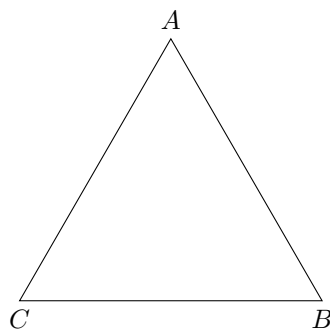


# MAT347 Abstract Algebra

Jonah Chen

## 1 Groups

Groups are generally associated with symmetries. Consider the equilateral triangle:



We know that there are six symmetries of the triangle:

- Identity transformation (do nothing) denoted as  $\text{id}$  or  $e$
- Two rotations ( $A \rightarrow B \rightarrow C \rightarrow A$  and  $A \rightarrow C \rightarrow B \rightarrow A$ )
- Three reflections  $A \leftrightarrow B$ ,  $A \leftrightarrow C$ ,  $B \leftrightarrow C$

Note that these symmetries preserve the structure of the triangle, hence the composition of two symmetries must also be a symmetry. Let

- $\rho$  be the rotation  $A \rightarrow B \rightarrow C \rightarrow A$
- $\sigma$  be the reflections  $B \leftrightarrow C$

Note that  $\rho\sigma$  is the  $A \leftrightarrow C$  reflection and  $\sigma\rho$  is the  $A \leftrightarrow B$  reflection. Hence they may not be commutative.

We also know that all symmetries can be reversed.  $\alpha$  has an inverse  $\alpha^{-1}$  such that  $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$ . These inspire the following definition:

**Definition:** A **group** is a set  $G$  with a composition

$$G \times G \rightarrow G \tag{1}$$

$$(g, h) \mapsto g \cdot h \tag{2}$$

Satisfying:

- Associativity:  $(g \cdot h) \cdot k = g \cdot (h \cdot k)$

- Identity:  $\exists e \in G$  such that  $g \cdot e = e \cdot g = g$  for all  $g \in G$
- Inverse:  $\forall g \in G, \exists g^{-1} \in G$  such that  $g \cdot g^{-1} = g^{-1} \cdot g = e$

Examples:

- $\mathbb{Z}$  with  $+$  is a group. It is associative,  $e = 0$  and  $g^{-1} = -g$ .
- $\mathbb{Z}/n\mathbb{Z}$  with addition modulo  $n$ .
- If  $F$  is a field, it implicitly has two group structures:
  - Additive group:  $(F, +)$  is a group. It is associative,  $e = 0$  and  $g^{-1} = -g$ .
  - Multiplicative group:  $(F \setminus \{0\}, \times)$  is a group. It is associative,  $e = 1$  and  $g^{-1} = 1/g$ .
- $GL(n, F)$  – “general linear group” contains all invertible  $n \times n$  matrices.
- $SL(n, F)$  – “special linear group” contains all invertible  $n \times n$  matrices with determinant 1.
- $SO(n, F)$  – “special orthogonal group”  $= \{A \in SL(n, F) | A^t = A^{-1}\}$ .

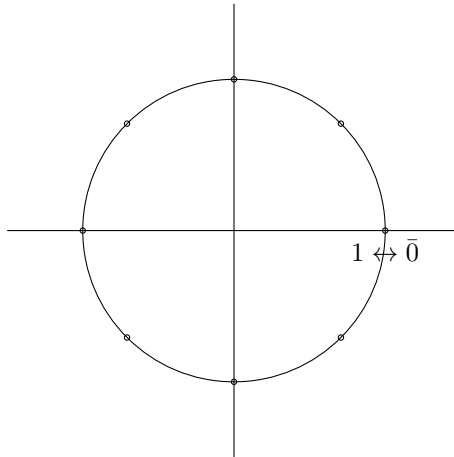
## 1.1 Cyclic Groups

One of the simplest groups is  $\mathbb{Z}/n\mathbb{Z}$  for  $n \in \mathbb{N}$  with the operation addition modulo  $n$ . This is known as the “cyclic group of order  $n$ ” or  $C_n$ . i.e. for  $n = 8$ ,  $5 + 7 = 4 \pmod{8}$ , which we denote  $\bar{5} + \bar{7} = \bar{4}$ .

