GEOMETRY AND SYMMETRY, FALL 2022

Contents

If you'd like to read more or find more exercise problems, here are some recommended reference books:

- M. A. Armstrong, *Groups and Symmetry*
- M. Artin, *Algebra*
- E. G. Rees, *Notes on Geometry*

1. Overview of the course

Lecture 1

We will explore the *symmetries* of various *geometric spaces* in this course. The spaces that we will consider include: the Euclidean spaces $\mathbb{R}^2$, $\mathbb{R}^3$, the spheres S^1, S^2, the hyperbolic space $\mathbb{H}^2$, and some of their interesting subsets.

Let us consider the following shapes in $\mathbb{R}^2$. Intuitively, we know that a square is "more symmetric" than a rectangle, and a rectangle is "more symmetric"

than an arbitrary 4-gon. In order to make sense of these statements, we have to define what are *symmetries* of these shapes.

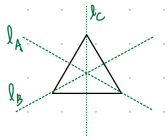
Each of the geometric spaces that we will consider ($\mathbb{R}^2$, $\mathbb{R}^3$, S^1, S^2, $\mathbb{H}^2$, etc.) has a natural metric (i.e. distance $d(x, y)$ between any two points x, y). The symmetries that we are interested in are the *isometries* (i.e. distance-preserving functions) of these spaces. For instance, an isometry of $\mathbb{R}^2$ is a function $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ such that $d(f(x), f(y)) = d(x, y)$ for any $x, y \in \mathbb{R}^2$.

Definition 1.1. Let $S \subseteq \mathbb{R}^2$ be a subset of $\mathbb{R}^2$. An isometry $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ is called a *symmetry of* S if we have $f(S) = S$, i.e.

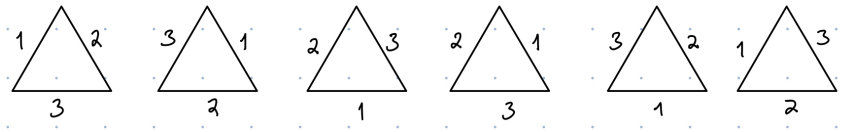
- for any $p \in S$, we have $f(p) \in S$; and
- for any $q \in S$, there exists $p \in S$ such that $f(p) = q$.

Example. Let us look at an easy example: an equilateral triangle. It has two kinds of symmetries:

- Rotational symmetries: one can rotate the triangle by $\frac{2\pi}{3}$, $\frac{4\pi}{3}$, or 2π without changing its appearance.
- Reflection symmetries: there are three "mirror lines" through which we can reflect the shape without changing its appearance.

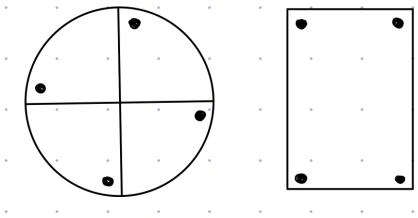


The easiest way to study the symmetries of a shape is by *counting*. In this example, it's easy to check that there are 6 symmetries. If we put labels on the edges of the triangle, then the effect of these symmetries look like:



However, counting alone is usually not good enough.

Example. Both of the following shapes have 4 symmetries. The shape on the



left has 4 rotational symmetries (by $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$, 2π), but no reflection symmetries. In contrast, the shape on the right has 2 rotational symmetries and 2 reflection symmetries. How can we distinguish them?

As we'll see later in this course, *group theory* provides rigorous tools to describe the symmetries of shapes. For any shape (or any geometric object), the set of its symmetries has a natural *group structure*. In the example above, although the sets of symmetries of both shapes have 4 elements, but their underlying group structures are different, and that's how we can tell them apart (e.g. consider the *orders* of elements in these two groups).

Another important tool that we will encounter is basic *linear algebra*, in particular *matrices* or *matrix groups*. The reason is that certain matrix groups ($\mathrm{O}(2,\mathbb{R})$, $\mathrm{O}(3,\mathbb{R})$, $\mathrm{SL}(2,\mathbb{R})$, $\mathrm{SL}(2,\mathbb{C})$, etc.) act naturally as isometries on the spaces that we are interested in like $\mathbb{R}^2$, $\mathbb{R}^3$, S^1, S^2, $\mathbb{H}^2$. For instance, you'll show in the homework that any isometry of the Euclidean space $\mathbb{R}^n$ is a composition of a translation and a linear transformation.

Now we mention some examples that we'll be studying in this course.

Example. Consider a regular n-gon P_n in $\mathbb{R}^2$. It is not hard to show that P_n has $2n$ symmetries. We'll:

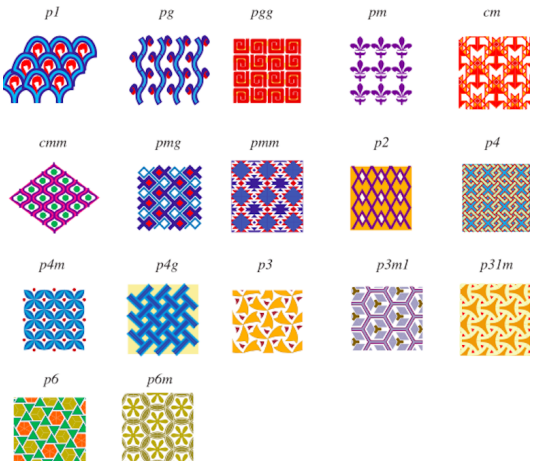
- discuss the group structure of the symmetry group of P_n (the resulting group is called the *dihedral group* D_n;
- prove that any finite subgroup of $\mathrm{O}(2,\mathbb{R})$ is either a cyclic group or the symmetry group of a regular n-gon.

Example. An important class of examples of subsets in $\mathbb{R}^3$, that possess many symmetries, are the Platonic solids (regular polyhedrons). We will:

- prove that there are only five of them;

- study their symmetry groups;
- more importantly, prove that any finite subgroup of $\mathrm{SO}(3,\mathbb{R})$ is either a cyclic group, a dihedral group, or the (rotational) symmetry group of one of the Platonic solids.

Example. A *wallpaper* is a mathematical object that covers the whole $\mathbb{R}^2$ by repeating a pattern indefinitely. The symmetry group of a wallpaper is called a *wallpaper group* (we will provide more precise definition later on). We will show that there are exactly 17 different wallpaper groups.



In later parts of this course, we'll discuss the isometries of some important non-Euclidean spaces, including the Riemann sphere S^2 (whose isometries are certain *Möbius transformations*), and the hyperbolic plane $\mathbb{H}$ (whose isometries form the *modular group*).

2. A crash course on basic group theory

2.1. **Binary operators.**

Before discussing the actual definition of a *group*, let us first consider a more general notion of *binary operators*.

Definition 2.1. Let S be a set. A *binary operator* on S is a function

$$\circ\colon S \times S \to S.$$

Example. Addition on the set of positive integers (denoted by $\mathbb{N}$), or the set of integers (denoted by $\mathbb{Z}$), or the set of rational numbers (denoted by $\mathbb{Q}$) or the set of real numbers (denoted by $\mathbb{R}$), is a binary operator. Same for multiplication.

Non-example. Subtraction on the set of positive integers is *not* a binary operator. Division on the set of integers is *not* a binary operator.

Definition 2.2. Let $(S, \circ)$ be a set with a binary operator. We say an element $e \in S$ is an *identity element* if $e \circ a = a \circ e = a$ for any $a \in S$.

Example. The element $0 \in \mathbb{Z}$ is an identity element of $(\mathbb{Z}, +)$. The element $1 \in \mathbb{Z}$ is an identity element of $(\mathbb{Z}, \times)$.

Non-example. $(\mathbb{N}, +)$ has no identity element.

Exercise. Prove that any set with a binary operator $(S, \circ)$ has at most one identity element.

Definition 2.3. Let $(S, \circ, e)$ be a set with a binary operator and an identity element. We say an element $a' \in S$ is an *inverse* of $a \in S$ if $a \circ a' = a' \circ a = e$.

Example. For $(\mathbb{Z}, +)$, the inverse of $a \in \mathbb{Z}$ is given by $-a$. For $(\mathbb{R}, \times)$, the inverse of $a \in \mathbb{R}$ is given by $1/a$, provided that $a \neq 0$.

Non-example. For $(\mathbb{Z}, \times)$, any element $a \in \mathbb{Z}$ has no inverse unless $a = \pm 1$.

Definition 2.4. Let $(S, \circ)$ be a set with a binary operator. We say $(S, \circ)$ is *associative* if $(a \circ b) \circ c = a \circ (b \circ c)$ holds for any $a, b, c \in S$.

Exercise. Let $(S, \circ, e)$ be a set with an associative binary operator and an identity element. Prove that any element in S has at most one inverse.

Most of the examples that we'll be discussing are associative. Here is a non-example (which we will not encounter in this course):

Non-example. The cross product $\times$ on $\mathbb{R}^3$ is *not* associative. Rather, it satisfies the *Jacobi identity*

$$\vec{v}_1 \times (\vec{v}_2 \times \vec{v}_3) + \vec{v}_2 \times (\vec{v}_3 \times \vec{v}_1) + \vec{v}_3 \times (\vec{v}_1 \times \vec{v}_2) = 0$$

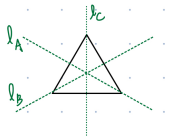
Definition 2.5. Let $(S, \circ)$ be a set with a binary operator. We say $(S, \circ)$ is *commutative* if $a \circ b = b \circ a$ for any $a, b \in S$.

Warning. Many of the examples that we'll consider are *not* commutative.

Non-example. Consider the set of all six geometric transformations that give the symmetries of an equilateral triangle:

$$S = \Big\{\text{rotate } 0,\ \text{rotate } \frac{2\pi}{3},\ \text{rotate } \frac{4\pi}{3},\ \text{reflect along } \ell_A,\ \text{reflect along } \ell_B,\ \text{reflect along } \ell_C\Big\}.$$

(note: rotations are typically assumed to be counterclockwise)

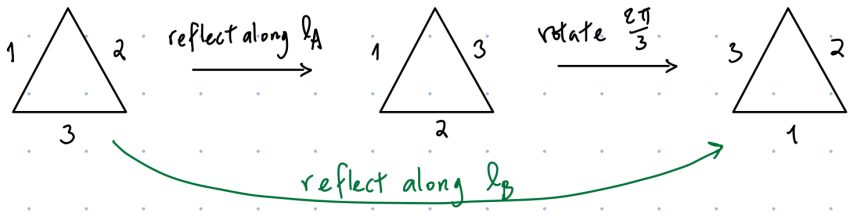


There is a binary operation on S given by *composing* these geometric transformations:

$$\circ\colon S \times S \to S,$$

where $a \circ b \in S$ is the transformation given by "do b, and then do a". For instance, we have

$$\Big(\text{rotate } \frac{2\pi}{3}\Big) \circ \Big(\text{reflect along } \ell_A\Big) = \text{reflect along } \ell_B.$$

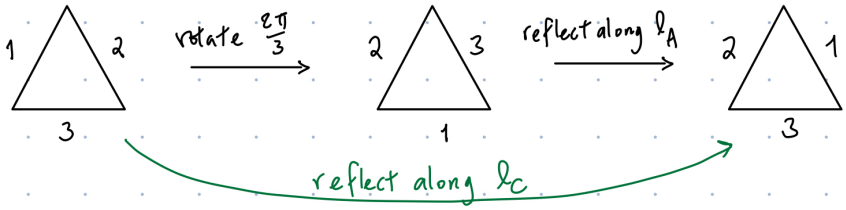


On the other hand, by reversing the order one gets

$$\Big(\text{reflect along } \ell_A\Big) \circ \Big(\text{rotate } \frac{2\pi}{3}\Big) = \text{reflect along } \ell_C.$$

This shows that $(S, \circ)$ is *not* commutative.

