and has inverses, therefore  $M_8$  is a group.  $Q_8$  is isomorphic to  $M_8$ , so it follows that it is also a group.

Therefore,  $Q_8$  is closed, has identity, has inverses and is associative.

## 7.3 Subgroups

Consider the following

- $G$  is a group with operation  $\cdot$
- $H$  is a subset of  $G$
- $H$  is a group with the same operation  $\cdot$

Then  $H$  is a **subgroup** of  $G$ . We denote subgroups as  $H \leq G$  or  $H < G$

$$(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$$

**Example:**

$$(\mathbb{Z}_3, +) \not\leq (\mathbb{Z}_5, +)$$



This is the case because

$$\mathbb{Z}_3 = \{0, 1, 2\} = \{[0], [1], [2]\} \not\subseteq \{[0], [1], [2], [3], [4]\} = \{0, 1, 2, 3, 4\} = \mathbb{Z}_5$$

These sets are equivalence classes **not** numbers so they are not subsets of each other.

### 7.3.1 Subgroup Test

**Proposition 7.3.1.** *Suppose  $H$  is a subset of  $G$ , if  $H \neq \emptyset$*

$$x, y \in H \implies xy \in H$$

$$x \in H \implies x^{-1} \in H$$

*then  $H$  is a subgroup.*

*Proof.* Show that  $H$  is a group

- **Closure:** Is given.
- **Associative:**  $G$  is associative so any subset "inherits" associativity.
- **Identity:** Let  $\epsilon_g$  be the identity in  $G$ .  $\epsilon_a \cdot a = a \forall a \in H$ .  $\exists a \in H$ , so  $a^{-1} \in H$ , since  $H$  is a subset of  $G$ ,  $a, a^{-1} \in G$ , therefore  $a \cdot a^{-1} = \epsilon_g \in H$ .
- **Inverse:** Given

□

**Proposition 7.3.2.**  *$H$  a subgroup of  $G \implies \epsilon_g \in H$  and so  $\epsilon_H \in G$*

*Proof.*  $H \neq \emptyset$ , so let  $x \in H$ , then  $x^{-1} \in H$ , then  $x \cdot x^{-1} = \epsilon_G \in H$ . Furthermore

$$\epsilon_G \cdot h = h \cdot \epsilon_G = h \forall h \in H$$

Since  $H \subseteq G$ , and  $H$  has a unique identity, then  $\epsilon_G = \epsilon_H$

□

### 7.3.2 Alternative Versions of Subgroup Test

Suppose  $H$  is a subset of  $G$ , if

- $H \neq \emptyset$

- $x, y \in H \implies xy \in H$

- $x \in H \implies x^{-1} \in H$

then  $H$  is a subgroup.

## Lecture 8

# Lattices and Cyclic Groups

**Recall:**  $H$  is a subgroup of  $G$  if

- $H \subseteq G$
- They have the same operation (Cayley table of  $H$  is obtained by deleting rows/columns from  $G$ )
- $H$  is a group

**Subgroup Test:** If  $H \subseteq G$  with the same operation and  $H$  is not empty,

$$x, y \in H \implies xy \in H$$

$$x \in H \implies x^{-1} \in H$$

then  $H$  is a subgroup of  $G$ .

### 8.1 Find all subgroups of $(\mathbb{Z}, +)$

Say  $H$  is a subgroup of  $\mathbb{Z}$ ,  $H \neq \{0\}$ . Let  $n$  be the smallest positive integer in  $H$ , then

$$\{\dots, -n, 0, n, 2n, 3n, \dots\} \subseteq H$$

$$n\mathbb{Z} = \{nK : K \in \mathbb{Z}\} \subseteq H$$

Suppose  $x \in H \setminus n\mathbb{Z}$ , then write  $x = qn + r$  for  $0 \leq r < n$ . By closure, we have

$$x - qn = r \in H$$

But, this contradicts the minimality of  $n$  unless  $r = 0$ , but if  $r = 0$ , then  $x \in n\mathbb{Z}$ .  
Therefore,  $H = n\mathbb{Z}$

**Subgroups of  $\mathbb{Z}$ :**  $n\mathbb{Z} \forall n \in \mathbb{Z}, (n = 0 \implies H = \{0\})$

## 8.2 Symmetries of a Square

**Lemma 8.2.1.** *There are at most eight symmetries of a square.*

*Proof.* Let  $\gamma$  be a symmetry,  $\gamma$  maps corners to corners.

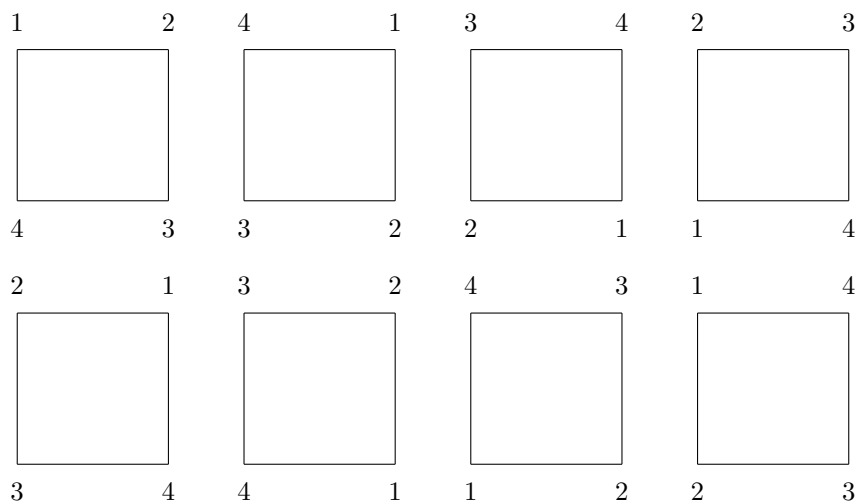
- $\gamma(1)$  has at most four possibilities, then  $\gamma(2)$  must be one of the corners adjacent to  $\gamma(1)$
- $\gamma(2)$  has at most two possibilities, then  $\gamma(4)$  must be the other corner adjacent to  $\gamma(1)$
- $\gamma(4)$  has at most one possibility, then  $\gamma(3)$  must be  $\{1, 2, 3, 4\} \setminus \{\gamma(1), \gamma(2), \gamma(3), \gamma(4)\}$
- $\gamma(3)$  has at most one possibility

So, we have  $4 \cdot 2 \cdot 1 \cdot 1 = 8$  possibilities. □

**Question:** Do all possibilities work?

**Lemma 8.2.2.** *There are at least eight symmetries of a square*

*Proof.* Consider the symmetries of a square.



