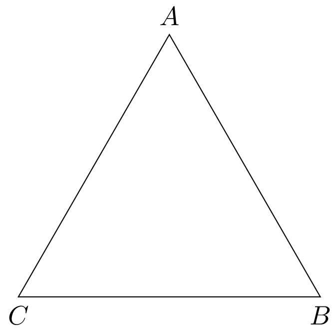
MAT347 Abstract Algebra

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

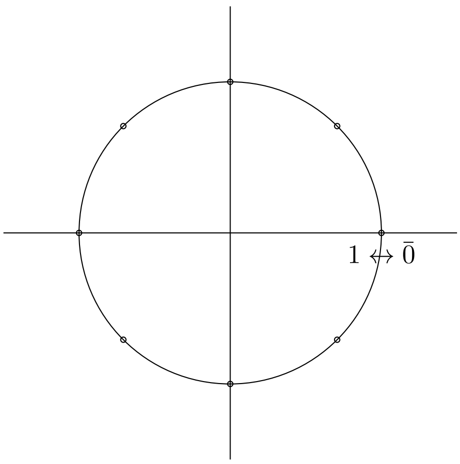
1.1 Cyclic Groups

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 $n = 8$, $5 + 7 = 4 \,(\mathrm{mod}\, 8)$, 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 $H = \{e, \sigma_A\}$.

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

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 different.

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.

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

Theorem–(Third) Isomorphism: $N \trianglelefteq G$ and $H \leq G$, then $N \leq H \implies N \trianglelefteq G$.

Proof. ???? □

Theorem–:

$$G/H \cong G/N \Big/ H/N \tag{30}$$

Proof. Define $\varphi : G \to G/N \Big/ H/N$ by

$$\varphi(g) = (gN)H/N \tag{31}$$

We need to show φ is a homomorphism. Let

$$\begin{aligned} \varphi(gg') &= gg'N\ H/N && (32)\\ &= gNg'N\ H/N && (33)\\ &= gN\ H/N \cdot g'N\ H/N && (34)\\ &= \varphi(g)\varphi(g') && (35)\\ & && (36) \end{aligned}$$

□

We will then ask what is $\ker(\varphi)$. Suppose $\varphi(g) = H/N$, so $gN\ H/N = H/N$. But g is a representation for gN, so gH/N for this to be in H/N we want $g \in H$ so $\ker(\varphi) = H$. An arbitrary element of $G/N \Big/ H/N$ is $gN\ H/N$ for some $g \in G$, so $\mathrm{im}(\varphi) = G/N \Big/ H/N$.

- $G = \mathbb{Z}, H = 3\mathbb{Z}, K = 4\mathbb{Z}$. By the second isomorphism theorem, $\mathbb{Z}/3\mathbb{Z} \cong 4\mathbb{Z}/12\mathbb{Z}$, and also $Z/4\mathbb{Z} \cong 3\mathbb{Z}/12\mathbb{Z}$.

Definition–Equivilence Class: Being in the same coset of a subgroup H is an equivalence relation. So, the large group is a disjoint union of equivalence classes (cosets) of H.

- The cosets of $\mathbb{Z}$ in $\mathbb{R}$ is $r + \mathbb{Z}$ for $r \in [0, 1)$.
- Homomorphism $\varphi : \mathbb{R} \to \mathbb{C}^\times, t \mapsto e^{2\pi i t}$. Then, $\ker(\varphi) = \mathbb{Z}$. Observe tat φ is **onto** the unit circle, by the first isomorphism theorem, $\mathbb{R}/\ker(\varphi) = \mathbb{R}/\mathbb{Z} \cong S^1$.
- $\mathbb{Z}^2 \triangleleft \mathbb{R}^2$