Non-example. Another important class of groups that we will discuss is the *matrix groups*. They are *not* commutative in most cases.



2.2. **Groups.**

Definition 2.6. Let $(G, \circ)$ be a set with a binary operator. It is called a *group* if it satisfies the following conditions:

(1) It is associative.
(2) It has the identity element (which will usually be denoted by e, e_G, 1, or 1_G).
(3) Any element $a \in G$ has an inverse (which will be denoted by $a^{-1} \in G$).

Remark 2.7. Here are some notions that we will be using frequently:

- If a group $(G, \circ)$ is commutative, then it is called an *abelian group*.
- We'll use $|G|$ to denote the number of elements in the set G, and will call it the *order* of G. Note that the order of a group could be infinite in general.
- We quite often would omit "$\circ$", and simply denote $a \circ b$ by ab, denote $a \circ a$ by a^2, denote $a \circ a \circ a$ by a^3, and so on.

Example. Consider the set of integers modulo n

$$\mathbb{Z}/n\mathbb{Z} \coloneqq \left\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\right\}.$$

Addition and multiplication are well-defined on $\mathbb{Z}/n\mathbb{Z}$. It's not hard to show that $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group of order n, with the identity given by $\bar{0}$.

Example. Consider the subset of $\mathbb{Z}/n\mathbb{Z}$ consisting of elements that are coprime with n:

$$(\mathbb{Z}/n\mathbb{Z})^* \coloneqq \left\{\overline{m} \in \mathbb{Z}/n\mathbb{Z} \colon \gcd(m, n) = 1\right\}.$$

It's not hard to show that $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ is an abelian group, with the identity given by $\bar{1}$.

Example. The set of all integers $\mathbb{Z}$ under addition is an example of an abelian group with infinite order.

Example. The set $\{0\}$ under addition is an example of a group with only one element (a trivial group).

Example. Let G_1 and G_2 be two groups. Consider the set

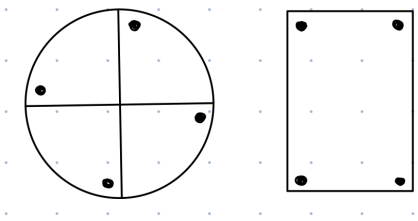
$$G_1 \times G_2 \coloneqq \Big\{(g_1, g_2) \colon g_1 \in G_1 \text{ and } g_2 \in G_2\Big\}.$$

Define a binary operator on $G_1 \times G_2$ as follows:

$$(g_1, g_2) \circ (g_1', g_2') \coloneqq (g_1 \circ g_1', g_2 \circ g_2').$$

It's not hard to show that $(G_1 \times G_2, \circ)$ is also a group. It's called the *direct product* of G_1 and G_2.

Example. Let's come back to the following examples again. As discussed ear-



lier, the symmetries of a shape form a group, where the binary operation is given by composition. The symmetry group of the first shape is

$$G_1 \coloneqq \Big\{\text{rotate } 0,\ \text{rotate } \frac{\pi}{2},\ \text{rotate } \pi,\ \text{rotate } \frac{3\pi}{2}\Big\}.$$

One thing we might notice about this group is that all elements of the group can be obtained by taking one element of the set, and combining it different number of times. Let's denote rotate $\frac{\pi}{2}$ by a. Then G_1 can be rewritten as

$$G_1 = \{e, a, a^2, a^3\}.$$

Notice that $a^4 = e$ since rotate 2π is the same as rotate 0, i.e. the identity map. The same is true for $\mathbb{Z}/4\mathbb{Z}$ (under addition) if one lets $a = \bar{1}$ and note that $a^4 = \bar{4} = \bar{0} = e$ in $\mathbb{Z}/4\mathbb{Z}$. In fact, we'll see that the symmetry group of the first shape and $\mathbb{Z}/4\mathbb{Z}$ are *isomorphic*, which means that they are essentially the same group.

On the other hand, the symmetry group of the second shape is

$$G_2 \coloneqq \Big\{\text{rotate } 0,\ \text{rotate } \pi,\ \text{reflect along } \ell_1,\ \text{reflect along } \ell_2\Big\}.$$

It's not hard to see that there is no element $a \in G_2$ such that $G_2 = \{e, a, a^2, a^3\}$. Therefore, G_2 and G_1 are not isomorphic. In fact, one can show that G_2 is isomorphic to the direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2.3. **Homomorphisms.** For any mathematical structure (like groups), it is crucially important to understand how two structures of the same type (like two groups) are related in a meaningful way. Functions that bridge such two structures are called *homomorphisms*. (In the Ancient Greek language, "homos" means "same", and "morphe" means "form" or "shape".) In general, a homomorphism is a function between two mathematical structures of the same type, that preserves the operations of the structures.

Definition 2.8. Let G and H be two groups. A function $f\colon G \to H$ is called a *homomorphism* if for any $g_1, g_2 \in G$ we have

$$f(g_1 g_2) = f(g_1) f(g_2)$$

Furthermore, a homomorphism that is both injective and surjective is called an *isomorphism*. In this case, we'll use the notation "$G \cong H$".

In other words, a homomorphism is a function that is compatible with the binary operations on the two groups.

Exercise. Let $f\colon G \to H$ be a group homomorphism. Prove that

- It preserves the identity: $f(e_G) = e_H$.
- It preserves the inverses: $f(g^{-1}) = f(g)^{-1}$ for any $g \in G$.

Example. We considered the symmetry group

$$G_1 \coloneqq \left\{\text{rotate } 0,\ \text{rotate } \frac{\pi}{2},\ \text{rotate } \pi,\ \text{rotate } \frac{3\pi}{2}\right\} = \{e, a, a^2, a^3\}$$

where $a^4 = e$. One can define a function

$$G_1 \to \mathbb{Z}/4\mathbb{Z}$$

by sending $e \mapsto \bar{0}$, $a \mapsto \bar{1}$, $a^2 \mapsto \bar{2}$, and $a^3 \mapsto \bar{3}$. It's an easy exercise to show that this function is an isomorphism.

Remark 2.9. A convenient way to present a group is by choosing elements that *generate* the group (which means that any element of the group can be

written as a product of some of these generators and their inverses), and a set of *relations* among these generators. For instance, $\mathbb{Z}/4\mathbb{Z}$ can be presented by

$$\mathbb{Z}/4\mathbb{Z} = \langle a \colon a^4 = e \rangle,$$

which means that one can find an element $a \in \mathbb{Z}/4\mathbb{Z}$ such that any element in $\mathbb{Z}/4\mathbb{Z}$ can be written as a power of a, and it satisfies $a^4 = e$ (it's not hard to see that a can be chosen to be $\bar{1}$ or $\bar{3}$ in this case).

Definition 2.10. A group G that can be generated by a single element g is called a *cyclic* group (i.e. any element of G is of the form g^k for some $k \in \mathbb{Z}$).

Definition 2.11. Let g be an element in a group G. If there exists a positive integer n such that $g^n = e$, then the smallest possible n satisfying $g^n = e$ is called the *order* of g. If such n does not exist, then we say g is of infinite order.

Exercise. Let G be a cyclic group, and say it can be generated by an element $g \in G$.

- If g is of finite order, say $\text{order}(g) = n$. Prove that $G \cong \mathbb{Z}/n\mathbb{Z}$.
- If g is of infinite order, then prove that $G \cong \mathbb{Z}$.

Therefore, any cyclic group is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some positive integer n.

Exercise. Prove that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not a cyclic group.

Example. Let D_n be the symmetry group of a regular n-gon. It is not hard to show that D_n is generated by rotation by $2\pi/n$ (which we'll denote by r), and a reflection (which we'll denote by s). The group D_n is of order $2n$, with elements given by

$$D_n = \left\{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\right\}.$$

The generators r and s satisfy the relations $r^n = s^2 = 1$ and $s^{-1}rs = r^{-1}$.

$$\begin{aligned} D_n &= \left\langle r, s \mid r^n = s^2 = 1,\ s^{-1}rs = r^{-1} \right\rangle \\ &= \left\langle r, s \mid r^n = s^2 = (rs)^2 = 1 \right\rangle. \end{aligned}$$

Remark 2.12. Since D_n is not commutative, it is not isomorphic to the direct product $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On the other hand, it is isomorphic to the *semi-direct product* of its order 2 *subgroup* $\langle s \rangle$ and its order n *normal subgroup* $\langle r \rangle$: $D_n \cong \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/n\mathbb{Z}$. We'll introduce these notations later on.

2.4. **Subgroups.**

Definition 2.13. Let G be a group. We say a subset $H \subseteq G$ is a *subgroup* if:

(1) it is closed under the binary operation of G: for any $a, b \in H$, we have $ab \in H$;
(2) it contains the identity element of G: $e_G \in H$;
(3) it is closed under taking inverse: for any $a \in H$, we have $a^{-1} \in H$.

Exercise. A subgroup $H \subseteq G$ is itself a group, with the binary operator and the identity element inherit from G.

Example. For any group G, the subset $\{e_G\} \subseteq G$ is always a subgroup, called the *trivial* subgroup of G. Also, the group G itself is a subgroup of G.

Example. For any positive integer n, the subset $n\mathbb{Z} \subseteq (\mathbb{Z}, +)$ is a subgroup.

Exercise. Let G be a group and $g_1, \ldots, g_n$ be elements of G. Prove that the following two statements are equivalent:

- any $g \in G$ can be written as $g = g_{i_1}^{a_1} g_{i_2}^{a_2} \cdots g_{i_k}^{a_k}$ for some $i_1, \ldots, i_k \in \{1, \ldots, n\}$ and $a_1, \ldots, a_k \in \mathbb{Z}$;
- the smallest subgroup of G that contains $g_1, \ldots, g_n$ is the group G itself.

In this case, we say $\{g_1, \ldots, g_n\}$ *generates* the group G.

If H is a subgroup of G, then one can break G up into pieces, each of which looks like H. These pieces are called *cosets* of H, and they arise by "multiplying" H by elements of G.

Definition 2.14. Let G be a group and $H \subseteq G$ be a subgroup. A *left coset* of H in G is a subset of the form

$$gH = \{gh \mid h \in H\} \text{ for some } g \in G.$$

The element g is called a *representative* of the coset gH. The collection of all left cosets is denoted by G/H. Its order $|G/H|$ is called the *index* of H in G, and will sometimes be denoted by $[G : H]$.

Similarly, a *right coset* is a subset of the form

$$Hg = \{hg \mid h \in H\} \text{ for some } g \in G.$$

The collection of all right cosets is denoted by $H\backslash G$.

Example. Consider the subgroup $n\mathbb{Z} \subseteq (\mathbb{Z}, +)$. Since the group $(\mathbb{Z}, +)$ is abelian, its left cosets and right cosets are identical. It is clear that the subgroup has exactly n cosets $\bar{0}, \bar{1}, \ldots, \overline{n-1}$, where $\bar{i} = i + n\mathbb{Z}$ consists of integers $\equiv i$ modulo n. Hence $n\mathbb{Z} \subseteq \mathbb{Z}$ is a subgroup of index n.

Lecture 2

Exercise. The representative of a coset is *not* unique. In fact, show that a coset gH can be represented by any element of the form gh where $h \in H$.

