

# MAT301 Notes

QiLin Xue

May 20, 2021

## Contents

1	Lecture One	1
2	Lecture Two	3
3	Lecture Three	8
4	Lecture Four	10
5	Permutation Groups	14
6	Lecture Six	16

## 1 Lecture One

- Groups are everywhere in mathematics and nature in one of two forms:
  - as groups of symmetries
  - as groups of “numbers” or quantities
- We will call a subset  $F \subseteq \mathbb{R}^n$  a **figure** in  $\mathbb{R}^n$  when we consider  $F$  not just as a set, but as a set together with the structure of its distance functions:

$$d : F \times F \rightarrow \mathbb{R}_{\geq 0}, \quad d(x, y) = \|x - y\| \quad (1)$$

A figure is then defined as the pair  $(F, d)$ .

**Definition:** A **symmetry** of a figure  $F \subseteq \mathbb{R}^n$  is a bijection  $\sigma : F \rightarrow F$  such that  $\sigma$  and  $\sigma^{-1}$  preserve distances:

$$\forall x, y \in F, \quad d(\sigma(x), \sigma(y)) = d(x, y) \quad (2)$$

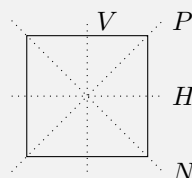
$$\iff d(\sigma^{-1}(x), \sigma^{-1}(y)) = d(x, y) \quad (3)$$

Therefore:

$$\text{Sym}(F) \equiv \{\sigma : F \rightarrow F \mid \sigma \text{ is a symmetry}\} \quad (4)$$

- For example, any point, line, shape, or form is a figure. However, we are only interested in figures that have interesting symmetries.

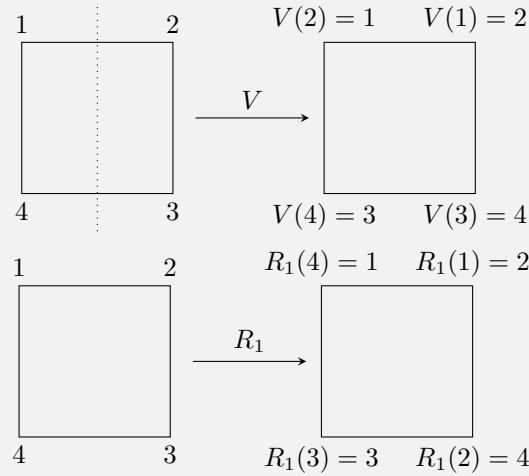
**Example 1:** Let  $F$  be a square in  $\mathbb{R}^2$ . There are four different lines of reflections:



and there are three rotations:  $R_1$ ,  $R_2$ , and  $R_3$ , which represent  $90^\circ$ ,  $180^\circ$ , and  $270^\circ$  clockwise rotations.  $I$

represents the identity transformation (do nothing).

We can combine symmetries. For example, what is  $R_1 \circ V$ ? To do so, we can label the vertices:



Applying the computations:

$$(R_1 \circ V)(1) = R_1(V(1)) = R_1(2) = 3 \quad (5)$$

$$(R_1 \circ V)(2) = R_1(V(2)) = R_1(1) = 2 \quad (6)$$

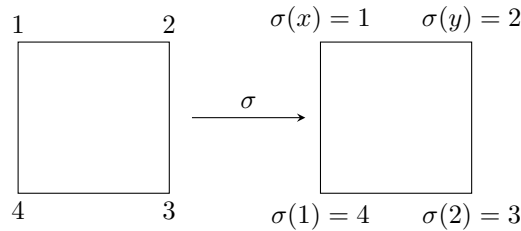
$$(R_1 \circ V)(3) = 1 \quad (7)$$

$$(R_1 \circ V)(4) = 4 \quad (8)$$

Check that  $V \circ R_1 = N$ . Also notice that these operations are not commutative:  $R_1 \circ V \neq V \circ R_1$ .

- In the above example, how are we sure that these are all of the symmetries of a square? To answer this, we will need the following facts:

1. A symmetry maps vertices to vertices. The vertices are the points of the square that are furthest from the center.
2. Symmetries map adjacent vertices to adjacent vertices. If  $x, y$  are adjacent vertices, then  $\sigma(x), \sigma(y)$  are vertices, and  $d(\sigma(x), \sigma(y)) = d(x, y) = \text{side length}$ .
3. A symmetry  $\sigma$  is completely determined by  $(\sigma(1), \sigma(2))$ . For example, suppose we have the symmetry  $\sigma$  on a square such that:



From this, we know that we must have  $y = 3$ , from fact 1, as well as  $x = 4$ .

4. For all  $x, y \in \{1, 2, 3, 4\}$  such that  $x$  is adjacent to  $y$ ,  $\exists!$  symmetry  $\sigma$  of the square such that:

$$(\sigma(1), \sigma(2)) = (x, y) \quad (9)$$

By the above facts, we must count the ordered pairs  $(x, y)$  such that  $x, y \in \{1, 2, 3, 4\}$  and  $x$  is adjacent to  $y$ :

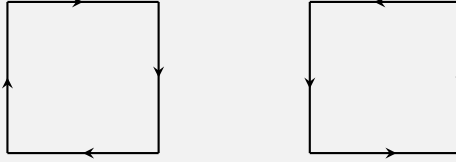
- There are 4 choices for  $x$ .
- For each choice of  $x$ , there are two choices of  $y$ . Therefore, there are  $4 \times 2 = 8$  symmetries.

Since we listed 8 different symmetries of a square, we have therefore defined all of them.

## 2 Lecture Two

- Let  $X$  be a set with some **structures**. Then a symmetry of  $X$  (w.r.t. the structures) is a bijection  $\sigma : X \mapsto X$ , such that  $\sigma$  and  $\sigma^{-1}$  preserve the structures.
- The set of symmetries of  $X$  is denoted as  $\text{Sym}(X)$ .

**Example 2:** We can consider a square not only with the structure of its distance function but with additional structure of its orientations. There are two orientations of a square:



A symmetry of the square with respect to its orientation is a bijection from the square to itself that maps each orientation to itself.

– Rotations preserve orientations, but reflections don't.

Therefore, the symmetries preserving orientations are  $\{I, R_1, R_2, R_3\}$ .

- In general:

0. If  $\sigma_1, \sigma_2 : X \rightarrow X$  are symmetries, then:

$$\sigma_1 \circ \sigma_2 : X \rightarrow X \quad (10)$$

is also a symmetry. Consequently, composition of symmetries restrict a map:

$$\text{Sym}(X) \times \text{Sym}(X) \mapsto \text{Sym}(X), \quad (\sigma_1, \sigma_2) \mapsto \sigma_1 \circ \sigma_2 \quad (11)$$

*Remarks:* A map  $m : S \times S \rightarrow S$  is called a binary operation on  $S$ .

1. Associativity: For all  $\sigma_1, \sigma_2, \sigma_3 \in \text{Sym}(X)$ , we have:

$$(\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1 \circ (\sigma_2 \circ \sigma_3) \quad (12)$$

2. The identity  $\text{id} : X \mapsto X$  is a symmetry and  $\text{id} \in \text{Sym}(X)$ .

3. Immediately from the "definition," we have:  $\sigma \in \text{Sym}(X) \implies \sigma^{-1} \in \text{Sym}(X)$

- The notion of a group is an abstraction of  $\text{Sym}(X)$  and its properties.

**Definition:** A group is an ordered pair  $(G, *)$  consisting of a set  $G$  and a binary operation  $* : G \times G \rightarrow G$  such that:

1.  $*$  is associative,  $\forall g_1, g_2, g_3 \in G$ , we have:

$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3) \quad (13)$$

2. There exists an element  $e \in G$  such that for all  $g \in G$ , we have  $g * e = g = e * g$ .

3. For all  $g \in G$ , there exists an element  $h \in G$  such that  $g * h = e = h * g$ .

These numberings are abstractions of the properties listed above.

- The binary operator  $*$  is called the **group law** or **group operation**. It is often denoted by a dot  $\cdot$  or by juxtaposition ( $gh$  instead of  $g * h$ ).
- The *cardinality* of  $G$ ,  $|G|$ , is called the **order** of  $G$ .
- It is common to denote  $e$  by 1 or  $I$ .

