Group Theory

Edith Law

27.03.2007

Puzzle
Group Theory in the Bedroom

Reference: Scientific American, 93(5)-395

What is a Group?

A Familiar Group

To solve the equation $4 + x = 20$

$-4 + (4+x) = -4 + 20$	Closure
$(-4+4) + x = 16$	Associativity
$0 + x = 16$	Inverse
$x = 16$	Identity

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

Reference: Group Theory Lecture by Steven Rudich, 2000

Group

An ordered pair $(S, \blacklozenge)$ where S is a set and $\blacklozenge$ is a binary operation on S.

Closure

$a, b \in S \Rightarrow (a \blacklozenge b) \in S$

Associativity

$a, b, c \in S \Rightarrow (a \blacklozenge b) \blacklozenge c = a \blacklozenge (b \blacklozenge c)$

Identity

$\exists\, e \in S \quad \text{s.t.} \quad \forall\, a \in S \;\; a \blacklozenge e = e \blacklozenge a = a$

Inverse

$\forall\, a \in \mathrm{S}\; \exists\, a^{-1} \in S \quad \text{s.t.} \quad a \blacklozenge a^{-1} = a^{-1} \blacklozenge a = e$

$(\mathbb{Z},+)$ 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

	Closure	Associativity	Identity	Inverse
$(Z, +)$	✓	✓	✓	✓
$(Z-\{0\}, \times)$	✓	✓	✓	×
$(\{x \in R \mid -5 < x < 5\},+)$	×	×	✓	✓
$(R, -)$	✓	×	×	×
$(Z_n, +)$	✓	✓	✓	✓

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

Cayley Table

Finite Groups can be represented by a Cayley Table.

$(Z_4, +)$

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Abstraction

Unique Identity

Theorem

A group has at most one identity element.

Proof

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

Cancellation Theorem

Theorem

The left and right cancellation laws hold.

$$a \blacklozenge b = a \blacklozenge c \quad \Rightarrow \quad b = c$$
$$b \blacklozenge a = c \blacklozenge a \quad \Rightarrow \quad b = c$$

Proof

$$\begin{aligned}
& a \blacklozenge b = a \blacklozenge c \\
\Leftrightarrow\ & a^{-1} \blacklozenge (a \blacklozenge b) = a^{-1} \blacklozenge (a \blacklozenge c) \\
\Leftrightarrow\ & (a^{-1} \blacklozenge a) \blacklozenge b = (a^{-1} \blacklozenge a) \blacklozenge c \\
\Leftrightarrow\ & e \blacklozenge b = e \blacklozenge c \\
\Leftrightarrow\ & b = c
\end{aligned}$$

Unique Inverse

Theorem

Every element in a group has an unique inverse.

Proof

Suppose b and c are both inverses of a, then

$$a \blacklozenge b = e$$
$$a \blacklozenge c = e$$

i.e. $a \blacklozenge b = a \blacklozenge c$. By cancellation theorem, $b = c$.

Permutation Theorem

Theorem

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

$G_k = \{ e \blacklozenge g_k, g_1 \blacklozenge g_k, g_2 \blacklozenge g_k, \ldots, g_n \blacklozenge g_k\}$

must be a permutation of the elements in G.

Proof

Suppose that two elements of G_k are equal, i.e. $g_i \blacklozenge g_k = g_j \blacklozenge g_k$. By cancellation theorem, $g_i = g_j$. Therefore, G_k contains each element in G once and once only.

Implications

◆	e	a
e	e	a
a	a	e

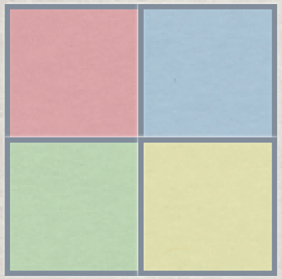
◆	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

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. $\forall\, a, b \in S \quad a \blacklozenge b = b \blacklozenge a$