□

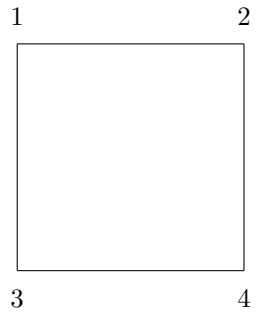
Let

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

**Proposition 8.2.1.**

$$\rho\mu = \mu\rho^{-1} = \mu\rho^3$$

*Proof.* Consider the square and function  $\mu, \rho$ .



$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\begin{aligned} \rho\mu &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 2 & 1 & 4 \end{pmatrix} & \mu\rho^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 2 & 1 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} & & = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \end{aligned}$$

The 2 functions are equal.

□

**Example:**

$$\rho^2\mu\rho\mu\rho^3 = \mu\rho^6\rho\mu\rho^3 = \mu\rho^7\mu\rho^3 = \mu\mu\rho^{21}\rho^3 = \mu\rho^{24} = \epsilon$$

$$\mu\rho\mu\rho^2\mu\rho = \mu\mu\rho^3\rho^2\mu\rho = \mu^2\rho^5\mu\rho = \rho\mu\rho = \mu\rho^3\rho = \mu\rho^3\rho = \mu$$

**Corollary 8.2.1.**

$$\begin{aligned} G &= \langle \mu, \rho : \mu^2 = \epsilon, \rho^4 = \epsilon, \rho\mu = \mu\rho^3 \rangle \\ &= \{\mu^i \rho^j : 0 \leq i \leq 1, 0 \leq j \leq 3\} \\ &= \{\rho^i \mu^j : 0 \leq i \leq 1, 0 \leq j \leq 3\} \end{aligned}$$

*Proof.* Any sequence of  $\mu$ 's and  $\rho$ 's can be written as  $\mu^s \rho^t$  using  $\rho\mu = \mu\rho^3$  ( $\rho^t \mu^s$  using  $\mu\rho = \rho^3 \mu$ ) reduce powers on  $\mu$  and  $\rho$  using  $\mu^2 = \epsilon$   $\rho^4 = \epsilon$

$$G = \{\mu^i \rho^j : 0 \leq i \leq 1, 0 \leq j \leq 3\}$$

These are all distinct since  $|G| = 8$  so the relations  $\mu^2 = \epsilon$   $\rho^4 = \epsilon$   $\rho\mu = \mu\rho^3$  are sufficient to characterize  $G$   $\square$

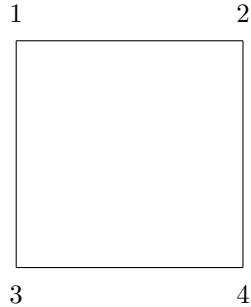
**Compare:**

$$F = \langle \alpha, \beta : \alpha^2 = \epsilon, \beta^4 = \epsilon \rangle$$

$\alpha\beta, \alpha\beta\alpha, \alpha\beta\alpha\beta, \dots$  are all distinct

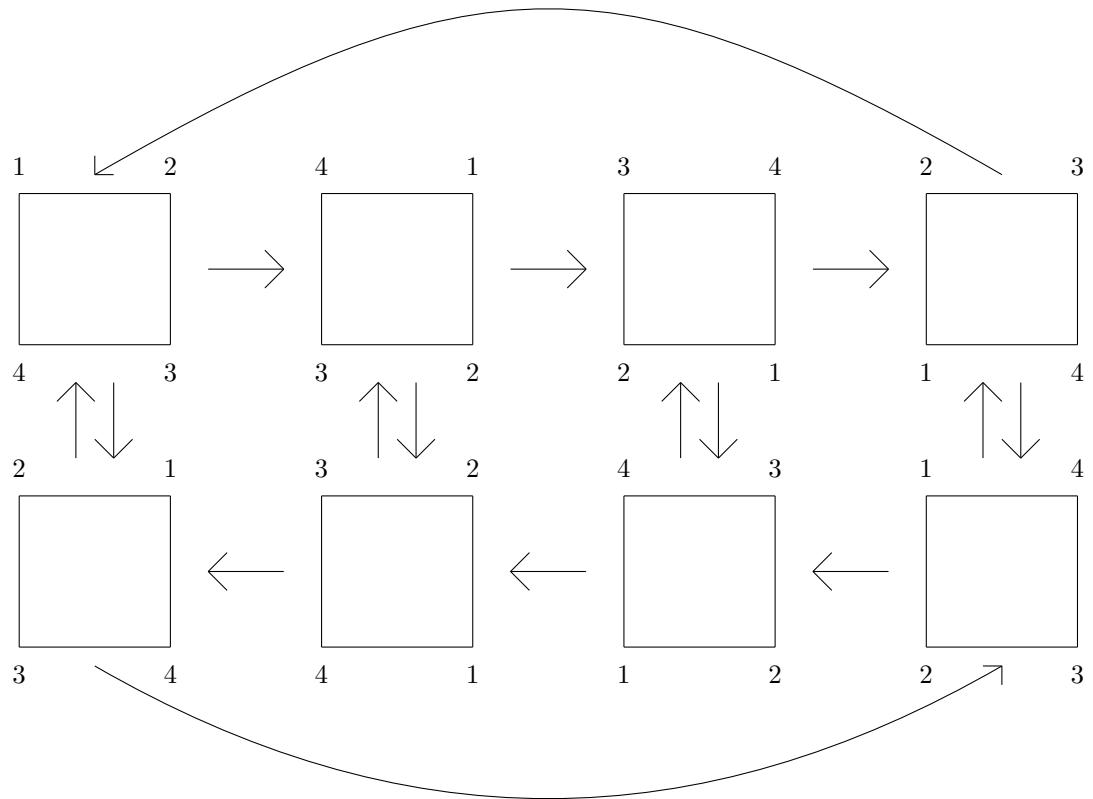
$$\alpha^3 \beta^7 \alpha \beta = \alpha \beta^3 \alpha \beta$$

