A Group

- A group consists of a set $G$ and a binary operation $\ast$, satisfying the following.
  - **Closure.** For every $x, y \in G$, we have $x \ast y \in G$.
  - **Associativity.** For every $x, y, z \in G$, we have $(x \ast y) \ast z = x \ast (y \ast z)$.
  - **Identity.** The exists $e \in G$, such that for every $x \in G$, we have $e \ast x = x \ast e = x$.
  - **Inverse.** For every $x \in G$ there exists $x^{-1} \in G$ such that $x \ast x^{-1} = x^{-1} \ast x = e$. 

By Adam Sheffer
Reminder: Subgroups

- A **subgroup** of a group $G$ is a group with the same operation as $G$, and whose set of members is a subset of $G$.

[Diagram of subgroups]

Lagrange’s Theorem

- **Theorem.** If $G$ is a group of a finite order $n$ and $H$ is a subgroup of $G$ of order $m$, then $m | n$.
  - We will not prove the theorem.

- **Example.** The symmetry group of the square is of order 8.
  - The subgroup of rotations is of order 4.
  - The subgroup of the identity and rotation by $180^\circ$ is of order 2.
Reminder: Parity of a Permutation

- **Theorem.** Consider a permutation \( \alpha \in S_n \). Then
  - Either every decomposition of \( \alpha \) consists of an **even** number of transpositions,
  - or every decomposition of \( \alpha \) consists of an **odd** number of transpositions.

- \((1 \ 2 \ 3)(4 \ 5 \ 6)\):
  - \((1 \ 3)(1 \ 2)(4 \ 6)(4 \ 5)\).
  - \((1 \ 4)(1 \ 6)(1 \ 5)(3 \ 4)(2 \ 4)(1 \ 4)\).

Subgroup of Even Permutations

- Consider the group \( S_n \):
  - **Recall.** A product of two even permutations is even.
  - The subset of even permutations is a subgroup. It is called the **alternating group** \( A_n \).
  - **Recall.** Exactly half of the permutations of \( S_n \) are even. That is, **the order of** \( A_n \) **is half the order of** \( S_n \).
Application of Lagrange’s Theorem

**Problem.** Let $G$ be a finite group of order $n$ and let $g \in G$ be of order $m$. Prove that $m|n$ and $g^n = 1$.

**Proof.**

- Notice that $\{1, g, g^2, \ldots, g^{m-1}\}$ is a cyclic subgroup of order $m$.
- By **Lagrange’s theorem** $m|n$.
- Write $n = mk$ for some integer $k$. Then $g^n = g^{mk} = (g^m)^k = 1$. 

---

**Atlas of Finite Groups**

- (only in class)
Groups of a Prime Order

- **Claim.** Every group $G$ of a prime order $p$ is isomorphic to the cyclic group $C_p$.

- **Proof.**
  - By Lagrange’s theorem, $G$ has no subgroups.
  - Thus, by the previous slide, every element of $G \setminus \{1\}$ is of order $p$.
  - $G$ is cyclic since any element of $G \setminus \{1\}$ generates it.

Symmetries of a Tiling

- Given a repetitive tiling of the plane, its symmetries are the transformations of the plane that
  - Map the tiling to itself (ignoring colors).
  - Preserve distances.

- These are combinations of translations, rotations, and reflections.
Example: Square Tiling

- What symmetries does the square tiling have?
  - Translations in every direction.
  - Rotations around a vertex by $0^\circ, 90^\circ, 180^\circ, 270^\circ$.
  - Rotations around the center of a square by $0^\circ, 90^\circ, 180^\circ, 270^\circ$.
  - Reflections across vertical, horizontal and diagonal lines.
  - Rotations around the center of an edge by $180^\circ$.

Wallpaper Groups

- Given a tiling, its set of symmetries is a group called a wallpaper group (not accurate! More technical conditions).
  - **Closure.** Composing two symmetries results in a transformation that preserves distances and takes the lattice to itself.
  - **Associativity.** Holds.
  - **Identity.** The “no operation” element.
  - **Inverse.** Since symmetries are bijections from the plane to itself, inverses are well defined.
Wallpaper Groups

• There are exactly 17 different wallpaper groups.

• That is, the set of all repetitive tilings of the plane can be divided into 17 classes. Two tilings of the same class have the same “behavior”.