We know the inverse  $\bar{k}^{-1} = \overline{n - k}$  for nonzero  $k$  or  $\bar{0}^{-1} = \bar{0}$ .

Another way to express the cyclic group is  $\bar{k} \leftrightarrow e^{2\pi i k/n}$  with multiplication operation. Then,

$$\overline{k+n} = e^{2\pi i(k+n)/n} = e^{2\pi i k/n} e^{2\pi i n/n} = e^{2\pi i k/n} = \bar{k}. \quad (3)$$



**Definition:** [Order] The **order** of a group  $G$  is its cardinality denoted  $\text{ord}(G)$  or  $|G|$ . It could be a finite or infinite ordinal. In particular,  $|C_n| = n$ .

## 1.2 Quaternion Group

The quaternion group  $\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$  is a group of order 8 with the multiplication operation. It has

**Definition:** [Subgroup] A **subgroup** of a group  $G$  is a subset  $H \subseteq G$  such that  $H$  is a group.

**Definition:** [Coset] If  $G$  is a group and  $H \leq G$ , consider sets of the form

$$Hg = \{hg | h \in H\} \quad (4)$$

This is a **right coset** of  $H$ .

**Theorem:** [Partitioning with Cosets] Consider  $Hg$  and  $Hg'$  for  $g, g' \in G$ . There are two cases:

- They might be disjoint:  $Hg \cap Hg' = \emptyset$ .
- They might intersect. Suppose  $hg = h'g'$  for some  $h, h' \in H$

$$h^{-1}hg = h^{-1}h'g' \quad (5)$$

$$g = h^{-1}h'g' \in Hg' \quad (6)$$

Similarly,  $g' \in Hg$ . Consider an arbitrary element of  $Hg$  with  $k \in H$ . Then,  $kg = kh^{-1}h'g' \in Hg'$  i.e.  $Hg \leq Hg'$ . Similarly,  $Hg' \leq Hg$ . Thus,  $Hg = Hg'$ .

The right cosets of  $H$  partition  $G$ . In particular,

$$G = \bigsqcup Hg_i \quad (7)$$

For fixed  $g$ , if  $hg = h'g$  for  $h, h' \in H$  then  $hgg^{-1} = h'gg^{-1}$  so  $h = h'$ . So in  $Hg$ , every element can be matched with an element of  $H$ . So,  $|Hg| = |H|$ .

**Theorem:** [Lagrange] If  $|G| < \infty$  and  $H \leq G$ , then  $|H| \mid |G|$

**Definition:** [Index] For  $H \leq G$ , the **index** of  $H$  in  $G$  is  $[G : H] = |G|/|H|$ .

If  $|G| = 13$ , the only subgroups of  $G$  are  $\{e\}, G$ .

If  $G = \mathbb{Z}$  and  $H = 2\mathbb{Z}$  (even numbers). Then  $H + 0 = H$  is one coset, and  $H + 1 =$  the odd integers is another coset. So,  $\mathbb{Z} = (2\mathbb{Z}) \sqcup (2\mathbb{Z} + 1)$ .

Same for Left Cosets Interaction of left and right cosets?

Consider the triangle group with rotations  $e, \rho, \rho^2$  and reflections  $\sigma_A, \sigma_B, \sigma_C$ . Consider the subgroup  $H =$

$$\{e, \sigma_A\}.$$

$$He = \{e, \sigma_A\} \quad (8)$$

$$H\rho = \{\rho, \sigma_B\} \quad (9)$$

$$H\rho^2 = \{\rho^2, \sigma_C\} \quad (10)$$

$$eH = \{e, \sigma_A\} \quad (11)$$

$$\rho H = \{\rho, \sigma_C\} \quad (12)$$

$$\rho^2 H = \{\rho^2, \sigma_B\} \quad (13)$$

Note that the left and right cosets are different. They are the same if the group is commutative.

**Definition:** [Action] An **action** of a group  $G$  on a set  $X$  is a map

$$G \times X \rightarrow X \quad (14)$$

$$(g, x) \mapsto gx \quad (15)$$

such that

$$(gh)x = g(hx) \quad (16)$$

$$ex = x \quad (17)$$