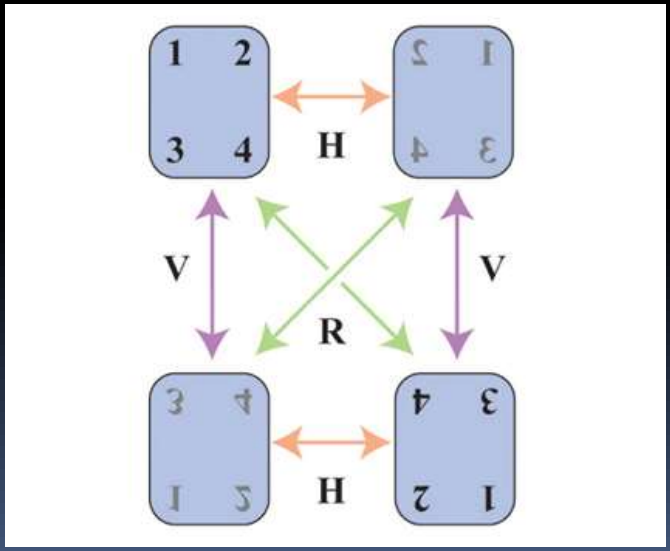
15-251: Great Theoretical Ideas in Computer Science

Fall 2016 Lecture 22

November 10, 2016

Group Theory



.	R_0	R_{90}	R_{180}	R_{270}	V	H	D_1	D_2
R_0	R_0	R_{90}	R_{180}	R_{270}	V	H	D_1	D_2
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D_2	D_1	V	H
R_{180}	R_{180}	R_{270}	R_0	R_{90}	H	V	D_2	D_1
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D_1	D_2	H	V
V	V	D_1	H	D_2	R_0	R_{180}	R_{90}	R_{270}
H	H	D_2	V	D_1	R_{180}	R_0	R_{270}	R_{90}
D_1	D_1	H	D_2	V	R_{270}	R_{90}	R_0	R_{180}
D_2	D_2	V	D_1	H	R_{90}	R_{270}	R_{180}	R_0

Il est peu de notions en mathematiques qui soient plus primitives que celle de loi de composition.

- Nicolas Bourbaki

There are few concepts in mathematics that are more primitive than the composition law.

Group Theory

Study of **symmetries** and **transformations** of mathematical objects.

Also, the study of abstract algebraic objects called '**groups**'.

(of which $\mathbb{Z}_N$ and $\mathbb{Z}_N^*$ are special cases)

What is group theory good for?

In theoretical computer science:

Checksums, error-correction schemes

Minimizing randomness-complexity of algorithms

Cryptosystems

Algorithms for quantum computers

Hard instances of optimization problems

Ketan Mulmuley’s approach to P vs. NP

Laci Babai’s graph isomorphism algorithm

What is group theory good for?

In puzzles and games:

"15 Puzzle"

Rubik's Cube

SET

What is group theory good for?

In math:

There's a quadratic formula:

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

What is group theory good for?

In math:

There's a cubic formula:

$$
\begin{aligned}
x_1 = &-\frac{b}{3a} \\
&-\frac{1}{3a}\sqrt[3]{\frac{1}{2}\left[2b^3-9abc+27a^2d+\sqrt{\left(2b^3-9abc+27a^2d\right)^2-4\left(b^2-3ac\right)^3}\right]} \\
&-\frac{1}{3a}\sqrt[3]{\frac{1}{2}\left[2b^3-9abc+27a^2d-\sqrt{\left(2b^3-9abc+27a^2d\right)^2-4\left(b^2-3ac\right)^3}\right]} \\
x_2 = &-\frac{b}{3a} \\
&+\frac{1+i\sqrt{3}}{6a}\sqrt[3]{\frac{1}{2}\left[2b^3-9abc+27a^2d+\sqrt{\left(2b^3-9abc+27a^2d\right)^2-4\left(b^2-3ac\right)^3}\right]} \\
&+\frac{1-i\sqrt{3}}{6a}\sqrt[3]{\frac{1}{2}\left[2b^3-9abc+27a^2d-\sqrt{\left(2b^3-9abc+27a^2d\right)^2-4\left(b^2-3ac\right)^3}\right]} \\
x_3 = &-\frac{b}{3a} \\
&+\frac{1-i\sqrt{3}}{6a}\sqrt[3]{\frac{1}{2}\left[2b^3-9abc+27a^2d+\sqrt{\left(2b^3-9abc+27a^2d\right)^2-4\left(b^2-3ac\right)^3}\right]} \\
&+\frac{1+i\sqrt{3}}{6a}\sqrt[3]{\frac{1}{2}\left[2b^3-9abc+27a^2d-\sqrt{\left(2b^3-9abc+27a^2d\right)^2-4\left(b^2-3ac\right)^3}\right]}
\end{aligned}
$$

