MAT301 Notes

QiLin Xue

June 9, 2021

Contents

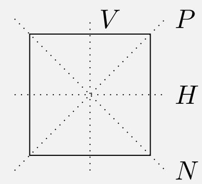
1 Lecture One

- 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:
$$d : F \times F \to \mathbb{R}_{\geq 0}, \quad d(x, y) = \|x - y\| \tag{1}$$
  A figure is then defined as the pair (F, d).

> **Definition**: A **symmetry** of a figure $F \subseteq \mathbb{R}^n$ is a bijection $\sigma : F \to F$ such that σ and σ^{-1} preserve distances:
> $$\forall x, y, \in F, \quad d(\sigma(x), \sigma(y)) = d(x, y) \tag{2}$$
> $$\iff d(\sigma^{-1}(x), \sigma^{-1}(y)) = d(x, y) \tag{3}$$
> Therefore:
> $$\text{Sym}(F) \equiv \{\sigma : F \to F | \sigma \text{ is a symmetry}\} \tag{4}$$

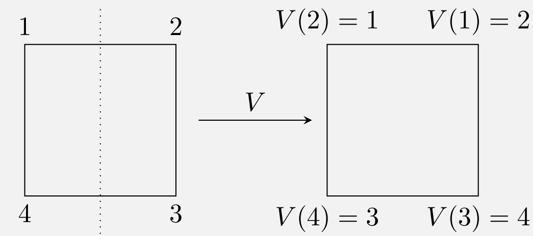
- For example, any point, line, shape, or form is a figure. However, we are only interested in figures that have interesting symmetries.

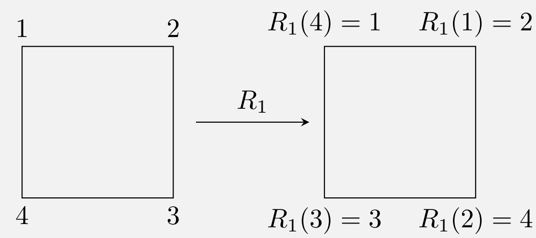
Example 1: Let F be a square in $\mathbb{R}^2$. There are four different lines of reflections:



and there are three rotations: R_1, R_2, and R_3, which represent $90°$, $180°$, and $270°$ 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:





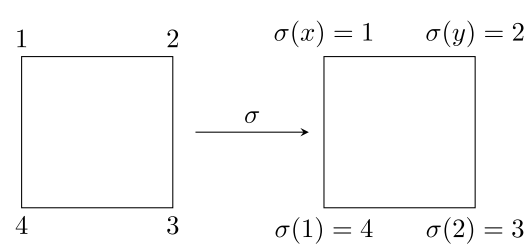
Applying the computations:

$$(R_1 \circ V)(1) = R_1(V(1)) = R_1(2) = 3 \tag{5}$$
$$(R_1 \circ V)(2) = R_1(V(2)) = R_1(1) = 2 \tag{6}$$
$$(R_1 \circ V)(3) = 1 \tag{7}$$
$$(R_1 \circ V)(4) = 4 \tag{8}$$

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 tto adjacent vertices. If x, y are adjacent vertices, then $\sigma(x)$, $\sigma(y)$ are vertices, and $d(\sigma(x), \sigma(y)) = d(x, y) =$ side length.
  3. A symmetry σ is completely determined by $(\sigma(1), \sigma(2))$. For example, suppose we have the symmetry σ 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 σ of the square such that:

$$(\sigma(1), \sigma(2)) = (x, y) \tag{9}$$

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:

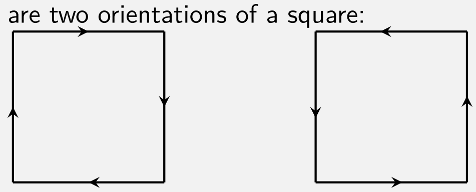
- There are 4 choices for x.
- For each choice of x, there are two choices of y. Therefore, there are $4 \times 2 = 8$ symmetries.

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 σ and σ^{-1} preserve the structures.
- The set of symmetries of X is denoted as $\mathrm{Sym}(X)$.

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 σ_1, σ_2:$X \to X$ are symmetries, then:
$$\sigma_1 \circ \sigma_2 : X \to X \tag{10}$$
is also a symmetry. Consequently, composition of symmetries restrict a map:
$$\mathrm{Sym}(X) \times \mathrm{Sym}(X) \mapsto \mathrm{Sym}(X), \quad (\sigma_1, \sigma_2) \mapsto \sigma_1 \circ \sigma_2 \tag{11}$$
Remarks: A map $m : S \times S \to S$ is called a binary operation on S.
1. Associativity: For all $\sigma_1, \sigma_2, \sigma_3 \in \mathrm{Sym}(X)$, we have:
$$(\sigma_1 \circ \sigma_2) \circ \sigma_3 = \sigma_1 \circ (\sigma_2 \circ \sigma_3) \tag{12}$$
2. The identity id : $X \mapsto X$ is a symmetry and id $\in \mathrm{Sym}(X)$.
3. Immediately from the "definition," we have: $\sigma \in \mathrm{Sym}(X) \implies \sigma^{-1} \in \mathrm{Sym}(X)$

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

Definition: A group is an ordered pair $(G, *)$ consisting of a set G and a binary operation $* : G \times G \to G$ such that:
1. $*$ is associative, $\forall g_1, g_2, g_3 \in G$, we have:
$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3) \tag{13}$$
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 $g \star h = e = h \star g$.

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:

$$(G, *) \text{ is a group} \tag{14}$$
$$\iff G \text{ is a group under } * \tag{15}$$

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

$$g * h = h * g \tag{16}$$

- Here are some examples of groups:
  - $(\text{Sym}(X), \circ)$
  - $(\mathbb{Z}, +)$
  - $(\mathbb{R}^x, \cdot)$ where:
  $$F^x = \{x \in F : \exists y \in F \text{ with } xy = 1 = yx\} \tag{17}$$
  - $(\mathbb{Q}_{>0}, \cdot)$, $(\mathbb{R}_{>0}, \cdot)$.
  - $(\mu_n, \cdot)$ where for $n \in \mathbb{Z}_{>0}$, let
  $$\mu_n = \{z \in \mathbb{C} | z^n = 1\} = \{e^{2\pi ki/n} | k = 0, 1, \ldots, n-1\} \tag{18}$$
  - $(\mathbb{R}^n, +)$
  - $(\mathsf{GL}_n(F), \cdot)$ where $\mathsf{GL}_n(F) = \{A \in \mathsf{Mat}_{n\times n}(F) | A \text{ invertible}\}$, $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. For all $n \geq 2$, $\mathsf{GL}_n(F)$ is non-abelian. Note that GL stands for *general linear*
  - $(\mathsf{SL}_n(F), \cdot)$ where $\mathsf{SL}_n(F) = \{A \in \mathsf{GL}_n(F) | \det A = 1\}$. Note that SL stands for special linear.
  - $(\mathsf{Mat}_{n\times n}(F), +)$

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

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

$$g * e = g = e * g \tag{19}$$

and

$$g * e' = g = e' * g, \tag{20}$$

then $e = e'$.

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

$$e * e' = e' \tag{21}$$

Similarly, by 20, we have:

$$e * e' = e \tag{22}$$

Therefore, $e = e * e' = e'$. □

- 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:

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

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:

$$g * h = e = h * g \tag{24}$$

and

$$g * h' = e = h' * g \tag{25}$$

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

$$h * g = e. \tag{26}$$

By 25, we have:

$$g * h' = e. \tag{27}$$

Therefore:

$$\begin{aligned}
h &= h * e && \text{(property 2)} \quad (28)\\
&= h * (g * h') && (27) \quad (29)\\
&= (h * g) * h' && \text{(property 1)} \quad (30)\\
&= e * h' && (26) \quad (31)\\
&= h' && \text{(property 2)} \quad (32)
\end{aligned}$$

- 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:

$$x * z = y * z \implies x = y \tag{33}$$

and left cancellation tells us:

$$z * x = z * y \implies x = y \tag{34}$$

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

$$\begin{aligned}
& z^{-1} * (z * x) = z^{-1} * (z * y) && (35)\\
\implies & (z^{-1} * z) * x = (z^{-1} * z) * y && (36)\\
\implies & e * x = e * y && (37)\\
\implies & x = y && (38)
\end{aligned}$$

The other implication is similar. □

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 $g_1 * g_2 * \cdots * g_n$ to determine a well defined product in G results in the same element of G.