Equivalence Relations

• **Recall.** A relation $R$ on a set $X$ is an **equivalence relation** if it satisfies the following properties.
  ◦ **Reflexive.** For any $x \in X$, we have $xRx$.
  ◦ **Symmetric.** For any $x, y \in X$, we have $xRy$ if and only if $yRx$.
  ◦ **Transitive.** If $xRy$ and $yRz$ then $xRz$. 
Example: Equivalence Relations

- **Problem.** Consider the relation of congruence mod 31, defined over the set of integers \( \mathbb{Z} \). Is it an equivalence relation?
- **Solution.**
  - Reflexive. For any \( x \in \mathbb{Z} \), we have \( x \equiv x \mod 31 \).
  - Symmetric. For any \( x, y \in \mathbb{Z} \), we have \( x \equiv y \mod 31 \) iff \( y \equiv x \mod 31 \).
  - Transitive. If \( x \equiv y \mod 31 \) and \( y \equiv z \mod 31 \) then \( x \equiv z \mod 31 \).

Equivalence Via Permutation Groups

- Let \( G \) be a group of permutations of the set \( X \). We define a relation on \( X \):
  \( x \sim y \iff g(x) = y \) for some \( g \in G \).
- **Claim.** \( \sim \) is an equivalence relation.
  - Reflexive. The group \( G \) contains the identity permutation \( \text{id} \). For every \( x \in X \) we have \( \text{id}(x) = x \) and thus \( x \sim x \).
  - Symmetric. If \( x \sim y \) then \( g(x) = y \) for some \( g \in G \). This implies that \( g^{-1} \in G \) and \( x = g^{-1}(y) \). So \( y \sim x \).
Equivalence Via Permutation Groups

- Let $G$ be a group of permutations of the set $X$. We define a relation on $X$:
  
  $x \sim y \iff g(x) = y$ for some $g \in G$.

- **Claim.** $\sim$ is an equivalence relation.
  
  - **Transitive.** If $x \sim y$ and $y \sim z$ then $g(x) = y$ and $h(y) = z$ for $g, h \in G$. Then $hg \in G$ and $hg(x) = z$, which in turn implies $x \sim z$.

Orbits

- Given a permutation group $G$ of a set $X$, the equivalence relation $\sim$ partitions $X$ into *equivalence classes* or *orbits*.
  
  - For every $x \in X$ the orbit of $x$ is
    
    $Gx = \{ y \in X \mid x \sim y \}$

    $= \{ y \in X \mid g(x) = y \text{ for some } g \in G \}$. 

Example: Orbits

- Let $X = \{1, 2, 3, 4, 5\}$ and let $G = \{\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$.
- What are the equivalence classes that $G$ induces on $X$?
  - $G1 = G2 = \{1, 2\}$.
  - $G3 = G4 = \{3, 4\}$.
  - $G5 = \{5\}$.

Stabilizers

- Let $G$ be a permutation group of the set $X$.
- Let $G(x \rightarrow y)$ denote the set of permutations $g \in G$ such that $g(x) = y$.
- The stabilizer of $x$ is $G_x = G(x \rightarrow x)$. 
Example: Stabilizer

- Consider the following permutation group of \{1,2,3,4\}:
  \[ G = \{ \text{id, (1 2 3 4), (1 3)(2 4), (1 4 3 2), (2 4), (1 3), (1 2)(3 4), (1 4)(2 3)} \}. \]

- The stabilizers are:
  \[ \begin{align*}
  G_1 &= \{ \text{id, (2 4)} \}. \\
  G_2 &= \{ \text{id, (1 3)} \}. \\
  G_3 &= \{ \text{id, (2 4)} \}. \\
  G_4 &= \{ \text{id, (1 3)} \}. 
  \end{align*} \]

Stabilizers are Subgroups

- **Claim.** \( G_x \) is a subgroup of \( G \).
  - **Closure.** If \( g, h \in G_x \) then \( g(x) = x \) and \( h(x) = x \). Since \( gh(x) = x \) we have \( gh \in G_x \).
  - **Associativity.** Implied by the associativity of \( G \).
  - **Identity.** Since \( \text{id}(x) = x \), we have \( \text{id} \in G_x \).
  - **Inverse.** If \( g \in G_x \) then \( g(x) = x \). This implies that \( g^{-1}(x) = x \) so \( g^{-1} \in G_x \).
Cosets

- Let $H$ be a subgroup of the group $G$. The left coset of $H$ with respect to $g \in G$ is $gH = \{a \in G \mid a = gh \text{ for some } h \in H\}$.

Example. The coset of the alternating group $A_n$ with respect to a transposition $(x \ y) \in S_n$ is the subset of odd permutations of $S_n$.

$G(x \rightarrow y)$ are Cosets

- Claim. Let $G$ be a permutation group and let $h \in G(x \rightarrow y)$. Then $G(x \rightarrow y) = hG_x$.

