A Little Group Theory

- A Group is a set $G$ equipped with a binary operation $G \times G$: $(a,b) \rightarrow ab$ such that the following properties hold:
  1. $a(bc) = a(bc)$. (Associative Law)
  2. There is an $e \in G$ such that $ea = ae = a$ for all $a \in G$. (Existence of identity)
  3. For every $a \in G$ there is a $b \in G$ such that $ab = TBA = e$. (Existence of inverses)

- There is only one identity element:
  Suppose $ea = ae = a$ and $e'a = ae' = a$ for all $a \in G$. Then $e = ee' = e'$.

- The element $b$ in (3) is unique: Suppose
  
  \[
  ab = ba = e \\
  ab' = b'a = e
  \]

  Then
  
  \[
  b'ab = (b'a)b = eb = b \\
  b'ab = b'(ab) = b'e = b'
  \]

  so $b' = b$. This unique element is denoted $b^{-1}$.

- A subset $H \subseteq G$ is a subgroup of $G$ if it is a group under the binary operation of $G$, i.e.,
  1. $e \in H$
  2. $a,b \in H \implies ab \in H$.
  3. $a \in H \implies a^{-1} \in H$

- If $H_1$ and $H_2$ are subgroups of $G$, so is $H_1 \cap H_2$.

- We write $H \leq G$ to indicate that $H$ is a subgroup of $G$. 
• $G \subseteq G$ and $\{e\} \subseteq G$ are subgroups.

• If $S \subseteq G$, the set $\{H \mid H \leq G, H \supseteq S\}$ is non-empty because it contains $G$. Set

$$\langle S \rangle = \bigcap \{H \mid H \leq G, H \supseteq S\}$$

Then $\langle S \rangle$ is a subgroup of $G$. It is the smallest subgroup of $G$ that contains $S$, i.e., $S \subseteq \langle G \rangle$ and if $H \leq G$ and $H \supseteq S$, then $\langle S \rangle \subseteq H$. The subgroup $\langle S \rangle$ is called the subgroup of $G$ generated by $S$. If $\langle S \rangle = G$, we say that $S$ generates $G$.

• If $a \in G$ then $\langle a \rangle$ is a subgroup. It’s clear that

$$\langle a \rangle = \{a^n \mid n = 0, \pm 1, \pm 2, \ldots\}.$$  

(By definition $a^0 = e$ and $a^{-k}$ for $k > 0$ means $(a^{-1})^k$.)

There are two possibilities: Either all of the powers $a^n$ are distinct, or two of them are the same. Suppose $a^m = a^n$ and choose the notation so that $m > n$. Then $m = n + k$ where $k > 0$. Then $a^n = a^m = a^{n+k} = a^na^k$, so $a^n = a^na^k$.

Multiplying this equation on the left by $a^{-n}$ gives $a^k = e$. Thus, some power of $a$ is the identity. Let $p$ be the smallest positive integer so that $a^p = e$. We call $p$ the order of $a$, denoted by $o(a)$. In this case, $\langle a \rangle$ is finite, namely

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{p-1}\}.$$  

• A group $G$ is cyclic if $G = \langle a \rangle$ for some $a \in G$. We say $a$ is a generator of $G$. 
Equivalence Relations

- Let $X$ be a nonempty set. A relation $\sim$ on $X$ is an equivalence relation if it satisfies the following properties.
  1. $x \sim x$ for all $x \in X$. (Reflexive)
  2. $x \sim y \Rightarrow y \sim x$. (Symmetric)
  3. $x \sim y, y \sim z \Rightarrow x \sim z$. (Transitive)

- If $x \in X$ we define $[x]$, the equivalence class of $x$ by
  \[[x] = \{ y \mid y \sim x \}.
  
  Since $x \sim x$, $x \in [x]$.

- **Proposition**
  1. $[x] = [y]$ if and only if $x \sim y$.
  2. Either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.
  3. The equivalence classes partition $X$.

- **Proof:** If $[x] = [y]$ then $x \in [x] = [y]$, so $x \in [y]$. By the definition of $[y]$, $x \sim y$.