Proof. Proved in tutorial worksheet. □

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

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

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

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

$$g^m * g^n = g^{m+n} \tag{40}$$

and:

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

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

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

$$(ab)^n \neq a^n b^n \tag{42}$$

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

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

Proof. We just need to check the two conditions:

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

and:

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

Therefore, it is the inverse. □

- **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 $v_1, v_2, \ldots, v_n$ in some clockwise order. By the same reasoning from the case $n = 4$ when we were considering a square, we have a bijection:

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

$$\sigma \mapsto (\sigma(v_1), \sigma(v_2)) \tag{47}$$

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:

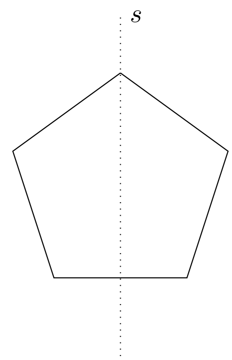
$$|D_n| = |\{(v_i, v_j) | j \equiv i \pm 1 \pmod n\}| = n \cdot 2 \tag{48}$$

□

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

$$rs = sr^4, \quad r^2s = sr^3, \quad r^3s = sr^2, \quad r^4s = sr, \quad r^5s = sr \tag{49}$$

where s represents a reflection and r is a $72°$ 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 $\dfrac{2\pi}{n}$, and let s be any reflectional symmetry of P_n. Then:

1. $r^n = 1$, $s^2 = 1$
2. For all $k = 0, 1, \ldots, n-1$, sr^k is a reflection and:
$$sr^k = r^{-k}s = r^{n-k}s \tag{50}$$
3. $1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}$ are all distinct.
4. $D_n = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$.

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, $\forall k = 0, 1, \ldots, n-1$, sr^k is a reflection (orientation is not preserved). Therefore:
$$(sr^k)^2 = 1 \tag{51}$$
$$sr^k sr^k = 1 \tag{52}$$
$$sr^k s = r^{-k} \tag{53}$$
$$sr^k = r^{-k}s^{-1} \tag{54}$$
Since $s^2 = 1$, $s^{-1} = s$, this is proved. Furthermore, since $r^n = 1$, we must also have:
$$sr^k = r^{n-k}s \tag{55}$$
3. Since r^k is a rotation CW or CCW by $2\pi k/n$, then $1, r, \ldots, r^{n-1}$ 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 $i, j \in \{0, \ldots, n-1\}$.

   Therefore, $1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}$ are distinct.
4. This follows directly from the previous property and the order of the dihedral group is $|D_n| = 2n$.

$\square$

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:
$$*_G : G \times G \to G \tag{56}$$
restricts to a binary operation on H:
$$*_H : H \times H \to H, \quad (h_1, h_2) \mapsto h_1 *_H h_2 := h_1 *_G h_2 \tag{57}$$
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 $\{(\cos(2\pi k/n), \sin(2\pi k/n)) | k = 0, \ldots, n-1\}$.

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

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:
$$e_H e_H = e_H \tag{58}$$
Let x be the inverse of e_H in G, then:
$$e_H e_H x = e_H x \tag{59}$$
$$\implies e_H e_G = e_G \tag{60}$$
$$\implies e_H = e_G \tag{61}$$
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:
$$hx = e_H = e_G \tag{62}$$
and
$$xh = e_H = e_G \tag{63}$$
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 $h_1, h_2, h_3 \in H$

$$\begin{aligned} h_1 *_H (h_2 *_H h_3) &= h_1 *_G (h_2 *_G h_3) && (64)\\ &= (h_1 *_G h_2) *_G h_3 && (65)\\ &= (h_1 *_H h_2) *_H h_3 && (66)\end{aligned}$$

- 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:

$$he_G = h = e_G h \tag{67}$$

  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, $h \in H \to h^{-1} \in H$.

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:

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

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 $\mathrm{SL}_3(\mathbb{R})$ 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:

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

and carrying out the computation:

$$g_1 g_2^{-1} = I \tag{70}$$

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:
$$\{a^n | n \geq 1\} = \{a, a^2, a^3, \dots\} \tag{71}$$
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 $\{a^n | m \geq 1\}$. Therefore, $\exists m, n \geq 1, m \neq n$ such that:
$$a^m = a^n \tag{72}$$
WLOG, we may assume that $m > n$, so $m - n > 0$. We have:
$$a^{m-n} = e \tag{73}$$
Since $a \neq e$, $m - n \neq 1$. Therefore, $m - n \geq 2$, so $m - n - 1 \geq 1$. Thus:
$$a^{m-n-1} \in \{a^k | k \geq 1\} \subseteq H \tag{74}$$
and
$$a^{m-n-1}a = a^{m-n} = e \tag{75}$$
so:
$$a^{m-n-1} = a^{-1} \tag{76}$$

□

- 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:
> $$\langle a \rangle = \{a^n | n \in \mathbb{Z}\} \tag{77}$$
> 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 $\langle a \rangle \neq \varnothing$.

If $g, h \in \langle a \rangle$, then $g = a^m$ and $h = a^n$ for some $m, n \in \mathbb{Z}$ and:
$$gh^{-1} = a^m (a^n)^{-1} = a^m a^{-n} = a^{m-n} \in \langle a \rangle \tag{78}$$

□

Example 7: Let $G = (\mathbb{Z}/14\mathbb{Z})^\times = \{1, 3, 5, 9, 11, 13\}$. We have:
$$a = 3,\ a^2 = 9,\ a^3 = 27 = 13 = -1 = -1,\ a^4 = -3 = 11,\ a^5 = -9 = 5,\ a^6 = 15 = 1 \tag{79}$$
Similarly:
$$a^0 = 1,\ a^{-1} = 5,\ a^{-2} = 11,\ a^{-3} = 13,\ a^{-4} = 9,\ a^{-5} = 3,\ a^{-6} = 1 \tag{80}$$
Therefore:
$$\langle a \rangle = \{1, 3, 5, 9, 11, 13\} = (\mathbb{Z}/14\mathbb{Z})^x \tag{81}$$
Therefore, $(\mathbb{Z}/14\mathbb{Z})^\times$ is cyclic. **Remarks:** If $a^n = e$, then for all $k \in \mathbb{Z}$, we have:
$$a^{-k} = a^{n-k} \tag{82}$$

so we can easily figure out negative exponents.

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

$$-a = 10,\ 0a = 0,\ 2a = 4,\ 3a = 6,\ 4a = 8,\ 5a = 10,\ 6a = 12 = 0,\ 7a = 2 \tag{83}$$

so:

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

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

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

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:

$$\begin{aligned} a^{i-j} = e &\iff i - j = 0 && (86) \\ &\iff i = j && (87) \end{aligned}$$

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

$$\begin{aligned} a^i = a^j &\iff n | i - j && (88) \\ &\iff i \equiv j \pmod{n} && (89) \end{aligned}$$

  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 $0 \le r < n$ such that:

$$i - j = qn + r \tag{90}$$

   We have:

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

   Since n is the smallest positive integer with $a^n = e$ and $0 \le r < n$ 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

$$o(ab) | o(a)o(b) \tag{92}$$

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

$$\begin{aligned}
(ab)^{o(a)o(b)} &= a^{o(a)o(b)} b^{o(a)o(b)} && (93)\\
&= (a^{o(a)})^{o(b)} (b^{o(b)})^{o(a)} && (94)\\
&= e^{o(b)} e^{o(a)} && (95)\\
&= e && (96)
\end{aligned}$$

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:

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

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

$$\begin{aligned}
(a^k)^m = e &\iff a^{mk} = e && (98)\\
&\iff n | mk && (99)
\end{aligned}$$

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 $mk = \operatorname{lcm}(n, k)$, then $m = o(a^k)$. Recall that:

$$\frac{nk}{\gcd(n, k)} = \operatorname{lcm}(n, k) \tag{100}$$

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

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

Therefore:

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

□

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

$$\forall x \in G, \quad o(x) \Big| |G| \tag{103}$$

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 from $\langle a^m \rangle$ 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 $o(a^k) = \dfrac{n}{\gcd(n,k)}$ 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:

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

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 Toitent function.