Exercise. Consider the subgroup $\mathbb{Z} \subseteq (\mathbb{R}, +)$. The set of cosets $\mathbb{R}/\mathbb{Z}$ can be identified with S^1, the unit circle in $\mathbb{R}^2$: Points of the circle are of the form $e^{2\pi i\theta}$ where $\theta \in \mathbb{R}$. Show that the map $t \mapsto e^{2\pi it}$ gives a bijection between $\mathbb{R}/\mathbb{Z}$ and S^1.

Proposition 2.15. *Let $H \subseteq G$ be a subgroup. Prove that for any two cosets aH and bH, we have:*

- *either aH and bH are disjoint: $aH \cap bH = \emptyset$,*
- *or aH and bH are exactly the same: $aH = bH$.*

Proof. Suppose aH and bH are not disjoint. Then there exists $h_1, h_2 \in H$ such that $ah_1 = bh_2$. For any $h \in H$, we have

$$ah = a(h_1 h_1^{-1})h = b(h_2 h_1^{-1} h) \in bH.$$

Hence $aH \subseteq bH$. Similarly, one can show that $bH \subseteq aH$. Therefore $aH = bH$. □

Theorem 2.16 (Lagrange)**.** *Let G be a finite group, and $H \subseteq G$ be a subgroup. Then $|G|$ is divisible by $|H|$. Moreover, we have $|G| = |H|[G : H]$.*

Proof. Since $g \in gH$, any element of G belongs to a left coset of H. Then the previous proposition shows that G is the disjoint union of the left cosets of H. Since each coset has exactly $|H|$ elements, we can conclude that $|G| = |H|[G : H]$. □

Exercise. Let G be a finite group and g be an element of G. Prove that the order of g divides the order of G.

Remark 2.17. In the example $n\mathbb{Z} \subseteq (\mathbb{Z}, +)$, one can notice that the set of all cosets $\{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ also has a natural group structure inherits from the group structure on $(\mathbb{Z}, +)$: one defines $\bar{i} + \bar{j}$ to be $\overline{i+j}$.

However, the set of all left cosets does *not* always admit a group structure! Let $H \subseteq G$ be a subgroup and $a, b \in G$ be two elements in G. It is tempting to define a group structure on G/H simply by declaring "$aH \circ bH = (ab)H$". In order for this definition to make sense, we need to show that, if a' is a representative of aH and b' is a representative of bH, then $a'b'H = abH$. This is equivalent to, for any $a, b \in G$ and $h_1, h_2 \in H$, one needs $ah_1bh_2H = abH$, or equivalently, $b^{-1}h_1b \in H$. This is equivalent to the condition that for any $g \in G$ one needs $gH = Hg$, i.e. the left and right cosets of H in G coincide, which is *not* true in general.

Definition 2.18. A subgroup $H \subseteq G$ is called *normal* if $gH = Hg$ for any $g \in G$.

By the previous remark, if $H \subseteq G$ is a normal subgroup, then the set of (left) cosets G/H admits a group structure inherit from G: let aH and bH be two cosets, then $aH \circ bH \coloneqq (ab)H$ gives a well-defined group structure on G/H. The resulting group G/H is called the *quotient group*.

Theorem 2.19 (First isomorphism theorem)**.** *Let $f\colon G \to H$ be a group homomorphism. Define*

$$\mathrm{Ker}(f) \coloneqq \{g \in G \mid f(g) = 1_H\} \subseteq G$$

and

$$\mathrm{Im}(f) \coloneqq \{h \in H \mid h = f(g) \text{ for some } g \in G\} \subseteq H.$$

Then

(1) $\mathrm{Ker}(f)$ *is a normal subgroup of* G*.*

(2) $\mathrm{Im}(f)$ *is a subgroup of* H*.*

(3) There is an isomorphism between $G/\mathrm{Ker}(f)$ *and* $\mathrm{Im}(f)$*.*

Proof. It is not hard to show that $\mathrm{Ker}(f) \subseteq G$ and $\mathrm{Im}(f) \subseteq H$ are subgroups (homework). To show that $\mathrm{Ker}(f) \subseteq G$ is normal, one needs to show that for any $g \in \mathrm{Ker}(f)$ and $g' \in G$, we have $g'gg'^{-1} \in \mathrm{Ker}(f)$. This is true because

$$f(g'gg'^{-1}) = f(g')f(g)f(g'^{-1}) = f(g')f(g')^{-1} = 1_H.$$

Now we define a map $\overline{f}$ from $G/\mathrm{Ker}(f)$ to $\mathrm{Im}(f)$: For any coset $g\mathrm{Ker}(f)$, we define $\overline{f}(g\mathrm{Ker}(f)) \coloneqq f(g)$. This is a well-defined function on the set of cosets $G/\mathrm{Ker}(f)$, because any representative of $g\mathrm{Ker}(f)$ is of the form gg' for some $g' \in \mathrm{Ker}(f)$, and we have $f(gg') = f(g)f(g') = f(g)$. It is not hard to

check that $\overline{f}\colon G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ is a surjective group homomorphism. It is also injective: if $\overline{f}(g_1\mathrm{Ker}(f)) = \overline{f}(g_2\mathrm{Ker}(f))$, then we have $f(g_1) = f(g_2)$, or equivalently $g_2^{-1}g_1 \in \mathrm{Ker}(f)$. Hence the cosets $g_1\mathrm{Ker}(f) = g_2\mathrm{Ker}(f)$ coincide. □

2.5. **Symmetry groups.** For any set X, a *permutation* of X is a bijective function $f\colon X \to X$. The *symmetric group S_X defined over X* is the set of all permutations of X, equipped with the group structure given by compositions. In particular, when X is a finite set of n elements $\{1, 2, \ldots, n\}$, its symmetric group would be denoted by S_n. It is not hard to see that $|S_n| = n!$.

Remark 2.20. One of the reasons that symmetric groups are important is that, any group is isomorphic to a subgroup of a symmetric group (Cayley's theorem). More specifically, one can show that any group G is isomorphic to a subgroup of the symmetric group S_G whose elements are the permutations of the underlying set of G. Explicitly, for each $g \in G$, we define a permutation of G (called left multiplication) $\ell_g\colon G \to G$ by $\ell_g(x) \coloneqq gx$. It is an easy exercise to check that the map $G \to S_G$ given by $g \mapsto \ell_g$ is an injective group homomorphism. Hence G is isomorphic to the image of $G \to S_G$, which is a subgroup of S_G. In particular, if G is a finite group of order n, then this argument shows that G is isomorphic to a subgroup of S_n.

Remark 2.21. Symmetric groups will also arise naturally when we discuss the symmetry groups of Platonic solids. Let G be the symmetry group of a tetrahedron T. It is not hard to see that any symmetry of T sends a vertex of T to a vertex (not necessarily the same one); in other words, it gives rise to a permutation of the four vertices of T. This gives a group homomorphism $\rho\colon \mathrm{Aut}(T) \to S_4$. Note that ρ is injective (why?), hence the symmetry group $\mathrm{Aut}(T)$ is isomorphic to a subgroup of the symmetric group S_4. (In fact, one can use the *orbit-stabilizer theorem* to show that $\mathrm{Aut}(T) \cong S_4$.)

Any element of S_n can be represented by Cauchy's "two-line notation". Let $\sigma \in S_n$ be a permutation of the set $\{1, 2, \ldots, n\}$. Then we'll write

$$\sigma = \begin{bmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n). \end{bmatrix}$$

As usual, the composition $\sigma_1\sigma_2 \in S_n$ is given by $k \mapsto \sigma_1(\sigma_2(k))$, i.e. first apply σ_2 then apply σ_1. For instance, verify that

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}.$$

Permutations are also often written in *cycle notation* ("decomposition into disjoint cycles"). To write down $\sigma \in S_n$ in cycle notation, one proceeds as follows:

- Write an open bracket then select an arbitrary element $x \in \{1, \dots, n\}$, and write down: $(x$
- Then trace the orbit of x: write down its value under successive applications of σ: $(x\ \sigma(x)\ \sigma^2(x) \cdots$
- Repeat until the value return to x, and write down a closing parenthesis rather than x: $(x\ \sigma(x)\ \sigma^2(x) \cdots)$
- Continue with any element y that is not yet written down, and proceed in the same way: $(x\ \sigma(x)\ \sigma^2(x) \cdots)(y\ \sigma(y) \cdots)$
- Repeat until all elements of $\{1, \dots, n\}$ are written in one of the cycles.

For instance,

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 6 & 2 & 3 & 5 \end{bmatrix} = (1)(24)(365) = (24)(365).$$

Here $\sigma(1) = 1$ forms an 1-cycle, which is often omitted.

A 2-cycle is called a *transposition*. An important fact is that any element $\sigma \in S_n$ can be written as a product of transpositions. To see this, it suffices to show that any cycle can be written as a product of transpositions, as any σ is a product of cycles. This can be easily verified:

$$(i_1 i_2 \cdots i_k) = (i_1 i_k)(i_1 i_{k-1}) \cdots (i_1 i_2).$$

It is not hard to see that there is no unique way to represent a permutation by a product of transpositions. For instance, $(123) = (13)(12) = (12)(23) = (12)(23)(13)(13)$. However, the *parity* (i.e. even or odd) of the numbers of transpositions of such representations is unique. (For instance, (123) can not be written as the product of odd number of transpositions.) This permits the *parity of a permutation* to be a well-defined notion.

The key idea of the proof is to define a group homomorphism

$$\operatorname{sgn}\colon S_n \to \{+1, -1\} \text{ (under multiplication)}$$

so that all transpositions map to -1. Indeed, if we can find such a homomorphism, then for any representation $\sigma = \tau_1 \cdots \tau_k$ where τ_i's are transpositions, we have

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1) \cdots \operatorname{sgn}(\tau_k) = (-1)^k.$$

This shows that the parity of k is independent of the choice of the decomposition.

Now, to define such group homomorphism sgn, we consider the Vandermonde polynomial

$$P(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j).$$

For $\sigma \in S_n$, define

$$\operatorname{sgn}(\sigma) \coloneqq \frac{P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})}{P(x_1, \ldots, x_n)}.$$

Observe that the polynomials $P(x_1, \ldots, x_n)$ and $P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ have the same factors except for the signs, therefore $\operatorname{sgn}(\sigma) = \pm 1$. It defines a group homomorphism $\operatorname{sgn}\colon S_n \to \{\pm 1\}$ since

$$\begin{aligned}
\operatorname{sgn}(\sigma_1\sigma_2) &= \frac{P(x_{\sigma_1(\sigma_2((1))}, \ldots, x_{\sigma_1(\sigma_2((n))})}{P(x_1, \ldots, x_n)} \\
&= \frac{P(x_{\sigma_1(\sigma_2((1))}, \ldots, x_{\sigma_1(\sigma_2((n))})}{P(x_{\sigma_2(1)}, \ldots, x_{\sigma_2(n)})} \cdot \frac{P(x_{\sigma_2(1)}, \ldots, x_{\sigma_2(n)})}{P(x_1, \ldots, x_n)} \\
&= \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2).
\end{aligned}$$

Also, it is easy to check that sgn sends any transposition to -1. This finishes the proof.

Definition 2.22. The subset of S_n consisting of all *even* permutations will be denoted by A_n. It is a *normal subgroup* of S_n since it is the kernel of the group homomorphism sgn. The group A_n is called the *alternating group* (of n elements).

Exercise. Show that $A_n \subseteq S_n$ is a normal subgroup of index 2; it has two cosets, one of them consists of all even permutations, the other consists of all odd permutations.