Theorem–Fourth Isomorphism Theorem/Lattice Theorem: Consider a lattice of subgroups with $N \trianglelefteq G$. In G/N, the subgroup lattice has the same structure as the subgroup lattice of G that contains N.
Specifically, if $N \trianglelefteq G$, and $N \trianglelefteq H < G$, we write $\bar{H} = H/N$. Including $\bar{G} = G/N$ and $\bar{N} = \bar{e} = N/N$. Then, the lattice of $\bar{H}$s in $\bar{G}$ has the same lattice structures as the part of the lattice for G consisting

of subgroups that are intermediate between N and G. Moreover,

$$H \leq K \iff \bar{H} \leq \bar{K} \tag{37}$$
$$H \trianglelefteq K \iff \bar{H} \trianglelefteq \bar{K} \tag{38}$$
$$[H : K] = [\bar{H} : \bar{K}] \text{ if } K \leq H \tag{39}$$
$$\overline{H \cap K} = \bar{H} \cap \bar{K} \tag{40}$$
$$\overline{\langle H, K \rangle} = \langle \bar{H}, \bar{K} \rangle \tag{41}$$

If G, G' are groups, consider the cartesian product $G \times G' = \{(g, g')|g \in G, g' \in G'\}$. Note that $|G \times G'| = |G||H|$. There is an obvious way to turn this into a group by

$$(g, g')(h, h') = (gh, g'h') \tag{42}$$
$$(g, g')^{-1} = (g^{-1}, g'^{-1})e = (e, e) \tag{43}$$

In $G \times G'$, the subset $G_0 =: \{(g, e)|g \in G\} \cong G$ is a subgroup. Likewise, $G'_0 =: \{(e, g')|g' \in G'\} \cong G'$. Also notice that G_0 and G'_0 commute. So, $(G \times G')/G_0 \cong G'$.

1.4 Symmetric Groups

Definition–Symmetric Group: The symmetric group S_n is the group of permutation of n elements, with composition as the operation.

- $|S_n| = n!$
- A cycle is a permutation that cycles through some subset of $\{1, \ldots, n\}$, denoted as

  $$(a_1\, a_2\, \ldots\, a_k), \quad k \leq n \text{ and } a_i \text{ are distinct.} \tag{44}$$

  Represents the permutation $a_1 \to a_2 \to \cdots \to a_k \to a_1$.
- Note that these are ambiguous, as $(a_1\, a_2\, \ldots\, a_k)$ is the same as $(a_2\, a_3\, \ldots\, a_k\, a_1)$. So by convention, we often start with the smallest number first so they are unique.
- k is the length of the cycle, it is also called a **k-cycle**.
- Every permutation can be written as a product of disjoint cycles. If given a permutation, we will start from 1 and write a cycle until we get back to 1. Then, we will start from the next number that hasn't been included yet and repeat until we get to the end.
- If $\sigma = (1\,3\,6)(4\,5)$, then $\sigma^{-1} = (4\,5)^{-1}(1\,3\,6)^{-1} = (4\,5)(1\,6\,3) = (1\,6\,3)(4\,5)$. We will order the cycles by their first element, and omit 1-cycles.
- Two **disjoint cycles** (i.e. without any numbers in common) will commute.
- If cycles are not disjoint, like $\sigma = (1\,4\,2)(2\,3\,5)(3\,4\,7) \in S_7$ will not commute.
  - $1 \to 4$
  - $4 \to 7$
  - $7 \to 3 \to 5$
  - $5 \to 2 \to 1$
  - $2 \to 3$
  - $3 \to 4 \to 2$

  So $\sigma = (1\,4\,7\,5)(2\,3)$.

- Any k-cycle is a product of 2-cycles. Thus, every element in the symmetric group can be written as a product of 2-cycles so S_n is generated by 2-cycles. For example, if $k = 4$ and $\sigma = (a\,b\,c\,d)$, then $\sigma = (a\,d)(a\,c)(a\,b)$.
- We can ask what is the minimum number of 2-cycles needed to generate any $\sigma \in S_n$. In general, this is a very difficult question to answer. However, the **parity** of the number of 2-cycles in a product equalling σ is well-defined.
- If $\sigma = (a_1\,b_1)(a_2\,b_2)\dots(a_k\,b_k)$ is a product of 2-cycles, then σ is **even** if k is even, and **odd** if k is odd.
- **Warning: a k-cycle is even if k is odd, and odd if k is even.**
- To make odd and even well defined, we need to know that the parity of a permutation is independent of the way we write the cycles.