5 Permutation Groups

- Let X be a set. A is a symmetry of X as a set is just a bijection $\sigma : X \to X$ because there is no structure that σ should preserve.
- We call bijections $\sigma : X \to X$ 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 $\sigma : X \to X$ defined by $\sigma(a) = b$, $\sigma(b) = a$, $\sigma(c) = c$ is a permutation of X, so $\sigma \in S_x$.
Similarly, the map $\tau : X \to X$ 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 $\{\sigma : X \to Y | \sigma \text{ is a bijection}\}$ 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 $x_1, \ldots, x_n$ of the elements of X, then we can regard X as the set $\{1, \ldots, n\}$.
- We may as well, and we will, assume that $X = \{1, \ldots, n\}$.
- We denote $S_{\{1,\ldots,n\}}$ 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 ϵ.
- If $\sigma \in S_n$, we write:

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

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:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} and \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \tag{110}$$

- 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:

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

  but

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

  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 $c_1, \ldots, c_r \in \{1, \ldots, n\}$ 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 $k \in \{1, \ldots, n\} \setminus \{c_1, \ldots, c_r\}$.
In this case, we write the r-cycle γ as:

$$\gamma = \begin{pmatrix} c_1 & c_2 & \ldots & c_r \end{pmatrix} \tag{113}$$

That is, γ is an r-cycle if it moves precisely r elements of $\{1, \ldots, n\}$ 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 γ is a 6-cycle.
Note that γ fixes $1, 3, 7$. We then need to show that the remaining elements are mapped by γ in a cyclic pattern:

$$2 \mapsto 5 \mapsto 6 \mapsto 9 \mapsto 8 \mapsto 4 \mapsto 2 \tag{114}$$

Therefore, $\gamma = \begin{pmatrix} 2 & 5 & 6 & 9 & 8 & 4 \end{pmatrix}$. Note that this is also equivalent to:

$$\gamma = \begin{pmatrix} 5 & 6 & 9 & 8 & 4 & 2 \end{pmatrix}. \tag{115}$$

Proposition 6: Let $r \geq 2$ and let $\gamma = \begin{pmatrix} c_1 & c_2 & \cdots & c_r \end{pmatrix}$ be an r-cycle in S_n.
1. For all $2 \leq i \leq r$ we have:

$$\gamma = \begin{pmatrix} c_i & c_{i+1} & \ldots & c_r & c_1 & c_2 & \ldots & c_{i-1} \end{pmatrix} \tag{116}$$

2. The inverse γ^{-1} is given by:

$$\gamma^{-1} = \begin{pmatrix} c_r & c_{r-1} & \ldots c_1 \end{pmatrix} \tag{117}$$

Proof. We prove both parts of the above proposition.

1. Exercise left to reader.
2. Let $\delta = \begin{pmatrix} c_r & c_{r-1} & \ldots c_1 \end{pmatrix}$. 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 $\forall i \in \{1, \ldots, n\}$, we have $\delta\gamma(i) = i$.

By definition of cycles, we have:

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

and:

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

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

$$\delta\gamma(k) = \gamma(k) = k \tag{120}$$

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

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

For $k = c_r$, we have:

$$\delta\gamma(k) = \delta(c_1) = c_r = k. \tag{122}$$

□

- Let us investigate the product of two cycles.

Example 14: Let $\gamma = \begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}$ and $\delta = \begin{pmatrix}2 & 6 & 3\end{pmatrix}$ where $\gamma, \delta \in S_8$. Then:

$$\begin{aligned} \delta\gamma &= \begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}\begin{bmatrix}2 & 6 & 3\end{bmatrix} && (123) \\ &= \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 1 & 5 & 2 & 7 & 8\end{pmatrix} && (124) \end{aligned}$$

Notice that:

$$1 \mapsto 3 \mapsto 4 \mapsto 1 \tag{125}$$

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:

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

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

$$\sigma(k) \neq k \implies \tau(k) = k \tag{127}$$

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

$$\tau(k) \neq k \implies \sigma(k) = k \tag{128}$$

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

- Note that two cycles $\gamma = \begin{pmatrix}c_1 & \cdots & c_r\end{pmatrix}$ and $\delta = \begin{pmatrix}d_1 & \cdots & d_s\end{pmatrix}$ are disjoint if and only if:

$$\{c_1, \dots, c_r\} \cap \{d_1, \dots, d_s\} = \emptyset \tag{129}$$

- This is because

$$\mathrm{Fix}\begin{pmatrix}c_1 & \cdots & c_r\end{pmatrix} = \{1, \ldots, n\} \setminus \{c_1, \ldots, c_r\} \tag{130}$$

and:

$$\mathrm{Fix}\begin{pmatrix}d_1 & \cdots & d_s\end{pmatrix} = \{1, \ldots, n\} \setminus \{d_1, \ldots, d_s\}. \tag{131}$$

Lemma 7: Let $\sigma \in S_n$. Then:
1. If $k \in \mathrm{Fix}(\sigma)$, then $k \in \mathrm{Fix}(\sigma^m)$ for all $m \in \mathbb{Z}$.
2. If $k \notin \mathrm{Fix}(\sigma)$, then $\sigma^m(k) \notin \mathrm{Fix}(\sigma)$ for all $m \in \mathbb{Z}$.

Proof. We will prove both of the above:

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

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

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

$$\sigma(k), \sigma^{-1}(k) \notin \mathrm{Fix}(\sigma) \tag{132}$$

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

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

$$\sigma(\sigma^m(k)) = \sigma^m(k) \tag{133}$$

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

□

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

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

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

$$\sigma\tau(k) = \sigma(k) = k \tag{134}$$

and:

$$\tau\sigma(k) = \tau(k) = k \tag{135}$$

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

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

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

$$\tau\sigma(k) = \sigma\tau(k) \tag{136}$$

For the last case, we consider $k \notin \mathrm{Fix}(\tau)$. 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 $k \in \{1, \ldots, n\}$, the set:

$$\begin{aligned} O_\sigma(k) &= \{\sigma^m(k) | m \in \mathbb{Z}\} && (137)\\ &= \{\ldots, \sigma^{-2}, \sigma^{-1}, k, \sigma(k), \ldots && (138) \end{aligned}$$

is called the **orbit** of k under the set σ.

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

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

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

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

$$\sigma^m(j) = j \tag{140}$$

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 ℓ.

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 $0 \le r < \ell$ by the division algorithm. Now,

$$\begin{aligned}
\sigma^m(k) &= \sigma^{q\ell + r}(k) && (141)\\
&= (\sigma^\ell)^q \sigma^r(k) && (142)\\
&= \sigma^r(\sigma^\ell)^q(k) && (143)\\
&= \sigma^r(k) && (144)
\end{aligned}$$

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:

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

□

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 σ are disjoint. If $O_\sigma(j) \neq O_\sigma(k)$, then:

   $$O_\sigma(j) \cap O_\sigma(k) = \emptyset. \tag{146}$$

   Consequently, the orbits of σ 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:

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

   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:

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

   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 σ. 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:

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

- We can define a cycle $\gamma_O = \begin{pmatrix} k & \sigma(k) & \cdots & \sigma^{\ell-1}(k) \end{pmatrix}$ which is an ℓ-cycle in S_n.
- The ℓ-cycle γ_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 σ, then they are disjoint so the cycles γ_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 $\gamma_1, \ldots, \gamma_r$ such that γ_i and γ_j are disjoint if $i \neq j$ and $\sigma = \gamma_1 \cdots \gamma_r$.
> Moreover, if $\gamma_1, \ldots, \gamma_r$ are as above,
> then $\{\gamma_1, \ldots, \gamma_r\} = \{\gamma_0 : O$ is an orbit of σ and $|O| \geq 2$. In particular, the set $\{\gamma_1, \ldots, \gamma_r\}$ 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 $O_1, \ldots, O_s$ be the distinct orbits of σ of size at least 2. The cycles $\gamma_O, \ldots, \gamma_{O_s}$ are mutually disjoint because the orbits $O_1, \ldots, O_s$ are mutually disjoint.

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

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

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

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

$$\tau(k) = \gamma_{O_1} \ldots \gamma_{O_s}(k) = k = \sigma(k) \tag{151}$$

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

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

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

We have:

$$\begin{aligned} \tau(k) &= \gamma_{O_i} \prod_{j \neq i} \gamma_{O_j}(k) && (153) \\ &= \gamma_{O_i}(k) && (154) \\ &= \sigma(k). && (155) \end{aligned}$$

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

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

$$\{\gamma_1, \ldots, \gamma_r\} = \{\gamma_O : O \text{ is an orbit of } \sigma \text{ and } |O| \geq 2\}. \tag{156}$$

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

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

$$= \gamma_i c_k \tag{158}$$

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

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

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

Proof of $\supseteq$*:* Let O be an orbit of σ 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 $i \in \{1, \ldots, r\}$ such that:

$$\gamma_i(k) \neq k. \tag{160}$$

Let us write $\gamma_i = \begin{pmatrix} c_1 & \ldots & c_\ell \end{pmatrix}$. Since $\gamma_i(k) \neq k$, we have $k = c_j$ for some $j \in \{1, \ldots, \ell\}$. By relabelling $c_1, \ldots, c_\ell$, 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 σ^{m_1}, τ^{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 $k \in \{1, \ldots, n\}$ and $\sigma^{m_1}(k) \neq k$, then $\sigma(k) \neq k$. Therefore, $\tau(k) = k$ (since σ and τ are disjoint), and therefore $\tau^{m_2}(k) = k$.

Similarly, if $k \in 1, \ldots, n$ 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 σ. (When $\sigma =$ id, $r = 0$ and σ is an empty product of mutually disjoint cycles.)

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

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

$$\sigma^m = \gamma_1^m \cdots \gamma_r^m. \tag{161}$$

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

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

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

$$\gamma_1^m \cdots \gamma_r^m(k) = \gamma_i^m(k) \neq k, \tag{162}$$

contradicting the fact that:

$$\gamma_1^m \cdots \gamma_r^m = \text{id}. \tag{163}$$

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

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

7 Transpositions

- We start with the definition:

Definition: A transposition is just a 2-cycle

Lemma 9: Let $\begin{pmatrix} c_1 & \cdots & c_r \end{pmatrix} \in S_n$ be an $r-$cycle. Then:

$$\begin{pmatrix} c_1 & \cdots & c_r \end{pmatrix} = (c_1\, c_2)(c_2\, c_3)\cdots(c_{r-1}\, c_r), \tag{164}$$

a product of $r-1$ transpositions.