Remark 2.23. The *center* $Z(G)$ of a group G is defined to be

$$Z(G) = \{g \in G \mid gh = hg \text{ for any } h \in G\} \subseteq G.$$

It is not hard to show that $Z(G)$ is a subgroup of G. The center measures the *commutativity* of the group: for instance, if G is abelian then $Z(G) = G$. In the homework, you'll show that the symmetric group S_n has trivial center $Z(S_n) = \{e\}$ if $n \geq 3$.

Lecture 3

2.6. **Group actions.** We will be interested in groups G that act as symmetries of a set X (for instance, the symmetry group of a tetrahedron acting on the set of its vertices). Let us introduce the formal definition of group actions.

Definition 2.24. We say that a group G *acts on a set* X if there is a map

$$G \times X \to X; \quad (g, x) \mapsto g \cdot x$$

satisfying:

- $e_G \cdot x = x$ for any $x \in X$,
- $g \cdot (h \cdot x) = (gh) \cdot x$ for any $g, h \in G$ and $x \in X$.

The dot " $\cdot$ " is sometimes omitted when the context is clear.

Exercise. Show that to give a group action of G on X is equivalent to give a group homomorphism $\rho\colon G \to S_X$. (Hint: Relate them by $g \cdot x = \rho(g)(x)$.)

Example. The symmetric group S_n acts on the set $\{1, \ldots, n\}$.

Example. $\mathrm{Isom}(\mathbb{R}^n)$ acts on $\mathbb{R}^n$.

Example. $\mathrm{O}(n, \mathbb{R})$ acts on the unit sphere $S^{n-1} \subseteq \mathbb{R}^n$, where

$$S^{n-1} = \{\vec{x} \in \mathbb{R}^n \mid ||\vec{x}|| = 1\}.$$

Example. The dihedral group D_n acts on the set of vertices of a regular n-gon, which gives a group homomorphism $D_n \to S_n$. Similarly, the symmetry group of a Platonic solid P acts on the set of its vertices.

Example. Let G be a group. The left multiplication action of G on itself is defined to be

$$G \times G \to G; \quad (g, h) \mapsto g \cdot h \coloneqq gh.$$

Equivalently, it's a group homomorphism

$$G \to S_G; \quad g \mapsto L_g,$$

where $L_g(h) \coloneqq gh$.

Exercise. Check that the right multiplication $g \cdot h \coloneqq hg$ is *not* an action of G on itself. Instead, $g \cdot h \coloneqq hg^{-1}$ is an action of G on itself.

Example. Let G be a group. An important action of G on itself is the *conjugacy action*:

$$G \times G \to G; \quad (g, h) \mapsto g \cdot h \coloneqq ghg^{-1}.$$

Equivalently, the conjugacy action is given by

$$G \to S_G; \quad g \mapsto \mathrm{Ad}_g,$$

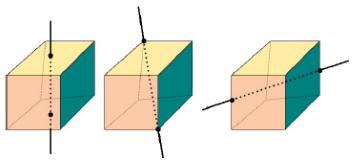
where $\mathrm{Ad}_g(h) \coloneqq ghg^{-1}$. Note that the permutation $\mathrm{Ad}_g \colon G \to G$ is in fact a group isomorphism.

Two elements h and h' of G are said to be *conjugate* if there exists $g \in G$ such that $h' = ghg^{-1}$. In this case, we say h and h' belong to the same conjugacy class. The study of conjugacy classes of non-abelian groups is fundamental for the study of their structure.

Exercise. Elements in the same conjugacy class behave similarly in many ways. For instance, prove that $\mathrm{order}(h) = \mathrm{order}(ghg^{-1})$.

Exercise. Let G be a group and $g \in G$. Show that g is in the center $Z(G)$ of G if and only if the conjugacy class of g consists of a single element $\{g\}$.

Example. Let C be a cube in $\mathbb{R}^3$ centered at the origin. Denote $\mathrm{Aut}^+(C)$ the *rotational symmetric group* of C. Each element of $\mathrm{Aut}^+(C)$ is a rotation that fixes a line through the origin, and sends the cube C to itself. For instance:



- identity map;
- rotate $\pi/2, \pi, 3\pi/2$ along the first (left-most) line: there are 3 such lines, so this gives in total 9 elements of $\mathrm{Aut}^+(C)$;
- rotate $2\pi/3, 4\pi/3$ along the second line: there are 4 such lines, so this gives in total 8 elements of $\mathrm{Aut}^+(C)$;
- rotate π along the third line: there are 6 such lines, so this gives in total 6 elements of $\mathrm{Aut}^+(C)$.

Hence $|\operatorname{Aut}^+(C)|$ is at least 24.

On the other hand, observe that $\operatorname{Aut}^+(C)$ gives an action on the set of the four main diagonals of C, therefore induces a group homomorphism

$$\rho\colon \operatorname{Aut}^+(C) \to S_4.$$

One can show that ρ is injective (this is not a trivial observation: one needs to show that the antipodal map $(x_1, x_2, x_3) \mapsto (-x_1, -x_2, -x_3)$ is *not* a rotation). Now, combining with the fact that $|\operatorname{Aut}^+(C)| \geq 24$, we can conclude that ρ is an isomorphism $\operatorname{Aut}^+(C) \cong S_4$.

Definition 2.25. Let X be a set admitting a group action by G. For any $x \in X$, define its *orbit* to be

$$\operatorname{orb}(x) \coloneqq \{g \cdot x \mid g \in G\} \subseteq X.$$

It sometimes is also denoted by Gx.

The subset of G fixing x

$$\operatorname{Stab}(x) \coloneqq \{g \in G \mid g \cdot x = x\}$$

is called the *stabilizer* of x, which is a subgroup of G (why?).

Exercise. Determine the orbits and stabilizers of the examples of group actions we mentioned above.

Exercise. Let X be a set admitting a group action by G. Let $\operatorname{orb}(x)$ and $\operatorname{orb}(y)$ be two orbits of the action. Prove that either $\operatorname{orb}(x) = \operatorname{orb}(y)$ or $\operatorname{orb}(x) \cap \operatorname{orb}(y) = \emptyset$.

In other words, a group G acting on a set X decomposes X into disjoint union of the orbits of the action. The set of all orbits is denoted by X/G.

Theorem 2.26. *Let X be a set admitting a group action by G. Let $g \in G$ and $x \in X$.*

1. *(1)* $\operatorname{Stab}(gx) = g\operatorname{Stab}(x)g^{-1}$. *In other words, the stabilizers of points on the same orbit are conjugate to each other.*
2. *(2) (Orbit-stabilizer theorem) There is a bijective map between the orbit* $\operatorname{orb}(x)$ *and the set of left cosets* $G/\operatorname{Stab}(x)$. *In particular, if* $|G|$ *is finite then* $|G| = |\operatorname{Stab}(x)||\operatorname{orb}(x)|$.

Proof. The first statement follows from

$$h \in \mathrm{Stab}(gx) \Leftrightarrow hgx = gx \Leftrightarrow g^{-1}hgx = x \Leftrightarrow g^{-1}hg \in \mathrm{Stab}(x).$$

To prove the second statement, consider the map

$$f\colon G \to \mathrm{orb}(x); \quad g \mapsto gx.$$

The map is clearly surjective. For any two elements $g_1, g_2 \in G$,

$$f(g_1) = f(g_2) \Leftrightarrow g_1x = g_2x \Leftrightarrow g_2^{-1}g_1x = x \Leftrightarrow g_2^{-1}g_1 \in \mathrm{Stab}(x) \Leftrightarrow g_1 \in g_2\mathrm{Stab}(x).$$

Hence $f(g_1) = f(g_2)$ if and only if g_1 and g_2 lie in the same coset for the stabilizer subgroup $\mathrm{Stab}(x) \subseteq G$. This proves the second statement. □

Example. Given a cube, we would like to put $\{1, 2, 3, 4, 5, 6\}$ on its faces to make it a dice. How many different dice can we build (up to rotational symmetry)?

In terms of group actions, let X be the set of all possible ways of labeling $\{1, 2, 3, 4, 5, 6\}$ on a dice, and G be the rotational symmetric group of the cube $\mathrm{Aut}^+(C)$ which acts naturally on X. The question is equivalent to counting the number of orbits of this group action. Observe that $\mathrm{Stab}(x) = \{e\}$ for any $x \in X$. By the orbit-stabilizer theorem, we have $|\mathrm{orb}(x)| \cdot 1 = |\mathrm{Aut}^+(C)| = 24$ for each $x \in X$, i.e. each orbit has exactly 24 elements. The set X has 6! elements, so the number of orbits is $6!/24 = 30$.

Theorem 2.27 (Burnside's lemma)**.** *Let X be a finite set admitting a group action by a finite group G. For any $g \in G$, denote $X^g = \{x \in X \mid gx = x\}$ the collection of points fixed by g. Then the number of disjoint orbits satisfies*

$$|X/G| = \frac{1}{|G|}\sum_{g\in G} |X^g|.$$

Proof. Consider the set of pairs

$$Z = \{(g, x) \in G \times X \mid gx = x\}.$$

On the one hand, for each $g_0 \in G$ there exists $|X^{g_0}|$ many elements in X such that $(g_0, x) \in Z$. Hence $|Z| = \sum_{g\in G} |X^g|$. On the other hand, for each $x_0 \in X$, there are $\mathrm{Stab}(x_0)$ many elements in G such that $(g, x_0) \in Z$. Hence

$$|Z| = \sum_{x\in X} |\mathrm{Stab}(x)| = \sum_{x\in X} \frac{|G|}{|\mathrm{orb}(x)|}.$$

Denote $O_1, \ldots, O_k$ the orbits of X under the G-action, where $k = |X/G|$. Then

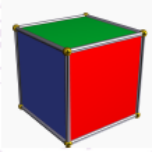
$$\sum_{x \in X} \frac{|G|}{|\mathrm{orb}(x)|} = |G| \sum_{i=1}^{k} \sum_{x \in O_i} \frac{1}{|\mathrm{orb}(x)|} = |G| \sum_{i=1}^{k} 1 = |G||X/G|.$$

Therefore, we have

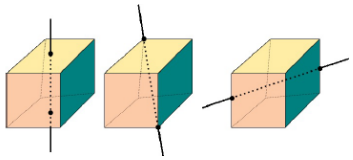
$$|G||X/G| = |Z| = \sum_{g \in G} |X^g|.$$

□

Example. How many different ways are there to color the faces of a cube with three colors (up to rotational symmetry)? Let X be the set of all possible



colorings of the cube, and let $G = \mathrm{Aut}^+(C)$. The problem is equivalent to calculating the number of orbits $|X/G|$. By Burnside's lemma, it suffices to compute the size of the fixed point sets for each element of G.



- identity map: fixes all colorings, there are 3^6 of them;
- rotate $\pi/2, 3\pi/2$ along lines of the first type (6 such rotations): each fixes 3^3 colorings;
- rotate π along lines of the first type (3 such rotations): each fixes 3^4 colorings;
- rotate $2\pi/3, 4\pi/3$ along lines of the second type (8 such rotations): each fixes 3^2 colorings;
- rotate π along lines of the third type (6 such rotations): each fixes 3^3 colorings.

By Burnside's lemma, we have

$$|X/G| = \frac{1}{24}\left(1 \cdot 3^6 + 6 \cdot 3^3 + 3 \cdot 3^4 + 8 \cdot 3^2 + 6 \cdot 3^3\right) = 57.$$

3. Platonic solids and finite subgroups of $\mathrm{SO}(3,\mathbb{R})$

3.1. **Classification of the Platonic solids.**

Definition 3.1. A *Platonic solid* is a convex polyhedron satisfying the following conditions:

(1) all its faces are convex regular polygons, and are congruent (identical in shape and size);
(2) none of its faces intersect except at their edges;
(3) the same number of faces meet at each of its vertices.