$$|F| = \infty$$



$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\begin{aligned} G &= \{\mu^i \rho^j : 0 \leq i \leq 1, 0 \leq j \leq 3\} \\ &= \{\rho^i \mu^j : 0 \leq i \leq 1, 0 \leq j \leq 3\} \end{aligned}$$



Elements of  $G$  are symmetries of a square, they also permute  $G$  itself! But they are not symmetries of  $G$ .

$$\mu \cdot \rho = \mu\rho$$

$$\mu\mu\rho = \mu(\mu)\mu(\rho) \neq \mu(\mu\rho) = \mu\mu\rho$$

### 8.2.1 Subgroups of Symmetries of a Square

$$G = \text{Sym}(\square) = \{\mu^i \rho^j : 0 \leq i \leq 1, 0 \leq j \leq 3\}$$

$\langle \epsilon \rangle = \{\epsilon\}$	$\langle \mu, \rho \rangle = G = \langle \mu, \rho^3 \rangle$
$\langle \mu \rangle = \{\epsilon, \mu\}$	$\langle \mu, \rho^2 \rangle = \{\epsilon, \mu, \rho^2, \mu\rho^2\}$
$\langle \rho \rangle = \{\epsilon, \rho, \rho^2, \rho^3\}$	
$\langle \rho^2 \rangle = \{\epsilon, \rho^2\}$	$\langle \mu, \mu\rho \rangle = \{\epsilon, \mu, \rho, \dots\} = G$
$\langle \rho^3 \rangle = \{\epsilon, \rho^3, \rho^2, \rho\}$	$\langle \mu, \mu\rho^3 \rangle = \{\epsilon, \mu, \rho^3, \dots\} = G$
$\langle \mu\rho \rangle = \{\epsilon, \mu\rho\}$	$\langle \mu, \mu\rho^2 \rangle = \{\epsilon, \mu, \rho^2, \mu\rho^2\}$
$\langle \mu\rho^2 \rangle = \{\epsilon, \mu\rho^2\}$	
$\langle \mu\rho^3 \rangle = \{\epsilon, \mu\rho^3\}$	$\langle \rho, \mu\rho \rangle = \{\epsilon, \mu, \rho, \dots\} = G$
	$\langle \rho, \mu\rho^3 \rangle = \{\epsilon, \mu, \rho, \dots\} = G$
	$\langle \rho, \mu\rho^2 \rangle = \{\epsilon, \mu, \rho, \dots\} = G$
	$\langle \rho^2, \mu\rho^2 \rangle = \{\epsilon, \rho^2, \mu\rho, \mu\rho^3\} = G$
	$\langle \rho^2, \mu\rho^3 \rangle = \{\epsilon, \rho^2, \mu\rho^3, \mu\rho\} = G$
	$\langle \rho^2, \mu\rho^2 \rangle = \{\epsilon, \rho^2, \mu\rho^2, \mu\} = G$
	$\langle \mu\rho, \mu\rho^2 \rangle = \{\epsilon, \rho, \mu, \dots\} = G$
	$\langle \mu\rho, \mu\rho^3 \rangle = \{\epsilon, \mu\rho, \mu\rho^3, \rho^2\} = G$
	$\langle \mu\rho^2, \mu\rho^3 \rangle = \{\epsilon, \rho, \mu, \dots\} = G$



## Lecture 9

# Cyclic Groups

### 9.1 Cyclic Groups

$G$  is **cyclic** if  $G = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$  for some  $g \in G$ .  $g$  is a **generator** of  $G$ , there could be other generators. For addition,

$$G\langle g \rangle = \{kg : k \in \mathbb{Z}\}$$

The **order of  $g$**  is the smallest positive integer  $n$  with  $g^n = \epsilon$ , written as  $|g|$ . For addition, it's the smallest positive integer  $n$  with  $ng = \epsilon$ .

**Proposition 9.1.1.**  $G$  is cyclic  $\implies G$  is abelian

*Proof.* Since  $G$  is cyclic, then  $G = \langle g \rangle$  for some  $g \in G$ , take  $x, y \in G$ . Then  $x = g^s$  and  $y = g^t$ . So

$$xy = g^s g^t = g^{s+t} = g^{t+s} = g^t g^s = yx$$

□

However,  $G$  being abelian  $\not\Rightarrow G$  is cyclic. **Examples:** Are the following in cyclic? Find generators, and all orders

$Q_8$ :

- $\langle 1 \rangle = \{1\}$  Order 1
- $\langle -1 \rangle = \{-1, 1\}$  Order 2

- $\langle i \rangle = \{i, -1, -i, 1\}$  Order 4
- $\langle -i \rangle = \{-i, -1, i, 1\}$  Order 4
- $\langle \pm j \rangle = \{\pm j, -1, \mp j, 1\}$  Order 4
- $\langle \pm k \rangle = \{\pm k, -1, \mp k, 1\}$  Order 4

Not cyclic

$\mathbb{Z}$ :

- $\langle 1 \rangle = \{k \cdot 1 : k \in \mathbb{Z}\} = \mathbb{Z}$  Order is  $\infty$ , so no finite order

Are there other generators? Consider  $-1$

- $\langle -1 \rangle = \{k \cdot (-1) : k \in \mathbb{Z}\} = \mathbb{Z}$

$\mathbb{Z}_5$ :