**Warning:** A common *misconceptions* is saying " $G$  is a group" instead of " $(G, *)$  is a group."

- These are equivalent statements:

$$(G, *) \text{ is a group} \quad (14)$$

$$\iff G \text{ is a group under } * \quad (15)$$

**Definition:** A group  $(G, *)$  is **abelian** (or commutative) if for all  $g, h \in G$ , we have:

$$g * h = h * g \quad (16)$$

- Here are some examples of groups:

- $(\text{Sym}(X), \circ)$
- $(\mathbb{Z}, +)$
- $(\mathbb{R}^x, \cdot)$  where:

$$F^x = \{x \in F : \exists y \in F \text{ with } xy = 1 = yx\} \quad (17)$$

- $(\mathbb{Q}_{>0}, \cdot), (\mathbb{R}_{>0}, \cdot)$ .
- $(\mu_n, \cdot)$  where for  $n \in \mathbb{Z}_{>0}$ , let

$$\mu_n = \{z \in \mathbb{C} | z^n = 1\} = \{e^{2\pi ki/n} | k = 0, 1, \dots, n-1\} \quad (18)$$

- $(\mathbb{R}^n, +)$
- $(\text{GL}_n(F), \cdot)$  where  $\text{GL}_n(F) = \{A \in \text{Mat}_{n \times n}(F) | A \text{ invertible}\}$ ,  $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ . For all  $n \geq 2$ ,  $\text{GL}_n(F)$  is non-abelian. Note that GL stands for *general linear*
- $(\text{SL}_n(F), \cdot)$  where  $\text{SL}_n(F) = \{A \in \text{GL}_n(F) | \det A = 1\}$ . Note that SL stands for special linear.
- $(\text{Mat}_{n \times n}(F), +)$

and non-groups:

- $(\mathbb{Z}, \cdot)$
- $(\mathbb{Z}_{>0}, +)$
- $(\mathbb{Z}, -), (\mathbb{Q}^x, \div)$ .
- $(\text{Mat}_{n \times n}(F), \cdot)$

**Proposition 1:** Let  $(G, *)$  be a group. If  $e, e' \in G$  such that  $\forall g \in G$  we have

$$g * e = g = e * g \quad (19)$$

and

$$g * e' = g = e' * g, \quad (20)$$

then  $e = e'$ .

*Proof.* Consider  $e * e'$ . By 19, we have:

$$e * e' = e' \quad (21)$$

Similarly, by 20, we have:

$$e * e' = e \quad (22)$$

Therefore,  $e = e * e' = e'$ .  $\square$

- We call the unique element  $e \in G$  satisfying the second property in the definition of a group, the identity element of  $G$ .
- The **trivial group**: For any singleton  $\{e\}$ , there exists a unique binary operation  $\cdot$  such that:

$$\{e\} \times \{e\} \mapsto \{e\}, \quad (e, e) \mapsto e \quad (23)$$

and  $(\{e\}, \cdot)$  is a group, called a trivial group.

**Proposition 2:** Let  $(G, *)$  be a group and let  $g \in G$ . If  $h, h' \in G$  satisfies:

$$g * h = e = h * g \quad (24)$$

and

$$g * h' = e = h' * g \quad (25)$$

then  $h = h'$ . By 24, we have:

$$h * g = e. \quad (26)$$

By 25, we have:

$$g * h' = e. \quad (27)$$

Therefore:

$$h = h * e \quad (\text{property 2}) \quad (28)$$

$$= h * (g * h') \quad (27) \quad (29)$$

$$= (h * g) * h' \quad (\text{property 1}) \quad (30)$$

$$= e * h' \quad (26) \quad (31)$$

$$= h' \quad (\text{property 2}) \quad (32)$$

- For each  $g \in G$ , the unique element  $h \in G$  such that  $g * h = e = h * g$  is called the inverse of  $g$  and denoted by  $g^{-1}$ .

**Lemma 1:** Let  $(G, *)$  be a group and let  $x, y, z \in G$ . Then, right cancellation tells us:

$$x * z = y * z \implies x = y \quad (33)$$

and left cancellation tells us:

$$z * x = z * y \implies x = y \quad (34)$$

*Proof.* If  $z * x = z * y$ , then:

$$z^{-1} * (z * x) = z^{-1} * (z * y) \quad (35)$$

$$\implies (z^{-1} * z) * x = (z^{-1} * z) * y \quad (36)$$

$$\implies e * x = e * y \quad (37)$$

$$\implies x = y \quad (38)$$

The other implication is similar.  $\square$

**Warning:** The notation  $\frac{a}{b}$  is ambiguous. Does it mean  $a * b^{-1}$  or  $b^{-1} * a$ ? These can be different in a non-abelian group.

**Lemma 2:** Let  $(G, *)$  be a group and let  $g_1, \dots, g_n \in G$ . Every way of way inserting parentheses into  $g_1 * g_2 * \dots * g_n$  to determine a well defined product in  $G$  results in the same element of  $G$ .

*Proof.* Proved in tutorial worksheet.  $\square$

- The consequence of the above lemma is that the notation  $g_1 * g_2 * \dots * g_n$  is unambiguous.

**Definition:** Let  $(G, *)$  be a group and let  $n \in \mathbb{Z}$ . We define:

$$g^n = \begin{cases} \underbrace{g * g * \dots * g}_{n \text{ copies}}, & n > 0 \\ e, & n = 0 \\ \underbrace{g^{-1} * \dots * g^{-1}}_{n \text{ copies}} = (g^{-1})^{-n}, & n < 0 \end{cases} \quad (39)$$

**Lemma 3:** Let  $(G, *)$  be a group. For all  $g \in G$  and  $m, n \in \mathbb{Z}$ , we have:

$$g^m * g^n = g^{m+n} \quad (40)$$

and:

$$(g^m)^n = g^{mn} \quad (41)$$

- To prove the above lemma, we can use induction.

**Warning:** If  $G$  is a non-abelian group and  $a, b \in G$  and  $n \in \mathbb{Z}$ , then it can happen that:

$$(ab)^n \neq a^n b^n \quad (42)$$

**Lemma 4:** Let  $G$  be a group and let  $a, b \in G$ . Then:

$$(ab)^{-1} = b^{-1}a^{-1} \quad (43)$$

*Proof.* We just need to check the two conditions:

$$(ab)(b^{-1}a^{-1}) = aea^{-1} = aa^{-1} = e \quad (44)$$

and:

$$(b^{-1}a^{-1})(ab) = b^{-1}eb = b^{-1}b = e \quad (45)$$

Therefore, it is the inverse.  $\square$

- **Dihedral Groups.** Let  $n \in \mathbb{Z}$ ,  $n \geq 3$ . Let  $P_n$  be a regular  $n$ -gon.

**Definition:** The group of symmetries of the regular  $n$ -gon  $P_n$  is called the dihedral group of order  $2n$  and is denoted by  $D_n$ .

**Warning:** Some people use  $D_{2n}$  instead of  $D_n$ .

**Lemma 5:** The order of  $D_n$  is  $2n$ .

*Proof.* Label the vertices of  $P_n$  by  $v_1, v_2, \dots, v_n$  in some clockwise order. By the same reasoning from the case  $n = 4$  when we were considering a square, we have a bijection:

$$D_n = \text{Sym}(P_n) \rightarrow \{(v_i, v_j) | v_i \text{ adjacent to } v_j\} \quad (46)$$

$$\sigma \mapsto (\sigma(v_1), \sigma(v_2)) \quad (47)$$

Note that  $\{(v_i, v_j) | v_i \text{ adjacent to } v_j\} = \{(v_i, v_j) | j \equiv i \pm 1 \pmod{n}\}$ . We have:

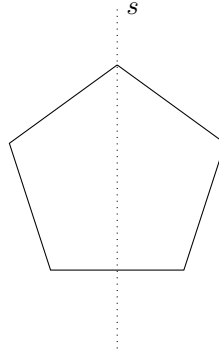
$$|D_n| = |\{(v_i, v_j) | j \equiv i \pm 1 \pmod{n}\}| = n \cdot 2 \quad (48)$$

$\square$

- For example, consider  $D_5$ . There are 5 lines of reflection, 4 rotational symmetries, and the identity. We can further compose transformations, for example:

$$rs = sr^4, \quad r^2s = sr^3, \quad r^3s = sr^2, \quad r^4s = sr, \quad r^5s = sr \quad (49)$$

where  $s$  represents a reflection and  $r$  is a  $72^\circ$  clockwise rotation.



**Lemma 6:** Let  $P_n$  be a regular  $n$ -gon. Let  $r$  be either a clockwise or counterclockwise rotation about the center of  $P_n$  by  $\frac{2\pi}{n}$ , and let  $s$  be any reflectional symmetry of  $P_n$ . Then:

1.  $r^n = 1, s^2 = 1$
2. For all  $k = 0, 1, \dots, n-1$ ,  $sr^k$  is a reflection and:

$$sr^k = r^{-k}s = r^{n-k}s \quad (50)$$

3.  $1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}$  are all distinct.
4.  $D_n = \{1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$ .