Suppose $x \sim y$. Let $z$ be an element of $[x]$. Then $z \sim x$; combining this with $x \sim y$ we get $z \sim y$. Thus, $z \in [y]$. This shows $[x] \subseteq [y]$. Similarly, $[y] \subseteq [x]$, so $[x] = [y]$.

Suppose that $[x] \cap [y] \neq \emptyset$. Then there is some $z \in [x] \cap [y]$. But this means that $z \sim x$ and $z \sim y$. But then $x \sim y$, so $[x] = [y]$.

Each $x \in X$ is in some equivalence class (namely $[x]$) and the equivalence classes are disjoint, so we have $X$ described as a union of a collection of disjoint subsets. That’s what it means to partition $X$. 

Cosets

- Let $H$ be a subgroup of $G$. Define a relation $\sim$ on $G$ by $a \sim b$ if there is some $h \in H$ so that $ah = b$.

  We claim this is an equivalence relation. If $a \in G$ then $ae = a$ and $e \in H$ so $a \sim a$.

  Suppose that $a \sim b$. Then there is some $h \in H$ so that $ah = b$. Multiplying this equation on the right by $h^{-1}$ gives $bh^{-1} = ahh^{-1} = ae = a$. Since $h^{-1} \in H$, $b \sim a$.

  Suppose that $a \sim b$ and $b \sim c$. Then there are elements $h_1, h_2 \in H$ such that $ah_1 = b$ and $bh_2 = c$. Multiply the equation $ah_1 = b$ on the right by $h_2$.

  This gives $ah_1h_2 = bh_2 = c$. Thus, $ah_1h_2 = c$. Since $h_1h_2 \in H$, we get $a \sim c$.

- What is $[a]$?

  $$[a] = \{ ah \mid h \in H \} = aH.$$  

  This is called the left coset of $a$ modulo $H$. Thus, $G$ is the disjoint union of the left cosets. The collection of left cosets modulo $H$ is called $G/H$.

- We can similarly define a relation $\sim$ by $a \sim b$ if there is an element $h$ of $H$ so that $ha = b$. The equivalence class of $a$ with respect to this relation is $[a] = Ha$, which is called the right coset of $a$ modulo $H$. The collection of right cosets is called $H \setminus G$.

- A group is called finite if it has only finitely many elements.

- $|X|$ denotes the number of elements in $X$. If $G$ is a group, $|G|$ is often called the order of $G$. 

- Let $G$ be a group and $H$ a finite subgroup. We can define a 1-1 and onto map $f: H \rightarrow aH$ by $f(h) = ah$.

Thus, $H$ and $aH$ are in 1-1 correspondence, so $|aH| = |H|$, i.e., every left coset has the same number of elements as $H$. Similarly, every right coset has the same number of elements as $H$.

- **Lagrange's Theorem** Let $G$ be a finite group and let $H$ be a subgroup. Then

$$|G/H| |H| = |G|.$$ 

In particular, $|H|$ divides $|G|$ and

$$|G/H| = \frac{|G|}{|H|}.$$ 

Similarly,

$$|H \setminus G| = \frac{|G|}{|H|}.$$ 

- It’s possible that $G/H$ is finite even if $G$ and $H$ are infinite. The number of elements in $G/H$ is often denoted $[G : H]$, called the index of $H$ in $G$.

- **An Example**

Let $Z = \{0, \pm 1, \pm 2, \pm 3 \ldots \}$ be the set of integers. This is a group under the operation of addition. In this case the group is commutative.

Let $n$ be a positive integer and write

$$nZ = \{ nk \mid k \in Z \} = \{ 0, \pm n, \pm 2n, \pm 3n, \ldots \},$$

i.e., $nZ$ is the set of all multiples of $n$. It should be easy to see that $nZ$ is a subgroup of $Z$.

Since $Z$ is commutative, there’s really no difference between right and left cosets. The relation for the cosets is $a \sim b$ if there is an $h \in nZ$ so that $a + h = b$. In other words $b - a = nk$ for
some \( k \in \mathbb{Z} \). Another way to say it then is that \( a \sim b \) if \( b - a \) is divisible by \( n \).