Each Platonic solid is completely determined by two numbers p and q, where

- p is the number of edges (or equivalently, vertices) of each face;
- q is the number of faces (or equivalently, edges) that meet at each vertex.

Fact 3.2. *There are only five Platonic solids.*

Polyhedron	*Vertices* V	*Edges* E	*Faces* F	(p,q)
Tetrahedron	4	6	4	$(3,3)$
Cube	8	12	6	$(4,3)$
Octahedron	6	12	8	$(3,4)$
Dodecahedron	20	30	12	$(5,3)$
Icosahedron	12	30	20	$(3,5)$

Proof. We would like to show that there is no other possible (p,q) that can be used to form a Platonic solid.

A topological proof: It is not hard to see that $pF = 2E$ and $qV = 2E$. By the Euler's formula $V - E + F = 2$, one obtains

$$\frac{1}{p} + \frac{1}{q} = \frac{1}{2} + \frac{1}{E} > \frac{1}{2}.$$

Also, note that p and q must both be at least 3. One can then check that there are only 5 possibilities for (p,q).

A geometric proof: Consider any vertex of a Platonic solid. The angle between two edges that meet at a vertex is $\pi - \frac{2\pi}{p}$. Now we use the fact that at each vertex of a convex polyhedron, the total (among the adjacent faces) of the angles between their respective adjacent sides is strictly less than 2π. Therefore, we have

$$q\left(\pi - \frac{2\pi}{p}\right) < 2\pi,$$

which is equivalent to $\frac{1}{p} + \frac{1}{q} > \frac{1}{2}$ that we obtained in the previous proof. □

3.2. **Symmetry groups of the Platonic solids.** In order to study the symmetry group $\mathrm{Aut}(P)$ of a Platonic solid P, one can move the solid so that its center is located at the origin $\vec{0} = (0,0,0) \in \mathbb{R}^3$. Then, any isometry of $\mathbb{R}^3$ that fixes P must also fixes the origin.

Definition 3.3. The *orthogonal group* $\mathrm{O}(3,\mathbb{R})$ is defined as:

$$\mathrm{O}(3,\mathbb{R}) \coloneqq \left\{ f \in \mathrm{Isom}(\mathbb{R}^3) \mid f(\vec{0}) = \vec{0} \right\},$$

which consists of isometries of $\mathbb{R}^3$ that fix the origin $\vec{0} = (0,0,0)$ of $\mathbb{R}^3$.

Exercise. Prove that $\mathrm{O}(3,\mathbb{R})$ is a subgroup of $\mathrm{Isom}(\mathbb{R}^3)$.

Definition 3.4. A *rotation* of $\mathbb{R}^3$ about the origin is a map $f \in \mathrm{O}(3,\mathbb{R})$ such that

- f fixes a line ℓ through the origin (called the *axis of rotation*), and
- f rotates the two-dimensional plane through the origin orthogonal to ℓ.

Exercise (Hard). Prove that the composition of two rotations is still a rotation. Therefore, the set of all rotations about the origin forms a subgroup of $\mathrm{O}(3,\mathbb{R})$.

Notation. The group of all rotations about the origin of $\mathbb{R}^3$ will be denoted by $\mathrm{SO}(3,\mathbb{R})$. We will call it the *rotation group* for now. (Its official name is the *special orthogonal group* in dimension 3. Both $\mathrm{O}(3,\mathbb{R})$ and $\mathrm{SO}(3,\mathbb{R})$ are important examples of *matrix groups*. We will discuss their further properties later.)

Given a Platonic solid P centered at the origin $\vec{0} \in \mathbb{R}^3$, we would like to study:

- the symmetry group $\mathrm{Aut}(P)$, which is a subgroup of the orthogonal group $\mathrm{O}(3,\mathbb{R})$;
- the intersection $\mathrm{Aut}(P) \cap \mathrm{SO}(3,\mathbb{R})$, consisting of rotations that fix the solid P, will be called the *rotational symmetry group* of P, and will be denoted by $\mathrm{Aut}^+(P)$.

We will prove that any finite subgroup of $\mathrm{SO}(3,\mathbb{R})$ is either cyclic, dihedral, or $\mathrm{Aut}^+(P)$ for some Platonic solid P. Therefore, the Platonic solids not only classify the regular polyhedrons in $\mathbb{R}^3$, but also provide a classification of finite subgroups of the rotation groups in dimension 3.

The tetrahedron: Let us first study the symmetry group of the tetrahedron T (centered at the origin). Any symmetry of T permutes its vertices, hence we have a group homomorphism

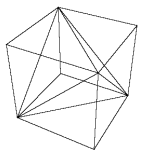
$$\rho\colon\ \mathrm{Aut}(T) \to S_4.$$

Note that ρ is injective: if a symmetry fixes all four vertices, then it is the identity. On the other hand, consider the action of $\mathrm{Aut}(T)$ on the set of vertices $\{1,2,3,4\}$. For any vertex, it is clear that its orbit consists of four elements, and its stabilizer consists of six elements. Hence $|\mathrm{Aut}(T)| = 24$ by the orbit-stabilizer theorem, and ρ is therefore an isomorphism.

Lecture 4

Exercise. Prove that $|\mathrm{Aut}^+(T)| = 12$ and $\mathrm{Aut}^+(T) \cong A_4$. Can you identify the corresponding rotations?

The cube: There are two tetrahedra embedded in a cube C, with vertices at the vertices of the cube, denoted by T^+ and T^- (see the figure below). Here



are some useful observations:

- Any symmetry of C either maps each of the two tetrahedra onto itself, or interchanges the tetrahedra.

- The symmetry $J\colon \mathbb{R}^3 \to \mathbb{R}^3$ which sends $(x_1, x_2, x_3) \mapsto (-x_1, -x_2, -x_3)$ would interchange T^+ and T^-. It is an exercise to show that J commutes with any other symmetry of the cube (i.e. $J \circ f = f \circ J$ for any symmetry f); or equivalently, J is in the center of $\mathrm{Aut}(C)$.

One can then define a map (which can be checked is a group homomorphism)

$$\rho\colon \mathrm{Aut}(C) \to \mathrm{Aut}(T^+) \times \mathbb{Z}/2\mathbb{Z}$$

where:

- $\rho(f) = (f, \overline{0})$ if $f(T^+) = T^+$;
- $\rho(f) = (J \circ f, \overline{1})$ if $f(T^+) = T^-$.

It is again easy to show that ρ is injective, and moreover is isomorphic by the orbit-stabilizer theorem. Hence $\mathrm{Aut}(C) \cong S_4 \times (\mathbb{Z}/2\mathbb{Z})$.

Exercise. Verify that the map ρ is indeed a group homomorphism.

Exercise. Prove that $\mathrm{Aut}^+(C) \cong S_4$. Can you identify the corresponding rotations?

The dodecahedron: By the orbit-stabilizer theorem, it is not hard to show that the rotational symmetry group of a dodecahedron has order $|\mathrm{Aut}^+(D)| = 60$. Let us try to identify these 60 rotations that fix the dodecahedron D:

- the identity map;
- for each pair of opposite faces (there are 6 such pairs), there are 4 rotations (by multiples of $2\pi/5$) about their centers;
- for each pair of opposite edges (there are 15 such pairs), there is 1 rotation (by π) about their centers;
- for each pair of opposite vertices (there are 10 such pairs), there are 2 rotations (by multiples of $2\pi/3$) about the line connecting them.

These add up to $1 + 6 \times 4 + 15 \times 1 + 10 \times 2 = 60$, which therefore are all the elements of $\mathrm{Aut}^+(D)$.

Consider the alternating group A_5. It has 24 elements that are 5-cycles, 20 elements that are 3-cycles, and 15 elements that are of the form $(\star\star)(\star\star)$. This suggests that we might have $\mathrm{Aut}^+(D) \cong A_5$. Let us try to prove it.

Similar to the two tetrahedra embedded in a cube, there are five cubes embedded in a dodecahedron D in such a way that any symmetry of the

dodecahedron permutes these five embedded cubes, therefore gives a group homomorphism

$$\rho\colon \operatorname{Aut}(D) \to S_5.$$

However, the homomorphism ρ is *not* surjective: in fact, one can check that any symmetry of D gives an *even* permutations of the set of the five cubes. So we actually get a homomorphism

$$\rho\colon \operatorname{Aut}(D) \to A_5.$$

Moreover, one can check that the kernel of ρ, namely symmetries of D that fix each of the five cubes, consists of the identity and the map J that sends $(x_1, x_2, x_3) \mapsto (-x_1, -x_2, -x_3)$. Hence ρ induces an injective homomorphism $\operatorname{Aut}(D) \Big/ \{1, J\} \hookrightarrow A_5$. By the orbit-stabilizer theorem, one can show that $|\operatorname{Aut}(D)| = 120$. Therefore by counting the orders of these groups, we have

$$\operatorname{Aut}(D) \Big/ \{1, J\} \cong A_5.$$

On the other hand, consider the composition τ of group homomorphisms

$$\tau\colon \operatorname{Aut}^+(D) \hookrightarrow \operatorname{Aut}(D) \to \operatorname{Aut}(D) \Big/ \{1, J\}.$$

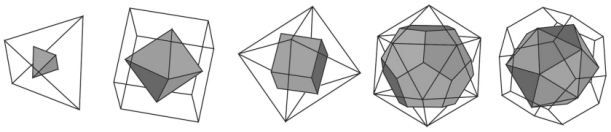
Since J is not a rotation, the composition τ is injective. Again by counting the orders of these groups, we obtain

$$\operatorname{Aut}^+(D) \cong \operatorname{Aut}(D) \Big/ \{1, J\} \cong A_5.$$

Now, let us study the full symmetry group $\operatorname{Aut}(D)$. Since $|\operatorname{Aut}(D)| = 120$, we know that $\operatorname{Aut}(D)$ contains $\operatorname{Aut}^+(D) \cong A_5$ as an index two subgroup. It is tempting to believe that $\operatorname{Aut}(D)$ is isomorphic to S_5. However, this is *not* true! One way to see this is by observing that $J \neq 1$ is in the center $\operatorname{Aut}(D)$, but we also know that the center of S_5 is trivial, hence $\operatorname{Aut}(D) \ncong S_5$. In fact, it is not hard to show the following.

Exercise. Prove that $\operatorname{Aut}(D) \cong A_5 \times (\mathbb{Z}/2\mathbb{Z})$.

Remark 3.5. Every polyhedron has a *dual polyhedron* with faces and vertices interchanged. One can construct the dual polyhedron by taking the vertices of the dual to be the centers of the faces of the original figure. Connecting the centers of adjacent faces in the original forms the edges of the dual and thereby interchanges the number of faces and vertices while maintaining the number of edges. The dual of every Platonic solid is another Platonic solid, so we can arrange the five solids into dual pairs (where the tetrahedron is self-dual).



Exercise. The symmetry group of any polyhedron coincides with the symmetry group of its dual. (This is not hard to show by examining the construction of the dual polyhedron.) Therefore, there are only three symmetry groups associated with the Platonic solids rather than five.

We summarize the symmetry groups of the Platonic solids as follows.

Polyhedron	Aut	Aut^+
Tetrahedron	S_4	A_4
Cube/Octahedron	$S_4 \times (\mathbb{Z}/2\mathbb{Z})$	S_4
Dodecahedron/Icosahedron	$A_5 \times (\mathbb{Z}/2\mathbb{Z})$	A_5

3.3. **Finite subgroups of the rotation group** $\mathrm{SO}(3,\mathbb{R})$**.** Before proving the classification result regarding the rotation group in three dimension, let us begin with a two-dimensional result.