  Proof. Given $\sigma \in S_n$ is a k-cycle. Define $\Delta = \prod_{1\le i<j\le n}(j-i)$. If $\tau \in S_n$, it acts on Δ with

  $$\tau \cdot \Delta = \prod_{1\le i<j\le n} (\tau(j) - \tau(i)). \tag{45}$$

  These two products are the same up to a factor of ± 1, you have to multiply by -1 for each pair $i < j$ for which $\tau(i) > \tau(j)$.

  We will consider how $(a\,b)$ with $a < b$ affect Δ. If neither i nor j is equal to a or b, the term is unaffected. Note that

  - If $i < a$, then $i < \tau(a) = b$ and $i < \tau(b) = a$. So $(i\,a)$ or $(i\,b)$ are unaffected.
  - Likewise, for $j > b$ then $(a\,j)$ or $(b\,j)$ are unaffected.

  The only pairs that will be affected are ones $(a\,i), (i\,b)$ with $a < i < b$ and $(a\,b)$. If $a < i < b$, then both $(a\,i)$ and $(i\,b)$ will change sign, so the product will be unaffected. $(a\,b)$ will change sign, so Δ will change sign under a transposition.

  If $\sigma \in S_n$, write it as any product of k transpositions. If $\sigma \cdot \Delta = \Delta$ then there must be an even number of transpositions. If $\sigma \cdot \Delta = -\Delta$ then there must be an odd number of transpositions. Thus, the parity of σ is independent of the way we write it. □

Definition–Sign: The sign of $\sigma \in S_n$ is

$$\text{sgn}(\sigma) = (-1)^k, \tag{46}$$

if σ is a product of k transpositions.

- Note that $\text{sgn}(\sigma\tau) = (-1)^k(-1)^l = (-1)^{k+l} = \text{sgn}(\sigma)\text{sgn}(\tau)$.
- Thus, $\text{sgn} : S_n \to \{\pm 1\}$ is a homomorphism.
- $\ker(\text{sgn}) = A_n \trianglelefteq S_n$ is the alternating group of k elements which contains all the even permutations. Note that

  $$S_n/A_n \cong \{\pm 1\} \quad [S_n : A_n] = 2 \quad |A_n| = \frac{n!}{2} \tag{47}$$

- for $n > 5$, A_n has no normal subgroups. What are the possible cycle types in A_5? There is $(a\,b\,c\,d\,e), (a\,b)(c\,d), (a\,b\,c)$
- Let $\sigma \in S_n$ with $a \to b \to c \to \cdots$, and suppose $\tau \in S_n$ takes $a \to a', b \to b', c \to c', \dots$. Consider the conjugation $\tau\sigma\tau^{-1}$.

  $$\tau\sigma\tau^{-1}(a') = \tau\sigma(a) = \tau(b) = b' \tag{48}$$
  $$\tau\sigma\tau^{-1}(b') = \tau\sigma(b) = \tau(c) = c' \tag{49}$$
  $$\tag{50}$$

  So $\tau\sigma\tau^{-1}$ takes $a' \to b' \to c' \to \cdots$. Conjugating by τ "relabels" what σ by replacing a with a', ...

1.5 Simple Group

One way we study groups is to write it as a chain of normal subgroups $G_0 = \{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r = G$, where G_{i+1}/G is a simple group $\forall i = 0, \ldots, r-1$. A decomposition like this is called a **Jordan-Holder Series** (composition series), and the quotients are called the **composition factors**. However, the same G may have different composition series.

> **Theorem–Jordan-Holder**: Any two Jordan-Holder series for G have the same length. Moreover, the composition factors are the same (but perhaps in different orders).

