

GEOMETRY AND SYMMETRY, FALL 2022

CONTENTS

| | |
|---------------------------|----|
| 1. Overview of the course | 1 |
| 2. Definition of a group | 4 |
| 2.1. Binary operators | 4 |
| 2.2. Groups | 6 |
| 2.3. Homomorphisms | 8 |
| 2.4. Subgroups | 10 |
| 2.5. Symmetry groups | 13 |

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).

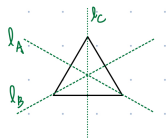
The symmetries that we are interested in are the *isometries* (i.e. distance-preserving functions) of these spaces. For instance, an isometry of \mathbb{R}^2 is a function $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ such that $d(f(x), f(y)) = d(x, y)$ for any $x, y \in \mathbb{R}^2$.

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

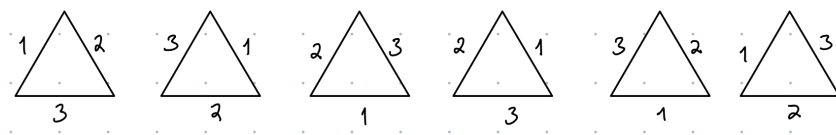
- for any $p \in S$, we have $f(p) \in S$; and
- for any $q \in S$, there exists $p \in S$ such that $f(p) = q$.

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.



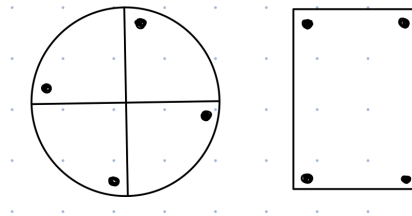
The easiest way to study the symmetries of a shape is by *counting*. In this example, it's easy to check that there are 6 symmetries. If we put labels on the edges of the triangle, then the effect of these symmetries look like:



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 ($O(2, \mathbb{R})$, $O(3, \mathbb{R})$, $SL(2, \mathbb{R})$, $SL(2, \mathbb{C})$, 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:

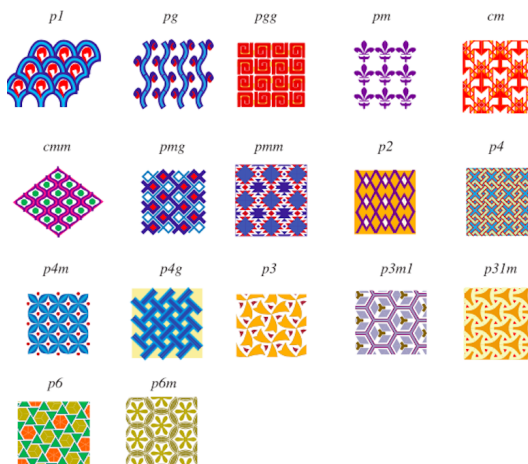
- discuss the group structure of the symmetry group of P_n (the resulting group is called the *dihedral group* D_n ;
- prove that any finite subgroup of $O(2, \mathbb{R})$ is either a cyclic group or the symmetry group of a regular n -gon.

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 $SO(3, \mathbb{R})$ 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. DEFINITION OF A GROUP

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

$$\circ: S \times S \rightarrow S.$$

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.

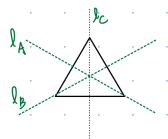
Non-example. Consider the set of all six geometric transformations that give the symmetries of an equilateral triangle:

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

(note: rotations are typically assumed to be counterclockwise)

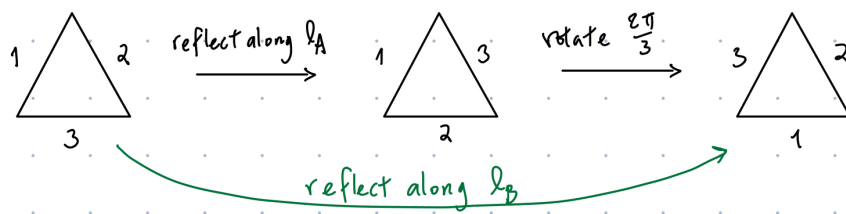
There is a binary operation on S given by *composing* these geometric transformations:

$$\circ: S \times S \rightarrow S,$$



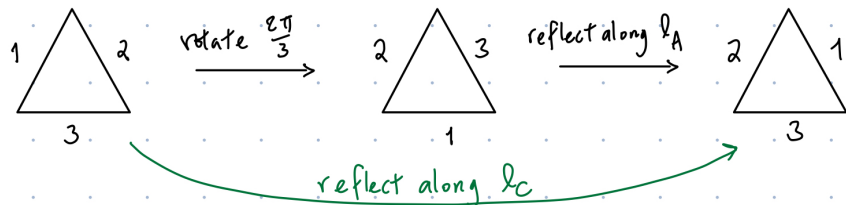
where $a \circ b \in S$ is the transformation given by “do b , and then do a ”. For instance, we have

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



On the other hand, by reversing the order one gets

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



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

$$\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

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 :

$$(\mathbb{Z}/n\mathbb{Z})^* := \{\bar{m} \in \mathbb{Z}/n\mathbb{Z} : \gcd(m, n) = 1\}.$$