Symmetry and Permutation

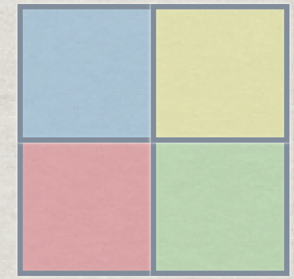
Symmetries of the square



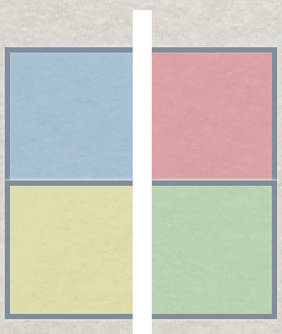
R_0

R_{90}

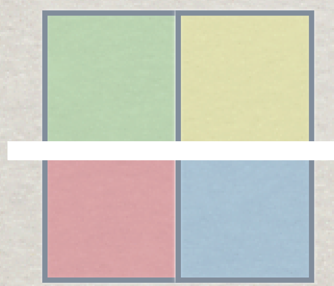
R_{180}



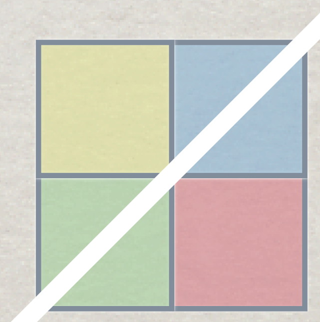
R_{270}



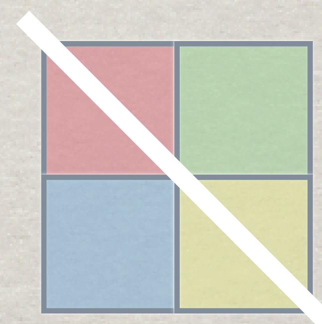
$F_{|}$



$F_{\_}$



$F_{/}$



$F_{\backslash}$

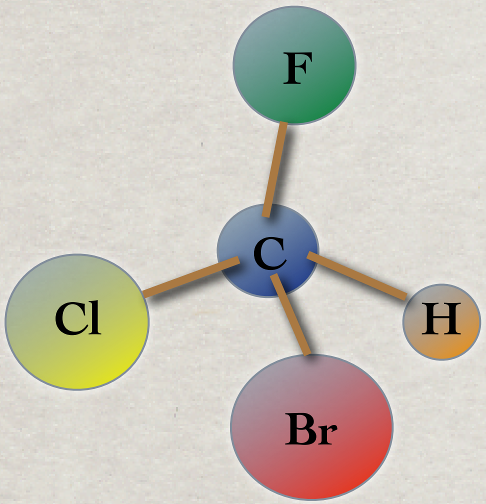
Symmetry Group

Let $Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F_{\vert}, F_{\_}, F_{/}, F_{\backslash} \}$
Let $\circ$ be the binary operation of *composition*

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

$\circ$	R_0	R_{90}	R_{180}	R_{270}	$F_{\vert}$	$F_{\_}$	$F_{/}$	$F_{\backslash}$
R_0	R_0	R_{90}	R_{180}	R_{270}	$F_{\vert}$	$F_{\_}$	$F_{/}$	$F_{\backslash}$
R_{90}	R_{90}	R_{180}	R_{270}	R_0	$F_{\backslash}$	$F_{/}$	$F_{\vert}$	$F_{\_}$
R_{180}	R_{180}	R_{270}	R_0	R_{90}	$F_{\_}$	$F_{\vert}$	$F_{\backslash}$	$F_{/}$
R_{270}	R_{270}	R_0	R_{90}	R_{180}	$F_{/}$	$F_{\backslash}$	$F_{\_}$	$F_{\vert}$
$F_{\vert}$	$F_{\vert}$	$F_{/}$	$F_{\_}$	$F_{\backslash}$	R_0	R_{180}	R_{90}	R_{270}
$F_{\_}$	$F_{\_}$	$F_{\backslash}$	$F_{\vert}$	$F_{/}$	R_{180}	R_0	R_{270}	R_{90}
$F_{/}$	$F_{/}$	$F_{\_}$	$F_{\backslash}$	$F_{\vert}$	R_{270}	R_{90}	R_0	R_{180}
$F_{\backslash}$	$F_{\backslash}$	$F_{\vert}$	$F_{/}$	$F_{\_}$	R_{90}	R_{270}	R_{180}	R_0