*Proof.* We will prove all four:

1.  $r$  is a rotation by  $2\pi/n$  CW or CCW so  $r^n = 1$ . Since  $s$  is a reflection,  $s^2 = 1$ .
2. The composition of a reflection and a rotation in the plane is a reflection. Therefore,  $\forall k = 0, 1, \dots, n-1$ ,  $sr^k$  is a reflection (orientation is not preserved). Therefore:

$$(sr^k)^2 = 1 \quad (51)$$

$$sr^k sr^k = 1 \quad (52)$$

$$sr^k s = r^{-k} \quad (53)$$

$$sr^k = r^{-k}s^{-1} \quad (54)$$

Since  $s^2 = 1, s^{-1} = s$ , this is proved. Furthermore, since  $r^n = 1$ , we must also have:

$$sr^k = r^{n-k}s \quad (55)$$

3. Since  $r^k$  is a rotation CW or CCW by  $2\pi k/n$ , then  $1, r, \dots, r^{n-1}$  are all distinct. Since rotations preserve orientation and reflections do not, then  $r^i \neq sr^j$  for all  $i, j$ . If  $sr^i = sr^j$ , then  $r^i = r^j$  so  $i = j$  if  $i, j \in \{0, \dots, n-1\}$ .

Therefore,  $1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}$  are distinct.

4. This follows directly from the previous property and the order of the dihedral group is  $|D_n| = 2n$ .

□

### 3 Lecture Three

- **Notation:** Sometimes the group operation for an **abelian** group is denoted by  $+$ .

If  $(A, +)$  is an abelian group, then:

- The identity is denoted by  $0$
- $a^{-1}$  is denoted by  $-a$
- $a^n$  is denoted by  $na$
- $a + (-b)$  is denoted by  $a - b$ .

- One way to get a better understanding of a group  $G$  is to find a group “inside of”  $G$  that you understand better.

**Definition:** Let  $(G, *_G)$  be a group. A subset  $H \subseteq G$  is a subgroup if:

1. For all  $h_1, h_2 \in H$ ,  $h_1 *_G h_2 \in H$ , and therefore the operation of  $G$ :

$$*_G : G \times G \rightarrow G \quad (56)$$

restricts to a binary operation on  $H$ :

$$*_H : H \times H \rightarrow H, \quad (h_1, h_2) \mapsto h_1 *_H h_2 := h_1 *_G h_2 \quad (57)$$

2.  $(H, *_H)$  is a group.

- We write  $H \leq G$  as a shorthand for “ $H$  is a subgroup of  $G$ .” If  $(G, *)$  is a group and  $H \subseteq G$ , we often denote the group operator for  $H$  by  $*$  as well.

**Example 3:** Let  $G$  be a group. Then  $G \leq G$  and  $\{e\} \leq G$ . We call  $\{e\}$  the trivial subgroup of  $G$ .

- If  $H \leq G$  and  $H \neq G$ , we write  $H < G$  and call  $H$  a **proper subgroup** of  $G$ .

**Example 4:** Let  $D_n$  be the symmetric group of the regular  $n$ -gon with vertices  $\{(\cos(2\pi k/n), \sin(2\pi k/n)) \mid k = 0, \dots, n-1\}$ .

From last lecture, we have  $D_n = \{1, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}$ . Then:  $H := \{1, r, \dots, r^{n-1}\} \leq D_n$ .

**Proposition 3:** Let  $G$  be a group and  $H \leq G$ .

1. The identity of  $H$  is the identity of  $G$ .
2. For all  $h \in H$ , the inverse of  $h$  in  $H$  is the inverse of  $h$  in  $G$ .

*Proof.* 1. Let  $e_H$  be the identity of  $H$  and  $e_G$  is that of  $G$ . Since  $e_H$  is the identity of  $H$ , we have:

$$e_H e_H = e_H \quad (58)$$

Let  $x$  be the inverse of  $e_H$  in  $G$ , then:

$$e_H e_H x = e_H x \quad (59)$$

$$\implies e_H e_G = e_G \quad (60)$$

$$\implies e_H = e_G \quad (61)$$

The first implication follows since  $x$  is the inverse of  $e_H$  in  $G$  and the second follows since  $e_G$  is the identity in  $G$ .

2. Let  $h \in H$ , let  $x$  be the inverse of  $h$  in  $H$ , and let  $y$  be the inverse of  $h$  in  $G$ . Then:

$$hx = e_H = e_G \quad (62)$$

and

$$xh = e_H = e_G \quad (63)$$

so  $x$  is the inverse of  $h$  in  $G$ .

□



**Theorem: Two-step subgroup test:** Let  $H$  be a nonempty subset of a group  $G$ . If:

1.  $a, b \in H \implies ab \in H$  ( $H$  is closed under the group operator)
  2.  $a \in H \implies a^{-1} \in H$  ( $H$  is closed under taking inverses)
- then  $H$  is a subgroup of  $G$ .

*Proof.* Assume that  $H$  is as in the theorem. We will prove that  $(H, *_H)$  is a group.

– Associative: Let  $h_1, h_2, h_3 \in H$

$$h_1 *_H (h_2 *_H h_3) = h_1 *_G (h_2 *_G h_3) \quad (64)$$

$$= (h_1 *_G h_2) *_G h_3 \quad (65)$$

$$= (h_1 *_H h_2) *_H h_3 \quad (66)$$

–  $H$  has an identity: Since  $H \neq \phi$ , there exists  $x \in H$ . By (2), we have  $x^{-1} \in H$ . By (1), we have  $e_G = xx^{-1} \in H$  since  $x, x^{-1} \in H$ .

For all  $h \in H$ , we have:

$$he_G = h = e_G h \quad (67)$$

since  $e_G$  is the identity of  $G$ . Therefore  $e_G$  is an identity of  $H$ .

–  $H$  has inverses: Let  $h \in H$ . By (2), we have that  $h^{-1} \in H$ . Since  $h^{-1}$  is the inverse of  $h$  in  $G$ , we have  $hh^{-1} = e_G = h^{-1}h$ . Therefore  $h^{-1}$  is an inverse of  $h$  in  $H$ .

□

**Theorem: One-step subgroup test:** Let  $G$  be a group and let  $H$  be a nonempty subset of  $G$ . Suppose that:

1.  $a, b \in H \implies ab^{-1} \in H$
- then  $H \leq G$ .

*Proof.* Let  $H$  be as in the theorem statement. Since  $H \neq \phi$ ,  $\exists h \in H$ . Taking  $a = b = h$  in (1) gives  $e = hh^{-1} \in H$ . Taking  $a = e, b = h$  in (1) gives  $h^{-1} = eh^{-1} = ab^{-1} \in H$ . Therefore,  $h \in H \rightarrow h^{-1} \in H$ .

Let  $h_1, h_2 \in H$ . Then  $h_2^{-1} \in H$ . Taking  $a = h, b = h_2^{-1}$  in (1) gives  $h_1 h_2 = ab^{-1} \in H$ . Therefore,  $h_1, h_2 \in H \implies h_1 h_2 \in H$ . By the two-step subgroup test,  $H \leq G$ .

□

**Example 5:** Let  $G$  be an abelian group. Prove that  $H = \{x \in G | x^2 = e\}$  is a subgroup of  $G$ .

*Proof.* Let  $a, b \in H$ . Then  $a^2 = b^2 = e$ . Since  $G$  is abelian:

$$(ab^{-1})^2 = a^2 b^{-2} = a^2 (b^2)^{-1} = ee^{-1} = e \quad (68)$$

Therefore,  $ab^{-1} \in H$  by the one-step subgroup test,  $H \leq G$ .

□

**Example 6:** Prove that matrices in the form of  $\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$  where  $x, y, z \in \mathbb{R}$  is a subgroup of  $SL_3(\mathbb{R})$  using either subgroup test.

*Proof.* Using the one-step subgroup test. Let  $g_1 = \begin{pmatrix} 1 & x_1 & y_1 \\ 0 & 1 & z_1 \\ 0 & 0 & 1 \end{pmatrix}$  and  $g_2 = \begin{pmatrix} 1 & x_2 & y_2 \\ 0 & 1 & z_2 \\ 0 & 0 & 1 \end{pmatrix}$ . The inverse of  $g_2$  is:

$$g_2^{-1} = \begin{pmatrix} 1 & -x & xz - y \\ 0 & 1 & -z \\ 0 & 0 & 1 \end{pmatrix} \quad (69)$$

and carrying out the computation:

$$g_1 g_2^{-1} = I \quad (70)$$

Since  $I$  is in the given group, we are done.

□

## 4 Lecture Four

- We begin with the **Finite Subgroup Test**

**Theorem:** Let  $G$  be a group and let  $H$  be a finite nonempty subset of  $G$ . If  $H$  is closed under the group operation of  $G$ , then  $H \leq G$ .

