Math 546
Set 11
- Groups of Small Order
- Lagrange's Theorem
Groups of small order

**Defn:** The order of a group \( G \) is the number of elts., \( |G| = o(G) \)

By defn. \( G \neq \emptyset \)

\( o(G) = 1 \) : trivial group

\[ G = \{ e \} \]

\[ e \quad e \]

\( o(G) = 2 \)

\( G = \{ e, a \} \)

\[ e \quad a \]

\[ e \quad e \quad a \]

\[ e \quad a \quad a \]

This is the group of order 2

forced in group by "Latin property" that every elt. appears once in every row & col.

[a "Latin Square"]

Every group opens a table, but is a Latin square, not vice-versa.
\( o(G) = 3 \)  \( G = \{ e, a, b \} \)

The table is forced, and this table does work (check axioms are satisfied).

This is the group of order 3.

\( o(G) = 4 \)

\( G = \{ e, a, b, c \} \)

Split into cases according to where \( e \) is in 2nd row:

**Case 1:** \( a \cdot a = e \)

**Case 1.1:** \( b \cdot b = e \)

Klein 4-group \( \mathbb{Z}_2 \times \mathbb{Z}_2 \)
This is called the Klein 4-group or $V_4$.

Case 1.2 $b \cdot b = a$

<table>
<thead>
<tr>
<th>e</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>e</td>
<td>e</td>
<td>a</td>
<td>b</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>e</td>
<td>c</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>e</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>e</td>
</tr>
</tbody>
</table>

Group?

- $c^2 = b^2 = a$
- $c^2 = b$
- $b^2 = c$
- $c^4 = b^4 = a^2 = e$

The group is generated by $c$ or by $b$.

Cyclic group of order 4

$\mathbb{Z}_4 = \langle b^4, + \rangle$

$e \rightarrow 0$  $a \rightarrow 2$  $b, c \rightarrow 1, 3$

abelian

Case 2 $a \cdot b = e$

Case 3 $a \cdot c = e$

These give the same groups, up to naming the elements.
Case 2
\[ e a b c \]
\[ e a b c \]
\[ e a b c \]
\[ e a b c \]
\[ e a b c \]

Recall if \( xy = e \) \( \Rightarrow y = x^{-1} \) \( \Rightarrow y x = e \)

\( \cdots \) e's appear symmetrically

\( \therefore \) this is all forced!

Notice \( c^2 = e \)

\[ e a b c \]
\[ e a b c \]
\[ e a b c \]
\[ e a b c \]
\[ e a b c \]

case \( e c b a \) seems to work.

Case 3
\[ a \cdot c = e \]

Same as case 2 except we switched \( b \) \( \& \) \( c \).

Again, must get \( \mathbb{Z}_4 \) (again).
We see that, up to naming the elts., there are exactly 2 groups of order 4 (concernsomorphic):
1. Klein group $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
2. $\mathbb{Z}_4$

Note that all groups of order $\leq 4$ are abelian; so is $\mathbb{Z}_5$, the only group of order 5 by similar arguments (more lengthy).

Consider a nonabelian group:
**Prop.** Every nonabelian group has \( \geq 6 \) elts.

**Pf.** Let \( G \) be nonabelian.

\[ \Rightarrow \exists a, b \in G : ab \neq ba \]

Then \( e, a, b, ab, ba \) are all distinct!

**e.g.** if \( a = e \Rightarrow ab = eb = b \)
\[ ba = be = b \neq b \]
if \( ab = e \Rightarrow b = a^{-1} \)
\[ ba = e = e = ab \neq b \]
\[ e = a, ab, b, ba \text{ } \text{ similarly} \]
if \( a = ab \Rightarrow b = e \neq \]

Similarly all pairs are distinct. Could these 5 elts. be the entire group?

Consider \( aba \)
if \( aba = e \Rightarrow ba = a^{-1} \neq \]
\[ ab = a \neq \]
\[ ab = e \neq \]
\[ aba = b \neq \text{ stuck?} \]
where is \( a^2 \) ?

if \( a^2 = a \) \( \Rightarrow \) \( a = e \) \( \neq \)
\( a^2 = ab \) \( \Rightarrow \) \( a = b \) \( \neq \)
\( a^2 = ba \) \( \Rightarrow \) \( a = b \) \( \neq \)
\( a^2 = e \) \( \Rightarrow \) \( a = a^{-1} \) ?

\( a^2 = b \)
\( \Rightarrow ab = a \cdot a^2 = a^3 \)
\( ba = a^2 \cdot a = a^3 \) \( \neq \)

It must be \( a^2 = e \)
\( b^2 = e \)

Similarly, \( (ab)(ba) \neq (ba)(ab) \)

\( (bc)(ac) \neq (ca)(cb) \)

\( ab = a \cdot b \)
\( a^2 = a \cdot b^2 \)
\( a = a^{-1} \)
\( e = e \)

so \( (ab)^{-1} = ba \) ?
Considering $a^2$, we saw that $a^2 = e$.

Therefore,

- $a \cdot b = ab$
- $a \cdot ab = b$
- $a \cdot ba = ba$

But $a = e$.
Lagrange's Thm.
If $G$ is a finite group, and $H \leq G$, then $|H|$ divides $|G|$. 

Cor. If $G$ is finite, then $\forall g \in G$, $o(g)$ divides $|G|$. 

Proof of cor.

\[
o(g) = \min \left\{ n > 0 : g^n = e \text{ in } G \right\}
\]

\[
= \left\{ g, g^2, \ldots, g^n = e \right\}
\]

\[
= \left\langle g \right\rangle
\]

which divides $|G|$ by Lagrange's Thm. 

$\square$
Ex. Let $G$ be a group of order 5.

By Lagrange’s Theorem, the possible orders of the elements are $1$ or $5$.