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

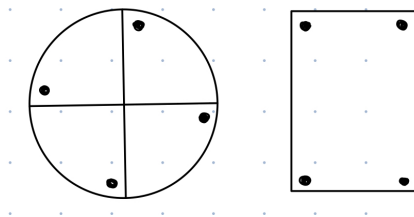
$$G_1 \times G_2 := \{(g_1, g_2) : g_1 \in G_1 \text{ and } g_2 \in G_2\}.$$

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

$$(g_1, g_2) \circ (g'_1, g'_2) := (g_1 \circ g'_1, g_2 \circ g'_2).$$

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

$$G_1 := \left\{ \text{rotate } 0, \text{ rotate } \frac{\pi}{2}, \text{ rotate } \pi, \text{ rotate } \frac{3\pi}{2} \right\}.$$

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

$$G_2 := \left\{ \text{rotate } 0, \text{ rotate } \pi, \text{ reflect along } \ell_1, \text{ reflect along } \ell_2 \right\}.$$

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, “homo-” 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 $f: G \rightarrow H$ 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 $f: G \rightarrow H$ 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

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

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

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

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

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

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

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

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

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

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, \dots, 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 $i_1, \dots, i_k \in \{1, \dots, n\}$ and $a_1, \dots, a_k \in \mathbb{Z}$;
- the smallest subgroup of G that contains g_1, \dots, g_n is the group G itself.

In this case, we say $\{g_1, \dots, g_n\}$ *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 $\bar{0}, \bar{1}, \dots, \overline{n-1}$, 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 $t \mapsto e^{2\pi i t}$ 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

$$ah = a(h_1h_1^{-1})h = b(h_2h_1^{-1}h) \in bH.$$

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

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 $|G| = |H|[G : H]$. \square

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 $\{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ 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 $aH \circ bH := (ab)H$ 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 $f: G \rightarrow H$ be a group homomorphism. Define*

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

and

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

Then

- (1) $\text{Ker}(f)$ is a normal subgroup of G .
- (2) $\text{Im}(f)$ is a subgroup of H .
- (3) There is an isomorphism between $G/\text{Ker}(f)$ and $\text{Im}(f)$.

Proof. It is not hard to show that $\text{Ker}(f) \subseteq G$ and $\text{Im}(f) \subseteq H$ are subgroups (homework). To show that $\text{Ker}(f) \subseteq G$ is normal, one needs to show that for any $g \in \text{Ker}(f)$ and $g' \in G$, we have $g'gg'^{-1} \in \text{Ker}(f)$. 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 \bar{f} from $G/\text{Ker}(f)$ to $\text{Im}(f)$: For any coset $g\text{Ker}(f)$, we define $\bar{f}(g\text{Ker}(f)) := f(g)$. This is a well-defined function on the set of cosets $G/\text{Ker}(f)$, because any representative of $g\text{Ker}(f)$ is of the form gg' for some $g' \in \text{Ker}(f)$, and we have $f(gg') = f(g)f(g') = f(g)$. It is not hard to check that $\bar{f}: G/\text{Ker}(f) \rightarrow \text{Im}(f)$ is a surjective group homomorphism. It is also injective: if $\bar{f}(g_1\text{Ker}(f)) = \bar{f}(g_2\text{Ker}(f))$, then we have $f(g_1) = f(g_2)$, or equivalently $g_2^{-1}g_1 \in \text{Ker}(f)$. Hence the cosets $g_1\text{Ker}(f) = g_2\text{Ker}(f)$ coincide. \square

2.5. Symmetry groups. For any set X , a *permutation* of X is a bijective function $f: X \rightarrow X$. 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 $\{1, 2, \dots, n\}$, 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) $\ell_g: G \rightarrow G$ by $\ell_g(x) := gx$. It is an easy

exercise to check that the map $G \rightarrow S_G$ given by $g \mapsto \ell_g$ is an injective group homomorphism. Hence G is isomorphic to the image of $G \rightarrow S_G$, 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 $\rho: \text{Aut}(T) \rightarrow S_4$. Note that ρ is injective (why?), hence the symmetry group $\text{Aut}(T)$ is isomorphic to a subgroup of the symmetric group S_4 . (In fact, one can use the *orbit-stabilizer theorem* to show that $\text{Aut}(T) \cong S_4$.)

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 $\{1, 2, \dots, n\}$. 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

$$\text{sgn}: S_n \rightarrow \{+1, -1\} \text{ (under multiplication)}$$

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

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

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

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

For $\sigma \in S_n$, define

$$\text{sgn}(\sigma) := \frac{P(x_{\sigma(1)}, \dots, x_{\sigma(n)})}{P(x_1, \dots, x_n)}.$$

Observe that the polynomials $P(x_1, \dots, x_n)$ and $P(x_{\sigma(1)}, \dots, x_{\sigma(n)})$ have the same factors except for the signs, therefore $\text{sgn}(\sigma) = \pm 1$. It defines a group

homomorphism $\text{sgn}: S_n \rightarrow \{\pm 1\}$ since

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

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 $n \geq 3$.