

# 1 Groups

## 1.1 Introduction

The lecturer is **Davesh Maulik**. These notes are taken by **Jakin Ng**, **Sanjana Das**, and **Ethan Yang**. Here is some basic information about the class:

- The text used in this class will be the 3rd edition of **Algebra**, by Artin.
- The course website is found on **Canvas**, and the problem sets will be submitted on **Gradescope**.
- The problem sets will be due every Tuesday at midnight.

Throughout this semester, we will discuss the fundamentals of *linear algebra* and *group theory*, which is the study of symmetries. In this class, we will mostly study groups derived from geometric objects or vector spaces, but in the next course, 18.702<sup>1</sup>, more exotic groups will be studied.

As a review of basic linear algebra, let's review invertible matrices.

### Definition 1.1

An  $n \times n$  matrix<sup>a</sup>  $A$  is invertible if there exists some other matrix  $A^{-1}$  such that  $AA^{-1} = A^{-1}A = I$ , the  $n \times n$  identity matrix. Equivalently,  $A$  is invertible if and only if the determinant  $\det(A) \neq 0$ .

<sup>a</sup>An array of numbers (or some other type of object) with  $n$  rows and  $n$  columns

### Example 1.2 ( $n = 2$ )

Let  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  be a  $2 \times 2$  matrix. Then its inverse  $A^{-1}$  is  $\frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ .

### Example 1.3 ( $GL_n(\mathbb{R})$ )

A main example that will guide our discussion of groups<sup>a</sup> is the **general linear group**,  $GL_n(\mathbb{R})$ , which is the group of  $n \times n$  invertible real matrices.

<sup>a</sup>The concept of a *group* will be fleshed out later in this lecture

Throughout the course, we will be returning to this example to illustrate various concepts that we learn about.

## 1.2 Laws of Composition

With our example in mind, let's start.

### Guiding Question

How can we generalize the nice properties of matrices and matrix multiplication in a useful way?

Given two matrices  $A, B \in GL_n(\mathbb{R})$ , there is an operation combining them, in particular *matrix multiplication*, which returns a matrix  $AB \in GL_n(\mathbb{R})$ .<sup>2</sup> The matrices under matrix multiplication satisfy several properties:

- **Noncommutativity.** Matrix multiplication is noncommutative, which means that  $AB$  is not necessarily the same matrix as  $BA$ . So the order that they are listed in *does* matter.
- **Associativity.** This means that  $(AB)C = A(BC)$ , which means that the matrices to be multiplied can be grouped together in different configurations. As a result, we can omit parentheses when writing the product of more than two matrices.
- **Inverse.** The product of two invertible matrices is also invertible. In particular,

$$(AB)^{-1} = B^{-1}A^{-1}.$$

---

<sup>1</sup>Algebra 2

<sup>2</sup>Since the determinant is multiplicative,  $\det(AB) = \det(A)\det(B)$ , which is nonzero.

Another way to think of matrices is as an *operation* on a different space. Given a matrix  $A \in GL_n(\mathbb{R})$ , a function or transformation on  $\mathbb{R}^n$ <sup>3</sup> can be associated to it, namely

$$T_A : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

$$\vec{v} = (x_1, \dots, x_n) \longmapsto A\vec{v}$$
<sup>4</sup>.

Since  $A\vec{v}$  is the matrix product, we notice that  $T_{AB}(\vec{v}) = T_A(T_B(\vec{v}))$ , and so matrix multiplication is the same as function composition.

With this motivation, we can define the notion of a group.

**Definition 1.4 (Group)**

A **group** is a set  $G$  with a composition (or product) law

$$G \times G \longrightarrow G$$

$$(a, b) \longmapsto a \cdot b$$
<sup>5</sup>

fulfilling the following conditions:

- **Identity.** There exists some element  $e \in G$  such that  $a \cdot e = e \cdot a = a$
- **Inverse.** For all  $a \in G$ , there exists  $b \in G$ , denoted  $a^{-1}$ , such that  $a \cdot b = b \cdot a = e$ .
- **Associative.** For  $a, b, c \in G$ ,

$$(ab)c = a(bc).$$

---

Also denoted  $ab$

In the definition, both the first and second conditions automatically give us a unique inverse and identity. For example, if  $e$  and  $e'$  both satisfy property 1, then  $e \cdot e' = e = e'$ , so they must be the same element. A similar argument holds for inverses.