Example: Suppose H, K are both normal subgroups of G. Apply 2nd isomorphism theorem. Note, $H \subseteq Norm_G(K) = G$ and $K \subseteq Norm_G(H) = G$. Thus, $HK/K \cong H/H \cap K$ and $HK/H \cong K/H \cap K$. In this example there are two composition series

$$\{e\} \triangleleft H \cap K \triangleleft H \triangleleft HK \triangleleft G \tag{51}$$

$$\{e\} \triangleleft H \cap K \triangleleft K \triangleleft HK \triangleleft G \tag{52}$$

Every group has a Jordan-Holder series. In genera, a group G is not determined by its Jordan-Holder series. However, if G is simple, then its Jordan-Holder series is $\{e\} \triangleleft G$.

> **Definition–Solvable**: If the composition factor G_{i+1}/G_i of G are all **abelian**, we say G is **solvable**.

If G acts on a set X, then each $g \in G$ permutes the element of X. So there is a map $G \to S_X$ (the symmetric group of X). It is easy to show that this map is a homomorphism. So, we will allow ourselves to go between group actions and Homomorphisms into S_X.

Suppose $H \leq G$ and let $X = G/H$ be the coset space. So, G acts on X by left multiplication $g(xH) \mapsto gxH$. If $n = [G : H] = |X|$, the action amounts to a homomorphism $\varphi : G \to S_n$.

Our first observation is that G acts **transitively**. For any $x, y \in X$, $\exists g \in G$ s.t. $gx = y$. i.e. the orbit of any $x \in X$ is X.

What is $\ker \varphi$? We know that if $h \in \ker \varphi$, that $hxH = xH$. Then consider $h', h'' \in H$ then

$$hxh' = xh'' \tag{53}$$

$$hx = xh''h'^{-1} \tag{54}$$

$$h = xh''h'^{-1}x^{-1} \tag{55}$$

$$\ker \varphi = \bigcap_{x \in G} xHx^{-1} \tag{56}$$

If $H = \{e\}$, then $G/H = G$, so $\ker \varphi = \{e\}$. then φ is injective. By the first isomorphism theorem, $G \cong \operatorname{im} \varphi = S_n$.

> **Theorem–Cayley**: Any group G with $|G| = n$ is isomorphic to a subgroup of S_n.
>
> *Proof.* We already proved it! □

Another example is to let G act on itself by conjugation. In this case, φ with $g \cdot x = gxg^{-1} = C_g(x)$. This is not a transitive action unless G is trivial. The orbits of conjugation are the **conjugacy classes** of G. They are disjoint (because conjugacy is an equivalence relation).

Note that $geg^{-1} = e, \forall g$. If $z \in Z(G)$, then $gzt^{-1} = zgg^{-1} = z \, \forall g$, then the conjugacy classes contain a single element.

If G is abelian, $Z(G) = G$ and every element is its own conjugacy class.

Because conjugacy is an equivalence relation, G is a disjoint union of all conjugacy classes.

If $Z(G) = \{e, z_1, \ldots, z_k\}$ and $g_1, \ldots, g_m$ are representatives from the non-central conjugacy classes. Let's write $C(g_i) = \{gg_ig^{-1} | g \in G\}$. So,

$$G = Z(G) \sqcup \left(\bigsqcup C(g_i) \right) \tag{57}$$

so

$$|G| = |Z(G)| + \sum_i |C(g_i)| \tag{58}$$

This is called the **Class Equation**.

Theorem–Orbit-Stabilizer: If G acts on X, for each $x \in X$, write $G \cdot x$ for its orbit. Then,

$$|G \cdot x| = [G : G_x] = [G : \mathrm{Stab}(x)] \tag{59}$$

The point is that two things in the same coset of G_x has the same effect on x.

Under conjugation,

$$\mathrm{Stab}(x) = G_x = \{g \in G | gxg^{-1} = x\} = Z(x), \tag{60}$$

the centralizer of x. So the class equation can be rewritten as

$$|G| = |Z(G)| + \sum_i [G : Z(g_i)] \tag{61}$$

Definition–p-group: Suppose p is prime, G is a **p-group** if $|G| = p^k$ for some $k \geq 1$.