Theorem 3.6. *Let G be a finite subgroup of $\mathrm{O}(2,\mathbb{R})$. Then G is isomorphic to either a cyclic group or a dihedral group.*

Proof. Any element of $\mathrm{O}(2,\mathbb{R})$ acts naturally on the unit circle $S^1 \subseteq \mathbb{R}^2$. Let $g \in G$ be a non-identity element. It is not hard to show that g is either a rotation (when g does not fix any point of S^1), or a reflection (when g fixes at least a point of S^1).

First, suppose that all elements of G are rotations. Write $r_\theta \in \mathrm{O}(2,\mathbb{R})$ for the counterclockwise rotation by θ, where $0 \leq \theta < 2\pi$. Choose $r_\phi \in G$ with the smallest positive ϕ (it is possible since G is finite). We claim that G is the

cyclic group generated by r_ϕ. Let $r_\theta \in G$, and write $\theta = m\phi + \psi$ where $m \in \mathbb{N}$ and $0 \leq \psi < \phi$. Then $r_\psi = (r_\phi)^{-m} r_\theta \in G$. Therefore $\psi = 0$ by the minimality of ϕ. Hence $r_\theta = (r_\phi)^m$.

Second, suppose G contains a reflection s. Let $H \subseteq G$ be the subgroup consisting of rotations (including the identity). By the first case, we have $H = \{1, r, \cdots, r^{n-1}\}$ for some positive integer n. Consider any other reflection $s' \in G$. One can show that the composition of any two reflections is a rotation, hence $ss' \in H$. So $s' = sr^k$ for some $0 \leq k \leq n-1$. This shows that

$$G = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}.$$

It is easy to show that a rotation r and a reflection s satisfy the relation $sr = r^{-1}s$. Hence we get $G \cong D_n$. □

Exercise. Prove (geometrically) that $\mathrm{O}(2, \mathbb{R})$ is a subgroup of $\mathrm{SO}(3, \mathbb{R})$.

Theorem 3.7. *Let G be a finite subgroup of $\mathrm{SO}(3, \mathbb{R})$. Then G is isomorphic to precisely one of the following groups:*

- *cyclic group $\mathbb{Z}/n\mathbb{Z}$,*
- *dihedral group D_n,*
- *A_4: the rotational symmetry group of a tetrahedron,*
- *S_4: the rotational symmetry group of a cube (or a octahedron),*
- *A_5: the rotational symmetry group of a dodecahedron (or a icosahedron).*

Proof. Observe that $G \subseteq \mathrm{SO}(3, \mathbb{R})$ acts on the unit sphere $S^2 \subseteq \mathbb{R}^3$. Each rotation (other than $e \in \mathrm{SO}(3, \mathbb{R})$) gives two poles on the unit sphere which are the intersection of the axis of rotation with the unit sphere. Let $X \subseteq S^2$ denote the set of all poles of all the elements in $G \backslash \{e\}$. We claim that G acts on the set X. To see this, let $g \in G$ and $x \in X$. Say x is a pole for $h \in G \backslash \{e\}$ (i.e. $h(x) = x$). Then $(ghg^{-1})(gx) = ghx = gx$. Hence gx is a pole for $ghg^{-1} \neq e$, so $gx \in X$.

Now the idea of the proof is to apply Burnside's lemma to the action of G on X, and show that X has to be a particularly nice configuration of points on the sphere.

Let N be the number of orbits of the G-action on X. Choose a representative from each orbit, say $x_1, \ldots, x_N \in X$. Observe that the identity e fixes every

pole, and each $g \neq e$ fixes exactly two poles. By Burnside's lemma, we have

$$\begin{aligned} N &= \frac{1}{|G|}\left(|X| + (|G|-1)\cdot 2\right) \\ &= \frac{1}{|G|}\left(2(|G|-1) + \sum_{i=1}^{N} |\mathrm{orb}(x_i)|\right) \end{aligned}$$

By orbit-stabilizer theorem, we have

$$\begin{aligned} 2\left(1 - \frac{1}{|G|}\right) &= N - \sum_{i=1}^{N} \frac{|\mathrm{orb}(x_i)|}{|G|} \\ &= N - \frac{1}{|\mathrm{Stab}(x_i)|} \\ &= \sum_{i=1}^{N} \left(1 - \frac{1}{|\mathrm{Stab}(x_i)|}\right) \end{aligned}$$

Since $|\mathrm{Stab}(x_i)| \geq 2$ for each i, it is then easy to deduce that $N \leq 3$. Clearly there is no solution with $N = 1$, so N is either 2 or 3.

Suppose $N = 2$. Then

$$2 - \frac{2}{|G|} = 2 - \frac{1}{|\mathrm{Stab}(x_1)|} - \frac{1}{|\mathrm{Stab}(x_2)|} \leq 2 - \frac{2}{|G|}.$$

Hence $\mathrm{Stab}(x_1) = \mathrm{Stab}(x_2) = G$ and $|\mathrm{orb}(x_1)| = |\mathrm{orb}(x_2)| = 1$. In other words, X consists of two unit vectors that are fixed by all elements of G. Suppose that one of the vectors is u, then the other must be $-u$. Therefore, any element of G has its axis of rotation given by u (or equivalently $-u$), and rotates the two-dimensional plane orthogonal to u. By what we discussed earlier about finite subgroups of $\mathrm{O}(2, \mathbb{R})$, G is a cyclic group.

Suppose $N = 3$. Let $|\mathrm{Stab}(x_1)| \geq |\mathrm{Stab}(x_2)| \geq |\mathrm{Stab}(x_3)| \geq 2$. Then

$$\frac{1}{|\mathrm{Stab}(x_1)|} + \frac{1}{|\mathrm{Stab}(x_2)|} + \frac{1}{|\mathrm{Stab}(x_3)|} = 1 + \frac{2}{|G|}.$$

This implies that $3/|\mathrm{Stab}(x_3)| > 1$, hence $|\mathrm{Stab}(x_3)| = 2$. Therefore

$$\frac{1}{|\mathrm{Stab}(x_1)|} + \frac{1}{|\mathrm{Stab}(x_2)|} = \frac{1}{2} + \frac{2}{|G|}.$$

This implies that $2/|\mathrm{Stab}(x_2)| > 1/2$, hence $|\mathrm{Stab}(x_2)|$ is either 2 or 3. There are four possible cases:

(a) $|\mathrm{Stab}(x_2)| = 2$.
(b) $|\mathrm{Stab}(x_2)| = 3$ and $|\mathrm{Stab}(x_1)| = 3$. ($|G| = 12$)
(c) $|\mathrm{Stab}(x_2)| = 3$ and $|\mathrm{Stab}(x_1)| = 4$. ($|G| = 24$)
(d) $|\mathrm{Stab}(x_2)| = 3$ and $|\mathrm{Stab}(x_1)| = 5$. ($|G| = 60$)

Case (a): Suppose $|\mathrm{Stab}(x_2)| = 2$. If $|\mathrm{Stab}(x_1)| = 2$, then we get $|G| = 4$. It is an easy exercise to show that any group of four elements is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong D_2 = \langle r, s \mid r^2 = s^2 = (rs)^2 = 1 \rangle$.

If $|\mathrm{Stab}(x_1)| = M \geq 3$, then $|G| = 2M$ and the orbit of x_1 consists of two elements. The stabilizer $\mathrm{Stab}(x_1)$ is a finite group of M rotations about the line ℓ_{x_1} through x_1, so it is a cyclic group of M elements generated by a rotation $R \in G$. Denote the plane orthogonal to ℓ_{x_1} and passes through the origin by P_{x_1}.

First, one observes that $\mathrm{orb}(x_1) = \{x_1, -x_1\}$, since they are the only two elements of X that have M elements in their stabilizers. Now, we consider the action of $\mathrm{Stab}(x_1) = \langle R \rangle$ on x_2. The points $\{x_2, Rx_2, \ldots, R^{M-1}x_2\}$ would form a regular M-gon in a plane orthogonal to ℓ_{x_1}. We claim they actually lie in P_{x_1}.

Lecture 5

Consider any $R^i x_2$. Let $g \neq e$ be a stabilizer of $R^i x_2$. Since g is not a stabilizer of x_1, it must exchange x_1 and $-x_1$. Therefore, $R^i x_2$ must lie in P_{x_1}, and g is a rotation (by π) with axis on P_{x_1}. This proves the claim. Also, this argument shows that g acts on the regular M-gon $\{x_2, Rx_2, \ldots, R^{M-1}x_2\}$ as a reflection, with the mirror line passes through $R^i x_2$.

Note that $x_2, Rx_2, \ldots, R^{M-1}x_2$ are M distinct points of $\mathrm{orb}(x_2)$; and since $|\mathrm{orb}(x_2)| = M$, we have $\mathrm{orb}(x_2) = \{x_2, Rx_2, \ldots, R^{M-1}x_2\}$. The group G acts naturally on $\mathrm{orb}(x_2)$, which is the set of vertices of a regular M-gon, therefore induces a group homomorphism

$$\rho \colon G \to D_M.$$

Now let us consider the image subgroup $\mathrm{Im}(\rho) \subseteq D_M$. It contains all M rotations induced by $\langle R \rangle$; it also contains the reflections along lines passing

through $R^i x_2$ induced by stabilizer of $R^i x_2$. Therefore $\mathrm{Im}(\rho) = D_M$, i.e. the homomorphism ρ is surjective. Since $|G| = |D_M| = 2M$, we have $G \cong D_M$.

Case (b): Suppose $|\mathrm{Stab}(x_2)| = 3$ and $|\mathrm{Stab}(x_1)| = 3$. Then $|G| = 12$ and $|\mathrm{orb}(x_1)| = 4$. Choose $v \in \mathrm{orb}(x_1)$ such that $v \neq \pm x_1$. Consider the stabilizer $\mathrm{Stab}(x_1) = \{1, R, R^2\}$ acting on v. We get three distinct elements $\{v, Rv, R^2v\} \subseteq \mathrm{orb}(x_1)$. They are all different from x_1, and they form an equilateral triangle. The same argument works if one replaces x_1 by another element in the same orbit. Therefore $\mathrm{orb}(x_1)$ forms a tetrahedron. Since G acts naturally on $\mathrm{orb}(x_1)$, we get a group homomorphism

$$\rho \colon G \to \mathrm{Aut}^+(T).$$

Since no rotation (other than e) fixes T, the homomorphism ρ is injective. Now as $|G| = |\mathrm{Aut}^+(T)| = 12$, we have that ρ is an isomorphism and $G \cong \mathrm{Aut}^+(T) \cong A_4$.

Note that one can also consider the orbit of x_2, which turns out to be the vertices of the *dual* tetrahedron of $\mathrm{orb}(x_1)$, consisting of $-x_1, -v, -Rv, -R^2v$.