Why does associativity matter? It allows us to define the product  $g_1 \cdot g_2 \cdots \cdots g_n$  without the parentheses indicating which groupings they're multiplied in.

**Definition 1.5**

Let  $g$  taken to the power  $n$  be the element  $g^n = \underbrace{g \cdots \cdots g}_{n \text{ times}}$  for  $n > 0$ ,  $g^n = \underbrace{g^{-1} \cdots \cdots g^{-1}}_{n \text{ times}}$  for  $n < 0$ , and  $e$  for  $n = 0$ .

**Example 1.6**

Some common groups include:

Group	Composition Law	Identity	Inverse
$GL_n(\mathbb{R})$ <sup>a</sup>	matrix multiplication	$I_n$	$A \mapsto A^{-1}$
$\mathbb{Z}$ <sup>b</sup>	+	0	$n \mapsto -n$
$\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ <sup>c</sup>	×	1	$z \mapsto \frac{1}{z}$

---

<sup>a</sup>The general linear group

<sup>b</sup>The integers under addition

<sup>c</sup>The complex numbers (except 0) under multiplication

For the last two groups, there is additional structure: the composition law is *commutative*. This motivates the following definition.

**Definition 1.7**

A group  $G$  is **abelian** if  $a \cdot b = b \cdot a$  for all  $a, b \in G$ . Otherwise,  $G$  is called **nonabelian**.

<sup>3</sup>Vectors with  $n$  entries which are real numbers.

<sup>4</sup>The notation  $A\vec{v}$  refers to the matrix product of  $A$  and  $\vec{v}$ , considered as  $n \times n$  and  $n \times 1$  matrices.

Often, the composition law in an abelian group is denoted  $+$  instead of  $\cdot$ .

### 1.3 Permutation and Symmetric Groups

Now, we will look at an extended example of another family of nonabelian groups.

**Definition 1.8**

Given a set  $S$ , a **permutation** of  $S$  is a *bijection*<sup>a</sup>  $p : S \rightarrow S$ .

<sup>a</sup>A function  $f : A \rightarrow B$  is a bijection if for all  $y \in B$ , there exists a unique  $x \in A$  such that  $f(x) = y$ . Equivalently, it must be one-to-one and onto.

**Definition 1.9**

Let  $\text{Perm}(S)$  be the set of permutations of  $S$ .

In fact,  $\text{Perm}(S)$  is a group, where the product rule is function composition.<sup>6</sup>

- **Identity.** The identity function  $e : x \mapsto x$  is the identity element of the group.
- **Inverse.** Because  $p$  is a bijection, it is invertible. Let  $p^{-1}(x)$  be the unique  $y \in S$  such that  $p(y) = x$ .
- **Associativity.** Function composition is always associative.

Like groups of matrices,  $\text{Perm}(S)$  is a group coming from a set of *transformations* acting on some object; in this case,  $S$ .

**Definition 1.10**

When  $S = \{1, 2, \dots, n\}$ , the permutation group  $\text{Perm}(S)$  is called the **symmetric group**, denoted  $S_n$ .

**Definition 1.11**

For a group  $G$ , the number of elements in the set  $G$ ,  $|G|$ , is called the **order** of the group  $G$ , denoted  $|G|$  or  $\text{ord}(G)$ .

The order of the symmetric group is  $|S_n| = n!$ <sup>7</sup> so the symmetric group  $S_n$  is a *finite* group.

For  $n = 6$ , consider the two permutations  $p$  and  $q$

$$\begin{array}{c|cccccc} i & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline p(i) & 2 & 4 & 5 & 1 & 3 & 6 \\ \\ i & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline q(i) & 3 & 4 & 5 & 6 & 1 & 2 \end{array},$$

where the upper number is mapped to the lower number.

We can also write these in **cycle notation**, which is a shorthand way of describing a permutation that does not affect what the permutation actually is. In cycle notation, each group of parentheses describes a cycle, where the number is mapped to the following number, and it wraps around.

**Example 1.12 (Cycle notation)**

In cycle notation,  $p$  is written as  $(124)(35)$ , where the 6 is omitted. In the first cycle, 1 maps to 2, 2 maps to 4, and 4 maps to 1, and in the second cycle, 3 maps to 5 and 5 maps back to 3.<sup>a</sup>

<sup>a</sup>In fact, we say that  $p$  has *cycle type*  $(3, 2)$ , which is the lengths of each cycle.