Theorem–: If G is a non-trivial p-group, then it has a non-trivial center.

Proof. Suppose $|G| = 1$. Then

$$|G| = |Z(G)| + \sum_i [G : Z(g_i)] \tag{62}$$

Claim $Z(g_i) < G$, otherwise $g_i \in Z(G)$. By Lagrange's theorem $|Z(g_i)| \Big| |G| = p^k$. So $|Z(g_i)| = p^l$ for some $l < k$. Then,

$$p^k = |G| = |Z| + \sum_i [G : Z(g_i)] \tag{63}$$

$$\tag{64}$$

Since $|Z| = 1$, the RHS is not divisible by p so this is a contradiction. □

Corollary: Suppose p is prime. If $|G| = p^2$, then G is abelian.

Proof. We know $Z(G)$ is a non-trivial subgroup so $1 \neq |Z(G)| \Big| p^2$. So $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$, then G is abelian by definition. If $|Z(G)| = p$, then $|G/Z(G)| = p$ hence $G/Z(G) \cong C_p$. So $x \notin Z(G)$, then $G/Z(G) = \{\bar{e}, \bar{x}, \bar{x}^2, \dots \bar{x}^{p-1}\}$ where $\bar{x} =: xZ(G)$. Also, $\bar{x}^p = \bar{e} \in G/Z(G)$. Note that $\mathrm{ord}(x)$ is either p or p^2.

- If $|\langle x \rangle| = p^2$ so $\langle x \rangle = G$ and G is cyclic hence abelian.
- If $\mathrm{ord}(p)$, then $G = \bigcup_{k=0}^{p-1} x^k Z(G)$. Recall $|Z(G)| = p$, so $Z(G)$ is cyclic. Then,

$$Z(G) = \{e, z, z^2, \dots, z^{p-1}\} \tag{65}$$

so

$$G = \{x^i z^j | 0 \leq i, j < p\} \tag{66}$$

These elements commute. $x^i z^j x^m z^n = x^i x^m z^j z^n = x^{i+m} z^{j+n}$

□

Note we need to be careful with the steps in this proof. Just because $\bar{x}^p = \bar{e}$ doesn't mean there is a representative $x \in \bar{x}$ that is order p.

- Now we consider the rotations of a tetrahedron. A easy way to think about this is to identify a "top" vertex, which is well defined (4 possibilities). Then, we fix the top and we have 3 rotations (like of the triangle). So, there are 12 rotations.
- Apart from e, there are two non-trivial rotations that fix any particular vertex. This only accounts for 8 rotations, and e, so we are missing 3 rotations.
- The other rotations does not fix any vertices and are like $(1\,2)(3\,4)$. Then, $2, 3, 4$ goes with 1 so we have 3 rotations. This accounts for all 12.
- In summary, we have e, and 8 rotations in the form $(a\,b\,c)$ and 3 rotations in the form $(a\,b)(c\,d)$. This is A_4.
- The rigid motions are S_4.

Proposition: A_5 is simple. $A_5 \triangleleft S_5$ with index 2, so $|A_5| = 60$.

Proof. We will enumerate the conjugacy classes of S_5

- $(a\,b\,c\,d\,e) \in A_5$
- $(a\,b\,c\,d) \notin A_5$
- $(a\,b\,c) \in A_5$
- $(a\,b\,c)(d\,e) \notin A_5$
- $(a\,b)(c\,d) \in A_5$
- $(a\,b) \notin A_5$
- $e \in A_5$

There are 24 elements in the conjugacy class of $(a\,b\,c\,d\,e)$. However, 24 does not divide 60 so it is not a conjugacy class of A_5.

