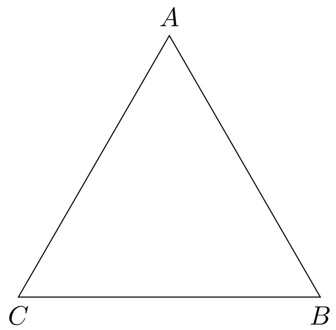
MAT347 Abstract Algebra

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 id or e
- Two rotations ($A \to B \to C \to A$ and $A \to C \to B \to A$)
- 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

- ρ be the rotation $A \to B \to C \to A$
- σ 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. α has an inverse α^{-1} such that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$. These inspires the following definition:

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

$$G \times G \to G \tag{1}$$
$$(g, h) \mapsto g \cdot h \tag{2}$$

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 invertiable $n \times n$ matrices.
- $SL(n, F)$ – "special linear group" contains all invertiable $n \times n$ matrices with determinant 1.
- $SO(n, F)$ – "special orthogonal group" $= \{A \in SL(n, F) | A^t = A^{-1}\}$.

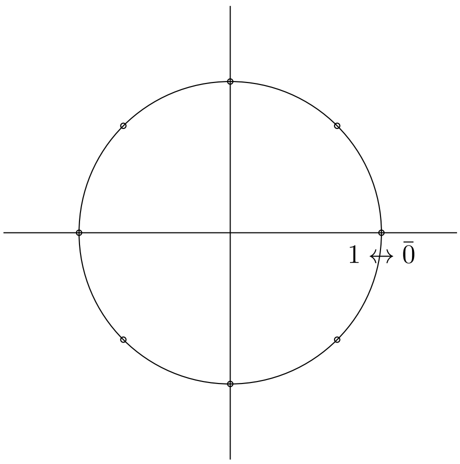
1.1 Cyclic Groups

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,

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



Definition: [Order] The **order** of a group G is its cardinality denoted $\mathrm{ord}(G)$ 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

$$Hg = \{hg | h \in H\} \tag{4}$$

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 $h, h' \in H$

$$h^{-1}hg = h^{-1}h'g' \tag{5}$$
$$g = h^{-1}h'g' \in Hg' \tag{6}$$

Similarly, $g' \in Hg$. Consider an arbitrary element of $kg \in Hg$ 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,

$$G = \bigsqcup Hg_i \tag{7}$$

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 $|H| \Big| |G|$

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

If $|G| = 13$, the only subgroups or 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, $\mathbb{Z} = (2\mathbb{Z}) \sqcup (2\mathbb{Z} + 1)$.

<u>Same for Left Cosets</u> Interaction of left and right cosets?

Consider the triangle group with rotations e, ρ, ρ^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

$$G \times X \to X \quad (14)$$
$$(g, x) \mapsto gx \quad (15)$$

such that

$$(gh)x = g(hx) \quad (16)$$
$$ex = x \quad (17)$$

If G is a group, it acts on itself. This is called a "left translation" or "left regular action".

How about the right action $(g, x) \mapsto xg$. The second condition may not be true

$$(gh, x) = xgh \quad (18)$$
$$(g, (hx)) = (g, xh) = xhg \quad (19)$$

which is not true. Instead, let $(g, x) = xg^{-1}$. Then,

$$(gh, x) = x(gh)^{-1} = xh^{-1}g^{-1} \quad (20)$$
$$(g, (h, x)) = (g, xh^{-1}) = xh^{-1}g^{-1} \quad (21)$$

This is the definition of the right action.

There is a third action of G on itself by $(g, x) = gxg^{-1}$. This action is called conjugation.

Take the following example: Let $G = SO(3)$ and let $X = S^2$. G acts on X by rotation. Let $H = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$ be the subgroup of rotations that fixes the z-axis.

H also acts on X ??

Definition: [Orbit] If G acts on X, the **orbit** of $x \in X$ is the set $Gx = \{gx | g \in G\}$. i.e. the set of all points x is taken to by elements of G.

The orbits of $H \approx SO(2)$ on the sphere are the lines of latitude (and the north and south poles).

H fixes the north pole, thus every coset gH takes the north pole to a point. Suppose gH and $g'H$ are cosets such that $gHN = g'HN \implies gN = g'N \implies (g')^{-1}gN = N \implies (g')^{-1}g \in H \implies gH$... so the points ofn the sphere are in 1-1 correspondence with the left cosets of H.

Definition: [Stabilizer] If G acts on X and $x \in X$, the "stabilizer" of x in G is $\{g \in G | gx = x\}$