<sup>6</sup>We can check that the composition of two bijections  $p \circ q$  is also a bijection.

<sup>7</sup>The number of permutations of the numbers 1 through  $n$  is  $n!$  — there are  $n$  possibilities for where 1 maps to, and then  $n - 1$  for where 2 maps to, and so on to get  $n(n - 1) \cdots (2)(1) = n!$

Similarly,  $q$  is written as  $(135)(246)$ .<sup>8</sup> In cycle notation, it is clear that there are multiple ways to write or represent the same permutation. For example,  $p$  could have been written as  $(241)(53)$  instead, but it represents the *same* element  $p \in S_6$ .

Cycle notation allows us to more easily invert or compose two permutations; we simply have to follow where each number maps to.

**Example 1.13 (Inversion)**

The inverse  $p^{-1}$  flips the rows of the table:

$$\begin{array}{c|cccccc} i & 2 & 4 & 5 & 1 & 3 & 6 \\ \hline p(i) & 1 & 2 & 3 & 4 & 5 & 6 \end{array}$$

In cycle notation, it reverses the cycles, since each number should be mapped under  $p^{-1}$  to the number that maps to it under  $p$ :

$$p^{-1} = (421)(53) = (142)(35).$$

**Example 1.14 (Composition)**

The composition is

$$q \circ p = (143)(26).$$

Under  $p$ , 1 maps to 2, which maps to 4 under  $q$ , and so 1 maps to 4 under  $q \circ p$ .<sup>a</sup> Similarly, 4 maps to 3 and 3 maps back to 1, which gives us the first cycle. The second cycle is similar.

<sup>a</sup>Remember that the rightmost permutation is applied first, and then the leftmost, and not the other way around, due to the notation used for function composition.

**Example 1.15 (Conjugation)**

Another example of composition is

$$p^{-1} \circ q \circ p = (126)(345).$$

This is also known as *conjugation* of  $q$  by  $p$ .<sup>a</sup>

<sup>a</sup>Notice that under conjugation,  $q$  retains its cycle type  $(3, 3)$ . In fact, this is true for conjugation of any element by any other element!

## 1.4 Examples of Symmetric Groups

For  $n \geq 3$ ,  $S_n$  is always non-abelian. Let's consider  $S_n$  for small  $n \leq 3$ .

**Example 1.16 ( $S_1$ )**

In this case,  $S_1$  only has one element, the identity element, and so it is  $\{e\}$ , the *trivial group*.

**Example 1.17 ( $S_2$ )**

For  $n = 2$ , the only possibilities are the identity permutation  $e$  and the transposition  $(12)$ . Then  $S_2 = \{e, (12)\}$ ; it has order 2.

Once  $n$  gets larger, the symmetric group becomes more interesting.

<sup>8</sup>It has cycle type  $(3, 3)$ .

**Example 1.18** ( $S_3$ )

The symmetric group on three elements is of order  $3! = 6$ . It must contain the identity  $e$ . It can also contain  $x = (123)$ . Then we also get the element  $x^2 = (132)$ , but

$$\boxed{x^3 = e.}$$

Higher powers are just  $x^4 = x$ ,  $x^5 = x^2$ , and so on. Now, we can introduce  $y = (12)$ , which is its own inverse, and so

$$\boxed{y^2 = e.}$$

Taking products gives  $xy = (13)$  and  $x^2y = (23)$ . So we have all six elements of  $S_3$ :

$$S_3 = \{e, (123), (132), (12), (13), (23)\}.$$

In fact,  $yx = (23) = x^2y$ , so taking products in the other order does not provide any new elements. The relation

$$\boxed{yx = x^2y}$$

holds. In particular, using the boxed relations, we can compute *any* crazy combination of  $x$  and  $y$  and reduce it to one of the elements we listed. For example,  $xyx^{-1}y = xyx^2y = xyyx = xy^2x = x^2$ .

MIT OpenCourseWare  
<https://ocw.mit.edu>

Resource: Algebra I Student Notes  
Fall 2021  
Instructor: Davesch Maulik  
Notes taken by Jakin Ng, Sanjana Das, and Ethan Yang

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.