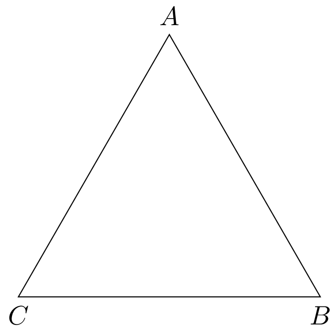
MAT347 Abstract Algebra

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

$$G \times G \to G \quad (1)$$
$$(g, h) \mapsto g \cdot h \quad (2)$$

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" $= \{A \in SL(n, F) | A^t = A^{-1}\}$.

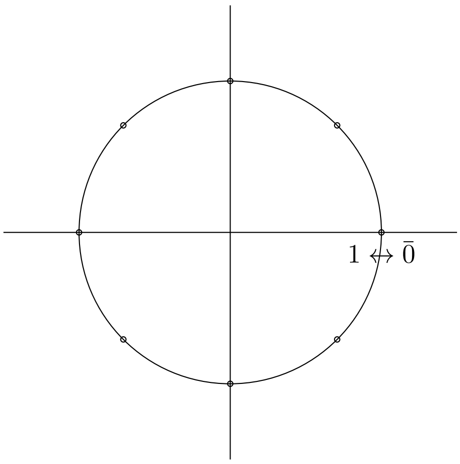
1.1 Cyclic Groups

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 $\operatorname{ord}(G)$ 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 $H = \{e, \sigma_A\}$.

$$He = \{e, \sigma_A\} \tag{8}$$
$$H\rho = \{\rho, \sigma_B\} \tag{9}$$
$$H\rho^2 = \{\rho^2, \sigma_C\} \tag{10}$$
$$eH = \{e, \sigma_A\} \tag{11}$$
$$\rho H = \{\rho, \sigma_C\} \tag{12}$$
$$\rho^2 H = \{\rho^2, \sigma_B\} \tag{13}$$

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

$$G \times X \to X \tag{14}$$
$$(g, x) \mapsto gx \tag{15}$$

such that

$$(gh)x = g(hx) \tag{16}$$
$$ex = x \tag{17}$$

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

$$(gh, x) = xgh \tag{18}$$
$$(g, (hx)) = (g, xh) = xhg \tag{19}$$

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

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

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 $\{g \in G | gx = x\}$

Definition: [Centralizer] If $A \subset G$, the **centralizer** of A in G is $C_G(A) = \{g \in G | ga = ag \forall a \in A\}$

- If G is abelian, then $C_G(A) = G$ for any A.
- In the triangle group, $C_G(\{\rho\}) = \{e, \rho, \rho^2\}$

Definition: [Center] The **center** of G is $Z(G) = \{g \in G | gg' = g'g \forall g' \in G\} = C_G(G)$

Proposition: For any $A \subset G$, $C_G(A) \leq Z(G)$ (is a subgroup).

Consider the regular n-gon ($n \geq 3$), what are its rigid motion symmetries?

- There are always n rotations by $\frac{2\pi}{n}$ about the origin.
- When n is even, there are $n/2$ reflections in each pair of edges, and each pair of vertices. When n is odd, there are n reflections in each pair of (edge, vertex). There are always n reflections.
- Write ρ for clockwise rotation by $\frac{2\pi}{n}$. Fix one vertex and let σ be the reflection that fixes that vertex.
- Note that $\rho\sigma = \sigma\rho^{-1}$. To show this, it suffices to find where two of the vertices gets mapped.

Proposition: The symmetries are $e, \rho, \rho^2, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \ldots, \sigma\rho^{n-1}$

Definition: [dihedral group] The group of symmetries of the regular n-gon is D_{2n}, the **dihedral group** of order $2n$.

Given $H \leq G$ we write G/H as the set of left cosets

$$G/H = \{gH | g \in G\} \tag{22}$$
$$H \setminus G = \{Hg | g \in G\} \tag{23}$$

Both of these are called "G mod H". In general, the two are <u>different</u>.