- $\langle 1 \rangle = \{1, 2, 3, 4, 5 = 0\}$  Order 5
- $\langle 2 \rangle = \{2, 4, 6 = 1, 3, 5 = 0\}$  Order 5
- $\langle -2 \rangle = \langle 3 \rangle = \{3, 1, 4, 2, 5 = 0\}$  Order 5
- $\langle -1 \rangle = \langle 4 \rangle = \{4, 3, 2, 1, 5 = 0\}$  Order 5
- $\langle 0 \rangle = \{0\}$

Therefore  $\langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle$  generate the group, so it is cyclic.  $\mathbb{Z}_9^\times$ :

- $\langle 1 \rangle = \{1\}$  Order 1
- $\langle 2 \rangle = \{2, 4, 8, 16 = 7, 14 = 5, 10 = 1\}$  Order 6
- $\langle -4 \rangle = \langle 4 \rangle = \{4, 7, 1\}$  Order 3
- $\langle -2 \rangle = \langle 5 \rangle = \{5, 7, 8, 4, 2, 1\}$  Order 6
- $\langle -1 \rangle = \langle 8 \rangle = \{8, 1\}$  Order 2

Therefore  $\langle 2 \rangle$  and  $\langle 5 \rangle$  generate the group, so it is cyclic.

$\mathbb{Z}_8^\times$

- $\langle 1 \rangle = \{1\}$  Order 1

- $\langle 3 \rangle = \{3, 1\}$  Order 2
- $\langle 5 \rangle = \{5, 1\}$  Order 2
- $\langle 7 \rangle = \{7, 1\}$  Order 2

Therefore not cyclic.

$\mathbb{Q}$ :

- $\langle 1 \rangle = \mathbb{Z}$
- $\langle 0 \rangle = \{0\}$
- $\langle q \rangle = q\mathbb{Z}, q \in \mathbb{Q}$

Therefore not cyclic.

$\mathbb{R}$ :

- $\langle 1 \rangle = \mathbb{Z}$
- $\langle 0 \rangle = \{0\}$
- $\langle r \rangle = r\mathbb{Z}$

Therefore not cyclic.

*Note:  $q\mathbb{Z} \cong \mathbb{Z}$  and  $r\mathbb{Z} \cong \mathbb{Z}$*

$\mathbb{Z}_2 \times \mathbb{Z}_4$ :

- $\langle 00 \rangle = \{00\}$  Order 1
- $\langle 01 \rangle = \{01, 02, 03, 00\}$  Order 4
- $\langle 02 \rangle = \{02, 00\}$  Order 2
- $\langle 03 \rangle = \{03, 02, 01, 00\}$  Order 4
- $\langle 10 \rangle = \{10, 00\}$  Order 2
- $\langle 11 \rangle = \{11, 02, 13, 00\}$  Order 4
- $\langle 12 \rangle = \{12, 00\}$  Order 2
- $\langle 13 \rangle = \{13, 02, 11, 00\}$  Order 4

Therefore not cyclic.

$\mathbb{Z}_2 \times \mathbb{Z}_3$ :

- $\langle 00 \rangle = \{00\}$  Order 1
- $\langle 01 \rangle = \{01, 02, 00\}$  Order 3
- $\langle 02 \rangle = \{02, 01, 00\}$  Order 3
- $\langle 10 \rangle = \{10, 00\}$  Order 2
- $\langle 11 \rangle = \{11, 02, 10, 01, 12, 00\}$  Order 6
- $\langle 12 \rangle = \{12, 01, 10, 02, 11, 00\}$  Order 6

Therefore cyclic

**Proposition 9.1.2.**  *$G$  is cyclic  $\implies$  all subgroups of  $G$  are cyclic*

*Proof.* Let  $G = \langle a \rangle = \{a^i : i \in \mathbb{Z}\}$ . Let  $H$  be a sub group of  $G$ .

$$H = \{a^i : \text{some } i \in \mathbb{Z}\}$$

could be  $H = \{a^0\} = \{\epsilon\}$ . Let

$$n = \min\{k : a^k \in H, k > 0\}$$

$$\langle a^n \rangle = \{(a^n)^k : k \in \mathbb{Z}\} = \{a^{kn} : k \in \mathbb{Z}\} = \{a^k : k \in n\mathbb{Z}\}$$

$$\langle a^n \rangle \leq H \leq G$$

Suppose  $a^j \in H$  with  $j \notin \mathbb{Z}$  so  $\langle a^n \rangle \neq H$ . Then

$$j = qn + r \quad 0 \leq r < n \quad r \neq 0$$

So

$$a^r = a^{j-qn} = a^j(a^n)^{-q} \in H$$

This contradicts the minimality of  $n$ . Therefore  $H = \langle a^n \rangle$ . □

**Definition 9.1.1** (Order). *The **order** of an element  $g \in G$  is the smallest positive integer  $n$  such that  $g^n = \epsilon$ . We write  $|g|$  for the order of  $g$ , if no such  $n$  exists we say  $|g| = \infty$ .*

**Proposition 9.1.3.** Suppose  $|a| = n < \infty$ , then

$$a^j = \epsilon \iff n|j$$

In other words,

$$\{j : a^j = \epsilon\} = n\mathbb{Z}$$

Furthermore,

$$a^s = a^t \iff n|s - t$$

**Example:**  $|a| = 5$

$$a^5 = a^{10} = a^{-15} = a^{1005} = \dots = \epsilon$$

$a^j \neq \epsilon$  when  $j$  is not a multiple of 5.