Proof. We can prove by induction that for all $i \in \{1, \ldots, r\}$, we have:

$$(c_1\, c_2)(c_2\, c_3)\cdots(c_{i-1}\, c_i)c_i = c_1. \tag{165}$$

Then, let $i \in \{1, \ldots, r-1\}$, and it remains to be shown that:

$$(c_1\, c_2)(c_2\, c_3)\cdots(c_{r-1}\, c_r)c_i = c_{i+1}. \tag{166}$$

For $j \in \{i+1, \ldots, r-1\}$, we have:

$$(c_j\, c_{j+1})c_i = c_i \tag{167}$$

Therefore:

$$(c_1\, c_2)\cdots(c_{r-1}\, c_r)c_i \tag{168}$$
$$= (c_1\, c_2)\cdots(c_{i-1}c_i)(c_i\, c_{i+1})c_i \tag{169}$$
$$= (c_1\, c_2)\cdots(c_{i-1}\, c_i)c_{i+1} \tag{170}$$

For $j \in \{1, \ldots, i-1\}$ we have:

$$(c_j\, c_{j+1})c_{i+1} = c_{i+1} \tag{171}$$

Therefore:

$$(c_1\, c_2)\cdots(c_{r-1}\, c_r)c_i = c_{i+1} \tag{172}$$

□

Corollary 7: If $\sigma \in S_n$, then σ is a (possibly empty) product of transpositions.

Definition: Let $\sigma \in S_n$. An **inversion** of σ is an ordered pair:

$$(i, j) \in \{1, \ldots, n\}^2 \tag{173}$$

s.t. $i < j$ and $\sigma(j) < \sigma(i)$.

Let $\mathrm{inv}(\sigma) = \{(i,j) \in \{1, \ldots, n\}^2 | i < j, \sigma(j) < \sigma(i)\}$.

Example 15: Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \in S_4$. Then:

$$\mathrm{inv}(\sigma) = \{(1,3), (2,3), (2,4)\} \tag{174}$$

Lemma 10: Let $\tau \in S_n$ be a transposition with $n \geq 2$. Write $\tau = (k\, \ell)$ with $1 \leq k < \ell \leq n$. Then:

$$\mathrm{inv}(\tau) = \{(k, k+1), (k, k+2), \ldots, (k, \ell-1), (k, \ell), (k+1, \ell), (k+2, \ell), \ldots, (\ell-1, \ell) \tag{175}$$

Thus:

$$|\,\mathrm{inv}(\tau)| = 2(\ell - k - 1) + 1 \tag{176}$$

Theorem: (Parity Theorem) Let $\sigma \in S_n$. If $\sigma = \tau_1 \cdots \tau_r$, where $\tau_1, \ldots, \tau_r$ are transpositions, then:

$$r \equiv |\,\mathrm{inv}(\sigma)| \pmod 2 \tag{177}$$

Consequently, if $\sigma = \tau_1 \cdots \tau_r = \tau_1' \cdots \tau_s'$, where $\tau_1, \ldots, \tau_r, \tau_1', \ldots, \tau_s'$ are transpositions, then $r \equiv s \pmod 2$.

Definition: If $\sigma \in S_n$ can be written as a product of an even (resp. odd) number of transpositions, we say that σ is even (respectively odd).

Corollary 8: A permutation is either even or odd, but not both. And, the parity of $\sigma \in S_n$ is equal to the parity of the number $|\operatorname{inv}(\sigma)|$.

- Note that $\operatorname{inv}(\sigma) = \emptyset \iff \sigma = \text{id}$.
- Therefore, $|\operatorname{inv}(\text{id})| = 0$, so id is an even permutation, i.e. id can only be written as a product of an even number of transpositions.
- Let $\mathbb{C}[x_1, \ldots, x_n]$ denote the set of polynomials in the variables $X_1, \ldots, X_n$ with complex coefficients. That is,

$$\mathbb{C}[x_1, \ldots, x_r] = \left\{ \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n} \right\} \tag{178}$$

  where $a_{i_1, \ldots, i_n} \in \mathbb{C}$ and all but finitely many of $a_{i_1, \ldots, i_n}$ are zero.

- For each $\sigma \in S_n$. Define:

$$A_\sigma : \mathbb{C}[X_1, \ldots, X_n] \to \mathbb{C}[X_1, \ldots, X_n] \tag{179}$$

  by:

$$A_\sigma \left(\sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n} \right) \tag{180}$$

$$= \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_{\sigma(1)}^{i_1} \cdots X_{\sigma(n)}^{i_n} \tag{181}$$

Example 16: Let $\sigma = (1\,3\,2)$. Then:

$$A_\sigma(3X_1X_2 + 2X_3^5) = 3X_3X_1 + 2X_2^5 \tag{182}$$

- It has the following properties:
  1. For all $\sigma \in S_n$, we have:
     (a) For all $P, Q \in \mathbb{C}[x+1, \ldots, x_n]$, we have

$$A_\sigma(P+Q) = A_\sigma(P) + A_\sigma(Q)$$

     (b) and:

$$A_\sigma(PQ) = A_\sigma(P)A_\sigma(Q) \tag{183}$$

  2. For all $\sigma, \tau \in S_n$, we have:

$$A_{\sigma\tau} = A_\sigma \circ A_\tau \tag{184}$$

     Proof. Let $P = \sum_{i_1, \ldots, i_n} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}$ be an arbitrary element of $\mathbb{C}[x_1, \ldots, x_n]$. Then:

$$A_\sigma(A_\tau(P)) = A_\sigma \left(\sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_{\tau(1)}^{i_1} \cdots X_{\tau(n)}^{i_n} \right) \tag{185}$$

$$= \sum_{i_1, \ldots, i_n} \geq 0 a_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} A_\sigma(X_\tau(1)^{i_1}) \cdots A_\sigma(X_{\tau(n)}^{i_n}) \tag{186}$$

$$= A_{\sigma\tau}(P) \tag{187}$$

$\square$

Definition: The Vandermonde polynomial in $\mathbb{C}[X_1, \ldots, X_n]$ is the polynomial $V_n = \prod_{1\le i<j\le n} (X_j - X_i)$.

- A key observation is that for all $\sigma \in S_n$, we have:

$$\begin{aligned} A_\sigma(V_n) &= \prod (X_{\sigma(j)} - X_{\sigma(i)}) && (188) \\ &= (-1)^{|\operatorname{inv}(\sigma)|} \prod_{1\le i<j\le n} (X_j - X_i) && (189) \\ &= (-1)^{|\operatorname{inv}(\sigma)|} V_n && (190) \end{aligned}$$

8 Lecture Eight

- Recall that for all $\sigma \in S_n$, if we apply it to the Vandermonde polynomial, we have:

$$\begin{aligned} A_\sigma(V_n) &= A_\sigma\left(\prod_{1\le i<j\le n} (X_j - X_i)\right) && (191) \\ &= \prod_{1\le i<j\le n} (X_{\sigma(j)} - X_{\sigma(i)}) && (192) \end{aligned}$$

Now, for all $1 \le i < j \le n$ we have:

$$\begin{aligned} X_{\sigma(j)} - X_{\sigma(i)} &= \begin{cases} X_{\sigma(j)} - X_{\sigma(i)}, & \text{if } \sigma(i) < \sigma(j) \\ -(X_{\sigma(j)} - X_{\sigma(i)}), & \text{if } \sigma(j) < \sigma(i) \end{cases} && (193) \\ &= \begin{cases} X_{\sigma(j)} - X_{\sigma(i)}, & \text{if } (i,j) \notin \operatorname{inv}(\sigma) \\ -(X_{\sigma(j)} - X_{\sigma(i)}), & \text{if } (i,j) \in \operatorname{inv}(\sigma) \end{cases} && (194) \end{aligned}$$

Therefore:

$$\begin{aligned} A_\sigma(V_n) &= (-1)^{|\operatorname{inv}(\sigma)} \prod_{1\le i<j\le n} (X_j - X_i) && (195) \\ &= (-1)^{|\operatorname{inv}(\sigma)|} V_n && (196) \end{aligned}$$

Definition: The **sign** of $\sigma \in S_n$ is given by:

$$\operatorname{sgn}(\sigma) = (-1)^{|\operatorname{inv}(\sigma)|} \tag{197}$$

and therefore:

$$A_\sigma(V_n) = \operatorname{sgn}(\sigma) V_n \tag{198}$$

Lemma 11: We have the following properties:

1. For all $\sigma, \tau \in S_n$, we have:
$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) \tag{199}$$
2. If $\tau \in S_n$ is a transposition, then $\operatorname{sgn}(\tau) = -1$.