Now we want to ask, is $H \setminus G$ a group?

- The most naive idea is to reuse multiplication in G, i.e. $Hg \cdot Hg' = Hgg'$, but it only sometimes works.
- This formula means: $hg \cdot h'g' = h''gg'$. For any $h, h' \in H, \exists h''$ s.t. this holds.
- Trick: $hg \cdot h'g' = hgh'eg' = hgh'(g^{-1}g)g' = h(ghg^{-1})gg'$. Now we can ask if $ghg^{-1} \in H$ (for every $h' \in H$)

Definition: [Normal Subgroup] A subgroup $H \leq G$ is **normal** if $ghg^{-1} \in H \forall g \in G, h \in H$, which is abbreviated as $gHg^{-1} = H$. $H \trianglelefteq G$ means H is a normal subgroup of G

- Notice that if $gHg^{-1} = H$ then $gH = Hg$. So H is normal, the left and right cosets must be the same.

Definition: [Quotient Group] If $H \trianglelefteq G$, then G/H is called the quotient group.

1.3 Homomorphisms

Definition: [Homomorphism] If G, K are groups, a **homomorphism** is a map $\varphi : G \to K$ such that $\varphi(gg') = \varphi(g)\varphi(g') \, \forall g, g' \in G$.

Observations: IF $\varphi : G \to K$ is a homomorphism and $g \in G$, then

1. $\varphi(g) = \varphi(eg) = \varphi(e)\varphi(g)$, so $\varphi(e) = e$ (the identity element of K)
2. $e = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$, so $\varphi(g^{-1}) = \varphi(g)^{-1}$

Examples

- $G = \mathbb{Z}$ and $\varphi : \mathbb{Z} \to \mathbb{Z}, \varphi(n) = 2n$ is a homomorphism, as $\varphi(n + m) = 2(n + m) = 2n + 2m = \varphi(n) + \varphi(m)$
- $G = \mathbb{Z}, K = \mathbb{R}$ and $\varphi : \mathbb{Z} \to \mathbb{R}, \varphi(n) = n$. This mapping is called an **inclusion** as $Z \subset \mathbb{R}$.
- If G is a group and $g_0 \in G$, then $C_{g_0} : G \to G, g \mapsto g_0 g g_0^{-1}$ is a homomorphism.
- A linear transformation $T : V \to W$ if V, W are vector spaces (the additive group).
- Note that $\varphi : g \mapsto g^{-1}$ is **only** a homomorphism if G is abelian.

Definition: [Kernel/Image] If $\varphi : G \to G'$ is a homomorphism, then the **kernel** of φ is

$$\ker(\varphi) = \{g \in G | \varphi(g) = e\}. \tag{24}$$

The **image** of φ is

$$\mathrm{im}(\varphi) = \{\varphi(g) | g \in G\} \subseteq G' \tag{25}$$

Theorem: $\ker(\varphi) \leq G$ and $\mathrm{im}(\varphi) \leq G'$ $\ker(\varphi) \trianglelefteq G$

Proof. Since $\varphi(e) = e$, $e \in \ker(\varphi)$, and $e \in \mathrm{im}(\varphi)$. So both are nonempty.
Suppose $g, h \in \ker(\varphi)$, $e = \varphi(e) = \varphi(hh^{-1}) = \varphi(h)\varphi(h^{-1}) \ldots$ □

- Suppose $N \trianglelefteq G$ and then define $G \to G/N, g \mapsto Ng$. We claim this is a homomorphism. Proof is simple $\varphi(gg') = Ngg'$, $\varphi(g)\varphi(g') = NgNg' = NgN(g^{-1}gg') = N(gNg^{-1})gg' = NNgg' = Ngg'$
- This map is called the (natural) **projection** of G onto G/N. Sometimes written $\Pi_{G/N}$ or $\mathrm{proj}_{G/N}$.
- $\mathrm{im}(\Pi_{G/N}) = G/N$ and $\ker(\Pi_{G/N}) = N$.
- Any homomorphism is related to this one, so this could be considered as the "generic homomorphism".