*Proof.*  $\Leftarrow$  if  $n|j$  then  $j = tn$  for some  $t \in \mathbb{Z}$

$$a^j = a^{tn} = (a^n)^t = \epsilon^t = \epsilon$$

$\Rightarrow$  : if  $a^j = \epsilon$ , then write  $j = qn + r$  for  $0 \leq r < n$

$$a^r = a^{j-qn} = (a^n)^{-q} = \epsilon(\epsilon^{-q}) = \epsilon$$

but  $n$  is the smallest positive integer with  $a^n = \epsilon$ , so  $0 \leq r < n$  implies  $r = 0$ .  
Therefore  $j = nq$  and  $n | j$ .  $\square$

Also,

$$a^s = a^t \iff a^{s-t} = \epsilon \iff n|s - t$$

**Corollary 9.1.1.**  $|a| = |b|$  is equivalent to

$$a^j = \epsilon \iff b^j = \epsilon$$

**Proposition 9.1.4.** Suppose  $a \in G$ ,  $|a| = n < \infty$ ,  $k \in \mathbb{Z}$ . Then

$$|a^k| = \frac{n}{\gcd(k, n)}$$

**Example:**  $|a| = 12$

- $\langle a^1 \rangle = \{a^1, a^2, a^3, \dots, a^{12}\}$

- $\langle a^5 \rangle = \{a^5, a^{10}, a^3, \dots, a^{12}\} = \langle a \rangle$
- $\langle a^4 \rangle = \{a^4, a^8, a^{12} = a^0\}$
- $\langle a^{10} \rangle = \{a^{10}, a^8, a^6, a^4, a^2, a^0\}$

*Proof.* Let  $|a^k| = m$ , then  $\epsilon = (a^k)^m = a^{km}$ . Therefore,  $n|km$  and  $km$  is a multiple of  $|a|$  by the previous theorem. Let  $d = \gcd(kn)$  and set

$$\begin{cases} n = n'd \\ k = k'd \end{cases}$$

$$\gcd(n', k') = 1$$

Since  $n|km$  for some  $t \in \mathbb{Z}$  we have,

$$km = tn$$

$$dk'm = tdn'$$

$$k'm = tn'$$

$$m = \frac{tn'}{k'} = \frac{t}{k'} \cdot n'$$

This must be an integer because  $\gcd(k', n') = 1 \implies k' \mid t$ . Smallest  $m \iff$  smallest  $t$  with  $\frac{tn'}{k'}$  positive integer. So  $\square$

**Corollary 9.1.2.** Suppose  $G = \langle a \rangle$ , with  $|a| = n < \infty$ , then the generators of  $G$  are  $\{a^k : \gcd(n, k) = 1\}$

*Proof.*

$$|a^k| = \frac{n}{\gcd(n, k)} = n \iff \gcd(n, k) = 1$$

$\square$

**Corollary 9.1.3.**  $\mathbb{Z}_n = \langle 1 \rangle$  and  $|1| = n$ . Generators of  $\mathbb{Z}$  with addition are

$$\{k \cdot 1 : \gcd(n, k) = 1\} = \{k : \gcd(n, k) = 1\} = \mathbb{Z}_n^\times$$

**Corollary 9.1.4.** all nonzero elements of  $\mathbb{Z}_n$  are generators of  $\mathbb{Z}_n \iff n$  is prime

*Proof.* We want  $|k| = \frac{n}{\gcd(n, k)} = n$  for  $k = 1, 2, 3, \dots, n-1$ . So  $\gcd(n, k) = 1$   $\square$

## Lecture 10

# Subgroups of Cyclic Groups, Lattices, $\mathbb{T}$

- $G$  **cyclic** means there exists  $g \in G$  with  $G = \langle g \rangle = \{g^k : k \in \mathbb{Z}\}$
- The **order** of an element  $g$  is the smallest positive integer  $n$  with  $g^n = \epsilon$
- Notation: **Order of an element**  $g$  is written  $|g|$ . **Order (=size!) of a group**  $G$  is written  $|G|$ .  $|g| = \infty$  means  $g^k \neq \epsilon \forall k \in \mathbb{Z}$
- $\{k : g^k = \epsilon\} = |g|\mathbb{Z}$  so  $g^k = \epsilon \iff |g| \text{ divides } k$
- $|x| = |y|$  is equivalent to  $x^k = \epsilon \iff y^k = \epsilon$
- if  $|g| = n < \infty$ , then

$$G = \langle g \rangle = \{g, g^2, \dots, g^n = \epsilon\}$$

$$|G| = |g|$$

$$|g^k| = \frac{n}{\gcd(n, k)}$$

generators of  $G$  are exactly  $\{g^k : \gcd(n, k) = 1\}$

**Corollary 10.0.1.** *All nonzero elements of  $\mathbb{Z}_n$  are generators of  $\mathbb{Z}_n \iff n$  is prime.*

*Proof.* We want  $k = \frac{n}{\gcd(n, k)} = n$  for  $k = 1, 2, 3, \dots, n-1$ . So  $\gcd(n, k) = 1$  for  $k = 1, 2, 3, \dots, n-1$ . Therefore  $n$  is prime.  $\square$

**Theorem 10.0.1.**  $G$  has no subgroups other than  $\{\epsilon\}$  and  $G \iff G$  is cyclic of prime order  $\iff |G|$  is prime.

*Proof.* Suppose  $g \in G$ , then  $\langle g \rangle$  is a subgroup of  $G$ . Therefore, either  $\langle g \rangle = G$  or  $\langle g \rangle = \{\epsilon\}$ .  $g$  is a generator of  $G$  So

$$G = \{g, g^2, g^3, \dots, g^n = \epsilon\}$$

$g^k$  is a generator for  $k = 1, 2, \dots, n-1$  Therefore,

$$\frac{n}{\gcd(n, k)} = n$$

So  $n$  is prime, therefore  $G$  is cyclic of prime order  $G \cong \mathbb{Z}_n$  for  $n$  prime.

Conversely,

$$G = \{g, g^2, \dots, g^n = \epsilon\}$$

then  $S \neq \emptyset$  and  $S \neq \{\epsilon\} \implies \langle S \rangle = G$ . So  $x \in S$ ,  $x = g^k$  then

$$|x| = |g^k| = \frac{n}{\gcd(n, k)}$$

So the only subgroups are  $\{\epsilon\}$  and  $G$  □

**Theorem 10.0.2.** Suppose  $G, H$  are both cyclic,  $G \cong H \iff |G| = |H|$

*Proof.* ( $\implies$ ) an isomorphism is a bijection.