Case (c): Suppose $|\mathrm{Stab}(x_2)| = 3$ and $|\mathrm{Stab}(x_1)| = 4$. Then $|G| = 24$ and $|\mathrm{orb}(x_1)| = 6$. Choose $v \in \mathrm{orb}(x_1)$ such that $v \neq \pm x_1$. Consider the stabilizer $\mathrm{Stab}(x_1) = \{1, R, R^2, R^3\}$ acting on v. By the same argument as above, $\{v, Rv, R^2v, R^3v\} \subseteq \mathrm{orb}(x_1)$ form a square equidistant from x_1. As $-x_1 \in X$ and $-x_1 \notin \mathrm{orb}(x_2) \cup \mathrm{orb}(x_3)$ (since the sizes of their stabilizers are different), we have

$$\mathrm{orb}(x_1) = \{x_1, -x_1, v, Rv, R^2v, R^3v\}.$$

Now, consider $-v \in X$. We have $-v \in \mathrm{orb}(x_1)$ (since $-v \notin \mathrm{orb}(x_2) \cup \mathrm{orb}(x_3)$) and $-v \neq \pm x_1$. Since $\{v, Rv, R^2v, R^3v\}$ forms a square, one can conclude that $-v = R^2v$. Similarly, we have $R^3v = -Rv$. This shows that $\mathrm{orb}(x_1)$ forms the vertices of a regular octahedron. We get a group homomorphism

$$\rho \colon G \to \mathrm{Aut}^+(O).$$

Since no rotation (other than e) fixes O, the homomorphism ρ is injective. Now as $|G| = |\operatorname{Aut}^+(O)| = |\operatorname{Aut}^+(C)| = 24$, we have that ρ is an isomorphism and $G \cong \operatorname{Aut}^+(O) \cong \operatorname{Aut}^+(C) \cong S_4$.

Case (d): Suppose $|\operatorname{Stab}(x_2)| = 3$ and $|\operatorname{Stab}(x_1)| = 5$. Then $|G| = 60$ and $|\operatorname{orb}(x_1)| = 12$. Consider the stabilizer $\operatorname{Stab}(x_1) = \{1, R, R^2, R^3, R^4\}$. It can be shown that we can pick $u \in \operatorname{orb}(x_1) \backslash \{\pm x_1\}$, and $v \in \operatorname{orb}(x_1)$ with $v \neq \pm x_1, u, Ru, R^2u, R^3u, R^4u$, and check that

$$\{x_1, -x_1, u, Ru, R^2u, R^3u, R^4u, v, Rv, R^2v, R^3v, R^4v\}$$

forms a regular icosahedron. Using the same argument as before, we obtain an isomorphism $G \cong \operatorname{Aut}^+(I) \cong \operatorname{Aut}^+(D) \cong A_5$.

□

4. A crash course on basic linear algebra

4.1. **Basics: matrix products, invertibility, determinants.** Elements of the vector space $\mathbb{R}^n$ are of the form

$$\vec{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

where $x_1, \ldots, x_n \in \mathbb{R}$. To save space, we sometimes write down the *transpose* of $\vec{x}$ instead: $\vec{x} = [x_1 \cdots x_n]^T$. There are two important operations on the vector space $\mathbb{R}^n$:

- *Addition*: Let $\vec{x} = [x_1 \cdots x_n]^T$ and $\vec{y} = [y_1 \cdots y_n]^T$ be two vectors in $\mathbb{R}^n$. Define $\vec{x} + \vec{y} \coloneqq [x_1 + y_1 \cdots x_n + y_n] \in \mathbb{R}^n$.
- *Scalar multiplication*: Let $\vec{x} = [x_1 \cdots x_n]^T$ and $\lambda \in \mathbb{R}$. Define $\lambda\vec{x} \coloneqq [\lambda x_1 \cdots \lambda x_n] \in \mathbb{R}^n$.

Definition 4.1. Let $\vec{v}_1, \ldots, \vec{v}_k$ be vectors in $\mathbb{R}^n$. Then, for any $c_1, \ldots, c_k \in \mathbb{R}$, the vector

$$c_1\vec{v}_1 + \cdots + c_k\vec{v}_k \in \mathbb{R}^n$$

is called a *linear combination* of the set of vectors $\vec{v}_1, \ldots, \vec{v}_k$ (with weights $c_1, \ldots, c_k$). The *span* of the set of vectors $\vec{v}_1, \ldots, \vec{v}_k$ is defined to be the collection of all of their linear combinations:

$$\begin{aligned}\mathrm{Span}\{\vec{v}_1,\dots,\vec{v}_k\} &= \{\text{linear combinations of } \vec{v}_1,\dots,\vec{v}_k\}\\ &= \{c_1\vec{v}_1+\cdots+c_k\vec{v}_k \mid c_1,\dots,c_k\in\mathbb{R}\}.\end{aligned}$$

Remark 4.2. The most fundamental question in linear algebra is to determine whether a linear system of equations has a solution:

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n=b_1\\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n=b_2\\ \cdots\\ a_{m1}x_1+a_{m2}x_2+\cdots+a_{mn}x_n=b_m\end{cases}$$

Consider the vectors $\vec{v}_i=\begin{bmatrix}a_{1i}\\ a_{2i}\\ \vdots\\ a_{mi}\end{bmatrix}$ $(1\le i\le n)$ and $\vec{b}=\begin{bmatrix}b_1\\ b_2\\ \vdots\\ b_m\end{bmatrix}$. Then the system has a solution is equivalent to the statement that

$$\vec{b}\in\mathrm{Span}\{\vec{v}_1,\dots,\vec{v_n}\}.$$

Definition 4.3. Let $A=\begin{bmatrix}\vec{a}_1 & \cdots & \vec{a}_n\end{bmatrix}$ be an $m\times n$ matrix with column vectors given by $\vec{a}_1,\dots,\vec{a}_n\in\mathbb{R}^m$. Let $\vec{x}=[x_1\cdots x_n]^T\in\mathbb{R}^n$. Define the *matrix-vector product* of A and $\vec{x}$ to be the linear combination:

$$A\vec{x}\coloneqq x_1\vec{a}_1+\cdots+x_n\vec{a}_n\in\mathbb{R}^m.$$

Remark 4.4. For any $m\times n$ matrix A, the matrix-vector product gives rise to a function

$$T_A\colon\mathbb{R}^n\to\mathbb{R}^m;\quad T_A(\vec{x})\coloneqq A\vec{x}.$$

The core of linear algebra is to study such a function. It is easy to check that the function T_A is *linear*, i.e. it is compatible with the additions and scalar multiplications on $\mathbb{R}^n$ and $\mathbb{R}^m$:

- $T_A(\vec{v}+\vec{w})=T_A(\vec{v})+T_A(\vec{w})$,
- $T_A(\lambda\vec{v})=\lambda T_A(\vec{v})$.

Exercise. Let $T\colon\mathbb{R}^n\to\mathbb{R}^m$ be a linear transformation (i.e. compatible with the additions and scalar multiplications on $\mathbb{R}^n$ and $\mathbb{R}^m$). Then there exists a

unique $m \times n$ matrix A such that $T_A = T$. In fact, the i-th column of A is given by $T(\vec{e_i})$, where $\vec{e_i} = [0 \cdots 010 \cdots 0]^T$ with the only nonzero entry at the i-th coordinate.

Therefore, there is a one-to-one correspondence between $m \times n$ matrices and linear transformations $\mathbb{R}^n \to \mathbb{R}^m$.

Exercise. Show that under the correspondence described above, the $n \times n$ matrix corresponds to the identity transformation $\mathrm{id}\colon \mathbb{R}^n \to \mathbb{R}^n$ ($\mathrm{id}(\vec{x}) = \vec{x}$ for all $\vec{x}$) is

$$I_n = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & & \\ 0 & & \cdots & & 1 \end{bmatrix}$$

and is called the *identity matrix*.

Definition 4.5. Let A be an $m \times n$ matrix and B be an $n \times p$ matrix. We would like to define the *matrix product* AB, which will be an $m \times p$ matrix.

The matrices A and B correspond to linear transformations $T_A\colon \mathbb{R}^n \to \mathbb{R}^m$ and $T_B\colon \mathbb{R}^p \to \mathbb{R}^n$. Consider the composition

$$T_A \circ T_B\colon \mathbb{R}^p \to \mathbb{R}^m; \quad \vec{x} \mapsto T_A(T_B(\vec{x})).$$

One can check the composition of linear maps is still linear, hence there exists a unique $m \times p$ matrix, of which we define to be the matrix product AB, such that $T_{AB} = T_A \circ T_B$.

Exercise. Write down the entries of AB explicitly in terms of the entries of A and B.

Remark 4.6. The definition of matrix product we give here is more conceptual. It has many advantages: for instance, the *associativity* of matrix product $A(BC) = (AB)C$ follows immediately from the associativity of compositions of functions.

Exercise. Let A be an $m \times n$ matrix. Then $A = AI_n = I_m A$.

Notation. Let A and B be $m \times n$ matrices. Let $\lambda \in \mathbb{R}$.

- (Addition) $A + B$ is an $m \times n$ matrix given by entry-wise addition.
- (Scalar multiplication) λA is an $m \times n$ matrix given by entry-wise scalar multiplication by λ.
- (Transpose) A^T is an $n \times m$ matrix given by $(A^T)_{ij} = A_{ji}$.

- If A is a square matrix (i.e. $m = n$), then $A \cdot A$ makes sense and we denote $A^2 = A \cdot A$. Similarly, $A^3 = A \cdot A \cdot A$, and so on.

Definition 4.7. Let A be an $n \times n$ matrix. We say A is *invertible* (or *non-singular*) if there exists $n \times n$ matrices B and C such that

$$AB = I_n = CA.$$

In fact, such B and C must coincide since $B = I_n B = (CA)B = C(AB) = CI_n = C$. Moreover, one can easily show that such B is unique if it exists. When A is invertible, the matrix B such that $AB = I_n = BA$ is called the *inverse* of A, and is denoted by A^{-1}.

Exercise. Prove the following statements.

- If A is invertible, then so is A^{-1}, and $(A^{-1})^{-1} = A$.
- If A, B are invertible matrices of the same size, then AB also is invertible, and $(AB)^{-1} = B^{-1}A^{-1}$.
- If A is invertible, then so is A^T, and $(A^T)^{-1} = (A^{-1})^T$.

A consequence of the first two statements is that, the set of all *invertible* $n \times n$ matrices form a *group*, with operation given by matrix multiplication and identity element given by I_n. The group is called the *general linear group* and denoted by $\mathrm{GL}(n, \mathbb{R})$.

Remark 4.8. Here is a basic fact on characterizing invertible matrices. Let A be an $n \times n$ matrix. The following statements are equivalent:

- A is invertible.
- T_A is bijective.
- T_A is injective.
- T_A is surjective.
- There exists an $n \times n$ matrix B such that $AB = I_n$.
- There exists an $n \times n$ matrix C such that $CA = I_n$.

Note that these equivalences do *not* hold in general: they only hold for square matrices.

Definition 4.9. Let A be an $n \times n$ matrix. Its *determinant* is defined to be

$$\det(A) \coloneqq \sum_{\sigma \in S_n} (-1)^{\mathrm{sgn}(\sigma)} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)} \in \mathbb{R}.$$

For instance, when $n = 2$, we have $\det(A) = a_{11}a_{22} - a_{12}a_{21}$.

Theorem 4.10. *Here are some important results of the determinants.*

- *A square matrix A is invertible if and only if* $\det(A) \neq 0$.
- *For any two square matrices A and B of the same size, we have* $\det(AB) = \det(A)\det(B)$.
- $\det(A) = \det(A^T)$.
- *Geometrically,* $|\det(A)|$ *coincides with the volume of the (n-dimensional) parallelogram spanned by the column (or row) vectors of A.*

Denote $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ with the group structure given by multiplications. Then the determinants give a group homomorphism

$$\det\colon \mathrm{GL}(n,\mathbb{R}) \to \mathbb{R}^*$$

Its kernel (i.e. matrices with determinant one) is called the *special linear group* and denoted by $\mathrm{SL}(n,\mathbb{R})$.