Proof. We prove both parts:

1. Let $\sigma, \tau \in S_n$. Then:

$$\begin{aligned} \operatorname{sgn}(\sigma\tau) V_n &= A_{\sigma\tau}(V_n) && (200) \\ &= A_\sigma(A_\tau(V_n)) && (201) \\ &= A_\sigma(\operatorname{sgn}(\tau) V_n) && (202) \\ &= A_\sigma(\operatorname{sgn}\tau) A_\sigma(V_n) && (203) \\ &= \operatorname{sgn}(\tau) A_\sigma(V_n) && (204) \\ &= \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma) V_n && (205) \\ &= \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) V_n && (206) \end{aligned}$$

2. Let $\tau \in S_n$ be a transposition. By an earlier lemma, we have $|\operatorname{inv}\tau|$ is odd. Therefore:

$$\operatorname{sgn}(\tau) = (-1)^{|\operatorname{inv}\tau|} = -1 \tag{207}$$

□

- We can now prove the Parity Theorem.

Proof. Let $\sigma \in S_n$ and write $\sigma = \tau_1 \cdots \tau_r$, where $\tau_1, \ldots, \tau_r$ are transpositions. Then:

$$(-1)^{|\operatorname{inv}(\sigma)|} = \operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1)\cdots\operatorname{sgn}(\tau_r) = (-1)^r \tag{208}$$

Therefore $(-1)^{|\operatorname{inv}(\sigma)|-r} = 1$, so:

$$|\operatorname{inv}(\sigma)| \equiv r \pmod 2 \tag{209}$$

□

Corollary 9: For all $\sigma \in S_n$, σ is even (respectively odd) if and only if $\operatorname{sgn}(\sigma) = 1$ (respectively $\operatorname{sgn}(\sigma) = -1$).

- We introduce the notion of alternating groups.

Definition: The set

$$\begin{aligned} A_n &= \{\sigma \in S_n | \sigma \text{ is even}\} \quad (210)\\ &= \{\sigma \in S_n | \operatorname{sgn}(\sigma) = 1\} \quad (211)\end{aligned}$$

is a subgroup of S_n called the alternating group on n letters.

Proof. Since A_n is finite, it suffices to show that A_n is closed under the group operation and A_n is nonempty, by the finite subgroup test.

Since id is even, id $\in A_n$ so $A_n \neq \emptyset$. Let $\sigma_1, \sigma_2 \in A_n$. We will prove that $\sigma_1\sigma_2 \in A_n$. There are a few methods to do so:

- First method: Since σ_1, σ_2 are even, there exist transpositions $\tau_1, \ldots, \tau_r, \tau_1', \ldots, \tau_s'$ such that:

  $$\sigma_1 = \tau_1 \cdots \tau_r, \quad \sigma_2 = \tau_1' \cdots \tau_s' \tag{212}$$

  and r and s are even. Then:

  $$\sigma_1\sigma_2 = \tau_1 \cdots \tau_r \tau_1' \cdots \tau_s' \tag{213}$$

  so it is a product of $r+s$ transpositions. Since $r+s$ is even, the permutation $\sigma_1\sigma_2$ is even, i.e. $\sigma_1\sigma_2 \in A_n$.

- We have:

  $$\operatorname{sgn}(\sigma_1\sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2) = 1 \tag{214}$$

  so $\sigma_1\sigma_2 \in A_n$.

□

Proposition 9: For $n > 1$, we have:

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2} \tag{215}$$

Note that $A_1 = S_1 = \{\text{id}\}$ so $|A_1| = 1$.

Proof. Since $n > 1$, $(1\,2) \in S_n$. Let $\tau = (1\,2)$. Then, the map

$$g : S_n \to S_n \tag{216}$$

defined by $g(\sigma) = \tau\sigma$, restricts to a bijection

$$g : A_n \to S_n \setminus A_n \tag{217}$$

The map g is well-defined since for all $\sigma \in S_n$, we have:

$$\operatorname{sgn}(\tau\sigma) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma) = -\operatorname{sgn}(\sigma) \tag{218}$$

and g is a bijection because

$$\begin{aligned} h : S_n \setminus A_n &\to A_n \tag{219}\\ \sigma &\mapsto \tau\sigma \tag{220}\end{aligned}$$

is its inverse. Therefore:

$$|A_n| = |S_n \setminus A_n|. \tag{221}$$

Since $S_n = A_n \sqcup (S_n \setminus A_n)$, we have:

$$\begin{aligned} |S_n| &= |A_n| + |S_n \setminus A_n| \tag{222}\\ &= 2|A_n| \tag{223}\end{aligned}$$

□

- We begin a look at isomorphisms. Let $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, $C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, and define $G = \{I, A, B, C\}$. Then G is a group under matrix multiplication.
- The Cayley table of G is:

	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

Notice that this is an abelian group.

- Let $\alpha = (12)(34)$, $\beta = (13)(24)$, and $\gamma = (14)(23)$. Define $H = \{\text{id}, \alpha, \beta, \gamma\}$. Then H is a subgroup of A_4.
- The Cayley Table of H is:

	id	α	β	γ
id	id	α	β	γ
α	α	id	γ	β
β	β	γ	id	α
γ	γ	β	α	id

- A key observation is that the two Cayley tables are the same. Specifically, if we define $\phi : G \to H$ by:

$$\phi(I) = id,\ \phi(A) = \alpha,\ \phi(B) = \beta,\ \phi(C) = \gamma \tag{224}$$

then ϕ is a bijection and the entry of the Cayley table of H corresponding to row x and the Cayley table of H is:

	$\phi(I)$	$\phi(A)$	$\phi(B)$	$\phi(C)$
$\phi(I)$				
$\phi(A)$			$\phi(C)$	
$\phi(B)$				
$\phi(C)$				

where we have only written down one entry.

- Note that $\phi(A)\phi(B) = \phi(C) = \phi(AB)$.
- In general, we have:

$$\phi(XY) = \phi(X)\phi(Y) \tag{225}$$

for all $X, Y \in G$.

Definition: Let G and H be groups. An isomorphism from G to H is a map $\phi : G \to H$ such that:

1. ϕ respects the group operations, i,e, for all $g_1, g_2 \in G$ we have

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \tag{226}$$

2. ϕ is a bijection.

If there exists an isomorphism from G to H, we say that G is isomorphic to H and we write:

$$G \simeq H \tag{227}$$

- **Etymology:** *isos* is ancient greek for "equal" and *morphe* is ancient greek for form/shape/appearance.

Example 17: Define $\phi : \mathbb{R} \to \mathbb{R}_{>0}$ by $\phi(x) = e^x$. Then ϕ is a bijection and for all $x, y \in \mathbb{R}$, we have:

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y) \tag{228}$$

Thus, ϕ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \cdot)$.

More generally, for any $a > 0$, $a \neq 1$, the map $\phi : \mathbb{R} \to \mathbb{R}_{>0}$ defined by $\phi(x) = a^x$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \cdot)$.

The inverse $\Psi : \mathbb{R}_{>0} \to \mathbb{R}$ is given by $\Psi(x) \log_a(x)$ and is also an isomorphism.

Example 18: Let X and Y be sets with $|X| = |Y|$. Choose a bijection $f : X \to Y$. Then, the map:

$$\Phi : S_X \to S_Y \tag{229}$$

defined by $\phi(\sigma) = f \circ \sigma \circ f^{-1}$ for all $\sigma \in S_X$ is an isomorphism.

Recall that $S_x = \{\sigma : X \to X | \sigma \text{ is a bijection}\}$.

Lemma 12:

1. For every group G, id : $G \to G$ is an isomorphism.
2. For every isomorphism $\phi : G \to H$, its inverse ϕ^{-1} is an isomorphism.
3. If $\phi : G \to H$ and $\psi : H \to K$ are isomorphisms, then so is $\psi \circ \phi : G \to K$.

Proof. We prove each individually

1. This is immediate.
2. Let $\phi : G \to H$ be an isomorphism. Then $\phi^{-1} : H \to G$ exists and is a bijection, since ϕ is a bijection. All we have to do now is to show it respects the group operation.

   Let $h_1, h_2 \in H$ and let $g_1 = \phi^{-1}(h_1)$ and $g_2 = \phi^{-1}(h_2)$. Then:

   $$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \tag{230}$$

   since ϕ is an isomorphism. Therefore:

   $$g_1 g_2 = \phi^{-1}(\phi(g_1 g_2)) = \phi^{-1}(h_1 h_2). \tag{231}$$

   Since $g_1 = \phi^{-1}(h_1)$ and $g_2 = \phi^{-1}(h_2)$, we get:

   $$\phi^{-1}(h_1 h_2) = \phi^{-1}(h_1)\phi^{-1}(h_2) \tag{232}$$

3. Let $\phi : G \to H$, $\psi : H \to K$ be isomorphisms. Then $\psi\phi : G \to K$ is a bijection since it is a composition of bijections.

