# MATH 171: Abstract Algebra I

## Connor Neely, Fall 2024

1 Groups		2	
	1.1	Basic Axioms and Properties	2
	1.2	Some Important Groups	3
	1.3	Homomorphisms	4
	1.4	Group Actions	5

st Adapted from FA24 Lecture Notes.

## 1 Groups

## 1.1 Basic Axioms and Properties

For most of this course, the central object of study will be the group.

## **Definition: Binary operation**

A binary operation on a set G is a function  $\star : G \times G \to G$ .

- If  $a \star (b \star c) = (a \star b) \star c$  for all  $a, b, c \in G$ , then we say  $\star$  is associative.
- If  $a \star b = b \star a$  for all  $a, b \in G$ , then we say  $\star$  is commutative.

For  $a, b \in G$  we'll typically write  $a \star b$  for  $\star (a, b)$ .

## **Definition: Group**

A group is an ordered pair  $(G,\star)$  where G is a set and  $\star$  is a binary operation on G such that

- ★ is associative,
- there exists an  $e \in G$ , called an identity, such that  $a \star e = e \star a = a$  for all  $a \in G$ , and
- for each  $a \in G$  there is an  $a^{-1} \in G$ , called an inverse of a, such that  $a \star a^{-1} = a^{-1} \star a = e$ .

We say the group  $(G,\star)$  is commutative (or abelian) if  $\star$  is commutative.

We've already encountered many groups in our previous studies! For example, under addition we have  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ , and  $\mathbb{Z}/n\mathbb{Z}$  (the integers modulo n), and under multiplication we have  $\mathbb{Q}^{\times}$ ,  $\mathbb{R}^{\times}$ ,  $\mathbb{C}^{\times}$ , and  $Z/n\mathbb{Z}^{\times}$  (where the  $\times$  denotes zero-exclusion). These examples help make the following properties a bit more concrete.

## Theorem 1.1

If  $(G,\star)$  is a group then

- (a) the identity of G is unique,
- (b)  $a^{-1}$  is unique for each  $a \in G$ ,
- (c)  $(a^{-1})^{-1} = a$ ,
- (d)  $(a \star b)^{-1} = b^{-1} \star a^{-1}$ , and
- (e) for all  $a_1, \dots, a_n \in G$ , the value of  $a_1 \star \dots \star a_n$  is independent of how the expression is bracketed.

*Proof.* We prove the first two parts.

(a) Suppose e and e' are both identities. Then we have the chain of equalities

$$e = e \star e' = e'$$
.

(b) Suppose some  $a \in G$  has two inverses a', a''. Then we have the chain of equalities

$$a' = a' \star e = a' \star (a \star a'') = (a' \star a) \star a'' = a''.$$

Other parts are left as exercises.  $\Box$ 

With these properties in mind, we'll make a few notes on notation.

• We read  $(G, \star)$  aloud as "G is a group under  $\star$ ". In practice, if the binary operation is self-evident, we'll simply write G to mean  $(G, \star)$ .

- For a group  $(G, \star)$  we'll usually write ab to mean  $a \star b$ . In the same spirit, we can write a length-n product  $x \star \cdots \star x$  as  $x^n$ , and  $x^{-n} = (x^{-1})^n$ . (This is called multiplicative notation.)
- When multiplicative notation is being used, we will usually denote the identity of G by 1 and set  $x^0 = 1$ .

We'll finish off here with a few definitions which will be useful in future discussions.

#### **Definition: Order of an element**

Let G be a group and let  $x \in G$ . The order |x| of x is the smallest  $n \in \mathbb{Z}^+$  such that  $x^n = 1$ .

#### **Definition: Generator**

Let G be a group, and let S be a subset of G. We say that S generates G if every element of G can be written as a finite product of elements in S and their inverses.

In this case, S is a set of generators for G and we write  $G\langle S\rangle$ .