The equivalence class of \( a \) is

\[
[a] = a + n\mathbb{Z} = \{ a + nk \mid k \in \mathbb{Z} \}.
\]

The set of equivalence classes is denoted by \( \mathbb{Z}/n\mathbb{Z} \) (read “ \( \mathbb{Z} \) mod \( n \) \( \mathbb{Z} \)” ) or \( \mathbb{Z}_n \) (read “ \( \mathbb{Z} \) mod \( n \)” ). The distance elements of \( \mathbb{Z}_n \) can be listed as

\[
[0], [1], [2], \ldots, [n - 1],
\]

for \( k \in \mathbb{Z} \), \([k]\) must be one of the elements of the above list. (How do you determine which one?)

- We show that \( \mathbb{Z}_n \) can be made into a group by defining the group operation by

\[
[r] + [s] = [r + s], \quad r, s \in \mathbb{Z}.
\]

The main point is to show that this definition makes sense! The problem is this: If \([r'] = [r]\) and \([s'] = [s]\), is it true that \([r' + s'] = [r + s] \)? If not, we would get a different answer for the sum of two cosets depending on which elements of the cosets we choose to represent them.

Fortunately, the required property holds. If \([r'] = [r]\) then \( r' \sim r \), equivalently, \( r \sim r' \), so \( r' = r + nk \) for some \( k \in \mathbb{Z} \).

Similarly, if \([s'] = [s]\), then \( s' = s + n\ell \) for some \( \ell \in \mathbb{Z} \). But then

\[
r' + s' = r + nk + s + n\ell = (r + s) + n(k + \ell).
\]

Since \( k + \ell \in \mathbb{Z} \), this shows that \( (r' + s') \sim (r + s) \) so \([r' + s'] = [r + s]\).

Now that the operation makes sense, the group properties follow easily form the group properties of \( \mathbb{Z} \).
For example, for $a, b, c \in \mathbb{Z}$,

$$[a + ([b] + [c])] = [a + [b + c]]$$
$$= [a + (b + c)]$$
$$= [(a + b) + c]$$
$$= [a + b] + [c]$$
$$= ([a] + [b]) + [c],$$

where we have used the associative law for $\mathbb{Z}$. Thus $\mathbb{Z}_n$ is associative.

We have $[0] + [a] = [0 + a] = [a]$, so $[0]$ is the identity element.

We then have $[a] + [-a] = [a + (-a)] = [0]$, so $[-a]$ is the inverse of $[a]$.

**Normal Subgroups**

- In the case of a noncommutative group, an additional condition is required to make $G/H$ a group.

- Let $G$ be a group and $H$ an subgroup. If $g \in G$, we define

$$g^{-1}Hg = \{ g^{-1}hg \mid h \in H \}.$$ 

- $H$ is called a normal subgroup of $G$ if

$$g^{-1}Hg \subseteq H, \quad \text{for all } g \in G.$$ 

We write $H \trianglelefteq G$ to indicate $H$ is a normal subgroup of $G$. 
• If $H \trianglelefteq G$, then $gH = Hg$ for all $g \in G$, i.e., there's no difference between the left coset and the right coset.

**Pf:** Take an element $gh$ of $gH$. Since $H$ is normal, $ghg^{-1} \in H$, so $ghg^{-1} = h'$ for some $h' \in H$. Multiply the equation $ghg^{-1} = h'$ on the right by $g$. This gives $gh = h'g$, thus $gh = h'g \in Hg$. This shows that $gH \subseteq Hg$.

Take an element $hg$ of $gH$. Since $H$ is normal $g^{-1}hg = h' \in H$. Thus, $hg = gh' \in gH$. This shows $Hg \subseteq gH$.

Thus, $gH = Hg$.

• If $H$ is a normal subgroup of $G$, the collection of cosets $G/H$ can be made into a group by defining $[a][b] = [ab]$.

As before, the main point is to show that this operation is well defined, i.e., if $[a'] = [a]$ and $[b'] = [b]$ then $[a'b'] = [ab]$.