4.2. **Change of basis, eigenvectors and eigenvalues.**

Example. Consider the matrix $A = \begin{bmatrix} 11 & -2 \\ -2 & 14 \end{bmatrix}$. As before, we would like to understand the linear map $T_A\colon \mathbb{R}^2 \to \mathbb{R}^2$. We have

$$T_A\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \left(\begin{bmatrix} 11 \\ -2 \end{bmatrix}\right) \quad \text{and} \quad T_A\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \left(\begin{bmatrix} -2 \\ 14 \end{bmatrix}\right).$$

If we consider a different *basis* of $\mathbb{R}^2$, say $\mathcal{B} = \left\{\begin{bmatrix} 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -2 \end{bmatrix}\right\}$, then we have

$$T_A\left(\begin{bmatrix} 2 \\ 1 \end{bmatrix}\right) = 10\begin{bmatrix} 2 \\ 1 \end{bmatrix} \quad \text{and} \quad T_A\left(\begin{bmatrix} 1 \\ -2 \end{bmatrix}\right) = 15\begin{bmatrix} 1 \\ -2 \end{bmatrix}.$$

By considering this new basis $\mathcal{B}$, we can understand the geometry of the linear map T_A easily: it expands in the $[2,1]^T$-direction by the factor of 10, and expands in the $[1,-2]^T$-direction by the factor of 15. Moreover, since $\mathcal{B}$ is a basis of $\mathbb{R}^2$, any vector $\vec{x} \in \mathbb{R}^2$ can be uniquely written as $\vec{x} = c_1\begin{bmatrix} 2 \\ 1 \end{bmatrix} + c_2\begin{bmatrix} 1 \\ -2 \end{bmatrix}$ for some $c_1, c_2 \in \mathbb{R}$. Since T_A is linear, one can easily deduce that $T_A(\vec{x}) = 10c_1\begin{bmatrix} 2 \\ 1 \end{bmatrix} + 15c_2\begin{bmatrix} 1 \\ -2 \end{bmatrix}$. In other words, the map T_A is easier to understand if we write vectors in $\mathbb{R}^2$ in the $\mathcal{B}$-coordinates.

A more conceptual way to understand this change of basis process is that, starting with the matrix $A = \begin{bmatrix} 11 & -2 \\ -2 & 14 \end{bmatrix}$, we consider an invertible matrix $P_{\mathcal{B}} = \begin{bmatrix} 2 & 1 \\ 1 & -2 \end{bmatrix}$ (where the columns are the vectors from $\mathcal{B}$). Then in terms of the $\mathcal{B}$-coordinates, T_A becomes

$$\mathbb{R}^2 \xrightarrow{T_{P_{\mathcal{B}}}} \mathbb{R}^2 \xrightarrow{T_A} \mathbb{R}^2 \xrightarrow{T_{P_{\mathcal{B}}^{-1}}} \mathbb{R}^2.$$

This linear map sends

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \mapsto \begin{bmatrix} 2 \\ 1 \end{bmatrix} \mapsto 10 \begin{bmatrix} 2 \\ 1 \end{bmatrix} \mapsto 10 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \mapsto \begin{bmatrix} 1 \\ -2 \end{bmatrix} \mapsto 15 \begin{bmatrix} 1 \\ -2 \end{bmatrix} \mapsto 15 \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

So the matrix corresponds to the composition is simply the diagonal matrix $D = \begin{bmatrix} 10 & 0 \\ 0 & 15 \end{bmatrix} = P_{\mathcal{B}}^{-1} A P_{\mathcal{B}}$.

Note that if A is also invertible, then the change of basis process $A \mapsto P_{\mathcal{B}}^{-1} A P_{\mathcal{B}}$ is the *conjugation* in the group $\mathrm{GL}(n, \mathbb{R})$ we discussed before. This process is called a *diagonalization* of the matrix A.

Definition 4.11. Let A be a square matrix. A nonzero vector $\vec{v} \neq \vec{0}$ is called an *eigenvector* of A if $A\vec{v} = \lambda\vec{v}$ for some λ, and the scalar λ is called an *eigenvalue* of A.

Observe that λ is an eigenvalue of A if and only if $A - \lambda I_n$ is not invertible, which is equivalent to

$$\det(A - \lambda I_n) = 0.$$

This is a degree n polynomial in λ, which is called the *characteristic polynomial* of A.

Remark 4.12. We allow eigenvalues and eigenvectors to take values in *complex* numbers, since the characteristic polynomial has complex roots in general.

4.3. **Inner products, orthogonal matrices.** In Homework 1, we showed that any element $T \in \mathrm{O}(n, \mathbb{R})$ of origin-preserving isometries of $\mathbb{R}^n$ is *linear*, and that T preserves the standard inner product on $\mathbb{R}^n$. There exists a unique $n \times n$ matrix A such that $T_A = T$. Since T preserves the inner product, for any $\vec{x}, \vec{y} \in \mathbb{R}^n$ we have

$$\langle \vec{x}, \vec{y} \rangle = \langle A\vec{x}, A\vec{y} \rangle, \text{ or equivalently } \vec{x}^T \vec{y} = \vec{x}^T A^T A \vec{y}.$$

It is an easy exercise to show that this would imply that $A^TA = I_n$. In fact, the converse is true, namely, if we have a matrix A satisfying $A^TA = I_n$, then T_A is an origin-preserving isometry of $\mathbb{R}^n$. Therefore, we can identify the origin-preserving isometries $\mathrm{O}(n, \mathbb{R})$ with the matrices satisfying $A^TA = I_n$.

Definition 4.13. An $n \times n$ matrix A is called *orthogonal* if $A^TA = I_n$. We will also denote the group of orthogonal matrices by $\mathrm{O}(n, \mathbb{R})$.

Remark 4.14. Let $\{\vec{v}_1, \ldots, \vec{v}_n\}$ be the columns of A. Then A is orthogonal if and only if $\{\vec{v}_1, \ldots, \vec{v}_n\}$ is an *orthonormal* set, i.e. $\langle \vec{v}_i, \vec{v}_i \rangle = 1$ for all i and $\langle \vec{v}_i, \vec{v}_j \rangle = 0$ for all $i \neq j$.

Observe that if A is orthogonal, then $\det(A)^2 = \det(A^TA) = 1$, hence $\det(A) = \pm 1$. The subgroup of $\mathrm{O}(n, \mathbb{R})$ with determinant one is called the *special orthogonal group*, and denoted by

$$\mathrm{SO}(n, \mathbb{R}) = \{A \in \mathrm{O}(n, \mathbb{R}) \mid \det(A) = 1\}.$$

There is a surjective group homomorphism $\det\colon \mathrm{O}(n, \mathbb{R}) \to \{\pm 1\}$ with kernel given by $\mathrm{SO}(n, \mathbb{R})$, hence we have $[\mathrm{O}(n, \mathbb{R}) : \mathrm{SO}(n, \mathbb{R})] = 2$.

In the previous section, we used $\mathrm{SO}(3, \mathbb{R})$ to denote the *rotation group* in three dimension. Now, we would like to show that these two notations actually coincide, i.e. $A \in \mathrm{SO}(3, \mathbb{R})$ is special orthogonal if and only if T_A is a rotation in $\mathbb{R}^3$.

First, we show that if T_A is a rotation then $A \in \mathrm{SO}(3, \mathbb{R})$. The rotation T_A would fix two unit vectors in $\mathbb{R}^3$, say $\pm\vec{v}_3$. One can find two more unit vectors $\vec{v}_1, \vec{v}_2$ so that $\{\vec{v}_1, \vec{v}_2, \vec{v}_3\}$ forms an orthonormal set. After possibly switching $\vec{v}_1$ and $\vec{v}_2$, we can assume that the matrix $B = [\vec{v}_1\vec{v}_2\vec{v}_3]$ with columns given by these three vectors is orthogonal and $\det(B) = 1$, i.e. $B \in \mathrm{SO}(3, \mathbb{R})$. We know that T_A fixes $\vec{v}_3$, and acts on the plane spanned by $\{\vec{v}_1, \vec{v}_2\}$ as a rotation, say by angle θ. So we have

$$\begin{aligned} T_A(\vec{v}_1) &= \cos\theta\vec{v}_1 + \sin\theta\vec{v}_2 \\ T_A(\vec{v}_2) &= -\sin\theta\vec{v}_1 + + \cos\theta\vec{v}_2 \\ T_A(\vec{v}_3) &= \vec{v}_3 \end{aligned}$$

therefore

$$B^{-1}AB = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{SO}(3,\mathbb{R}).$$

Thus we conclude that $A \in \mathrm{SO}(3,\mathbb{R})$.

Conversely, we would like to show that for any $A \in \mathrm{SO}(3,\mathbb{R})$, the linear map T_A is a rotation. First, we need to show that T_A fixes a unit vector, or equivalently, 1 is an eigenvalue of A. First, one can show that any 3×3 matrix has a real eigenvalue (the characteristic polynomial is of odd degree, one can use the intermediate value theorem to conclude that it must has a real root). Suppose $A\vec{v} = \lambda\vec{v}$ where $\lambda \in \mathbb{R}$ and $\vec{v} \neq \vec{0}$. Since A is orthogonal, we have

$$\lambda^2||\vec{v}||^2 = \langle\lambda\vec{v}, \lambda\vec{v}\rangle = \langle A\vec{v}, A\vec{v}\rangle = \langle\vec{v},\vec{v}\rangle = ||\vec{v}||^2.$$

Hence $\lambda = \pm 1$. If $\lambda = 1$, then we have shown that 1 is an eigenvalue of A. Now suppose $\lambda = -1$, and let $\vec{v}_3$ be a unit eigenvector of λ. By the same argument as before, we can find $\vec{v}_1, \vec{v}_2$ such that the matrix $B = [\vec{v}_1, \vec{v}_2, \vec{v}_3] \in \mathrm{SO}(3,\mathbb{R})$. Since A is orthgonal, the vectors $A\vec{v}_1, A\vec{v}_2$ are orthogonal to $A\vec{v}_3 = -\vec{v}_3$, hence they both lie in $\mathrm{Span}\{\vec{v}_1, \vec{v}_2\}$. So we have

$$B^{-1}AB = \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

for some $a, b, c, d \in \mathbb{R}$. Since $A, B \in \mathrm{SO}(3,\mathbb{R})$, the upper 2×2 block matrix lies in $\mathrm{O}(2,\mathbb{R})$ with determinant -1. This implies that it is a reflection. Thus, there exists a nonzero vector $\vec{v} \in \mathrm{Span}\{\vec{v}_1, \vec{v}_2\}$ such that $B^{-1}AB\vec{v} = \vec{v}$, and 1 is an eigenvalue of $B^{-1}AB$. Note that A and $B^{-1}AB$ have identical characteristic polynomials, hence 1 is also an eigenvalue of A.

Now we have shown that any $A \in \mathrm{SO}(3,\mathbb{R})$ has an eigenvalue 1. Choose a unit vector $\vec{v}_3$ such that $A\vec{v}_3 = \vec{v}_3$. By the same argument again, there exists $B \in \mathrm{SO}(3,\mathbb{R})$ such that

$$B^{-1}AB = \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

for some $a, b, c, d \in \mathbb{R}$. The upper 2×2 block lies in $\mathrm{SO}(2, \mathbb{R})$, which means that it is a rotation. Therefore T_A fixes $\vec{v}_3$ and is rotation on the plane $\vec{v}_3^{\perp} = \mathrm{Span}\{\vec{v}_1, \vec{v}_2\}$. Hence T_A is a rotation in $\mathbb{R}^3$.

Lecture 6

Upcoming topic:

- Classification of plane crystallographic groups (frieze groups, wallpaper groups, etc.)