Repeating the Basics

- We have a set of numbers
  \( X = \{1,2,3, \ldots, n\} \) and a permutation group \( G \) of \( X \).

- For example,
  \[
  X = \{1,2,3,4,5,6\}
  G = \{\text{id}, (1 \ 2), (3 \ 4), (1 \ 2)(3 \ 4)\}\]
Equivalence Classes

• The group $G$ partitions $X$ into **equivalence classes**.
  ◦ Two elements $x, y \in X$ are in the same class iff there exists a permutation $g \in G$ such that $g(x) = y$.

$$X = \{1, 2, 3, 4, 5, 6\}$$
$$G = \{\text{id}, (1 \ 2), (3 \ 4), (1 \ 2)(3 \ 4)\}$$

• The classes in this case are
  \{1, 2\}, \{3, 4\}, \{5\}, \{6\}.

Orbits

• The equivalence classes are also called **orbits**.
  ◦ For every $x \in X$ the orbit of $x$ is
    $$Gx = \{\text{The equivalence class that contains } x\}$$
    $$= \{y \in X \mid g(x) = y \text{ for some } g \in G\}.$$
Another Example: Orbits

- Let $X = \{1,2,3,4\}$ and let $G = \{\text{id}, (1 \ 2 \ 3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4 \ 3 \ 2),$
  $(2 \ 4), (1 \ 3), (1 \ 2)(3 \ 4), (1 \ 4)(2 \ 3)\}$.
- What are the orbits/equivalence classes that $G$ induces on $X$?
  - There is a single class
    $G1 = G2 = G3 = G4 = \{1,2,3,4\}$.

Stabilizers

- The stabilizer of $x \in X$ is the set of all permutations that take $x$ to itself ($x$ is “stable” in them). We denote this set as $G_x$.
- Example.
  $X = \{1,2,3,4,5,6\}$
  $G = \{\text{id}, (1 \ 2), (3 \ 4), (1 \ 2)(3 \ 4)\}$
  $G_1 = \{\text{id}, (3 \ 4)\}$. 
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
  - \( G_1 = \{\text{id}, (2 \ 4)\} \).
  - \( G_2 = \{\text{id}, (1 \ 3)\} \).
  - \( G_3 = \{\text{id}, (2 \ 4)\} \).
  - \( G_4 = \{\text{id}, (1 \ 3)\} \).

Reminder: 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 \( S_n\).
$G(x \to y)$ are Cosets

- **Claim.** Let $G$ be a permutation group and let $h \in G(x \to y)$. Then
  \[ G(x \to y) = hG_x. \]
  
  ◦ (This claim was proved in the previous class.)

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
  \[ |G_x| = |hG_x| \text{ for any } h \in G. \]
  
  ◦ **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 $G_1 = \{1,2,3,4\}$. So $|G_1| = 4$.
- We have the stabilizer $G_1 = \{\text{id}, (2 \ 4)\}$. So $|G_1| = 2$.
- Combining the above yields

$$|G| = 8 = |G_1| \cdot |G_1|.$$
A Useful Table

- Let $G = \{g_1, g_2, ..., g_n\}$ be a group of permutations of $X = \{x_1, x_2, ..., x_m\}$.

  - 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>...</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 1

- How many $\checkmark$’s are in the table?
  - Since $g_i(x)$ has a unique value, each row contains exactly one $\checkmark$.
  - The total number of $\checkmark$’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
    $$|G(x \rightarrow y)| = |G_x|.$$ 

<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>

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

• Our proof technique was to count the same value (the number of ✓’s in the table) in two different ways.
• This technique is called **double counting** and is very useful in combinatorics.

Another Problem

• **Problem.** Consider a group of permutations $G$ of the set $X$. Prove that if $x, y \in X$ are in the same orbit, then $|G_x| = |G_y|$.

• **Proof.**
  ◦ By the assumption, we have $|Gx| = |Gy|$.
  ◦ By the previous theorem
    $$|G_x| = \frac{|G|}{|Gx|} = \frac{|G|}{|Gy|} = |G_y|.$$
Distinct Identity Cards

• **(Silly) Problem.** A company produces identity cards that are $3 \times 3$ grids with holes in exactly two of the squares.

• How many distinct cards can be produced?

\[
\binom{9}{2} = 36.
\]

Distinct Identity Cards 2

• **Problem (part 2).** The identity cards are given to mathematicians, which might wear them upside down, sideways, back to front, etc.

• How many distinct cards can be produced without a chance of confusing two?
Rephrasing the Problem

- Let $X$ be the set of the original 36 cards.
- Let $G$ be the group of symmetries of the 3 × 3 grid (combinations of rotations and reflections taking the 3 × 3 grid to itself).
- Consider a symmetry $g \in G$.
  - Notice that $g$ is a bijection from $X$ to itself.
  - We think of $g$ as a permutation of the set $X$.