Only the identity has order $1$.

$\exists g \in G \quad o(g) = 5$

[In fact take any of the other 4 elts.]

So $G = \langle g \rangle$

$|\langle g \rangle| = 5 = 1|G|$

$G$ is cyclic of order 5.

(Similarly do this if $|G| = p$, prime.)
Ex. If $G$ is a group of order 16, the possible orders of its subgroups are: $1, 2, 4, 8, 16$.

Ex. In $G = S_n$, $n \geq 2$ define $H = \{\sigma \in S_n : \sigma \text{ is even}\}$.

Then $H \leq G$, called the alternating group $A_n$.

Check:

1. **Nonempty:** $\exists \sigma \in H$.
2. **Closure:** If $\sigma, \tau \in H$, then the parity of $\sigma \tau$ is even if $\sigma$ and $\tau$ are both even, or both odd.
3. **Inverse:** If $\sigma \in H$, then $\sigma^{-1}$ has the same parity as $\sigma$. Thus, $\sigma^{-1} \in H$.
In fact $|A_n| = \frac{1}{2} |S_n| = \frac{1}{2} (n!)$ for all $n \geq 2$.

Idea:

We can set up a 1-1 correspondence from even permutations to odd permutations by $f(\sigma) = \sigma \cdot (12)$.

Even \rightarrow Even

Odd \rightarrow Odd

We can check 1-1 and onto.

So $\# \text{even} = \# \text{odd}$.

$\Rightarrow |A_n| = \frac{1}{2} |S_n|$.

Notice $|A_n| / |S_n|$.
Lagrange's Thm. 
If \( G \) is a finite group and \( H \leq G \), then \( |H| \) divides \( |G| \).

Pf. Steps:
1. Define \( \sim \) on \( G \) by 
   
   \[ a \sim b \iff a^{-1}b \in H. \]

   This is an equivalence relation.

2. Show 
   
   \[ [g] = gH = \{ gh : h \in H \} \]

   for \( g \in G \).

3. Note \( |gH| = |H| \) \( \forall g \in G \).

4. \( |G| = |H| \times \# \text{parts (equi. classes)} \)

   \( G \) left cosets of \( H \):
   
   \[
   G = H \sqcup g_1H \sqcup g_2H \sqcup g_3H \sqcup \ldots
   \]
Reflexive:

\[ a \sim a \iff a^{-1}a \in H \]

which holds as \( a^{-1}a = e \) (identity element in \( H \)).

Symmetric:

\[ a \sim b \Rightarrow a^{-1}b \in H \]

\[ \Rightarrow (a^{-1}b)^{-1} = b^{-1}a \in H \]

\[ \Rightarrow \ b \sim a. \quad H \text{ has inverse} \]

Transitive:

\[ a \sim b, b \sim c \Rightarrow a \sim c. \]

What are the equivalence classes?
2. \([g] = gH\)

\[f \in [g] \Rightarrow f \sim g\]

\[\Rightarrow f^{-1}g = h \in H\]

for some \(h\)

\[\Rightarrow g = fh\]

\[\Rightarrow gh^{-1} = f\]

\[\Rightarrow f \in gH\] since \(h^{-1} \in H\).

Thus, \([g] \leq gH\)

On the other hand, \(f \in gH\) \(\Rightarrow \exists h \in H: f = gh\)

\[\Rightarrow fh^{-1} = g\]

\[\Rightarrow h^{-1} = f^{-1}g \in H\]

since \(H\) has inverses

\[\Rightarrow f \sim g\]

\[\Rightarrow f \in [g]\]

\[\therefore [g] = gH.\]
We see that elts. \( g_1, g_2 \in G \) s.t. \( g_1 \sim g_2 \) have the same cosets.

\( g_1 \cdot H = g_2 \cdot H \).

Note \( e \cdot H = H \) itself is a left coset.

3. \( |g \cdot H| = |H| \) since the elts. \( g \cdot h \) are distinct as \( h \) ranges over \( H \):

\[ g \cdot h_1 = g \cdot h_2 \quad \Rightarrow \quad h_1 = h_2 \]

4. Immediate from 3 + the fact that the equiv. reln. \( \sim \) partitions \( G \) into equivalence classes. Thus, the Equivalence Relation
Arb. Intersections of subgpt. $H_e \leq G$

Union of Two subgroups

$H_1, H_2 \leq G$
$H_1 \neq H_2$
$H_2 \nsubseteq H_1$

$H_1 \cup H_2$

We have $\neq \emptyset$ a inverses,
but if $h_1 \in H_1 - H_2$
$h_2 \in H_2 - H_1$
then \( h_1 h_2 \notin H_1 \cup H_2 \)
so closure fails:

else say \( h_1 h_2 \in H_1 \)
call it \( g_1 \)
\[
\begin{align*}
h_1 h_2 &= g_1 \in H_1 \\
h_2 &= h_1^{-1} g_1 \in H_1
\end{align*}
\]

\( \Rightarrow \)

Similarly, if \( h_1 h_2 \in H_2 \)
call it \( g_2 \)
\[
\begin{align*}
h_1 h_2 &= g_2 \in H_2 \\
h_1 &= g_2 h_2^{-1} \in H_2
\end{align*}
\]

\( \Rightarrow \)

\( h_1, h_2 \notin H_1 \cup H_2. \)

Con. No group is the union of just two of its proper subgroups.

Almost:

\[
\mathbb{Z}/6 = \{0, 2, 4\} \cup \{0, 3\} \cup \{1, 3\}
\]
\[ V_4 = \{ a, b, c, e \} \]
\[ a^2 = b^2 = c^2 = e \]
\[ = \langle a \rangle \cup \langle b \rangle \cup \langle c \rangle \]

is a union of three subgroups.