( $\longleftarrow$ )  $G = \langle a \rangle$  and  $H = \langle b \rangle$ , then

$$|a| = |G| = |H| = |b|$$

define

$$\phi : G \rightarrow H$$

$$\phi(a^k) = b^k$$

We have 2 cases, either the order is infinite.

$$\begin{cases} G = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\} \\ H = \{\dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots\} \end{cases}$$



Or their order is finite

$$\begin{cases} G = \{a, a^2, a^3, \dots, a^n \epsilon\} \\ H = \{b, b^2, b^3, \dots, b^n = \epsilon\} \end{cases}$$

In both cases  $\phi$  is a bijection.

$$\phi(a^s a^t) = \phi(a^{s+t}) = b^{s+t} = b^s b^t = \phi(a^s) \phi(a^t)$$

□

**Subgroups of  $C_n = \langle a \rangle = \{a, a^2, \dots, a^n\}$**

- $C_n$  is cyclic, therefore all subgroups are cyclic
- $|a^k| = \frac{n}{\gcd(k, n)}$
- Let  $d \mid n$  then  $|a^d| = \frac{n}{\gcd(d, n) = \frac{n}{d}}$

So for each  $d \mid n$ , then  $\langle a \rangle^d \cong C_{\frac{n}{d}}$  is a subgroup.

No let  $k \in \{1, 2, 3 \in n\}$ . Suppose  $\gcd(k, n) = d$  for some  $d \mid n$ , then

$$k \in \{d, 2d, 3d, \dots, \frac{n}{d}d\}$$

So  $a^k \in \langle a^d \rangle$ . i.e. all elements of order  $\frac{n}{d}$  are contained in the subgroup  $\langle a^d \rangle$

**Conclusion:** For all  $d \mid n$ , there is a unique subgroup of  $C_n$  of order  $\frac{n}{d}$ , generated by  $a^d$ .

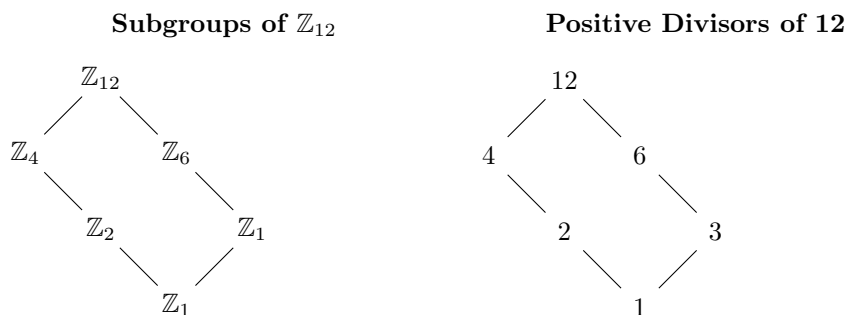
**Example:**  $n = 2$ .  $C_{12} = \langle a \rangle = \{a, a^2, a^3, \dots, a^{11}, a^{12}\}$

- **Order 12:**  $a^1, a^5, a^7, a^{11} \langle a \rangle = C_{12} = \langle a^5 \rangle = \langle a^7 \rangle = \langle a^{11} \rangle$
- **Order 6:**  $a^2, a^{10} \langle a^2 \rangle = \{a^2, a^4, a^6, a^8, a^{10}, a^{12}\} = \langle a^{10} \rangle$
- **Order 4:**  $a^3, a^9 \langle a^3 \rangle = \{a^3, a^6, a^9, a^{12}\} = \langle a^9 \rangle$
- **Order 3:**  $a^4, a^8 \langle a^4 \rangle = \{a^4, a^8, a^{12}\} = \langle a^8 \rangle$
- **Order 2:**  $a^6 \langle a^6 \rangle = \{a^6, a^{12}\}$
- **Order 1:**  $a^2 \langle a^2 \rangle = \{a^{12}\}$

**Example:**  $n = 12$   $\mathbb{Z}_{12} = \{1, 2, 3, \dots, 12\}$

- **Order 12:**  $1, 5, 7, 11$   $\langle 1 \rangle = \mathbb{Z}_{12} = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle$
- **Order 6:**  $2, 10$   $\langle 2 \rangle = \{2, 4, 6, 8, 10, 12\} = \langle 10 \rangle$
- **Order 4:**  $3, 9$   $\langle 3 \rangle = \{3, 6, 9, 12\} = \langle 9 \rangle$
- **Order 3:**  $4, 8$   $\langle 4 \rangle = \{4, 8, 12\} = \langle 8 \rangle$
- **Order 2:**  $6$   $\langle 6 \rangle = \{6, 12\}$
- **Order 1:**  $12$   $\langle 12 \rangle = \{12\}$

### 10.0.1 Lattices



Cyclic groups with subgroups  $\cong$  integers with divisibility

## 10.1 Complex Numbers

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$$

$$\mathbb{C} = \{re^{i\theta} : r, \theta \in \mathbb{R}\}$$

**Lemma 10.1.1.**

$$e^{i\theta} = \cos \theta + i \sin \theta$$

$$z = re^{i\theta} = re^{i(\theta+2k\pi)} = -re^{i(\theta+(2k+1)\theta)}$$

$$z = re^{i\theta} = r \cos \theta + ir \sin \theta$$

$$\begin{cases} |z| = |a + bi| = \sqrt{a^2 + b^2} = r \\ \frac{b}{a} = \tan \theta \end{cases}$$

Refer to the profs notes for the rest of the complex number stuff.