   And for all $g_1, g_2 \in G$, we have:

   $$\begin{aligned}
   (\psi \circ \phi)(g_1 g_2) &= \psi(\phi(g_1 g_2)) && (233) \\
   &= \psi(\phi(g_1)\phi(g_2)) && (234) \\
   &= \psi(\phi(g_1)\psi(\phi(g_2)) && (235) \\
   &= (\psi \circ \phi)(g_1)(\psi \circ \phi)(g_2) && (236)
   \end{aligned}$$

   Therefore $\psi \circ \phi$ is an isomorphism.

□

- This is an important result because it means:
  1. For all groups G, we have $G \simeq G$.
  2. If $G \simeq H$, then $H \simeq G$.
  3. If $G \simeq H$ and $H \simeq K$, then $G \simeq K$.

  So, $\simeq$ is an equivalence relation on the class of all groups.

Definition: An automorphism of a group G is an isomorphism from G to itself.

Example 19: Let $p > 0$. Define $\phi : R_{>0} \to R_{>0}$ by $\phi(x) = x^p$ for all $x \in \mathbb{R}_{>0}$. This is an automorphism of $(\mathbb{R}_{>0}, \cdot)$.

This is true because for all $x, y \in \mathbb{R}_{>0}$, $\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$ and $\psi : R_{>0} \to R_{>0}$ is defined by $\psi(x) = x^{1/p}$ for all $x \; in \mathbb{R}_{>0}$ is the inverse of ϕ.

Example 20: For every $c \in \mathbb{R}^x$, the map $\phi : \mathbb{R} \to \mathbb{R}$ defined by $\phi(x) = cx$ is an automorphism of $(\mathbb{R}, +)$.

Example 21: If G is an abelian group, then $\phi : G \to G$ defined by $\phi(g) = g^{-1}$ for all $g \in G$ is an automorphism of G.

Definition: For each group G, define $\mathrm{Aut}(G)$ to be the set of automorphisms of G. Then $\mathrm{Aut}(G)$ is a group under composition and is called the automorphism group of G.

- The automorphisms of a group G are the "symmetries" of G and $\mathrm{Aut}(G)$ is the symmetry group of G.

9 Lecture Nine

- Recall that for a group G, $\mathrm{Aut}(G)$ is the set of all automorphisms of G, i.e. isomorphisms from G to itself, and $\mathrm{Aut}(G)$ is a group under composition. $\mathrm{Aut}(G)$ is called the automorphism group.

Proposition 10: Let G be a group and $a \in G$. The map

$$\mathrm{Int}(a) : G \to G \tag{237}$$

defined by $\mathrm{Int}(a)(g) = aga^{-1}$ for all $g \in G$ is an automorphism of G, called an **inner automorphism** of G. We define:

$$\mathrm{Int}(G) = \mathrm{Inn}(G) = \{\mathrm{Int}(a) : a \in G\} \tag{238}$$

We have $\mathrm{Int}(G) \le \mathrm{Aut}(G)$, called the group of inner automorphisms.

Proof. Let $a \in G$. Note that $\mathrm{Int}(a^{-1})$ is the inverse of $\mathrm{Int}(a)$ since for all $g \in G$ we have:

$$\mathrm{Int}(a)(\mathrm{Int}(a^{-1})(g)) = a(a^{-1}ga)a^{-1} = g \tag{239}$$

and:

$$\mathrm{Int}(a^{-1})(\mathrm{Int}(a)(g)) = a^{-1}(aga^{-1})a = g \tag{240}$$

Therefore, $\mathrm{Int}(a)$ is a bijection from G to itself.

Let $g_1, g_2 \in G$. Then:

$$\begin{aligned} \mathrm{Int}(a)(g_1 g_2) &= a(g_1 g_2)a^{-1} && (241)\\ &= a g_1 a^{-1} a g_2 a^{-1} && (242)\\ &= \mathrm{Int}(a)(g_1)\,\mathrm{Int}(a)(g_2) && (243) \end{aligned}$$

Therefore, $\mathrm{Int}(a) \in \mathrm{Aut}(G)$. For each $a \in G$, $\mathrm{Int}(a) \in \mathrm{Int}(G)$ by definition. Therefore: $\mathrm{Int}(G) \neq \emptyset$. Let $a, b \in G$. Then we claim that:

$$\mathrm{Int}(a)^{-1} = \mathrm{Int}(a^{-1}) \tag{244}$$

and $\mathrm{Int}(a)\,\mathrm{Int}(b) = \mathrm{Int}(ab)$. We already proved (1). Let $g \in G$. Then:

$$\begin{aligned}
\mathrm{Int}(a)(\mathrm{Int}(b)(g)) &= a(bgb^{-1})a^{-1} &(245)\\
&= abgb^{-1}a^{-1} &(246)\\
&= (ab)g(ab)^{-1} &(247)\\
&= \mathrm{Int}(ab)g &(248)
\end{aligned}$$

This proves part (2) of the 2-step subgroup test. By the 2 step subgroup test, $\mathrm{Int}(G) \leq \mathrm{Aut}(G)$. □

- In general, $\mathrm{Int}(G) \neq \mathrm{Aut}(G)$.
- We introduce the notion of homomorphisms.

Definition: Let G and H be groups. A homomorphism from G to H is a map $\phi : G \to H$ that respects the group operations, i.e. for all $g_1, g_2 \in G$, we have:

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) \tag{249}$$

The difference between a homomorphism and an isomorphism is that ϕ does not have to be bijective.

- Here are a few examples:
  1. Every isomorphism is a homomorphism.
  2. $\det : GL_n(F) \to F^\times$ is a homomorphism for any field F (i.e. $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z})^\times$)
  3. $\mathrm{sgn} : S_n \to \{\pm 1\}$ is a homomorphism.
  4. $|\cdot| : \mathbb{R}^\times \to \mathbb{R}_{>0}$ and $|\cdot| : \mathbb{C}^\times \to \mathbb{R}_{>0}$ are homomorphisms.
  5. If G is an abelian group and $k \in \mathbb{Z}$, then the map

     $$\phi : G \to G \tag{250}$$

     defined by $\phi(a) = a^k$ for all $a \in G$ is a homomorphism.

     Proof. If $a, b \in G$, then $\phi(ab) = (ab)^k = a^k b^k = \phi(a)\phi(b)$. □

     Remarks: Note that if G is written additively, then $\phi(a) = ka$.
  6. If $H \leq G$, then the map $i : H \to G$ defined by $i(h) = h$ for all $h \in H$ is an injective homomorphism.
  7. $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ defined by $\phi(x) = [x]$ for all $x \in \mathbb{Z}$ is a surjective homomorphism.
  8. $\phi : \mathbb{C} \to \mathbb{C}^\times$ defined by $\phi(z) = e^z$ is a surjective homomorphism.

Proposition 11: If $\phi : G \to H$ and $\phi : H \to K$ are homomorphisms, then $\phi \circ \phi : G \to K$ is a homomorphism.

Proposition 12: Let $\phi : G \to H$ be a homomorphism. Then:
1. $\phi(e) = e$ (note that the e belongs to different groups)
2. For all $n \in \mathbb{Z}$ and for all $g \in G$, we have

$$\phi(g^n) = \phi(g)^n \tag{251}$$

Proof. We prove both parts:

1. Since $\phi(e) = \phi(ee) = \phi(e)\phi(e)$, we have $e = \phi(e)$ by multiply on both sides by $\phi(e)^{-1}$.
2. For all $g \in G$ and for all $n \in \mathbb{Z}_{\geq 0}$, we have $\phi(g^n) = \phi(g)^n$ by a simple induction argument. Now,

   $$e = \phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) \tag{252}$$

MMultiplying both sides by $\phi(g)^{-1}$ on the left gives $\phi(g)^{-1} = \phi(g^{-1})$. For all $g \in G$ and all $n \in \mathbb{Z}_{>0}$, we have:

$$\begin{aligned} \phi(g^{-n}) &= \phi((g^{-1})^n) && (253)\\ &= \phi(g^{-1})^n && (254)\\ &= (\phi(g)^{-1})^n && (255)\\ &= \phi(g)^{-n} && (256) \end{aligned}$$

□

Corollary 10: Let $\phi : G \to H$ be a homomorphism. If $g \in G$ and $o(g) < \infty$, then $o(\phi(g))|o(g)$.

- Let $k_1, \ldots, k_r, \ell_1, \ldots, \ell_s \in \mathbb{Z}$ and consider the equation which we denote as (*):

$$x_1^{k_1} \cdots x_r^{k_r} = y_1^{\ell_1} \cdots y_s^{\ell_s} \quad (257)$$

For $(a_1, \ldots, a_r, b_1, \ldots, b_s) \in G$, we say that $(a_1, \ldots, a_r, b_1, \ldots, b_s)$ is a solution to the above equation if:

$$a_1^{k_1} \cdots a_r^{k_r} = b_1^{\ell_1} \cdots b_s^{\ell_s} \quad (258)$$

- Let $\phi : G \to H$ be a homomorphism. Then:
  1. For all $(a_1, \ldots, a_r, b_1, \ldots, b_s) \in G^{r+s}$, then $(a_1, \ldots, a_r, b_1, \ldots, b_s)$ is a solution to (8) in G, which implies:

  $$(\phi(a_1), \ldots, \phi(a_r), \phi(b_1), \ldots, \phi(b_s)) \quad (259)$$

  is a solution to $(*)$ in H.
  2. If ϕ is an isomorphism, then for all $(a_1, \ldots, a_r, b_1, \ldots, b_s) \in G^{r+s}$, then the converse of the above holds.