Suppose $[a'] = [a]$ then $a' \in [a] = aH$, so $a' = ah_1$ for some $h_1 \in H$. Similarly, if $[b'] = [b]$ then $b' = bh_2$ for some $h_2 \in H$.

Then $a'b' = ah_1bh_2$. Since $H$ is normal, $b^{-1}h_1b \in H$, say $h_3 = b^{-1}hb$, so $bh_3 = h_1b$, thus

$$a'b' = ah_1bh_2$$

$$= a(h_1b)h_2$$

$$= a(bh_3)h_2$$

$$= abh_3h_2$$

$$= (ab)(h_3h_2)$$

so $[a'b'] = [ab]$. The group properties follow easily from the group properties of $G$. 


Group Homomorphisms

- Let $G$ and $H$ be groups. A mapping $\varphi: G \to H$ is a group homomorphism or a group map if preserves the group operations, i.e.,
  1. $\varphi(e) = e$.
  2. $\varphi(ab) = \varphi(a)\varphi(b)$.

- It follows that $\varphi(a^{-1}) = \varphi(a)^{-1}$. To see this, note that
  $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e) = e$, so
  $\varphi(a^{-1})\varphi(a) = e$. Multiplying this equation on the right by $\varphi(a)^{-1}$ yields
  $\varphi(a^{-1}) = \varphi(a)^{-1}$.

- Exercise: Show that $\varphi(G) = \{ \varphi(g) \mid g \in G \} \subseteq H$ is a subgroup of $H$.

- Exercise: Suppose that $\varphi: G \to H$ is a group map that is 1-1 and onto, so the inverse mapping $\varphi^{-1}: H \to G$ exists. How $\varphi^{-1}$ is also a group map. We say that $\varphi$ is an isomorphism from $G$ to $H$.

- If $\varphi: G \to H$ is a group map, we define the kernel of $\varphi$, denoted $\ker(\varphi)$, by
  $\ker(\varphi) = \{ g \in G \mid \varphi(g) = e \}$.

- $\ker(\varphi)$ is a normal subgroup of $G$.
  First, we show it’s a subgroup.
  Since $\varphi(e) = e$, $e \in \ker \varphi$.
  If $k_1, k_2 \in \ker \varphi$, then
  $\varphi(k_1k_2) = \varphi(k_1)\varphi(k_2) = ee = e$, so $k_1k_2 \in \ker \varphi$.
  Finally, if $k \in \ker \varphi$ then
  $\varphi(k^{-1}) = \varphi(k)^{-1} = e^{-1} = e$, so $k^{-1} \in \ker(\varphi)$. Thus, $\ker(\varphi)$ is a subgroup.
To show that $\ker(\varphi)$ is normal, let $g \in G$ and $k \in \ker(\varphi)$. Then
\[
\varphi(g^{-1}kg) = \varphi(g^{-1})\varphi(k)\varphi(g)
= \varphi(g^{-1})\varphi(g)
= \varphi(g^{-1})\varphi(g)
= \varphi(g)^{-1}\varphi(g)
= e.
\]
Thus, $\varphi(g^{-1}kg) = e$, so $g^{-1}kg \in \ker(\varphi)$. This shows that $\ker(\varphi)$ is normal.

**Theorem** Let $\varphi: G \to H$ be a group map which is onto and let $K = \ker(\varphi)$. Then there is a well defined mapping $\bar{\varphi}: G/K \to H$ defined by $\bar{\varphi}([g]) = \varphi(g)$. The mapping $\bar{\varphi}$ is a group isomorphism from $G/K$ to $H$.

**Pf:** To show that the formula for $\bar{\varphi}$ makes sense we have to show that if $[g'] = [g]$ then $\varphi(g') = \varphi(g)$. But if $[g'] = [g]$ then $g' = gk$ for some $k \in K$. But then
\[
\varphi(g') = \varphi(gk) = \varphi(g)\varphi(k) = \varphi(g)e = \varphi(g).
\]
Thus, $\bar{\varphi}$ is well defined.

**Exercise:** Complete the proof.
Discrete Groups of Isometries

- The collection of isometries of the plane is a group denoted \( E(2) \), and called the Euclidean Group.