## Lecture 11

# Subgroups of $\mathbb{T}$ , Permutations, Disjoint Cycles

### 11.1 Subgroups of a Finite Cyclic Subgroup

$G = \langle g \rangle$  with  $|g| = |G| = n = md$ , choose  $r$  with  $\gcd(n, r) = d$ , then

$$|g^r| = \frac{n}{\gcd(n, r)} = \frac{n}{d} = m$$

Any subgroup of order  $m$  can be obtained this way. If

$$H = \langle g^r \rangle$$

is a subgroup of  $G$  of order  $m$ , then

$$H = \langle g^r, g^{2r}, \dots, g^{mr} = \epsilon \rangle \text{ and } |g| = n = |nr|$$

Furthermore,

$$(g^{tr})^m = (g^{mr})^t = (\epsilon)^t = \epsilon$$

So  $H$  consists of  $m$  elements and  $x \in H \rightarrow x^m = \epsilon$ . So

$$\begin{aligned}
 x^m = (g^k)^m = \epsilon &\iff g^{km} = \epsilon \\
 &\iff |g| \text{ divides } km \\
 &\iff n \mid km \\
 &\iff dm \mid km \\
 &\iff k \text{ is a multiple of } d \\
 &\iff x \in \{g^d, g^{2d}, \dots, g^{md}\}
 \end{aligned}$$

$$\left. \begin{aligned} |g| = n = md \\ |g^r| = m \end{aligned} \right\} \implies \langle g^r \rangle = \{x : x^m = \epsilon\}$$

**Proposition 11.1.1.** Let  $x = (a_1, a_2, \dots, a_t) \in G_1 \times G_2 \times \dots \times G_t$ , then  $|x| = (|a_1|, |a_2|, \dots, |a_t|)$

*Proof.*  $x^k = \epsilon$  means  $(a_i)^k = \epsilon_i \forall i = 1, 2, \dots, t$ ,  $k$  is a multiple of each  $|a_i|$  smallest such  $k$  is  $\text{lcm}(|a_1|, |a_2|, \dots, |a_t|)$ .  $\square$

**Proposition 11.1.2.** Let  $G_1, G_2, \dots, G_t$  be finite groups.

$$G_1 \times G_2 \times \dots \times G_t \text{ cyclic} \iff \begin{cases} \text{each } G_i \text{ is cyclic} \\ \gcd(|G_i|, |G_j|) = 1 \forall 1 \leq i < j \leq t \end{cases}$$

*Proof.* See assignment 3.  $\square$

Subgroups of

$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$$

$$R = \{e^{2\pi i j/n} : 0 \leq j < n, n \geq 1\}$$

Consider only reduced fractions  $\gcd(i, n) = 1$  so

$$e^{2\pi i 4/12} \rightarrow e^{2\pi i 1/3}$$

then  $e^{2\pi i j/n}$  generates

$$R_n = \{e^{2\pi i j/n} : 0 \leq j < n\}$$

order of  $e^{2\pi i j/n}$  is  $n$  finite. If  $S \subseteq R$ , then let  $m = \text{lcm}$  of all the  $n$ , then

- $S \subseteq \langle e^{2\pi i 1/m} \rangle$
- $e^{2\pi i 1/m} \in \langle S \rangle$
- So  $\langle S \rangle = \langle e^{2\pi i 1/m} \rangle$

every finite subgroup is cyclic.

Suppose  $S \subseteq R$ . Choose

TBC

## Lecture 12

## Lecture 13



## Lecture 14

## Lecture 15

## Lecture 16

## Lecture 17

## Lecture 18

## Lecture 19

# Normal Subgroups, Quotient Groups

**Recall:** The external direct product is defined as

$$H, K \text{ groups} \implies G = H \times K = \{(x, y) : x \in H, y \in K\}$$

The internal direct product is defined on subgroups  $H, K$  of  $G$  with

$$H \cap K = \{\epsilon\}$$

$$xy = yx \quad \forall x \in H \quad y \in K$$

**Uniqueness:** If  $G = HK$  as an internal direct product, then  $\forall g \in G, \exists! x \in H, y \in K$  such that  $g = xy$ .

**Isomorphisms:** If  $G = H \times K$  as an external direct product, then

$$G = (H \times \{\epsilon\})(\{\epsilon\} \times K)$$

as an internal direct product. If  $G = HK$  as an internal direct product then  $G \cong H \times K$  as an external direct product.

**Theorem 19.0.1.** *If  $G = HK$  as internal direct product, then*

$$G \cong H \times K$$

*Proof.* For  $g \in G$ ,  $\exists! x \in H, y \in K$  such that  $g = xy$ . Define

$$\psi : G \mapsto H \times K$$

by  $\psi(g) = (x, y)$ . So

$$\left. \begin{array}{l} g_1 = x_1 y_1 \\ g_2 = x_2 y_2 \end{array} \right\} \implies g_1 g_2 = x_1 y_1 x_2 y_2 =$$

**Claim:**  $\psi$  is an isomorphism. TBC □

**Theorem 19.0.2.** *If  $G = H \times K$  as an external direct product, then  $G \cong MN$  as an internal direct product where*

$$M = H \times \{\epsilon_K\} \text{ and } N = \{\epsilon_H\} \times K$$

*Proof.* •  $M$  and  $N$  are subgroups of  $G$

$$\bullet (x, y) \in M \implies y = \epsilon_K \text{ and } (x, y) \in N \implies x = \epsilon_H \text{ so}$$

$$(x, y) \in M \cap N \implies (x, y) = (\epsilon_H, \epsilon_K)$$

So  $M \cap N = \{\epsilon\}$

•

$$\begin{aligned} (x, \epsilon_K)(\epsilon_H, y) &= (x\epsilon_H, \epsilon_K y) \\ &= (\epsilon_H x, y\epsilon_K) \\ &= (\epsilon_H y)(x, \epsilon_K) \end{aligned}$$

So  $hK = Kh$  if  $h \in H$  and  $k \in K$

$$\bullet (x, y) \in G \implies (x, y) = (x, \epsilon_K)(\epsilon_H, y) \text{ So } HK = G$$

□

**Example:** Consider  $D_6 = \langle \mu, \rho \rangle$ . Set  $H = \langle \mu \rangle$  and  $K = \langle \rho \rangle$ . Is  $D_6 = HK$  as an inner direct product?

