Puzzle

Group Theory in the Bedroom

It’s easy to turn your mattress properly!
Turn it over and end-to-end.

1. Push at opposite corners A and B while your mattress is lying flat.
2. Position mattress across bed so it hangs over a foot or more.
3. Raise mattress up on edge as indicated in this illustration:
4. Let mattress fall gently towards head of bed as shown here:
5. Push alternately on corners A and B to position mattress on bed.

AND THERE YOU ARE... Turned Over and End to End as well!

TURNING A MATTRESS IS A JOB FOR TWO PEOPLE
Don’t risk damage to the mattress or personal injury by doing it yourself.

Reference: Scientific American, 93(5)-395
What is a Group?
To solve the equation $4 + x = 20$

$$-4 + (4+x) = -4 + 20 \quad \text{Closure}$$

$$(-4+4) + x = 16 \quad \text{Associativity}$$

$$0 + x = 16 \quad \text{Inverse}$$

$$x = 16 \quad \text{Identity}$$

What makes this calculation possible are the abstract properties of integers under addition.

Reference: Group Theory Lecture by Steven Rudich, 2000
An ordered pair \((S, \circ)\) where \(S\) is a set and \(\circ\) is a binary operation on \(S\).

**Closure**
\[ a, b \in S \implies (a \circ b) \in S \]

**Associativity**
\[ a, b, c \in S \implies (a \circ b) \circ c = a \circ (b \circ c) \]

**Identity**
\[ \exists e \in S \text{ s.t. } \forall a \in S \ a \circ e = e \circ a = a \]

**Inverse**
\[ \forall a \in S \ \exists a^{-1} \in S \text{ s.t. } a \circ a^{-1} = a^{-1} \circ a = e \]
(\mathbb{Z},+) IS A GROUP

Closure
The sum of two integers is an integer

Associativity
\[(a + b) + c = a + (b + c)\]

Identity
For every integer \(a\), \(a + 0 = 0 + a = a\)

Inverse
For every integer \(a\), \(a + (-a) = (-a) + a = 0\)
## Group or Not

<table>
<thead>
<tr>
<th></th>
<th>Closure</th>
<th>Associativity</th>
<th>Identity</th>
<th>Inverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(\mathbb{Z}, +)$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$(\mathbb{Z}\setminus{0}, \times)$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$({x \in \mathbb{R} \mid -5 &lt; x &lt; 5}, +)$</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>$(\mathbb{R}, -)$</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>$(\mathbb{Z}_n, +)$</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

N.B. $(\{x \in \mathbb{R} \mid -5 < x < 5\}, +)$ is not closed, so it doesn’t make sense to talk about associativity when some of the results of addition can be undefined.
Finite Groups can be represented by a Cayley Table.

\((\mathbb{Z}_4,+)\)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
Abstraction
Unique Identity

Theorem
A group has at most one identity element.

Proof
Suppose $e$ and $f$ are both identities of $(S, \bullet)$, then $f = e \bullet f = e$. 
Theorem

The left and right cancellation laws hold.

\[ a \diamond b = a \diamond c \quad \Rightarrow \quad b = c \]
\[ b \diamond a = c \diamond a \quad \Rightarrow \quad b = c \]

Proof

\[ a \diamond b = a \diamond c \]
\[ \Leftrightarrow \quad a^{-1} \diamond (a \diamond b) = a^{-1} \diamond (a \diamond c) \]
\[ \Leftrightarrow \quad (a^{-1} \diamond a) \diamond b = (a^{-1} \diamond a) \diamond c \]
\[ \Leftrightarrow \quad e \diamond b = e \diamond c \]
\[ \Leftrightarrow \quad b = c \]
Unique Inverse

Theorem

Every element in a group has an unique inverse.

Proof

Suppose $b$ and $c$ are both inverses of $a$, then

$$ a \bullet b = e $$

$$ a \bullet c = e $$

i.e. $a \bullet b = a \bullet c$. By cancellation theorem, $b = c$. 
Permutation Theorem

Theorem

Let \( \{e, g_1, g_2, \ldots, g_n\}, \cdot \) be a group and \( k \in \{1, \ldots, n\} \),

\[ G_k = \{ e \cdot g_k, g_1 \cdot g_k, g_2 \cdot g_k, \ldots, g_n \cdot g_k \} \]

must be a permutation of the elements in \( G \).

Proof

Suppose that two elements of \( G_k \) are equal, i.e.

\[ g_i \cdot g_k = g_j \cdot g_k \].