#### **Definition: Presentation**

Let G be a group that is generated by S with a set of relations R. G has presentation  $\langle S | R \rangle$ .

## 1.2 Some Important Groups

Now we'll look at a few different kinds of well-known groups.

## **Definition: Dihedral group**

The dihedral group of order 2n is the group  $D_{2n}$  of symmetries of a regular n-gon.

In general we'll use  $r \in D_{2n}$  to denote clockwise rotation by  $2\pi/n$  and  $s \in D_{2n}$  for reflection through a fixed line of symmetry. We can get a few nice results from this!

- $D_{2n} = \{1, r, r^2, \dots, r^{n-1}\} \cup \{s, sr, sr^2, \dots, sr^{n-1}\}$  (where the two sets are disjoint).
- |r| = n and |s| = 2.
- $r^i s = s r^{-i}$  for all  $i \in \mathbb{Z}$ .

Thinking of the elements of  $D_{2n}$  as physical transformations is useful. But they're perhaps better understood as *equivalence classes* of physical moves since, for example,  $r^n$  is equivalent to  $r^{2n}$ .

## **Definition: Symmetric group**

Let  $\Omega$  be a non-empty set, and let  $S_{\Omega}$  be the set of all bijections from  $\Omega$  to  $\Omega$ . The set  $S_{\Omega}$  forms a group under function composition, and it is called the symmetric group on  $\Omega$ .

Note that if  $\Omega = \{1, 2, ..., n\}$  then we write  $S_{\Omega} = S_n$ . Permutations on such  $\Omega$  can be communicated in several different ways—for example, if we had the bijection

$$1 \mapsto 3$$
  $2 \mapsto 5$   $3 \mapsto 1$   $4 \mapsto 2$   $5 \mapsto 4$ ,

then we have the two-line, one-line, and cycle notations, respectively:

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{bmatrix}, \qquad \begin{bmatrix} 3 & 5 & 1 & 2 & 4 \end{bmatrix}, \qquad (1\ 3)(2\ 5\ 4).$$

We again have a few important facts about symmetric groups.

- The order of  $S_n$  is n! ( $|S_n| = n!$ ).
- $S_n$  is non-abelian for  $n \geq 3$ .
- Disjoint cycles commute.
- The order of a permutation is the least common multiple of the cycle lengths in its decomposition.
- $S_n$  is generated by the adjacent transpositions (the 2-cycles comprised of adjacent elements). The group can also be generated by  $\{(1\ 2), (1\ 2\ \cdots\ n)\}.$

As a fun fact,  $S_3$  can be used to create a permutation representation of  $D_6$ —if we label the vertices of a triangle with 1, 2, and 3, the movements of the vertices are represented by

$$e' \mapsto e$$
  $s \mapsto (2\ 3)$   
 $r \mapsto (1\ 2\ 3)$   $sr \mapsto (1\ 3)$   
 $r^2 \mapsto (1\ 3\ 2)$   $sr^2 \mapsto (1\ 2)$ 

Thus  $S_3$  is isomorphic to  $D_6$  ( $S_3 \cong D_6$ ).

## **Definition: General linear group**

For each  $n \in \mathbb{Z}^+$  let  $GL_n(F)$  be the set of all invertible  $n \times n$  matrices whose entries come from a field F.  $GL_n(F)$  is a group under matrix multiplication and is called the general linear group of degree n.

## **Definition: Quaternion group**

The quaternion group  $Q_8$  has elements

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\},\$$

where 1 is the identity. For any  $a \in Q_8$ , the elements multiply as follows.

$$(-1)^2 = 1$$
,  $(-1) \cdot a = a \cdot (-1) = -a$   
 $i^2 = j^2 = k^2 = -1$   
 $ij = k$ ,  $jk = i$ ,  $ki = j$   
 $ji = -k$ ,  $kj = -i$ ,  $ik = -k$ 

## 1.3 Homomorphisms

Now we'll look at different kinds of maps between groups, starting with the simplest one posible.