10 Lecture Ten

- As a consequence of the result from last lecture, we have the following proposition:

Proposition 13: Let $\phi : G \to H$ be an isomorphism.
1. For all $a, b \in G$, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
2. G is abelian if and only if H is abelian.
3. For all $n \in \mathbb{Z}_{>0} \cap \{\infty\}$ and for all $a \in G$, $o(a) = n$ if and only if $o(\phi(a)) = n$.
4. G is cyclic if and only if H is cyclic.
5. For all $S \subseteq G$ and $a \in G$, $a \in C_G(S)$ if and only if $\phi(a) \in C_H(\phi(S))$ (i.e. a commutes with every element of S if and only if $\phi(a)$ commutes with every element of $\phi(S)$).
   In particular, $\phi(C_G(S)) = C_H(\phi(S))$. Taking $S = G$ gives $\phi(Z(G)) = Z(H)$. Recall that:

   $$C_G(S) = \{g \in G | gs = sg, \forall s \in S\} \quad (260)$$

   This is a subgroup of G called the centralizer of S in G. And:

   $$Z(G) = C_G(G) = \{g \in G | gx = xg, \forall x \in G\} \quad (261)$$

   and is called the center of G.

- Next, we relate homomorphisms and subgroups.

Proposition 14: Let $\phi : G \to H$ be a homomorphism.
1. If $K \leq G$, then $\phi(K) := \{\phi(k) : k \in K\} \leq H$.
2. If $K \leq H$, then:

$$\phi^{-1}(K) := \{g \in G | \phi(g) \in K\} \leq G. \quad (262)$$

This can be proved via the one-step subgroup test.

Definition: Let $\phi : G \to H$ be a homomorphism. The image of ϕ is the subgroup:

$$\operatorname{im}(\phi) := \phi(G) \tag{263}$$

of H. The kernel of ϕ is the subgroup:

$$\ker(\phi) := \phi^{-1}(\{e\}) \tag{264}$$

of G.

- Note that if we let $\phi : G \to H$ be a homomorphism.
  1. If $K \leq G$, then $\phi|_K : K \to H$ is a homomorphism.
  2. If $K \leq H$ and $\operatorname{im}(\phi) \subseteq K$, then the map $\phi|^K : G \to K$ defined by restricting the codomain of ϕ is a homomorphism.
- Remark: If G is a group, $K_1, K_2 \leq G$, and $K_1 \subseteq K_2$, then $K_1 \leq K_2$.
- Note that a homomorphism $\phi : G \to H$ is surjective iff $\operatorname{im}\phi = H$ and is injective iff the map $\phi|^K : G \to \operatorname{im}\phi$ is an isomorphism.

Proposition 15: Let $\phi : G \to H$ be a homomorphism.
1. For all $a, b\, inG$, the following are equivalent:
   (a) $\phi(a) = \phi(b)$
   (b) $ab^{-1} \in \ker(\phi)(\iff ba^{-1} \in \ker\phi)$
   (c) $b^{-1}a \in \ker\phi$
2. ϕ is injective iff $\ker\phi = \{e\}$

Proof. We prove both parts:

1. Let $a, b \in G$. Then:

$$\phi(a) = \phi(b) \iff \phi(a)\phi(b)^{-1} = e \tag{265}$$
$$\iff \phi(ab^{-1}) = e \tag{266}$$
$$\iff ab^{-1} \in \ker\phi \tag{267}$$

   Similarly, $\phi(a) = \phi(b) \iff b^{-1}a \in \ker\phi$.

2. Suppose ϕ is injective. Then for all $a \in G$ with $a \neq e$, we have $\phi(a) \neq \phi(e) = e$, so $a \notin \ker\phi$. Therefore $\ker\phi \subseteq \{e\}$. Since $e \in \ker\phi$, $\ker\phi = \{e\}$.

   Suppose $\ker\phi = \{e\}$. Let $a, b \in G$ and assume $\phi(a) = \phi(b)$. By (1), we have $ab^{-1} \in \ker\phi = \{e\}$. Therefore, $ab^{-1} = e$, i.e. $a = b$.

□

Proposition 16: Let $\phi : G \to H$ be a homomorphism and let $K \leq G$.
1. If K is abelian, then $\phi(K)$ is abelian.
2. If K is cyclic, then $\phi(K)$ is cyclic. In fact, if $a \in G$, then:

$$\phi(\langle a \rangle) = \langle \phi(a) \rangle. \tag{268}$$

Proof. 1. Suppose K is abelian. Let $h_1, h_2 \in \phi(K)$. There exists $k_1, k_2 \in K$ s.t. $h_1 = \phi(k_1)$ and $h_2 = \phi(k_2)$. Then:

$$h_1h_2 = \phi(k_1)\phi(k_2) = \phi(k_1k_2) \tag{269}$$

and:

$$h_2h_1 = \phi(k_2)\phi(k_1) = \phi(k_2k_1) \tag{270}$$

Since K is abelian, $k_1k_2 = k_2k_1$. Therefore, $h_1h_2 = h_2h_1$. Thus, $\phi(K)$ is abelian.

2. Let K be a cyclic subgroup of G and let a be a generator of K. Then:

$$\begin{aligned}
\phi(K) &= \phi(\langle a\rangle) && (271)\\
&= \phi(\{a^k : k \in \mathbb{Z}\}) && (272)\\
&= \{\phi(a^k) : k \in \mathbb{Z}\} && (273)\\
&= \{\phi(a)^k : k \in \mathbb{Z}\} && (274)\\
&= \langle \phi(a)\rangle. && (275)
\end{aligned}$$

□

Warning: The converse is not necessarily true. Note that if G is non-abelian, H is any group, and $\phi : G \to H$ is the trivial homomorphism, then $\phi(G) = \{e\}$, which is cyclic (hence abelian), but G is non-abelian (hence non-cyclic).

- Define $L_g : G \to G$ by $L_g(x) = gx$. For all $g_1, g_2 \in G$, we have:

$$L_{g_1 g_2} = L_{g_1} \circ L_{g_2} \tag{276}$$

Proof. Let $g_1, g_2 \in G$. For all $x \in G$, we have:

$$\begin{aligned}
L_{g_1 g_2}(x) &= (g_1 g_2)x && (277)\\
&= g_1(g_2 x) && (278)\\
&= g_1 L_{g_2}(x) && (279)\\
&= L_{g_1}(L_{g_2}(x)) && (280)
\end{aligned}$$

□

Therefore, $L_{g_1 g_2} = L_{g_1} \circ L_{g_2}$.

- Notice that $L_e = \text{id}_G$. Indeed, for all $x \in G$, we have $L_e(x) = ex = x$.
- For all $g \in G$, we have $(L_g)^{-1} = L_{g^{-1}}$.

Proof. Let $g \in G$. Then:

$$L_{g^{-1}} \circ L_g = L_{g^{-1}g} = L_e = \text{id} \tag{281}$$

and:

$$L_g \circ L_{g^{-1}} = L_{gg^{-1}} = L_e = \text{id} \tag{282}$$

Therefore, for all $g \in G$ the map $L_g : G \to G$ is a permutation. □

- We have a map $L : G \to L_g$, $g \mapsto L_g$. Recall that $S_g = \{f : G \to G | f \text{ is a bijection}\}$.

Theorem: Cayley's Theorem: The map $L : G \to S_G$ is an injective homomorphism. Therefore $L : G \to \operatorname{im} L$ is an isomorphism from G to the permutation group $\operatorname{im} L$.

Proof. We already proved that L is a homomorphism. To prove that L is injective, we must prove that $\ker L = \{e\}$. Let $g \in \ker L$, i.e. $L_g = \text{id}_G$. Therefore $g = ge = L_g(e) = \text{id}_G(e) = e$. Thus $\ker L \subseteq \{e\}$. Since $e \in \ker L$, we have $\ker L = \{e\}$. □

- The map $L : G \to S_G$ is called the Cayley permutation representation of G and the left regular permutation representation of G.
- Let us study homomorphisms from cyclic groups..

Theorem: Let G be an infinite cyclic group, let a be a generator of G, and let H be a group.
1. For every $b \in H$, the map:
$$\phi_b = \phi_{a,b} : G \to H \tag{283}$$
defined by $\phi_b(a^k) = b^k$ for all $k \in \mathbb{Z}$ is well defined and is a homomorphism.
2. Every homomorphism $\phi : G \to H$ is of the form ϕ_b for a unique $b \in H$.
3. For all $b \in H$, ϕ_b is injective iff $o(b) = \infty$ and ϕ_b is surjective iff $H = \langle b\rangle$.