What is group theory good for?

In math:

There's a quartic formula:

x_1 & = & {\frac{-a}{4} - \frac{1}{2}{\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d) } {3{(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd +

{\sqrt{-4{(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^{\frac{1}{3}}} + (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd +

{\sqrt{-4 {(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} }} {54})^\frac{1}{3}}} - \frac{1}{2}{\sqrt{\frac{a^2}{2} - \frac{4b}{3}

- \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d) } {3{(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4{(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^{\frac{1}{3}}}
- - (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} }} {54})^\frac{1}{3} –
- \frac{-a^3 + 4ab - 8c} {4{\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}} (b^2 - 3ac + 12d) }{3 {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd +
- {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^ {\frac{1}{3}}} + (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd +
- {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} } }{54})^\frac{1}{3}}}}}}}} \\ x_2 & = & {\frac{-a}{4}
- \frac{1}{2}{\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d) } {3{(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4{(b^2 - 3ac + 12d) }^3 +
- {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^{\frac{1}{3}}} + (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 +
- {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} }} {54})^\frac{1}{3}}} + \frac{1}{2}{\sqrt{\frac{a^2}{2} - \frac{4b}{3} - \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d) }
- {3{(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4{(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^{\frac{1}{3}}} –
- (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} }} {54})^\frac{1}{3} - \frac{-a^3 + 4ab - 8c}
- {4{\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}} (b^2 - 3ac + 12d) }{3 {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 +
- {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^ {\frac{1}{3}}} + (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 +
- {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} } }{54})^\frac{1}{3}}}}}}}} \\ x_3 & = & {\frac{-a}{4} + \frac{1}{2}{\sqrt{\frac{a^2}{4} - \frac{2b}{3} +
- \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d) } {3{(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4{(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^{\frac{1}{3}}} +
- (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} }} {54})^\frac{1}{3}}} –
- \frac{1}{2}{\sqrt{\frac{a^2}{2} - \frac{4b}{3} - \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d) } {3{(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4{(b^2 - 3ac + 12d) }^3 +
- {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^{\frac{1}{3}}} - (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 +
- {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} }} {54})^\frac{1}{3} + \frac{-a^3 + 4ab - 8c} {4{\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}} (b^2 - 3ac + 12d) }
- {3 {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^ {\frac{1}{3}}} +
- (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} } }{54})^\frac{1}{3}}}}}}}} \\
- x_4 & = & {\frac{-a}{4} + \frac{1}{2}{\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d) } {3{(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd +
- {\sqrt{-4{(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^{\frac{1}{3}}} + (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd +
- {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} }} {54})^\frac{1}{3}}} + \frac{1}{2}{\sqrt{\frac{a^2}{2} - \frac{4b}{3} –
- \frac{2^{\frac{1}{3}}(b^2 - 3ac + 12d) } {3{(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4{(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^{\frac{1}{3}}} –
- (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 + {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} }} {54})^\frac{1}{3} + \frac{-a^3 + 4ab - 8c}
- {4{\sqrt{\frac{a^2}{4} - \frac{2b}{3} + \frac{2^{\frac{1}{3}} (b^2 - 3ac + 12d) }{3 {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 +
- {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}}) }^ {\frac{1}{3}}} + (\frac{{ 2b^3 - 9abc + 27c^2 + 27a^2d - 72bd + {\sqrt{-4 {(b^2 - 3ac + 12d) }^3 +
- {(2b^3 - 9abc + 27c^2 + 27a^2d - 72bd) }^2}} } }{54})^\frac{1}{3}}}}}}}

What is group theory good for?