*Proof.* By the 2-step subgroup test, it suffices to prove that  $H$  is closed under taking inverses. Let  $a \in H$ :

- If  $a = e$ , then  $a^{-1} = e \in H$ .
- If  $a \neq e$ , consider the set:

$$\{a^n | n \geq 1\} = \{a, a^2, a^3, \dots\} \quad (71)$$

Since  $H$  is closed under the group operation and  $a \in H$ , we have  $\{a^n | n \geq 1\} \subseteq H$  by a short induction argument. Since  $H$  is finite, so is  $\{a^n | n \geq 1\}$ . Therefore,  $\exists m, n \geq 1, m \neq n$  such that:

$$a^m = a^n \quad (72)$$

WLOG, we may assume that  $m > n$ , so  $m - n > 0$ . We have:

$$a^{m-n} = e \quad (73)$$

Since  $a \neq e$ ,  $m - n \neq 1$ . Therefore,  $m - n \geq 2$ , so  $m - n - 1 \geq 1$ . Thus:

$$a^{m-n-1} \in \{a^k | k \geq 1\} \subseteq H \quad (74)$$

and

$$a^{m-n-1}a = a^{m-n} = e \quad (75)$$

so:

$$a^{m-n-1} = a^{-1} \quad (76)$$

□

- We will look at a special class of subgroups: **subgroups generated by one element**.

**Definition:** Let  $G$  be a group and let  $a \in G$ . Define:

$$\langle a \rangle = \{a^n | n \in \mathbb{Z}\} \quad (77)$$

We call  $\langle a \rangle$  the subgroup of  $G$  generated by  $a$ .

- We propose that  $\langle a \rangle \leq G$ .

*Proof.* Since  $e = a^0 \in \langle a \rangle$ , we have  $\langle a \rangle \neq \emptyset$ .

If  $g, h \in \langle a \rangle$ , then  $g = a^m$  and  $h = a^n$  for some  $m, n \in \mathbb{Z}$  and:

$$gh^{-1} = a^m(a^n)^{-1} = a^m a^{-n} = a^{m-n} \in \langle a \rangle \quad (78)$$

□

**Example 7:** Let  $G = (\mathbb{Z}/14\mathbb{Z})^\times = \{1, 3, 5, 9, 11, 13\}$ . We have:

$$a = 3, a^2 = 9, a^3 = 27 = 13 = -1 = -1, a^4 = -3 = 11, a^5 = -9 = 5, a^6 = 15 = 1 \quad (79)$$

Similarly:

$$a^0 = 1, a^{-1} = 5, a^{-2} = 11, a^{-3} = 13, a^{-4} = 9, a^{-5} = 3, a^{-6} = 1 \quad (80)$$

Therefore:

$$\langle a \rangle = \{1, 3, 5, 9, 11, 13\} = (\mathbb{Z}/14\mathbb{Z})^\times \quad (81)$$

Therefore,  $(\mathbb{Z}/14\mathbb{Z})^\times$  is cyclic. **Remarks:** If  $a^n = e$ , then for all  $k \in \mathbb{Z}$ , we have:

$$a^{-k} = a^{n-k} \quad (82)$$

so we can easily figure out negative exponents.

**Example 8:** Let  $G = \mathbb{Z}/12\mathbb{Z}$  and  $a = 2$ . We have:

$$-a = 10, 0a = 0, 2a = 4, 3a = 6, 4a = 8, 5a = 10, 6a = 12 = 0, 7a = 2 \quad (83)$$

so:

$$\langle a \rangle = \{0, 2, 4, 6, 8, 10\}. \quad (84)$$

**Example 9:** Let  $G = \mathbb{R}$  and  $a = 2\pi$ . Here,

$$\langle a \rangle = \{n2\pi | n \in \mathbb{Z}\} = 2\pi\mathbb{Z} \quad (85)$$

**Definition:** Let  $G$  be a group and  $a \in G$ . If there exists  $n \in \mathbb{Z}_{>0}$  such that  $a^n = e$ , then we say that  $a$  has **finite order** and the **order of  $a$**  is defined to be the smallest  $n \in \mathbb{Z}_{>0}$  such that  $a^n = e$ .

If there does not exist  $n \in \mathbb{Z}_{>0}$  such that  $a^n = e$ , then we say that  $a$  has infinite order.

The order of  $a$  is denoted by  $o(a)$  or  $|a|$ . If  $a$  has infinite order, we write  $o(a) = \infty$ .

• Note that:

- $o(a) = 1 \iff a = e$
- If  $o(a) = \infty$ , then  $a^n = e \iff n = 0$ .

• Let  $G$  be a group and  $a \in G$ .

1. If  $o(a) = \infty$ , then  $\forall i, j \in \mathbb{Z}$  we have:

$$a^{i-j} = e \iff i - j = 0 \quad (86)$$

$$\iff i = j \quad (87)$$

2. If  $o(a) = n < \infty$ , then  $\forall i, j \in \mathbb{Z}$  we have:

$$a^i = a^j \iff n | i - j \quad (88)$$

$$\iff i \equiv j \pmod{n} \quad (89)$$

In particular,  $a^i = e (= a^0) \iff n | i$ .

*Proof.* Let  $i, j \in \mathbb{Z}$ . Note  $a^i = a^j \implies a^{i-j} = e$ .

1. Suppose  $o(a) = \infty$ . Then  $a^{i-j} = e$  iff  $i - j = 0 \iff i = j$ .

2. Suppose  $o(a) = n < \infty$ . We must show that  $a^{i-j} = e \iff n | i - j$ .

(Backwards): If  $n | i - j$ , then  $\exists k \in \mathbb{Z}$  such that  $i - j = kn$  so  $a^{i-j} = a^{kn} = (a^n)^k = e^k = e$ .

(Forwards) Now suppose  $a^{i-j} = e$ . By the division algorithm,  $\exists!$   $q$  and  $0 \leq r < n$  such that:

$$i - j = qn + r \quad (90)$$

We have:

$$e = a^{i-j} = a^{qn+r} = a^{qn}a^r = (a^n)^qa^r = e^qa^r = a^r \quad (91)$$

Since  $n$  is the smallest positive integer with  $a^n = e$  and  $0 \leq r < n$  and satisfies  $a^r = e$ , we must have  $r = 0$ .

Therefore,  $i - j = qn$  so  $n | i - j$ .

□

**Corollary 1:** Let  $G$  be a group and  $a \in G$ .

1. If  $o(a) = \infty$ , then  $\dots, a^{-2}, a^{-1}, e, a, a^2, \dots$  are distinct (and  $\langle a \rangle = \{a^n | n \in \mathbb{Z}\}$ )
2. If  $o(a) = n < \infty$ , then  $e, a, \dots, a^{n-1}$  are distinct and  $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$ .

**Corollary 2:** Let  $G$  be a group and  $a \in G$ . Then  $o(a) = |\langle a \rangle|$  where  $|\langle a \rangle| = \infty$  when  $\langle a \rangle$  is infinite.

**Corollary 3:** Let  $G$  be a group and  $a, b \in G$ . If  $ab = ba$  and  $o(a), o(b) < \infty$ , then

$$o(ab) | o(a)o(b) \quad (92)$$

*Proof.* Suppose  $ab = ba$  and  $o(a), o(b) < \infty$ . Since:

$$(ab)^{o(a)o(b)} = a^{o(a)o(b)} b^{o(a)o(b)} \quad (93)$$

$$= (a^{o(a)})^{o(b)} (b^{o(b)})^{o(a)} \quad (94)$$

$$= e^{o(b)} e^{o(a)} \quad (95)$$

$$= e \quad (96)$$

Therefore,  $o(ab) | o(a)o(b)$ . □

• **Remarks about notation:**

- $\mathbb{Z}/n\mathbb{Z}$  is sometimes denoted by  $\mathbb{Z}_n$  or  $\mathbb{Z}/(n)$ .
- $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} | [b] \in \mathbb{Z}/n\mathbb{Z} \text{ with } [a][b] = 1\} = \{[a] | \gcd(n, a) = 1\}$ .

**Theorem:** Let  $G$  be a group and  $a \in G$  with  $o(a) = n < \infty$ . For any  $k \in \mathbb{Z}$ , we have:

$$o(a^k) = \frac{o(a)}{\gcd(o(a), k)} = \frac{n}{\gcd(n, k)} \quad (97)$$

*Proof.* By definition,  $o(a^k)$  is the smallest  $m \in \mathbb{Z}_{>0}$  such that

$$(a^k)^m = e \iff a^{mk} = e \quad (98)$$

$$\iff n | mk \quad (99)$$

Since  $mk$  is a multiple of  $k$ , we have  $n | mk \iff mk$  is common multiple of  $n$  and  $k$ .

If there exists  $m \in \mathbb{Z}_{>0}$  such that  $mk = \text{lcm}(n, k)$ , then  $m = o(a^k)$ . Recall that:

$$\frac{nk}{\gcd(n, k)} = \text{lcm}(n, k) \quad (100)$$

Since  $\gcd(n, k) | n$ , then  $\frac{n}{\gcd(n, k)} \in \mathbb{Z}_{>0}$  with

$$\left( \frac{n}{\gcd(n, k)} \right) k = \text{lcm}(n, k) \quad (101)$$

Therefore:

$$o(a^k) = \frac{n}{\gcd(n, k)} \quad (102)$$

□

**Corollary 4:** In a finite group  $G$ , the order of every element divides the order of the group:

$$\forall x \in G, \quad o(x) | |G| \quad (103)$$

**Example 10:**  $\mathbb{Z} = \langle 1 \rangle$  is an infinite cyclic group. Meanwhile,  $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$  is a finite cyclic group.