Other Examples



•	I
I	I

•	I	$F_\mid$
I	I	$F_\mid$
$F_\mid$	$F_\mid$	I

•	R_0	R_{120}	R_{240}
R_0	R_0	R_{120}	R_{240}
R_{120}	R_{120}	R_{240}	R_{120}
R_{240}	R_{240}	R_0	R_{120}

Change Ringing

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

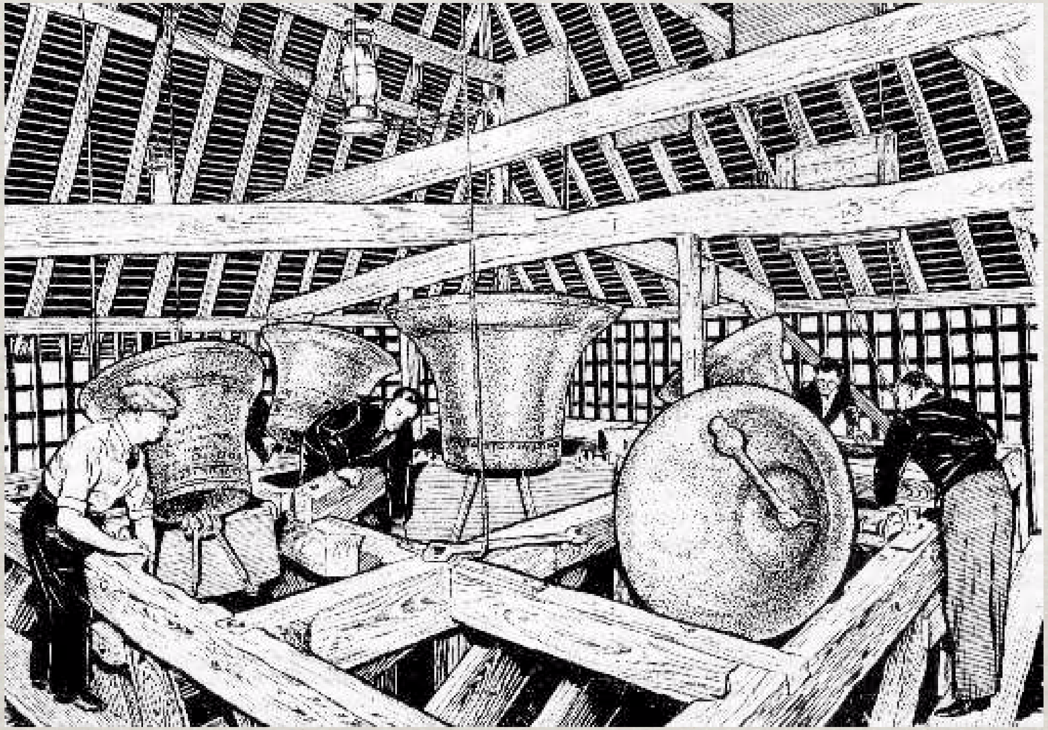


Image Source: MIT Guild of Bellringers

Plain Bob Minimus

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

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

Y_{BOB}	$(ab)^3ac\ Y_{BOB}$	$((ab)^3ac)^2\ Y_{BOB}$
↓	↓	↓
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

Audio: Courtesy of Tim Rose

Dihedral Group

Claim:

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

R_0	$F_{\vert}$	$F_{\vert} F_{/}$	$F_{\vert} F_{/} F_{\vert}$
1 2	2 1	2 4	4 2
3 4	4 3	1 3	3 1
R_0	**$F_{\vert}$**	**R_{270}**	**$F_{/}$**

$(F_{\vert} F_{/})^2$	$(F_{\vert} F_{/})^2 F_{\vert}$	$(F_{\vert} F_{/})^3$	$(F_{\vert} F_{/})^3 F_{\vert}$
4 3	3 4	3 1	1 3
2 1	1 2	4 2	2 4
R_{180}	**$F_{\_}$**	**R_{90}**	**$F_{\backslash}$**

$Y_{BOB}=Y_{SQ}$

↓

1 2 3 4
2 1 4 3
2 4 1 3
4 2 3 1
4 3 2 1
3 4 1 2
3 1 4 2
1 3 2 4

Error Correcting Code

A check digit is an alphanumeric 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 ($a \to b$) and transposition errors ($ab \to ba$).

Question

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

Verheoff Algorithm

Let ◇ be the operation for the non-abelian group D_5.

◇	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

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

$$\text{if } a \neq b, \text{ then } \sigma^i(a) \neq \sigma^i(b)$$

(b) detects all transposition errors

$$\text{if } a \neq b, \text{ then } \sigma^{i+1}(a) \diamond \sigma^i(b) \neq \sigma^{i+1}(b) \diamond \sigma^i(a)$$

Structure

Order

Order of a group

$|G|$ = The number of elements in the group.

Order of a group element

$|g|$ = The smallest number of times the binary operation is applied to g before the identity e is reached

$$|g| = k \text{ if } g^k = e$$

Examples

$|(Y_{SQ}, \circ)| = 8$ $|F_{|}| = 2$ $|R_{90}| = 4$ $|(Z,+)| = \infty$

Subgroup

Definition

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

Examples

- ✓ Is $(2Z,+)$ a subgroup of $(Z,+)$?
- ✗ Is $(\{F_|, F\_, F_/, F_\backslash\}, \circ)$ a subgroup of $(Y_{SQ}, \circ)$?
- ✓ Is $(\{R_0, R_{90}, R_{180}, R_{270}\}, \circ)$ a subgroup of $(Y_{SQ}, \circ)$?