Proof. 1. Let $b \in H$. The map ϕ_b is well defined since every element of G is of the form a^k for a unique $k \in \mathbb{Z}$. It is a homomorphism since for all $k_1, k_2 \in \mathbb{Z}$,

$$\begin{aligned} \phi_b(a^{k_1}a^{k_2}) &= \phi_b(a^{k_1+k_2}) && (284)\\ &= b^{k_1+k_2} && (285)\\ &= b^{k_1}b^{k_2} && (286)\\ &= \phi_b(a^{k_1})\phi_b(a^{k_2}) && (287) \end{aligned}$$

2. Let $\phi : G \to H$ be a homomorphism. Define $b = \phi(a)$ for all $k \in \mathbb{Z}$, we have $\phi(a^k) = \phi(a)^k = b^k$, so $\phi = \phi_b$.
3. Let $b \in H$. We know ϕ_b is injective if and only if for all $k \in \mathbb{Z} \setminus \{0\}$, $\phi(a^k) \neq e$. This is true if and only if $o(b) = \infty$.

   since:

$$\begin{aligned} \operatorname{im}\phi_b &= \phi_b(G) && (288)\\ &= \phi_b(\langle a \rangle) && (289)\\ &= \langle \phi_b(a) \rangle && (290)\\ &= \langle b \rangle && (291) \end{aligned}$$

   ϕ_b is surjective iff $H = \langle b \rangle$.

□

Theorem: Let G be a finite cyclic group of order n, let a be a generator of G, and let H be a group.
1. For every $b \in H$ with $b^n = e$, the map:
$$\phi_b = \phi_{a,b} : G \to H \quad (292)$$
defined by $\phi_b(a^k) = b^k$ for all $k \in \mathbb{Z}$ is a well defined homomorphism.
2. Every homomorphism $\phi : G \to H$ is of the form ϕ_b for a unique $b \in H$ with $b^n = e$.
3. For all $b \in H$ with $b^n = e$, ϕ_b is injective if and only if $o(b) = n$ and ϕ_b is surjective if and only iff $H = \langle b \rangle$.

11 Lecture Eleven

- We begin by proving the theorem from last lecture:

Proof. 1. Let $b \in H$ with $b^n = e$. To prove that ϕ_b is well defined, we must prove that for all $k_1, k_2 \in \mathbb{Z}$, if $a^{k_1} = a^{k_2}$, then $b^{k_1} = b^{k_2}$.

   Let $k_1, k_2 \in \mathbb{Z}$ with $a^{k_1} = a^{k_2}$. Then $n | k_1 - k_2$. Since $b^n = e$, we have $b^{k_1 - k_2} = e$ so $b^{k_1} = b^{k_2}$. Therefore the map $\phi_b : G \to H$ is well defined.

   For all $k_1, k_2 \in \mathbb{Z}$, we have:

$$\phi_b(a^{k_1}a^{k_2}) = \phi_b(a^{k_1+k_2}) = b^{k_1+k_2} = b^{k_1}b^{k_2} = \phi_b(a^{k_1})\phi_b(a^{k_2}) \quad (293)$$

   Therefore, ϕ_b is a homomorphism.

2. Let $\phi : G \to H$ be a homomorphism. Let $b = \phi(a)$. Then for all $k \in \mathbb{Z}$, we have:

$$b^k = \phi(a)^k = \phi(a^k). \quad (294)$$

   and if $k = n$, we get:

$$b^n = \phi(a^n) = \phi(e) = e \quad (295)$$

3. Since the non-identity element of $G = \langle a \rangle$ are $a, a^2, \ldots, a^{n-1}$,

$$\begin{aligned} \phi_b \text{ is injective} &\iff \ker\phi_b = \{e\} && (296)\\ &\iff \forall k = 1, \ldots, n-1,\ \phi_b(a^k) \neq e && (297)\\ &\iff \forall k = 1, \ldots, n-1,\ b^k \neq e && (298) \end{aligned}$$

Since $b^n = e$, this statement holds if and only if $o(b) = n$. Since

$$\operatorname{im}\phi_b = \phi_b(\langle a\rangle) = \langle \phi_b(a)\rangle = \langle b\rangle, \tag{299}$$

we have that ϕ_b is surjective if and only if $H = \langle b\rangle$.

□

Corollary 11: Let G and H be cyclic groups:

1. $G \simeq H$ iff $|G| = |H|$
2. If $|G| = |H|$, an a is a generator of G then the distinct isomorphisms from G to H are the maps $\phi_{a,b} : G \to H$ for b a generator of H.
   If we then show the converse in a similar manner, then we are done.

Corollary 12: Let G be a cyclic group.

1. If $|G| = \infty$, then the map:
   $$\theta_a : \{\pm 1\} \to \operatorname{Aut}(G) \tag{300}$$
   defined by $\theta_a(k) = \phi_{a,a^k}$ is an isomorphism. Thus:
   $$\operatorname{Aut}(G) \simeq \{\pm 1\} \tag{301}$$
2. If $|G| = n < \infty$, then the map
   $$\theta_a : (\mathbb{Z}/n\mathbb{Z})^\times \to \operatorname{Aut}(G) \tag{302}$$
   defined by $\theta_a([k]) = \phi_{a,a^k}$ is a well-defined isomorphism. Thus:
   $$\operatorname{Aut}(G) \simeq (\mathbb{Z}/n\mathbb{Z})^\times \tag{303}$$

- We introduce cosets and Lagrange's theorem. We start this by defining some notation.
- Let G be a group:
  1. For $S \subseteq G$, define $S^{-1} = \{s^{-1} : s \in S\}$.
  2. For $S_1, \ldots, S_r \subseteq G$, define:
     $$S_1 \cdots S_r = \{s_1 \ldots s_r : s_1 \in S_1, \ldots, s_r \in S_r\}. \tag{304}$$
     For $a \in G$, we write:
     $$aS = \{a\}S = \{as : s \in S\} \tag{305}$$
     $$Sa = S\{a\} = \{sa : s \in S\} \tag{306}$$
     and:
     $$aSa^{-1} = \{a\}S\{a\}^{-1} = \{asa^{-1} : s \in S\} \tag{307}$$
- Note that:
  1. $(S^{-1})^{-1} = S$ for all $S \subseteq G$.
  2. If $S_1, \ldots, S_r \subseteq G$, then:
     $$(S_1 \cdots S_r)^{-1} = S_r^{-1} \cdots S_1^{-1} \tag{308}$$
  3. If $S_1, S_2, S_3 \subseteq G$, then:
     $$(S_1S_2)S_3 = S_1(S_2S_3) \tag{309}$$
  4. If $S \subseteq G$ and $a, b \in S$, then $(aS)^{-1} = S^{-1}a^{-1}$ and $(Sa)^{-1} = a^{-1}S^{-1}$, $(ab)S = a(bS)$, and $S(ab) = (Sa)b$.

Definition: Let G be a group and $H \leq G$. Sets of the form aH for $a \in G$ are called **left corsets of H in G**, and sets of the form Ha for $a \in G$ are called right corsets of H in G.
We say that $a \in G$ is a representation of the left coset aH and a representative of the right coset Ha.

Proposition 17: If G is a group and $H \leq G$, then for all $a \in G$ we have $aHa^{-1} \leq G$.

Example 22: Let $G = D_3 = \{e, r, r^2, s, rs, r^2s\}$. Let $H = \langle s \rangle = \{1, s\} \leq G$. Let us find all the left cosets:

$$eH = \{e^2, es\} = \{e, s\} = H \tag{310}$$
$$rH = \{re, rs\} = \{r, s\} \tag{311}$$
$$r^2H = \{r^2e, r^2s\} = \{r^2, r^2s\} \tag{312}$$
$$sH = \{se, s^2\} = \{e, s\} \tag{313}$$
$$(rs)H = r(sH) = rH \tag{314}$$
$$r^2sH = r^2(sH) = r^2H \tag{315}$$

Note that r^2s and r^2 are not equal, but they represent the same coset. For the right cosets:

$$He = H \tag{316}$$
$$Hr = \{r, sr\} = \{r, r^2s\} \tag{317}$$
$$Hr^2 = \{r^2, sr^2\} = \{r^2, rs\} \tag{318}$$
$$Hs = H \tag{319}$$
$$H(rs) = H(sr^2) = (Hs)r^2 = Hr^2 \tag{320}$$
$$H(r^2s) = H(sr) = (Hs)r = Hr \tag{321}$$

Notice that the only left coset of H that is also a right coset is id$H = H = H$id.

This isn't always the case. If G is abelian and $H \leq G$, then $aH = Ha$ for all $a \in G$. Actually, you only need a to commute with every element of H, i.e. the center.