## **Definition: Homomorphism**

Let G and H be groups. A homomorphism from G to H is a function  $\varphi:G\to H$  such that, for all  $x,y\in G$ ,

$$\varphi(xy) = \varphi(x)\varphi(y).$$

The kernel and image of  $\varphi$  are, respectively,

$$\ker(\varphi) = \{x \in G \mid \varphi(x) = 1\}, \quad \operatorname{image}(\varphi) = \{\varphi(x) \mid x \in G\}.$$

## Theorem 1.2

Let  $\varphi:G\to H$  be a homomorphism. Then

(a)  $\varphi(1)$  is the identity of H.

- (b)  $\varphi(x^{-1}) = \varphi(x)^{-1}$  for all  $x \in G$ .
- (c)  $\varphi(x^n) = \varphi(x)^n$  for all  $x \in G$ ,  $n \in \mathbb{Z}$ .

If we want to do a better job at preserving structure in our map, we can go a step further.

## **Definition: Isomorphism**

A homomorphism  $\varphi:G\to H$  is an isomorphism if it is bijective. In this case we say G and H are isomorphic, and we write  $G\cong H$ .

The existence of the identity map on G is enough to show that  $G\cong G$ , but other isomorphisms may exist. For example, we may fix g and define  $\varphi_g:G\to G$  by setting  $\varphi_g(x)=gxg^{-1}$  for all  $x\in G$ . (This is a particular kind of isomorphism called an inner automorphism.)

## **Definition: Automorphism**

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

Notably, the set Aut(G) of automorphisms of G forms a group under function composition!

## 1.4 Group Actions

We'll finish off our preliminary discussion of groups by looking at what might happen when a group acts on some other set.

## **Definition: Group action**

A (left) group action of a group G on a set X is a map from  $G \times X$  to X, where the image of (g,x) is written as  $g \cdot x$  or simply gx, such that

- g(hx) = (gh)x for all  $g, h \in G$  and  $x \in X$ .
- 1x = x for all  $x \in X$ .

There are many easily accessible examples of group actions—here's the most glaring one.

## Definition: Left regular action

Every group acts on itself by left multiplication. This is called the left regular action of G.

As for some others:  $\mathbb{R}^{\times}$  acts on  $\mathbb{R}^n$  by scaling,  $S_{\Omega}$  acts on  $\Omega$  by permuting, and  $D_{2n}$  acts on the vertices of a regular n-gon.

## Theorem 1.3

Suppose G acts on X. For each  $g \in G$ ,  $\sigma_g(x) = g \cdot x$  defines a permutation of X. Moreover, the map from G to  $S_X$  defined by  $g \mapsto \sigma_g$  is a homomorphism.

*Proof.* Let  $g \in G$ . Since  $\sigma_g \circ \sigma_{g^{-1}}$  and  $\sigma_{g^{-1}} \circ \sigma_g$  are both the identity map on X,  $\sigma_g$  has a two-sided inverse and is therefore a bijection from X to X. In other words,  $\sigma_g$  is a permutation of X.

Now define a map  $\varphi:G\to S_X$  such that  $\varphi(g)=\sigma_g.$  We have

$$\varphi(gh)(x) = \sigma_{gh}(x)$$

$$= (gh) \cdot x$$

$$= g \cdot (h \cdot x)$$

$$= \sigma_g(\sigma_h(x))$$

$$= (\varphi(g) \circ \varphi(h)) (x)$$

Since these two expressions agree as functions on X, they must be equal. This holds for all  $g,h\in G$  and  $\varphi$  is a homomorphism.  $\square$ 

All this motivates the following.

## **Definition: Representation**

Let G be a group, and let  $n \in \mathbb{Z}^+$ .

- $\bullet$  A homomorphism  $\varphi:G\to S_n$  is called a permutation representation.
- A homomorphism  $\rho:G\to GL_n(\mathbb{C})$  is called a linear representation.