Generator

Definition

A set $T \subseteq S$ is said to generate the group $(S, \blacklozenge)$ 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

$\{F_{|}, R_{90}\}$ generates Y_{SQ}

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

$\{4\}$ is a generator for $(Z_7,+)$

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

Lagrange Theorem

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 $Z_n - \{0\} = \{1, 2, 3, \dots n-1\}$

Let $\odot$ = multiplication mod n

n=2

$\odot$	1
1	1

n=3

$\odot$	1	2
1	1	2
2	2	1

n=4

$\odot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

n=5

$\odot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

n=6

$\odot$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

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

Checking for Prime

Fermat's (Little) Theorem

If n is prime, and $a \in Z^*_n$, then

$$a^{n-1} = 1 \pmod{n}$$

Proof

If n is prime, ($Z^*_n = \{1, 2, \ldots, n-1\}, \times$) 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 $a^{n-1} \bmod n$ is not 1, then it is not prime.

15-PUZZLE

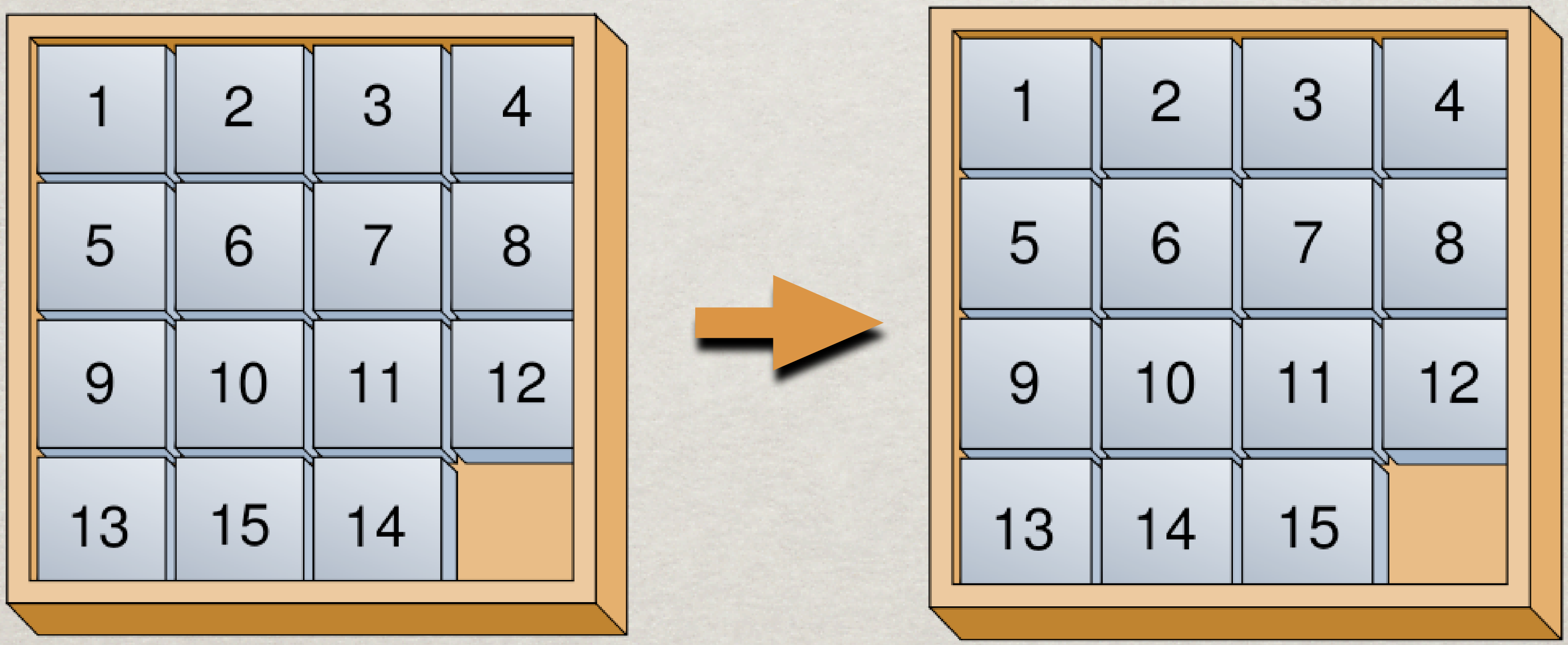
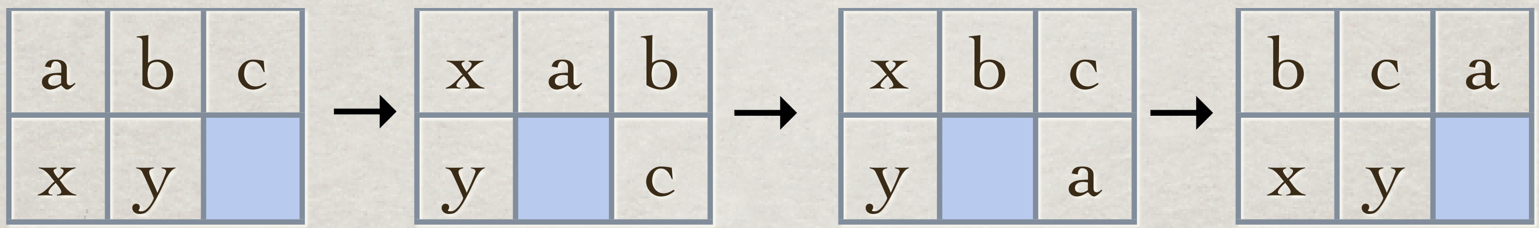