- Next we will study subgroups of cyclic groups. Choose a generator  $a \in G$  and  $G = \langle a \rangle$ .
- For each  $k \in \mathbb{Z}$ ,  $a^k \in \langle a \rangle$ . Therefore  $\langle a^k \rangle \subseteq \langle a \rangle$ .

**Proposition 4:** Let  $G$  be a group and let  $a \in G$ . If  $H \leq G$  and  $a \in H$ , then  $\langle a \rangle \subseteq H$ .

- One natural question is: *Do we get every subgroup in this way?* If  $k, \ell \in \mathbb{Z}$ , when is  $\langle a^k \rangle = \langle a^\ell \rangle$ ?

**Theorem: Classification of subgroups of cyclic groups:** Let  $G = \langle a \rangle$  be a cyclic group:

1. If  $|G| = \infty$  ( $\iff o(a) = \infty$ ) then every subgroup of  $G$  is of the form  $\langle a^m \rangle$  for a unique  $m \in \mathbb{Z}_{\geq 0}$ .

*Remarks:*  $\langle a^m \rangle = \langle a^{-m} \rangle$ .

2. If  $|G| = n < \infty$  ( $\iff o(a) = n < \infty$ ) then every subgroup of  $G$  is of the form  $\langle a^m \rangle$  for a unique  $m \in \mathbb{Z}_{>0}$  with  $m|n$ .

Said differently, the order of every subgroup of  $G$  divides  $n$  and for each  $d \in \mathbb{Z}_{>0}$  with  $d|n$  there is a unique subgroup of  $G$  of order  $d$ , namely  $\langle a^{n/d} \rangle$ .

*Proof.* Let  $H \leq G = \langle a \rangle$  with  $H \neq \{e\}$ . Then  $\exists k \in \mathbb{Z} \setminus \{0\}$  such that  $a^k, a^{-k} \in H$ . Therefore,  $a^{|k|} \in H$  so  $\exists k' \in \mathbb{Z}_{>0}$  such that  $a^{k'} \in H$ . Let  $m$  be the smallest positive integer such that  $a^m \in H$  (which exists by the well-ordering principle).

We will prove that  $H = \langle a^m \rangle$ . Since  $a^m \in H$ , we have  $\langle a^m \rangle \subseteq H$ . To prove  $H \subseteq \langle a^m \rangle$ , it suffices to prove:

- If  $a^k \in H$  where  $k \in \mathbb{Z}$ , then  $m|k$ .

Let  $k \in \mathbb{Z}$  and assume  $a^k \in H$ . By the division algorithm,  $\exists! q, r \in \mathbb{Z}$  such that  $0 \leq r < m$  and:

$$k = qm + r \tag{104}$$

Then:

$$a^k = a^{qm+r} = (a^m)^q a^r \implies a^r = (a^m)^{-q} a^k \tag{105}$$

Since  $(a^m)^{-q}, a^k \in H$ .

Since  $\langle a^m \rangle \subseteq H$ ,  $(a^m)^{-q} \in H$ . We assumed  $a^k \in H$ . Therefore,  $a^r \in H$ .

Since  $m$  is the smallest positive integer with  $a^m \in H$  and  $a^r \in H$  and  $0 \leq r < m$ , we have  $r = 0$ . Therefore  $k = qm$  so  $m|k$ .

If  $|G| = n < \infty$ , then  $o(a) = n$ , so  $a^n = e \in H$ . Therefore by the above point,  $m|n$ . Now we look at the two cases:

1. Suppose  $|G| = \infty$ . We prove that every nontrivial subgroup of  $G$  is of the form  $\langle a^m \rangle$  for some  $m \in \mathbb{Z}_{>0}$ . Since  $\{e\} = \langle a^0 \rangle$ , we have that every subgroup of  $G$  is of the form  $\langle a^m \rangle$  for some  $m \in \mathbb{Z}_{\geq 0}$ .

To prove that  $m$  is unique, suppose  $H \leq G$  and  $H = \langle a^m \rangle = \langle a^{m'} \rangle$  for some  $m, m' \in \mathbb{Z}_{\geq 0}$ .

Since  $a^m \in \langle a^m \rangle = \langle a^{m'} \rangle$ ,  $a^m \in \langle a^{m'} \rangle$ , so  $a^m = a^{m'k}$  for some  $k \in \mathbb{Z}$ . Since  $o(a) = \infty$ , we must have  $m = m'k$  so  $m'|m$ . Similarly,  $m|m'$ . Thus,  $m = m'$ .

2. Suppose  $|G| = n < \infty$ . Then  $o(a) = n$ , so  $a^n = e$  and therefore  $\{e\} = \langle a^n \rangle$ . We proved above that every nontrivial subgroup of  $G$  is of the form  $\langle a^m \rangle$  for some  $m \in \mathbb{Z}_{>0}$  with  $m|n$ .

3. Therefore, every subgroup of  $G$  is of the form  $\langle a^m \rangle$  for some  $m \in \mathbb{Z}_{>0}$  with  $m|n$ .

To prove that  $m$  is unique, suppose  $H \leq G$  with  $H = \langle a^m \rangle = \langle a^{m'} \rangle$  where  $m, m' \in \mathbb{Z}_{>0}$  with  $m, m'|n$ . Then:

$$o(a^m) = |\langle a^m \rangle| = |\langle a^{m'} \rangle| = o(a) \tag{106}$$

Since  $o(a^k) = \frac{n}{\gcd(n, k)}$  for all  $k \in \mathbb{Z}$ , we got:

$$\frac{n}{\gcd(n, m)} = \frac{n}{\gcd(n, m')} \tag{107}$$

which implies  $\gcd(n, m) = \gcd(n, m')$ . Since  $m, m'|n$  we have  $\gcd(n, m) = m$  and  $\gcd(n, m') = m'$  so  $m = m'$ .

□

**Corollary 5:** Criterion for  $\langle a^i \rangle = \langle a^j \rangle$  and  $o(a^i) = o(a^j)$ .

Let  $G = \langle a \rangle$  be a cyclic group and let  $i, j \in \mathbb{Z}$ .

1. If  $|G| = \infty$ , then  $\langle a^i \rangle = \langle a^j \rangle$  if and only if  $j = \pm k$ .
2. If  $|G| = n < \infty$ , then the following are equivalent:
  - $\langle a^i \rangle = \langle a^k \rangle$
  - $o(a^i) = o(a^j)$
  - $\gcd(n, i) = \gcd(n, j)$

**Corollary 6:** (The generators of a cyclic group) Let  $G = \langle a \rangle$  be a cyclic group. The generators of  $G$  are:

$$\begin{cases} \{a, a^{-1}\} & |G| = \infty \\ \{a^k \mid \gcd(n, k) = 1\} & |G| = n < \infty \end{cases} \quad (108)$$

This corollary follows from the first corollary.

- If  $G = \langle a \rangle$  is cyclic of order  $n < \infty$ , it follows that there are exactly  $\phi(n)$  generators where  $\phi(n)$  is Euler's Totient function.

## 5 Permutation Groups

- Let  $X$  be a set. A symmetry of  $X$  as a set is just a bijection  $\sigma : X \rightarrow X$  because there is no structure that  $\sigma$  should preserve.
- We call bijections  $\sigma : X \rightarrow X$  permutations of  $X$ .

**Definition:** The **symmetric group** on  $X$  is the group of all permutations of  $X$  with group operation given by composition. It is denoted by  $S_X$ .

**Example 11:** Let  $X = \{a, b, c\}$ , where  $a, b, c$  distinct. The map  $\sigma : X \rightarrow X$  defined by  $\sigma(a) = b$ ,  $\sigma(b) = a$ ,  $\sigma(c) = c$  is a permutation of  $X$ , so  $\sigma \in S_X$ .

Similarly, the map  $\tau : X \rightarrow X$  defined by  $\tau(a) = c$ ,  $\tau(b) = a$ ,  $\tau(c) = b$  is a permutation of  $X$ , so  $\tau \in S_X$  also.

**Proposition 5:** For every finite set  $X$ ,  $|S_X| = |X|!$ .

- To prove this proposition rigorously, we can prove this via induction on  $n \in \mathbb{Z}_{\geq 0}$  with  $|X| = |Y| = n$ , the set  $\{\sigma : X \rightarrow Y \mid \sigma \text{ is a bijection}\}$  has cardinality  $n!$ . Then apply that in the case  $X = Y$ .