We want to check if  $H \cap K = \{\epsilon\}$ .

$$H = \{\epsilon, \mu\} \quad K = \{\epsilon, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$$

So we have

$$H \cap K = \{\epsilon\}$$

We also want to show that

$$hk = kh \quad \forall h \in H \quad k \in K$$

No, since

$$\rho\mu = \mu\rho^{-1} \neq \rho\mu$$

Is  $D_6 = HK$ ? Yes, since

$$HK = \{hk : h \in H \quad k \in K\} = \{\mu^i \rho^j : 0 \leq i \leq 1 \quad 0 \leq j \leq 5\} = D_6$$

So this is not a direct product.

**Example:** Set  $H = \langle \rho^3 \rangle = \{\epsilon, \rho^3\}$ , and

$$K = \langle \mu, \rho^2 \rangle = \{\epsilon, \mu, \rho^2, \mu\rho^2, \rho^4, \mu\rho^4\}$$

Is  $D_6 = HK$  an inner direct product?

We have that  $\{H \cap K = \{\epsilon\}\}$ . We want to show that

$$hk = kh \quad \forall h \in H \quad k \in K$$

Yes, since  $(\rho^3)^{-1} = \rho^3$ , so  $\mu\rho^3 = \rho^3\mu$ , we can show that  $\rho^3$  commutes with every element in  $K$ . We can also just check that the generator of  $H$  ( $\rho^3$ ) commutes with the generator of  $K$  ( $\mu, \rho^2$ ). Now we want to check if  $D_6 = HK$ .

$$HK = \{hk : h \in H \quad k \in K\} = D_6$$

So this is a direct product.

**Notice:**  $H \cong \mathbb{Z}_2$  and  $K \cong D_3$ . To prove this, we want to show that

$$K = \langle \alpha, \beta : \alpha^2 = \beta^3 = \epsilon, \alpha\beta = \beta^{-1}\alpha \rangle$$

by mapping elements of  $K$  to  $\alpha, \beta$ .

**Question:** For which  $m$  is  $D_{2m} \cong \mathbb{Z}_2 \times D_m$ ?



## 19.1 Normal Subgroups

**Definition 19.1.1.** For  $K < G$ , we say  $K$  is a normal subgroup of  $G$  if

$$gK = Kg \quad \forall g \in G$$

We denote a normal subgroup as

$$K \triangleleft G$$

**Note:**  $gx = xg \forall x \in K \implies gK = Kg$  but  $gK = Kg \not\Rightarrow gx = xg$

**Facts:**

- $G$  abelian  $\implies$  every subgroup is normal
- $K < Z(G) \implies K \triangleleft G$
- $[G : K] = 2 \implies K \triangleleft G$

**Example:**

$$S_3 = \{\epsilon, (23), (13), (12), (123), (132)\}$$

Is  $K = \{\epsilon, (12)\}$  normal in  $S_3$ ?

$$g \in G \implies gK = \{g\epsilon, g(12)\}$$

$$Kg = \{\epsilon g, (12)g\}$$

The following statements are equivalent:

- $K \triangleleft G$
- $gK = Kg \quad \forall g \in G$
- $gKg^{-1} = K \quad \forall g \in G$
- Define  $\phi_g$  by  $\phi_g(x) = gxg^{-1} \quad \forall x \in G$  then  $\phi_g$  maps  $K$  to  $K$

**Lemma 19.1.1.** Suppose  $K \triangleleft G$ , then

$$g_1K = g_2K \iff g_1K = Kg_2 \iff g_1Kg_2^{-1} = K$$

TBC

## 19.2 Quotient Groups

**Definition 19.2.1.** Let  $K \triangleleft G$ . Define a group  $G/K$ , then the elements of the group are the cosets of  $K$  in  $G$ , so

$$G/K = \{gK : g \in G\}$$

The operation is on the representatives of the cosets

$$xK \cdot yK = xyK$$

The order of  $G/K$  is

$$[G : K] = \frac{|G|}{|K|}$$

**Question:** Is this operation well-defined?

$$x_1K = x_2K \quad y_1K = y_2K$$

$$\begin{cases} x_1K \cdot y_1K = x_1y_1K \\ x_2K \cdot y_2K = x_2y_2K \end{cases}$$

From the coset comparison theorem, is  $x_1y_1K = x_2y_2K$ ,  $(x_2y_2)^{-1}x_1y_1 \in K$ ?

$$(x_2y_2)^{-1}x_1y_1 = y_2^{-1}x_2^{-1}x_1y_1 = y_2^{-1}Ky_1$$

Since  $x_1K = x_2K$ ,  $x_2^{-1}x_1 \in K$ . So

$$ky_1 = Ky + 1 = y_1K$$

so

$$ky_1 = y_1k' \text{ some } k' \in K$$

Then

$$(x_2y_2)^{-1}x_1y_1 = y_2^{-1}y_1k' = k''k' \in K$$

$$\therefore x_1y_1K =$$

**Theorem 19.2.1.** If  $K \triangleleft G$ , then  $G/K$  is a group.

*Proof.* • **closure:**  $xK \cdot yK = xyK$

- **Associativity:**

$$aK \cdot (bK \cdot cK) = aK \cdot (bc)K = a(bc)K$$

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

$$a(bc) = (ab)c \text{ since } G \text{ is a group}$$

- **Identity:**

$$aK \cdot \epsilon K = a\epsilon K = aK$$

$$\epsilon K \cdot aK = \epsilon aK = aK$$

- **Inverses:**

$$aK \cdot a^{-1}K = aa^{-1}K = \epsilon K = K$$

$$a^{-1}K \cdot aK = a^{-1}1K = \epsilon K = K$$

□

## Lecture 20

# Quotient Groups

**Recap:** If  $H \triangleleft G$ , then define the quotient group  $G/H$  as

- Elements of  $G/H$  are the cosets  $gH$  for  $g \in G$
- The operation is  $aH \cdot bH = abH$