Image Source: Fifteen puzzle, Wikipedia

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.

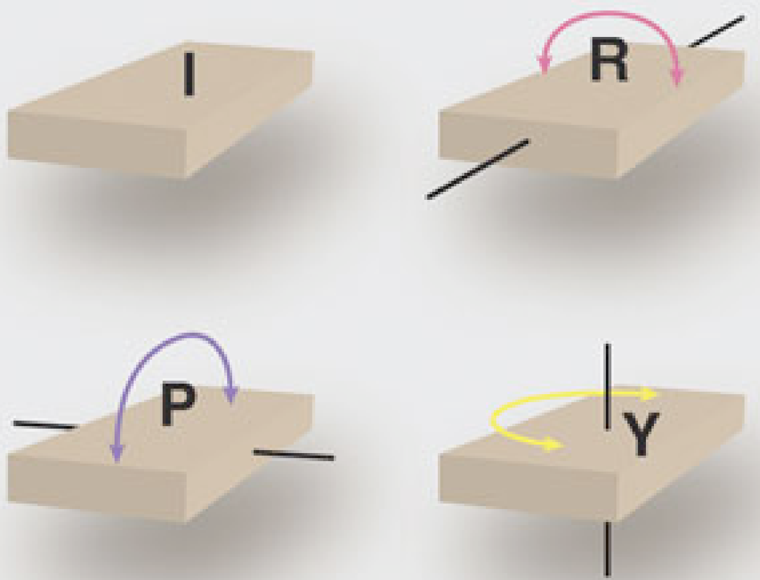
The Quintic Equation

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

800 900 1000 1100 1200 1300 1400 1500 1600 1700 1800 1900

Puzzles

Solution
Group Theory in the Bedroom



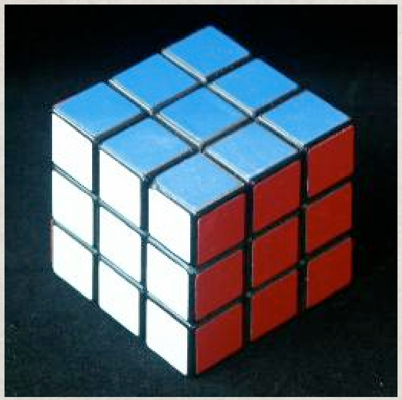
second operation

first operation	I	R	P	Y
I	I	R	P	Y
R	R	I	Y	P
P	P	Y	I	R
Y	Y	P	R	I

Klein Four-Group

Reference: Scientific American, 93(5)-395

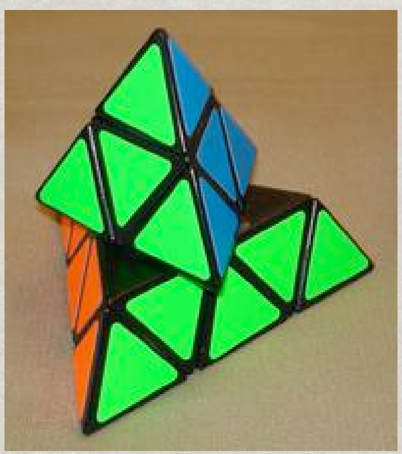
Permutation Puzzles



The Rubik's Cube

The Hockeypuck Puzzle

Masterball



Pyraminx

Lights Out

Megaminx

The End