**Definition:** A subgroup of  $S_X$  is called a permutation group on  $X$ .

- We are most interest in the case when  $0 < |X| < \infty$ .
- By choosing a linear ordering  $x_1, \dots, x_n$  of the elements of  $X$ , then we can regard  $X$  as the set  $\{1, \dots, n\}$ .
- We may as well, and we will, assume that  $X = \{1, \dots, n\}$ .
- We denote  $S_{\{1, \dots, n\}}$  by  $S_n$  and we call it the symmetric group on  $n$  letters.
- The identity of  $S_n$  is something denoted by  $id$ ,  $1$ ,  $e$ , or  $\epsilon$ .
- If  $\sigma \in S_n$ , we write:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \quad (109)$$

**Example 12:** Let  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$  and  $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ . Then:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad (110)$$

- For  $n \geq 3$ ,  $S_n$  is non-abelian.

*Proof.* Let  $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & \cdots & n \end{pmatrix}$  and  $\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 3 & 2 & \cdots & n \end{pmatrix}$ . Then:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 3 & 1 & \cdots & n \end{pmatrix} \quad (111)$$

but

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 3 & 1 & 2 & \cdots & n \end{pmatrix} \quad (112)$$

so  $\sigma\tau \neq \tau\sigma$ . □

- We will now introduce the notion of a cycle

**Definition:** Let  $r \in \mathbb{Z}$ ,  $r \geq 2$ . An **r-cycle** in  $S_n$  is a permutation  $\gamma \in S_n$  with the following property: There exist  $r$  distinct elements  $c_1, \dots, c_r \in \{1, \dots, n\}$  such that:

- (a)  $\gamma(c_i) = c_{i+1}$  for  $1 \leq i \leq r-1$ , and  $\gamma(c_r) = c_1$ .
- (b)  $\gamma(k) = k$  for all  $k \in \{1, \dots, n\} \setminus \{c_1, \dots, c_r\}$ .

In this case, we write the r-cycle  $\gamma$  as:

$$\gamma = (c_1 \ c_2 \ \dots \ c_r) \quad (113)$$

That is,  $\gamma$  is an r-cycle if it moves precisely  $r$  elements of  $\{1, \dots, n\}$  in a cyclic pattern (and leaves every other element fixed).

**Example 13:** Let  $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 3 & 2 & 6 & 9 & 7 & 4 & 8 \end{pmatrix} \in S_9$ . We claim that  $\gamma$  is a 6-cycle.

Note that  $\gamma$  fixes 1, 3, 7. We then need to show that the remaining elements are mapped by  $\gamma$  in a cyclic pattern:

$$2 \mapsto 5 \mapsto 6 \mapsto 9 \mapsto 8 \mapsto 4 \mapsto 2 \quad (114)$$

Therefore,  $\gamma = (2 \ 5 \ 6 \ 9 \ 8 \ 4)$ . Note that this is also equivalent to:

$$\gamma = (5 \ 6 \ 9 \ 8 \ 4 \ 2). \quad (115)$$

**Proposition 6:** Let  $r \geq 2$  and let  $\gamma = (c_1 \ c_2 \ \dots \ c_r)$  be an r-cycle in  $S_n$ .

1. For all  $2 \leq i \leq r$  we have:

$$\gamma = (c_i \ c_{i+1} \ \dots \ c_r \ c_1 \ c_2 \ \dots \ c_{i-1}) \quad (116)$$

2. The inverse  $\gamma^{-1}$  is given by:

$$\gamma^{-1} = (c_r \ c_{r-1} \ \dots \ c_1) \quad (117)$$

*Proof.* We prove both parts of the above proposition.

1. Exercise left to reader.
2. Let  $\delta = (c_r \ c_{r-1} \ \dots \ c_1)$ . To show that  $\delta = \gamma^{-1}$ , it suffices to show that  $\delta\gamma = \text{id}$ . (since  $S_n$  is a group). To do so, we must prove that  $\forall i \in \{1, \dots, n\}$ , we have  $\delta\gamma(i) = i$ .

By definition of cycles, we have:

$$\gamma(k) = \begin{cases} k & k \notin \{c_1, \dots, c_r\} \\ c_{i+1} & k = c_i, 1 \leq i \leq r-1 \\ c_1 & k = c_r \end{cases} \quad (118)$$

and:

$$\delta(k) = \begin{cases} k & k \notin \{c_1, \dots, c_r\} \\ c_{i-1} & k = c_i, 2 \leq i \leq r \\ c_r & k = c_1 \end{cases} \quad (119)$$

We can then check for  $k \notin \{c_1, \dots, c_r\}$ , we have:

$$\delta\gamma(k) = \gamma(k) = k \quad (120)$$

For  $k = c_i, 1 \leq i \leq r-1$ , we have:

$$\delta\gamma(k) = \delta\gamma(c_i) = \delta(c_{i+1}) = c_i = k \quad (121)$$

For  $k = c_r$ , we have:

$$\delta\gamma(k) = \delta(c_1) = c_r = k. \quad (122)$$

□

- Let us investigate the product of two cycles.

**Example 14:** Let  $\gamma = (1 \ 3 \ 2 \ 4)$  and  $\delta = (2 \ 6 \ 3)$  where  $\gamma, \delta \in S_8$ . Then:

$$\delta\gamma = (1 \ 3 \ 2 \ 4) [2 \ 6 \ 3] \quad (123)$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 5 & 2 & 7 & 8 \end{pmatrix} \quad (124)$$

Notice that:

$$1 \mapsto 3 \mapsto 4 \mapsto 1 \quad (125)$$

However, the other elements are not fixed since  $6 \mapsto 2$ . Therefore,  $\gamma\delta$  is not a cycle.

## 6 Lecture Six

- We continue our investigation of permutations.

**Definition:** Let  $\sigma \in S_n$ . Define:

$$\text{Fix}(\sigma) = \{k \in \{1, \dots, n\} | \sigma(k) = k\} \quad (126)$$

**Definition:** Let  $\sigma, \tau \in S_n$ . We say that  $\sigma$  and  $\tau$  are disjoint if for all  $k \in \{1, \dots, n\}$ ,

$$\sigma(k) \neq k \implies \tau(k) = k \quad (127)$$

which means that  $k \in \text{Fix}(\tau)$ . Similarly:

$$\tau(k) \neq k \implies \sigma(k) = k \quad (128)$$

which means that  $k \in \text{Fix}(\sigma)$ .

- Note that two cycles  $\gamma = (c_1 \ \dots \ c_r)$  and  $\delta = (d_1 \ \dots \ d_s)$  are disjoint if and only if:

$$\{c_1, \dots, c_r\} \cap \{d_1, \dots, d_s\} = \emptyset \quad (129)$$



- This is because

$$\text{Fix}(c_1 \cdots c_r) = \{1, \dots, n\} \setminus \{c_1, \dots, c_r\} \quad (130)$$

and:

$$\text{Fix}(d_1 \cdots d_s) = \{1, \dots, n\} \setminus \{d_1, \dots, d_s\}. \quad (131)$$

**Lemma 7:** Let  $\sigma \in S_n$ . Then:

1. If  $k \in \text{Fix}(\sigma)$ , then  $k \in \text{Fix}(\sigma^m)$  for all  $m \in \mathbb{Z}$ .
2. If  $k \notin \text{Fix}(\sigma)$ , then  $\sigma^m(k) \notin \text{Fix}(\sigma)$  for all  $m \in \mathbb{Z}$ .

*Proof.* We will prove both of the above:

1. Let  $k \in \text{Fix}(\sigma)$ , i.e.  $\sigma(k) = k$ . Then  $k = \sigma^{-1}(\sigma(k)) = \sigma^{-1}(k)$ . Therefore, we have  $k \in \text{Fix}(\sigma^{-1})$ . It follows by a simple induction argument that  $k \in \text{Fix}(\sigma^m)$  for all  $m \in \mathbb{Z}_{\geq 0}$  and  $k \in \text{Fix}(\sigma^m)$  for all  $m \in \mathbb{Z}_{\leq 0}$ .

The induction argument involves the fact that  $\sigma(\sigma(k)) = \sigma(k) = k$ .

2. Let  $k \notin \text{Fix}(\sigma)$ . It suffices to prove that  $\sigma(k) \notin \text{Fix} \sigma$ . It suffices to prove that:

$$\sigma(k), \sigma^{-1}(k) \notin \text{Fix}(\sigma) \quad (132)$$

To show why, suppose that  $\sigma(k), \sigma^{-1}(k) \notin \text{Fix}(\sigma)$ . Then, the idea is that we cannot have  $\sigma^2(k) \in \text{Fix}(\sigma)$  since  $\sigma(\sigma(k)) = \sigma(k) \notin \text{Fix}(\sigma)$ .