By cancellation theorem, \( g_i = g_j \).

Therefore, \( G_k \) contains each element in \( G \) once and once only.
Groups of two or three elements are unique and *abelian*. A group is *abelian* if its binary operation on the set is commutative, i.e. $\forall a, b \in S \ a \ast b = b \ast a$
Symmetry and Permutation
Symmetries of the square

- $R_0$
- $R_{90}$
- $R_{180}$
- $R_{270}$
- $F_1$
- $F_-$
- $F_{/}$
- $F\backslash$
Symmetry Group

Let $Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F|, F_-, F/, F\}$. 
Let $\circ$ be the binary operation of composition

$(Y_{SQ}, \circ)$ is a group!
Change Ringing

Cathedral bells in England have been rung by permuting the order of a round of bells.

Image Source: MIT Guild of Bellringers
Plain Bob Minimus

Let \( a = (1\ 2)(3\ 4), b = (2\ 3), c = (3\ 4) \)

\( Y_{\text{BOB}} = \{1, a, ab, aba, (ab)^2, (ab)^2a, (ab)^3, (ab)^3a\} \)

\begin{align*}
\begin{array}{cccc}
Y_{\text{BOB}} & (ab)^3ac & Y_{\text{BOB}} & ((ab)^3ac)^2 \ Y_{\text{BOB}} \\
\downarrow & \downarrow & \downarrow & \\
1\ 2\ 3\ 4 & 3\ 1\ 4\ 2 & 1\ 4\ 2\ 3 \\
2\ 1\ 4\ 3 & 3\ 1\ 2\ 4 & 4\ 1\ 3\ 2 \\
2\ 4\ 1\ 3 & 3\ 2\ 1\ 4 & 4\ 3\ 1\ 2 \\
4\ 2\ 3\ 1 & 2\ 3\ 4\ 1 & 3\ 4\ 2\ 1 \\
4\ 3\ 2\ 1 & 2\ 4\ 3\ 1 & 3\ 2\ 4\ 1 \\
3\ 4\ 1\ 2 & 4\ 2\ 1\ 3 & 2\ 3\ 1\ 4 \\
3\ 1\ 4\ 2 & 4\ 1\ 2\ 3 & 2\ 1\ 3\ 4 \\
1\ 3\ 2\ 4 & 1\ 4\ 3\ 2 & 1\ 2\ 4\ 3
\end{array}
\end{align*}

Audio: Courtesy of Tim Rose
**Dihedral Group**

Claim:

$Y_{BOB}$ and $Y_{SQ}$ are the same group, $D_4$.

\[
\begin{array}{cccc}
R_0 & F_1 & F_1 F_1 & F_1 F_1 / F_1 \\
1 & 2 & 2 & 4 \\
3 & 4 & 1 & 3 \\
4 & 2 & 3 & 1 \\
Y_{BOB} = Y_{SQ} \downarrow \\
1 & 2 & 3 & 4 \\
2 & 1 & 4 & 3 \\
2 & 4 & 1 & 3 \\
4 & 2 & 3 & 1 \\
\end{array}
\]
A check digit is an alphanumerical character added to a number to detect human errors.

\[ f(a_1, \ldots, a_{n-1}) + a_n = 0 \]

Most common errors are single digit errors (\(a \rightarrow b\)) and transposition errors (\(ab \rightarrow ba\)).

**Question**

Is there a method that detects 100% of both errors?
Verheoff Algorithm

Let $\diamond$ be the operation for the non-abelian group $D_5$.

Let $\sigma = (0)(1,4)(2,3)(5,6,7,8,9)$, then

$$\sigma^{n-1} (a_1) \diamond \sigma^{n-2} (a_2) \diamond \ldots \diamond \sigma^2 (a_{n-2}) \diamond \sigma (a_{n-1}) \diamond a_n = 0$$
Verheoff Algorithm

D5 and σ are chosen such that the algorithm

(a) detects all single digit errors
   if \( a \neq b \), then \( \sigma^i(a) \neq \sigma^i(b) \)

(b) detects all transposition errors
   if \( a \neq b \), then \( \sigma^{i+1}(a) \diamond \sigma^i(b) \neq \sigma^{i+1}(b) \diamond \sigma^i(a) \)
Structure
**Order**

Order of a group

\[ |G| = \text{The number of elements in the group.} \]

Order of a group element

\[ |g| = \text{The smallest number of times the binary operation is applied to } g \text{ before the identity } e \]

is reached

\[ |g| = k \text{ if } g^k = e \]

Examples

\[ |(Y_{SQ}, \mathcal{O})| = 8 \quad |F| = 2 \quad |R_{90}| = 4 \quad |(Z, +)| = \infty \]
Subgroup

Definition

\((H, \bullet)\) is a subgroup of \((S, \bullet)\) iff \(H\) is a group with respect to \(\bullet\) and \(H \subseteq S\).