Consider the centralizer $Z_{A_5}(a\,b\,c\,d\,e) \geq \langle(a\,b\,c\,d\,e)\rangle$ which has order 5. But $Z_{A_5}(a\,b\,c\,d\,e) \leq Z_{S_5}(a\,b\,c\,d\,e)$ so $Z_{A_5}(a\,b\,c\,d\,e) = \langle(a\,b\,c\,d\,e)\rangle$
So there are two A_5 conjugate classes of 5-cycles, each with 12 elements.
There are 20 3-cycles in S_5. Are they all conjugate in A_5? If $(a\,b\,c)$ is conjugate to $(x\,y\,z)$ by $\sigma \in S_5$, then it is also conjugate by $\sigma(d\,e)$ If $\sigma \notin A_5$ then $\sigma(d\,e) \in A_5$ so there is one conjugate class of 20 3-cycles.
There are 15 double transpositions.
If we have a normal subgroup, it is a union of the conjugacy classes, so if A_5 has a normal subgroup it must be a combination of $1+15, 20, 12, 12$ but there is no combination (apart from 1) that divides 60. Hence, A_5 is simple. □

2 Sylow Theorems

Theorem–: Suppose $|G| = p^\alpha n$ where $p \not| n$. Then, a subgroup $P \leq G$ is a Sylow p-subgroup if $|P| = p^\alpha$. We'll write $n_p(G)$ for the number of Sylow p-subgroups of G.

1. Sylow p-subgroups exist.
2. Suppose P is a Sylow p-subgroup of G and $Q \leq G$ s.t. $|Q| = p^r$ for some $r > 0$. Then, $\exists\, g \in G$ s.t. $gQg^{-1} \subseteq P$. In particular, all Sylow p-subgroups of G are conjugate.
3. $n_p(G) \equiv 1 \mod p$ and $n_p(G) = [G : \mathrm{Norm}_G(P)]$ for any Sylow p-subgroup. Hence $n_p(G)||G|$. It actually also divides $n = |G|/|P|$.

Before proving the theorem we will consider the following example: Let $G = S_3$. The Sylow 2 subgroups are $\{e, (1\,2)\}, \{e, (1\,3)\}, \{e, (2\,3)\}$ we know $n_2(S_3) = 3 \equiv 1 \mod 2$. The only Sylow 3 subgroup is A_3, so $n_3(S_3) = 1$.

Lemma 1: If G is abelian and $p\Big||G|$, then G contains an element of order p.

Proof. If $|G| = p$ then G is cyclic and every non-trivial element has order p.
If $|G| > p$, and $x \in G$ with order $p^r m$ where $p \not| m$. If $r \neq 0$,then $x^{p^{r-1}m}$ has order p.
This reduces us to the case where $p \nmid \mathrm{ord}(x), \forall x \in G$. We will use induction.

- Assume the result is true for all groups smaller than G.
- If $p \nmid \mathrm{ord}(x) = |\langle x\rangle| < |G|$. As G is abelian, then $N =: \langle x\rangle \triangleleft G$.
- By induction G/N contains an element of order p.
- i.e. $\exists y = y_0 N \in G/N$ s.t. $y^p = e = N$. so $y_0^p \in N$
- We claim that $\langle y_0^p\rangle < \langle y_0\rangle$ since otherwise $y_0 \in N$ which has order 1.
- This means $p \mid |y_0|$ otherwise $\langle y_0^p\rangle = \langle y_0\rangle$. This is a contradiction.
- This means a suitable power of y_0 must have order p.

□

Lemma 2: If $P \in \mathrm{Syl}_p(G)$ and Q is a non-trivial p-subgroup of G. Then, $Q \cap \mathrm{Norm}_G(P) = Q \cap P$.

Proof. Let $H = Q \cap \mathrm{Norm}_G(P) \geq Q \cap P$. We need to show that $H \leq Q \cap P$. But $H \leq Q$ so we only need to show that $H \leq P$.

$H \leq N_G(P) \implies HP$ is a subgroup. The result will follow if we can argue that HP is a p-group. We know that

$$|HP| = \frac{|H||P|}{|H \cap P|} \tag{67}$$

Since $|H|, |P|, |H \cap P|$ are all powers of P. So $HP \geq P$ but $|HP|$ can't be bigger than $|P|$. $\square$