Alternatively, we can have a direct proof. Let  $k \notin \text{Fix}(\sigma)$ . Let  $m \in \mathbb{Z}$ . Suppose for the sake of contradiction that  $\sigma^m(k) \in \text{Fix}(\sigma)$ . Then:

$$\sigma(\sigma^m(k)) = \sigma^m(k) \quad (133)$$

Therefore, applying  $\sigma^{-m}$  on both sides gives  $\sigma(k) = k$ . This contradicts  $k \notin \text{Fix}(\sigma)$ . Therefore,  $\sigma^m(k) \notin \text{Fix}(\sigma)$ . □

**Theorem:** (Disjoint permutations commute) Let  $\sigma, \tau \in S_n$  be disjoint. Then  $\sigma\tau = \tau\sigma$ .

*Proof.* Let  $k \in \{1, \dots, n\}$ , and let  $\sigma, \tau \in S_n$  be disjoint.

For the first case, suppose  $k \in \text{Fix}(\sigma) \cap \text{Fix}(\tau)$ . Then  $\sigma(k) = k = \tau(k)$ . Therefore:

$$\sigma\tau(k) = \sigma(k) = k \quad (134)$$

and:

$$\tau\sigma(k) = \tau(k) = k \quad (135)$$

so  $\sigma\tau(k) = \tau\sigma(k)$ .

For the second case, suppose  $k \notin \text{Fix}(\sigma)$ . Since  $\sigma$  and  $\tau$  are disjoint, we have  $k \in \text{Fix}(\tau)$ . Therefore  $\tau(k) = k$  and  $\sigma\tau(k) = \sigma(k)$ . Since  $k \notin \text{Fix}(\sigma)$ , we have  $\sigma(k) \notin \text{Fix}(\sigma)$  by part (2) of the above lemma. Since  $\sigma$  and  $\tau$  are disjoint and  $\sigma(k) \notin \text{Fix}(\sigma)$ , we have  $\sigma(k) \in \text{Fix}(\tau)$ .

Therefore,  $\tau\sigma(k) = \sigma(k)$ . As a result:

$$\tau\sigma(k) = \sigma\tau(k) \quad (136)$$

For the last case, we consider  $k \notin \text{Fix}(\tau)$ . It can be handled in the same way as the second case. □

- We now introduce the notion of an orbit.

**Definition:** Let  $\sigma \in S_n$ . For each  $k \in \{1, \dots, n\}$ , the set:

$$O_\sigma(k) = \{\sigma^m(k) | m \in \mathbb{Z}\} \quad (137)$$

$$= \{\dots, \sigma^{-2}, \sigma^{-1}, k, \sigma(k), \dots\} \quad (138)$$

is called the **orbit** of  $k$  under the set  $\sigma$ .

- Note that  $|O_\sigma(k)| = 1$  if and only if  $O_\sigma(k) = \{k\}$  if and only if  $k \in \text{Fix}(\sigma)$ .

**Proposition 7:** Let  $\sigma \in S_n$ . For all  $k \in \{1, \dots, n\}$ , there exists  $\ell \in \mathbb{Z}_{>0}$  such that  $\sigma^\ell(k) = k$ .

If  $\ell$  is the smallest positive integer such that  $\sigma^\ell(k) = k$ , then  $k, \sigma(k), \sigma^2(k), \dots, \sigma^{\ell-1}(k)$  are distinct and:

$$O_\sigma(k) = \{k, \sigma(k), \dots, \sigma^{\ell-1}(k)\}. \quad (139)$$

**Warning:** The smallest  $\ell \in \mathbb{Z}_{>0}$  such that  $\sigma^\ell(k) = k$  is not necessarily the order of  $\sigma$ , which is the smallest  $m \in \mathbb{Z}_{>0}$  such that:

$$\sigma^m(j) = j \quad (140)$$

for all  $j \in \{1, \dots, n\}$ .

*Proof.* The subset  $\{\sigma^m(k) | m \in \mathbb{Z}\}$  of  $\{1, \dots, n\}$  is finite.

Therefore, there exist  $m_1, m_2 \in \mathbb{Z}$  with  $m_1 < m_2$  such that  $\sigma^{m_1}(k) = \sigma^{m_2}(k)$ . Then  $\sigma^{m_2-m_1}(k) = k$  and  $m_2 - m_1 \in \mathbb{Z}_{>0}$ .

Let  $\ell \in \mathbb{Z}_{>0}$  be the smallest positive integer such that  $\sigma^\ell(k) = k$ . This exists by the well ordering principle.

If  $m_1, m_2 \in \{0, 1, \dots, \ell - 1\}$ ,  $m_1 < m_2$ , and  $\sigma^{m_1}(k) = \sigma^{m_2}(k)$ , then  $0 < m_2 - m_1 < \ell$  and  $\sigma^{m_2-m_1}(k) = k$ , contradicting the definition of  $\ell$ .

Thus,  $k, \sigma(k), \dots, \sigma^{\ell-1}(k)$  are distinct. All we have to do now is to prove all the element sin the orbit of  $k$  is one of these.

Let  $m \in \mathbb{Z}$ . While  $m = q\ell + r$  for unique  $q, \ell \in \mathbb{Z}$  with  $0 \leq r < \ell$  by the division algorithm. Now,

$$\sigma^m(k) = \sigma^{q\ell+r}(k) \quad (141)$$

$$= (\sigma^\ell)^q \sigma^r(k) \quad (142)$$

$$= \sigma^r(\sigma^\ell)^q(k) \quad (143)$$

$$= \sigma^r(k) \quad (144)$$

We are able to go through these steps by noting  $\sigma^\ell(k) = k \implies (\sigma^\ell)^q(k) = k$ . Therefore  $\sigma^m(k) = \sigma^r(k) = \{k, \sigma(k), \dots, \sigma^{\ell-1}(k)\}$  and:

$$O_\sigma(k) = \{k, \sigma(k), \dots, \sigma^{\ell-1}(k)\}. \quad (145)$$

□

**Proposition 8:** Let  $\sigma \in S_n$ .

1. For all  $k \in \{1, \dots, n\}$ , then  $j \in O_\sigma(k)$ , if and only if  $O_\sigma(j) = O_\sigma(k)$ .
2. Distinct orbits of  $\sigma$  are disjoint. If  $O_\sigma(j) \neq O_\sigma(k)$ , then:

$$O_\sigma(j) \cap O_\sigma(k) = \emptyset. \quad (146)$$

Consequently, the orbits of  $\sigma$  partition  $\{1, \dots, n\}$ .

*Proof.* Again, we prove both parts.

1. Let  $k \in \{1, \dots, n\}$ . Suppose  $j \in O_\sigma(k)$ . Then there exists  $m \in \mathbb{Z}$  such that  $\sigma^m(k) = j$ . Therefore, for all  $r \in \mathbb{Z}$ ,  $\sigma^r(j) = \sigma^{m+r}(k) \in O_\sigma(k)$ . Thus, we have proved that:

$$j \in O_\sigma(k) \implies O_{\sigma(k)} \subseteq O_\sigma(j). \quad (147)$$

Now since  $j = \sigma^m(k)$ , we have  $k = \sigma^{-m}(j) \in O_\sigma(j)$ . Therefore,  $O_\sigma(k) \subseteq O_\sigma(j)$  by the same argument. Thus,  $O_\sigma(j) = O_\sigma(k)$ .

Note that we also have to prove the reverse direction. We know that  $j \in O_\sigma(k)$  since  $j \in O_\sigma(j)$ .

2. We will prove the contrapositive. Suppose  $O_\sigma(j) \cap O_\sigma(k) \neq \emptyset$ . Then, there exist  $m_1, m_2 \in \mathbb{Z}$  such that:

$$\sigma^{m_1}(j) = \sigma^{m_2}(k). \quad (148)$$

Therefore,  $j = \sigma^{m_2-m_1}(k) \in O_\sigma(k)$ . By part (1), we have  $O_\sigma(j) = O_\sigma(k)$ .

□

- We introduce the cycle *attached* to an orbit of  $\sigma \in S_n$ .
- Let  $\sigma \in S_n$  and let  $O$  be an orbit of  $\sigma$ . Let  $\ell = |O|$ . Assume  $\ell \geq 2$ .
- Choose a  $k \in O$ . Then  $O = O_\sigma(k)$  (by part (1) in the proposition.) By an earlier proposition:

$$O = O_\sigma(k) = \{k, \sigma(k), \dots, \sigma^{\ell-1}(k)\}. \quad (149)$$

- We can define a cycle  $\gamma_O = (k \ \sigma(k) \ \dots \ \sigma^{\ell-1}(k))$  which is an  $\ell$ -cycle in  $S_n$ .
- The  $\ell$ -cycle  $\gamma_O$  does not depend on the choice of  $k \in O$ . Proof is left as an exercise.
- **Note:** If  $O, O'$  are distinct orbits of  $\sigma$ , then they are disjoint so the cycles  $\gamma_O$  and  $\gamma_{O'}$  are disjoint as well. Therefore, these two cycles commute.