- Let \( G \) be a subgroup of \( E(2) \). Let \( p \in \mathbb{R}^2 \) be a point. The orbit of \( p \), \( Gp \) is defined by
  \[
  Gp = \{ gp \mid g \in G \}.
  \]

- \( G \) is said to be discrete if the points on any orbit do not get arbitrarily close together. In other words, if \( p \) is a point, there is some number \( \delta > 0 \) so that \( d(x, y) \geq \delta \) for any two distinct points \( x \) and \( y \) of \( Gp \). (\( \delta \) can depend on the choice of \( p \)).

- Suppose that \( G \) is a discrete group of isometries and that \( R \) is a rotation in \( G \). Then \( R \) has finite order, i.e., \( R^n = \text{id} \) for some \( n \).

Suppose not. Then all the rotations \( R^n, n \in \mathbb{Z} \) are distinct. Pick at point \( p \) which is not the center \( c \) of the rotation \( R \). Then the points \( R^n p \) are all distinct. These points are in \( Gp \). All these points lie on the circle with center at \( c \) and radius \( d(p, c) \). Since we have infinitely many points on a circle, we can find points that are arbitrarily close together. This contradicts the fact that \( G \) is discrete.
Rosette Groups

- A discrete group $G$ of isometries is called a Rosette Group if there is a point that is fixed by all of the isometries in $G$. These are the symmetry groups of rosette patterns.

- **Theorem** A rosette group $G$ is either a finite cyclic group or is isomorphic to a dihedral group.

- **Pf:** We may as well assume the fixed point is origin, so $G \leq O(2)$

  If $G$ is $\{I\}$ it is cyclic.

Suppose that $G$ contains some rotations. We can choose the least positive number $\theta$ so that $R(\theta) \in G$ (Why?). As we saw, $R(\theta)$ has finite order, say $R(\theta)^n = I$. Thus, the cyclic group $C = \{I, R(\theta), R(\theta)^2, \ldots, R(\theta)^{n-1}\}$ is a subgroup of $G$.

We claim that $C$ contains all the rotations in $G$. Suppose not. Then there is some $\varphi > 0$, so that $R(\varphi) \in G$, but $R(\varphi) \notin C$. By our choice of $\theta$, $\varphi > \theta$.

Thus, we can find an integer $k \geq 0$ so that $\varphi = k\theta + \psi$, where $0 < \psi < \theta$. We then have $R(\varphi) = R(k\theta + \psi) = R(\theta)^k R(\psi)$.

Since $R(\varphi)$ and $R(\theta)^k$ are in $G$, $R(\psi) = R(\theta)^{-k} R(\varphi)$ is in $G$. But this contradicts our choice of theta!

Thus, we have a cyclic group $C \subseteq G$ that contains the all the rotations in $G$.

If $C = G$ we are done. If $G \neq C$, the extra elements must be reflections.
If $C = \{ I \}$ and we have one reflection $S$ so that $G = \{ I, S \}$, then $G$ is cyclic.

Suppose that $C \neq I$ and $C \neq G$. Then there is at least one reflection $S$ in $G$.

Setting $R = R(\theta)$, then $G$ contains the elements $I, R, R^2, \ldots, R^{n-1}, S, RS, R^2S, \ldots R^{n-1}S$. The elements $S, RS, \ldots, R^{n-1}S$ are reflections. We claim these are all the reflections in $G$. Suppose that $T$ is a reflection in $G$. Then $TS$ is a rotation in $G$, so $TS = R^k$, multiplying this by $S$ on the right gives $T = R^kS$, so $T$ is already in the list.

Now, $SR$ is a reflection, so it must be in the list. Which one is it? Since $SR$ is a reflection, $SRSR = I$. Multiply on the right by $R^{-1}$ to get $SRS = R^{-1}$. Now multiply on the left by $S$ ($S^2 = I$), to get $SR = R^{-1}S$. Since $R^{-1} = R^{n-1}$, we have $SR = R^{n-1}S$. It’s almost obvious that $G$ is isomorphic to $D_n$.

- What, if anything, is left to prove?