Definition: [Isomorphism] If $\varphi : G \to H$ is a homomorphism, and $\ker(\varphi) = \{e\}$ then φ is injective. If $\varphi(G) = H$ then φ is surjective. Thinking of G and H as sets, there is an inverse $\varphi^{-1} : H \to G$ such that $\varphi^{-1} \circ \varphi = 1_G$ and $\varphi \circ \varphi^{-1} = 1_H$. It is easy to check that φ^{-1} is also a homomorphism.
In this case, φ is an **isomorphism**

- Suppose we have an injective homomorphism $\varphi : G \to H$ where $\ker(\varphi) = \{e\}$. Then, we can consider $\varphi : G \to \mathrm{im}(\varphi) < H$. Sometimes we say $\varphi : G \to H$ is an **isomorphism into** H, as opposed to an isomorphism **onto** H or between G and H.

Definition: [Automorphism] If G is a group, an **automorphism** of G is an isomorphism $\varphi : G \to G$.

Examples:

- If $G = \mathbb{Z}, n \mapsto -n$ is the only automorphism apart from the identity.
- If G is abelian, $g \mapsto g^{-1}$ is an automorphism.
- If F is a field, and $G = GL(n, F)$ then $g \mapsto (g^t)^{-1}$ (transposed inverse) is an automorphism.
- If we fix $g_0 \in G$ then the conjugation $C_{g_0} : G \to G$ where $C_{g_0}(g) = g_0 g g_0{}^{-1}$ is an automorphism.

Definition: [Automorphism Group] $\mathrm{Alt}(G)$ is the **group** of automorphisms of G.

Definition: [Inner/Outer Automorphisms] The **inner automorphisms** of G are

$$\mathrm{Inn}(G) = \{\varphi \in \mathrm{Alt}(G) | \varphi = C_{g_0} \text{ for some } g_0 \in G\}. \tag{26}$$

If an element of $\mathrm{Alt}(G)$ that is not inner is **outer**.

- It is easy to show that $\mathrm{Inn}(G) \leq \mathrm{Alt}(G)$.
- Observe that if G is abelian, then $\mathrm{Inn}(G) = \{\mathrm{id}\}$
- In general, $\{\mathrm{id}\} \leq \mathrm{Inn}(G) \leq \mathrm{Alt}(G)$.

- The map

$$G \to \mathrm{Alt}(G) \tag{27}$$
$$g \to C_g \tag{28}$$

  is a homomorphism. Its image is $\mathrm{Inn}(G)$ and its kernel is Z_G (the center).

Definition: [Fiber] If p is a projection, then $p^{-1}(x)$ is the **fiber** over x

- If $N \triangleleft G$, the projection $\pi : G \to G/N$ is a homomorphism. The fibers of π is the cosets $gN = Ng$, and they are all the same size.
- Suppose $\varphi : G \to H$ is a homomorphism, and $N = \ker(\varphi) \trianglelefteq G$. The fibers of φ is the cosets of G/N.
- We have $\varphi : G \to H$ and $\pi : G \to G/N$. Wouldn't it be nice if $G/N \to H$ "induced by φ" were a homomorphism? Well, it is.

Theorem: [(First) Isomorphism] If $\varphi : G \to H$ is a homomorphism, and $N = \ker(\varphi)$, then there is a homomorphism $\bar{\varphi} : G/N \to H$ such that $\bar{\varphi} \circ \pi = \varphi$.
Moreover, $\ker(\bar{\varphi}) = \{eN\}$, the trivial subgroup of G/N, so $\bar{\varphi}$ is injective. So, $\bar{\varphi} : G/N \to \mathrm{im}(\varphi)$ is an **isomorphism**.

- This theorem suggests that you can construct an isomorphism from an arbitrary homomorphism. First, φ factors through G/N, then we can include it into H.

$$G \to^{\pi} G/N \to^{\bar{\varphi}} \mathrm{im}(\varphi) \to^{\text{inclusion}} H \tag{29}$$