Examples

✓ Is \((2\mathbb{Z}, +)\) a subgroup of \((\mathbb{Z}, +)\)?

✗ Is \((\{F|, F_-, F/, F\}, \mathcal{O})\) a subgroup of \((\text{Y}_{\text{SQ}}, \mathcal{O})\)?

✓ Is \((\{R_0, R_{90}, R_{180}, R_{270}\}, \mathcal{O})\) a subgroup of \((\text{Y}_{\text{SQ}}, \mathcal{O})\)?
Definition

A set $T \subseteq S$ is said to generate the group $(S, \bullet)$ if every element in $S$ can be generated from a finite product of the elements in $T$.

If $T$ is a single element, it is called a generator of the group.

Examples

$\{F_1, R_{90}\}$ generates $Y_{\mathbb{S}\mathbb{Q}}$

$\{1, -1\}$ generates $(\mathbb{Z}, +)$

$\{4\}$ is a generator for $(\mathbb{Z}_7, +)$

N.B. $F_1$ and $R_{90}$ is each a generator, but only the set of both generators generates a group.
Lagrange Theorem

If $H$ is a subgroup of a finite group $G$, then the order of $H$ divides the order of $G$.

Corollary

If $G$ is a finite group, $a^{|G|} = 1$.

Proof:

If $a$ generates the subgroup $H$, then $a^{|G|} = a^{k|H|} = (a^{|H|})^k = 1^k = 1$. 
Multiplication Modulo n

Let $\mathbb{Z}_n - \{0\} = \{1, 2, 3, \ldots, n-1\}$

Let $\circ = \text{multiplication mod } n$

$Z^*_n = \{ x \mid 1 \leq x \leq n \text{ and } \text{GCD}(x,n) = 1 \}$ is a group
Checking for Prime

Fermat’s (Little) Theorem

If \( n \) is prime, and \( a \in \mathbb{Z}_n^* \), then
\[
a^{n-1} = 1 \pmod{n}
\]

Proof

If \( n \) is prime, \( (\mathbb{Z}_n^* = \{1, 2, \ldots, n-1\}, \times) \) is a group with order \( n-1 \). The rest of the proof follows from Lagrange Theorem.

Application

To check if a number \( n \) is prime, pick any number \( a \), if \( a^{n-1} \pmod{n} \) is not 1, then it is not prime.
15-puzzle

Proof: A New Look at the Fifteen Puzzle, E.L. Spitznagel
3-cycles

To permute 3 blocks in a row cyclically, e.g. 
(a b c) → (b c a)

To permute any 3 blocks in the 15-puzzle
1. Move a, b, c to the first, second and third row
2. Move a, b, c to the extreme right column
3. Permute cyclically
4. Return a, b, c to original position, permuted

Every legal configuration can be obtained through a sequence of 3-cycle permutations.
Even Permutations

Going from 13-15-14 to 13-14-15 takes one transposition (**odd** permutation).

But the composition of 3-cycles generates only **even** permutation.

Why? Every product of two transpositions can be written as a product of 3-cycles.

\[(a, b)(b, c) = (a, c, b)\]
\[(a, b)(c, d) = (a, c, b)(b, d, c)\]
Proof of impossibility

Sketch of the Proof
All legal moves in the 15-puzzle are generated from 3-cycle permutations.

3-cycles generate $A_{15}$ (the group of even permutation) which is a subgroup of $S_{15}$, the group of all permutations of 15 objects.

Going from 13-15-14 to 13-14-15 takes an odd permutation. Therefore, no valid moves can achieve the 14-15 puzzle.
The Quintic Equation

\[ -b \pm \sqrt{b^2 - 4ac} \]

\[ \frac{2a}{} \]
Puzzles
Solution
Group Theory in the Bedroom

Klein Four-Group

Reference: Scientific American, 93(5)-395
Permutation Puzzles

The Rubik’s Cube

The Hockeypuck Puzzle

Masterball

Pyraminx

Lights Out

Megaminx
The End