Rephrasing the Problem (2)

- Let $X$ be the set of the original 36 cards.
- Let $G$ be the group of symmetries of the 3 × 3 grid.
- We think of $G$ is a group of permutations of $X$.
- The number of distinct cards under the new definition is the number of different orbits of $G$ on $X$.
  - We would like a simple way for computing the number of orbits.
Number of Fixed Elements

• For every $g \in G$, we define $F(g) = |\{x \in X : g(x) = x\}|$.
  ◦ $F(g)$ is the number of stabilizers that contain $g$.

• Example. Consider the following permutation group of $\{1,2,3,4\}$.
  $G = \{\text{id}, (1 \ 2 \ 3 \ 4), (1 \ 3)(2 \ 4), (1 \ 4 \ 3 \ 2),
      (2 \ 4), (1 \ 3), (1 \ 2)(3 \ 4), (1 \ 4)(2 \ 3)\}$.
  ◦ $F(\text{id}) = 4$.
  ◦ $F((1 \ 3)) = 2$.
  ◦ $F((1 \ 2)(3 \ 4)) = 0$.

The Number of Distinct Orbits

• Claim. Let $G$ be a group of permutations of the set $X$. The number of orbits of $G$ on $X$ is

$$\frac{1}{|G|} \sum_{g \in G} |F(g)|.$$ 

(= the average size of $F(g)$)
Proof by Double Counting

- We **double count** the size of the set $E = \{(g, x) \mid g \in G, x \in X, g(x) = x\}$.

- **For a fixed** $g \in G$, the number of pairs in $E$ that contain $g$ is $F(g)$. That is
  \[ |E| = \sum_{g \in G} F(g). \]

- **For a fixed** $x \in X$, the number of pairs that contain $x$ is $|G_x|$. That is,
  \[ |E| = \sum_{x \in X} |G_x|. \]

Proof (cont.)

- The double counting implies
  \[ \sum_{g \in G} |F(g)| = \sum_{x \in X} |G_x|. \]
  - Recall that if $x, y \in X$ are in the same orbit, then $|G_x| = |G_y|$.
  - An orbit $Gx$ corresponds to $|Gx|$ elements of the red sum, each of size $|G_x|$. Thus, the orbit contributes to the sum $|Gx||G_x| = |G|$.
  - If there are $t$ orbits then
    \[ \sum_{g \in G} |F(g)| = t|G| \quad \Rightarrow \quad t = \frac{\sum_{g \in G}|F(g)|}{|G|}. \]
Back to Identity Cards

• **Recall.** In the **identity cards problem** we have a set $X$ of 36 cards. The number of **distinct** cards is the number of orbits under the group $G$ of card symmetries.
  ◦ That is, we need to calculate
    $$\frac{\sum_{g \in G} |F(g)|}{|G|}.$$ 

Counting $|G|$ and $|F(g)|$

• Symmetries of the $3 \times 3$ grid and the number of elements they fix:

<table>
<thead>
<tr>
<th>Symmetry $g$</th>
<th>$F(g)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>36</td>
</tr>
<tr>
<td>Rotation $90^\circ$</td>
<td>0</td>
</tr>
<tr>
<td>Rotation $180^\circ$</td>
<td>4</td>
</tr>
<tr>
<td>Rotation $270^\circ$</td>
<td>0</td>
</tr>
<tr>
<td>Reflection: main diagonal</td>
<td>6</td>
</tr>
<tr>
<td>Reflection: other diagonal</td>
<td>6</td>
</tr>
<tr>
<td>Reflection: vertical bisector</td>
<td>6</td>
</tr>
<tr>
<td>Reflection: horizontal bisector</td>
<td>6</td>
</tr>
</tbody>
</table>
More Counting

- There are eight symmetries of a card, so $|G| = 8$.
- We have
  \[ \sum_{g \in G} F(g) = 36 + 0 + 4 + 0 + 6 + 6 + 6 + 6. \]
- Therefore, the number of distinct cards/orbits is
  \[ \frac{1}{|G|} \sum_{g \in G} F(g) = \frac{1}{8} \cdot 64 = 8. \]

Necklaces

- **Problem.** Necklaces are manufactured by arranging 13 blue beads and three red beads on a loop of string. How many such distinct necklaces are there?
Necklaces Solution

- Think of the necklace as a **regular 16-gon**.
  - The number of general configurations is $\binom{16}{3} = 560$.
  - Two necklaces are identical if their 16-gons are identical under **rotations and reflections** (that is, under a **symmetry**).
  - The number of distinct necklaces is the **number of orbits** under the symmetry group of the 16-gon.

- To count distinct necklaces, we count the **number of symmetries** and the **number of elements fixed by each symmetry**.
  - The **identity** symmetry fixes all 560 elements.
  - There are 15 rotations of angles $\frac{2\pi n}{16}$ where $1 \leq n \leq 15$. These **do not fix any elements**.
  - 8 reflections across lines that connect middles of opposite edges. **Do no fix anything**.
  - 8 reflections across lines that connect opposite points. **Each fixing 2 \cdot 7 = 14 configurations**.

- The number of distinct necklaces/orbits is
  \[ \frac{\sum_g |F(g)|}{|G|} = \frac{672}{32} = 21. \]
The End: A Bad Joke

Why did the algorithmist die in the shower?

Because the shampoo said:

LATHER. RINSE. REPEAT.