Proof.
- $hG_x \subseteq G(x \rightarrow y)$. If $a \in hG_x$, then $a = hg$ for some $g \in G_x$. We have $a \in G(x \rightarrow y)$ since $a(x) = hg(x) = h(x) = y$.
- $G(x \rightarrow y) \subseteq hG_x$. If $b \in G(x \rightarrow y)$ then $h^{-1}b(x) = h^{-1}(y) = x$.

That is, $h^{-1}b \in G_x$, which implies $b \in hG_x$. 
Sizes of Cosets and Stabilizers

- **Claim.** Let $G$ be a permutation group on $X$ and let $G_x$ be the stabilizer of $x \in X$. Then $|G_x| = |hG_x|$ for any $h \in G$.
  - **Proof.** By the Latin square property of $G$.

- **Corollary.** The size of $G(x \to y)$:
  - If $y$ is in the orbit $G_x$ then $|G(x \to y)| = |G_x|$.
  - If $y$ is not in the orbit $G_x$ then $|G(x \to y)| = 0$.

Sizes of Orbits and Stabilizers

- **Theorem.** Let $G$ be a group of permutations of the set $X$. For every $x \in X$ we have $|Gx| \cdot |G_x| = |G|$.
  - *The orbit of* $x$
  - *The stabilizer of* $x$
Example: Orbits and Stabilizers

- Consider the following permutation group of \{1,2,3,4\}:
  \[ G = \{ \text{id}, (1 \ 2 \ 3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4 \ 3 \ 2),
  (2 \ 4), (1 \ 3), (1 \ 2)(3 \ 4), (1 \ 4)(2 \ 3) \}. \]
  - We have \( |G| = 8 \).
  - We have the orbit \( G1 = \{1,2,3,4\} \). So \( |G1| = 4 \).
  - We have the stabilizer \( G_1 = \{ \text{id}, (2 \ 4) \} \). So \( |G_1| = 2 \).
  - Combining the above yields \( |G| = 8 = |G1| \cdot |G_1| \).

A Useful Table

- Let \( G = \{ g_1, g_2, \ldots, g_n \} \) be a group of permutations of \( X = \{ x_1, x_2, \ldots, x_m \} \).
  - For an element \( x \in X \), we build the following table, where \( \checkmark \) implies that \( g_i(x) = x_j \).

<table>
<thead>
<tr>
<th></th>
<th>( x_1 )</th>
<th>( x_2 )</th>
<th>( x_3 )</th>
<th>( x_4 )</th>
<th>( x_5 )</th>
<th>( x_6 )</th>
<th>( x_7 )</th>
<th>\ldots</th>
<th>( x_m )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( g_1 )</td>
<td>( \checkmark )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( g_2 )</td>
<td></td>
<td>( \checkmark )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( g_3 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( \checkmark )</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>\ldots</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( g_n )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( \checkmark )</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

14
Table Properties 1

• How many ✓’s are in the table?
  ◦ Since $g_i(x)$ has a unique value, each row contains exactly one ✓.
  ◦ The total number of ✓’s in the table is $|G|$.

<table>
<thead>
<tr>
<th></th>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>$x_4$</th>
<th>$x_5$</th>
<th>$x_6$</th>
<th>$x_7$</th>
<th>...</th>
<th>$x_m$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$g_1$</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$g_2$</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$g_3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$g_n$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Table Properties 2

• How many ✓’s are in the column of $x_i$?
  ◦ If $x_i$ is not in the orbit $Gx$, then 0.
  ◦ If $x_i$ is in the orbit $Gx$, then
    $$|G(x \to y)| = |G_x|.$$
Proving the Theorem

- **Theorem.** Let $G$ be a group of permutations of the set $X$. For every $x \in X$ we have
  \[ |Gx| \cdot |G_x| = |G|. \]

- **Proof.**
  - **Counting by rows**, the number of $\checkmark$’s in the table is $|G|$.
  - **Counting by columns**, there are $|Gx|$ non-empty columns, each containing $|G_x|$ $\checkmark$’s.
  - That is, $|G| = |Gx| \cdot |G_x|$. 

Double Counting

- Our proof technique was to count the same value (the number of $\checkmark$’s in the table) in two different ways.
- This technique is called *double counting* and is very useful in combinatorics.
The End: Alhambra

- **Alhambra** is a palace and fortress complex located in Granada, Spain.
  - The Islamic art on the walls is claimed to contain all 17 wallpaper groups.
  - Mathematicians like to visit the palace and look for as many types as they can find.