**Theorem:** (Cycle Decomposition Theorem) Every non-identity permutation can be written as a product of mutually disjoint cycles, i.e. there exist cycles  $\gamma_1, \dots, \gamma_r$  such that  $\gamma_i$  and  $\gamma_j$  are disjoint if  $i \neq j$  and  $\sigma = \gamma_1 \cdots \gamma_r$ . Moreover, if  $\gamma_1, \dots, \gamma_r$  are as above, then  $\{\gamma_1, \dots, \gamma_r\} = \{\gamma_O : O \text{ is an orbit of } \sigma \text{ and } |O| \geq 2\}$ . In particular, the set  $\{\gamma_1, \dots, \gamma_r\}$  is unique.

- **Remarks:** We can extend the theorem to the case where  $\sigma = \text{id}$  if we define an empty product (or a product of 0 elements of  $S_n$ ) to be id.

*Proof.* Let  $\sigma \in S_n$  and  $\sigma \neq \text{id}$ . Let  $O_1, \dots, O_s$  be the distinct orbits of  $\sigma$  of size at least 2. The cycles  $\gamma_{O_1}, \dots, \gamma_{O_s}$  are mutually disjoint because the orbits  $O_1, \dots, O_s$  are mutually disjoint.

Define  $\tau = \sigma_{O_1} \cdots \sigma_{O_s}$ . We will prove that  $\sigma = \tau$ . Let  $O_{s+1}, \dots, O_t$  be the distinct orbits of  $\sigma$  of size 1. Then:

$$\{1, \dots, n\} = \left( \dot{\bigcup}_{i=1}^s O_i \right) \dot{\bigcup} \left( \dot{\bigcup}_{j=s+1}^t O_j \right). \quad (150)$$

Let  $k \in \{1, \dots, n\}$ . We must show that  $\sigma(k) = \tau(k)$ . If  $k \notin O_1 \dot{\bigcup} \cdots \dot{\bigcup} O_s$ . Then  $k \in O_j$  for some  $j \in \{s+1, \dots, t\}$ . Since  $O_j$  is an orbit of size 1, we must have  $\sigma(k) = k$ .

For each  $i = \{1, \dots, s\}$ ,  $k \notin O_i$ , so  $\gamma_{O_i}(k) = k$ . Therefore:

$$\tau(k) = \gamma_{O_1} \cdots \gamma_{O_s}(k) = k = \sigma(k) \quad (151)$$

If  $k \in O_i$  for some  $i \in \{1, \dots, s\}$ , then by the definition of  $\gamma_{O_i}$ , we have:

$$\gamma_{O_i}(k) = \sigma(k) \quad (152)$$

for all  $j \neq i$ . Since  $\tau = \gamma_{O_1} \cdots \gamma_{O_s} = \gamma_{O_i} \prod_{j \neq i} \gamma_{O_j}$ .

We have:

$$\tau(k) = \gamma_{O_i} \prod_{j \neq i} \gamma_{O_j}(k) \quad (153)$$

$$= \gamma_{O_i}(k) \quad (154)$$

$$= \sigma(k). \quad (155)$$

Therefore,  $\sigma(k) = \tau(k)$  for all  $k \in \{1, \dots, n\}$ , i.e.  $\sigma = \tau$ .

Now suppose that  $\sigma = \gamma_1 \cdots \gamma_r$  where  $\gamma_1, \dots, \gamma_r$  are mutually disjoint cycles. We will prove that:

$$\{\gamma_1, \dots, \gamma_r\} = \{\gamma_O : O \text{ is an orbit of } \sigma \text{ and } |O| \geq 2\}. \quad (156)$$

*Proof of  $\subseteq$*  Let  $i \in \{1, \dots, r\}$  and write  $\gamma_i = (c_1 \dots c_\ell)$ . Since  $\gamma_1, \dots, \gamma_r$  are mutually disjoint, if  $j \neq i$ , then  $\gamma_j(c_k) = c_k$  for all  $k \in \{1, \dots, \ell\}$ . Therefore,

$$\sigma(c_k) = \gamma_i \prod_{j \neq i} \gamma_j(c_k) \quad (157)$$

$$= \gamma_i c_k \quad (158)$$

$$= \begin{cases} c_{k+1} & k < \ell \\ c_1 & k = \ell \end{cases} \quad (159)$$

for all  $k \in \{1, \dots, \ell\}$ . Consequently,  $\sigma(c_1) = c_2, \sigma^2(c_1) = c_3, \dots, \sigma^{\ell-1}(c_1) = c_\ell, \sigma^\ell(c_1) = c_1$ .

Therefore,  $O_\sigma(c_1) = \{c_1, c_2, \dots, c_\ell\}$  and  $\gamma_i = \gamma_{O_\sigma(c_1)}$ .

*Proof of  $\supseteq$* : Let  $O$  be an orbit of  $\sigma$  with  $|O| \geq 2$ . Let  $k \in O$ . Then as we have seen before,  $O = O_\sigma(k)$ . Since  $|O| \geq 2$ , we have  $\sigma(k) \neq k$ . Since  $\sigma = \gamma_1 \cdots \gamma_r$  and  $\sigma(k) \neq k$ , there exists  $i \in \{1, \dots, r\}$  such that:

$$\gamma_i(k) \neq k. \quad (160)$$

Let us write  $\gamma_i = (c_1 \dots c_\ell)$ . Since  $\gamma_i(k) \neq k$ , we have  $k = c_j$  for some  $j \in \{1, \dots, \ell\}$ . By relabelling  $c_1, \dots, c_\ell$ , we may assume that  $k = c_1$ . We showed above that  $\gamma_i = \gamma_{O_\sigma(c_1)}$ .

Since  $c_1 = k$ ,  $O_\sigma(c_1) = O_\sigma(k) = O$ . Therefore,  $\gamma_i = \gamma_O$ . □

**Lemma 8:** If  $\sigma, \tau \in S_n$  are disjoint, then so are  $\sigma^{m_1}, \tau^{m_2}$  for all  $m_1, m_2 \in \mathbb{Z}$ .

*Proof.* Suppose  $\sigma, \tau \in S_n$  are disjoint. Let  $m_1, m_2 \in \mathbb{Z}$ .

If  $k \in \{1, \dots, n\}$  and  $\sigma^{m_1}(k) \neq k$ , then  $\sigma(k) \neq k$ . Therefore,  $\tau(k) = k$  (since  $\sigma$  and  $\tau$  are disjoint), and therefore  $\tau^{m_2}(k) = k$ .

Similarly, if  $k \in \{1, \dots, n\}$  and  $\tau^{m_2}(k) \neq k$ , then  $\sigma^{m_1}(k) = k$ . □

**Theorem:** (Order of a Permutation) Let  $\sigma \in S_n$ . Let  $\sigma = \gamma_1 \cdots \gamma_r$  be the cycle decomposition of  $\sigma$ . (When  $\sigma = \text{id}$ ,  $r = 0$  and  $\sigma$  is an empty product of mutually disjoint cycles.)

Then  $o(\sigma) = \text{lcm}(o(\gamma_1), \dots, o(\gamma_r))$ . (If  $\sigma = \text{id}$ , then  $o(\sigma) = 1 = \text{lcm}(o(\emptyset))$ .)

*Proof.* Since  $\gamma_1, \dots, \gamma_r$  commute, for all  $m \in \mathbb{Z}$ , we have:

$$\sigma^m = \gamma_1^m \cdots \gamma_r^m. \quad (161)$$

Let  $m_i = o(\gamma_i)$  for each  $i$  and let  $M = \text{lcm}(m_1, \dots, m_r)$ . Since  $m_i | M$  for each  $i$ , we have  $\sigma^M = \sigma_1^M \cdots \sigma_r^M = \text{id} \cdots \text{id} = \text{id}$ .

Let  $m \in \mathbb{Z}$  and suppose  $\sigma^m = \text{id}$ . Then  $\gamma_1^m \cdots \gamma_r^m = \text{id}$ . Since  $\gamma_1, \dots, \gamma_r$  are mutually disjoint, so are  $\gamma_1^m, \dots, \gamma_r^m$  by the above lemma.

If  $\gamma_i^m(k) \neq k$ , then  $\gamma_j^m(k) = k$  for all  $j \neq i$ , so:

$$\gamma_1^m \cdots \gamma_r^m(k) = \gamma_i^m(k) \neq k, \quad (162)$$

contradicting the fact that:

$$\gamma_1^m \cdots \gamma_r^m = \text{id}. \quad (163)$$

Therefore,  $\gamma_i^m(k) = k$  for all  $i, k$ . So,  $\gamma_i^m = \text{id}$  for all  $i$ . Therefore  $m_i = o(\gamma_i) | m$  for all  $i$ . Thus,  $M = \text{lcm}(m_1, \dots, m_r) | m$ .

We proved that  $\sigma^M = 1$  and  $\sigma^m = 1 \implies M | m$ . Since  $M \in \mathbb{Z}_{>0}$ , it follows that  $M = o(\sigma)$ . □