MAT301 Notes

QiLin Xue

May 11, 2021

Contents

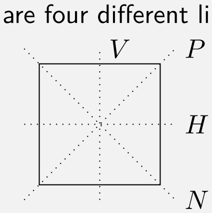
1 Lecture One

- 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:
$$\text{Sym}(F) \equiv \{\sigma : F \to F | \sigma \text{ is a symmetry}\} \tag{4}$$

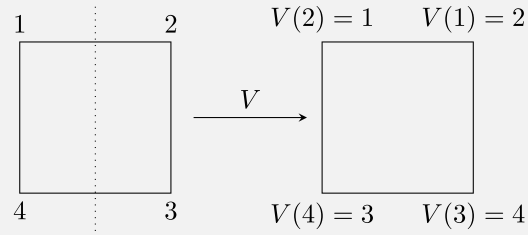
- For example, any point, line, shape, or form is a figure. However, we are only interested in figures that have interesting symmetries.

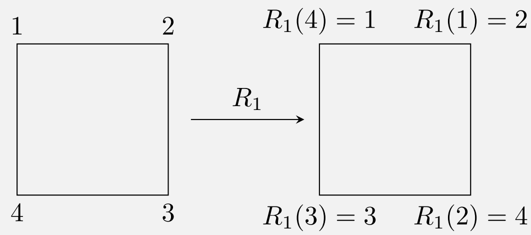
Example 1: Let F be a square in $\mathbb{R}^2$. There are four different lines of reflections:



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:



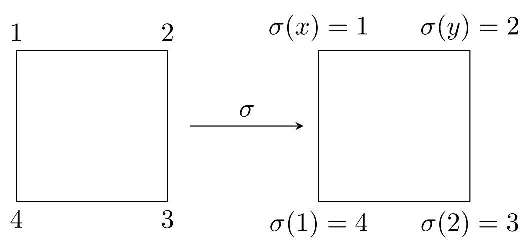


Applying the computations:

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

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

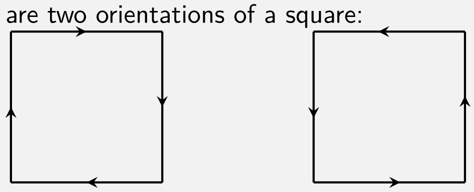
  By the above facts, we must count the ordered pairs (x, y) such that $x, y \in \{1, 2, 3, 4\}$ and x is adjacent to y:
  - There are 4 choices for x.
  - For each choice of x, there are two choices of y. Therefore, there are $4 \times 2 = 8$ symmetries.

  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:
  - $(\mathrm{Sym}\,(X), \circ)$
  - $(\mathbb{Z}, +)$
  - $(\mathbb{R}^x, \cdot)$ 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
  $$\mu_n = \{z \in \mathbb{C} | z^n = 1\} = \{e^{2\pi ki/n} | k = 0, 1, \dots, n-1\} \tag{18}$$
  - $(\mathbb{R}^n, +)$
  - $(\mathsf{GL}_n(F), \cdot)$ 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:

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

- 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:

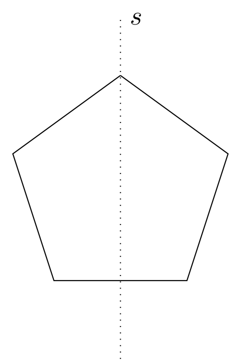
$$|D_n| = |\{(v_i, v_j) | j \equiv i \pm 1 \pmod{n}\}| = n \cdot 2 \tag{48}$$

□

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

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

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 $\frac{2\pi}{n}$, 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:
$$sr^k = r^{-k}s = r^{n-k}s \tag{50}$$
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:
$$(sr^k)^2 = 1 \tag{51}$$
$$sr^k sr^k = 1 \tag{52}$$
$$sr^k s = r^{-k} \tag{53}$$
$$sr^k = r^{-k}s^{-1} \tag{54}$$
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 $1, r, \dots, r^{n-1}$ 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:
$$*_G : G \times G \to G \tag{56}$$
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.

$\square$

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. □