In math:

There is **NO** quintic formula.

What is group theory good for?

In physics:

Predicting the existence of elementary particles **before** they are discovered.

So: What ***is*** group theory?

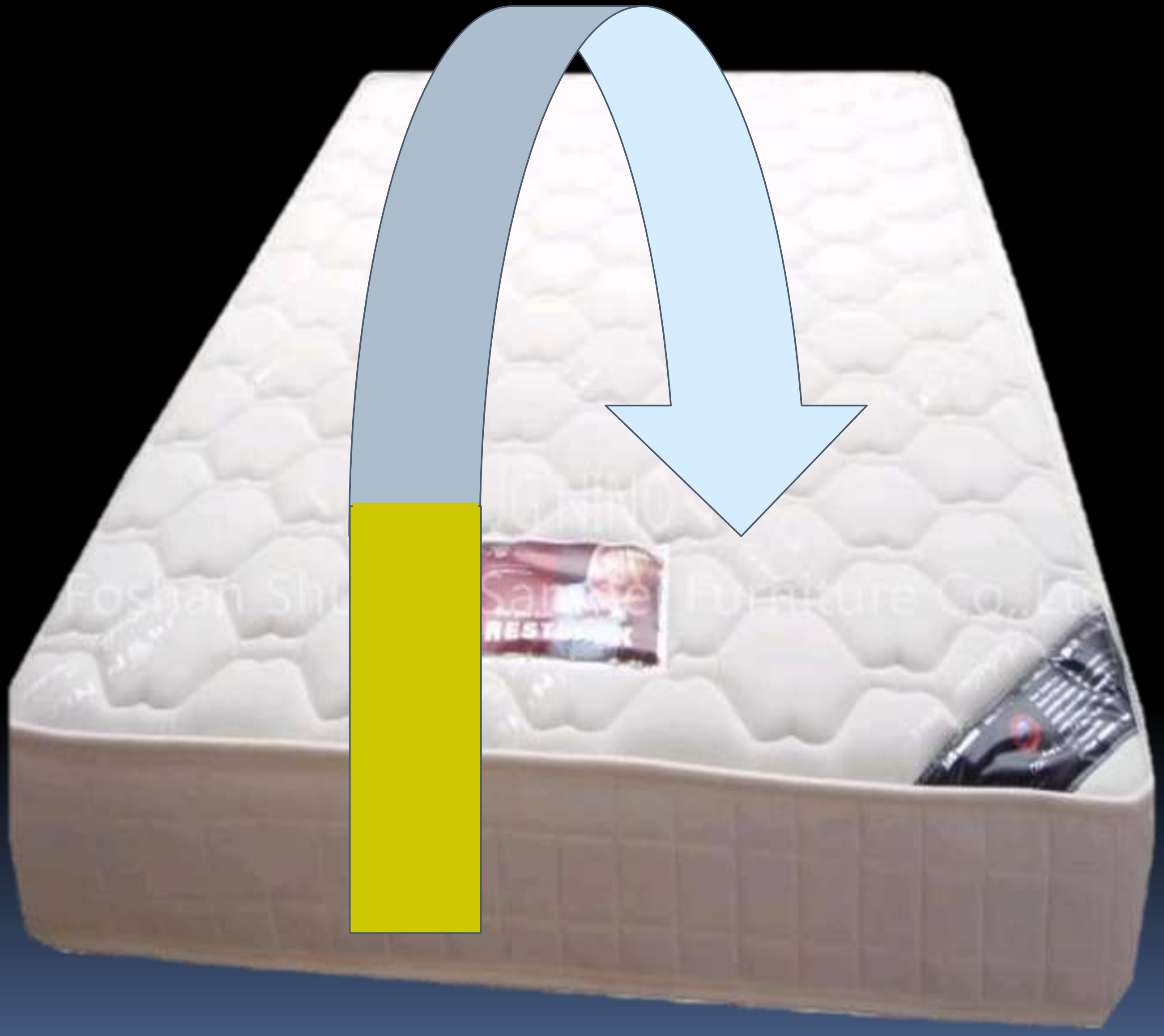
Let’s start with an example from

http://opinionator.blogs.nytimes.com/2010/05/02/group-think/

Rotate

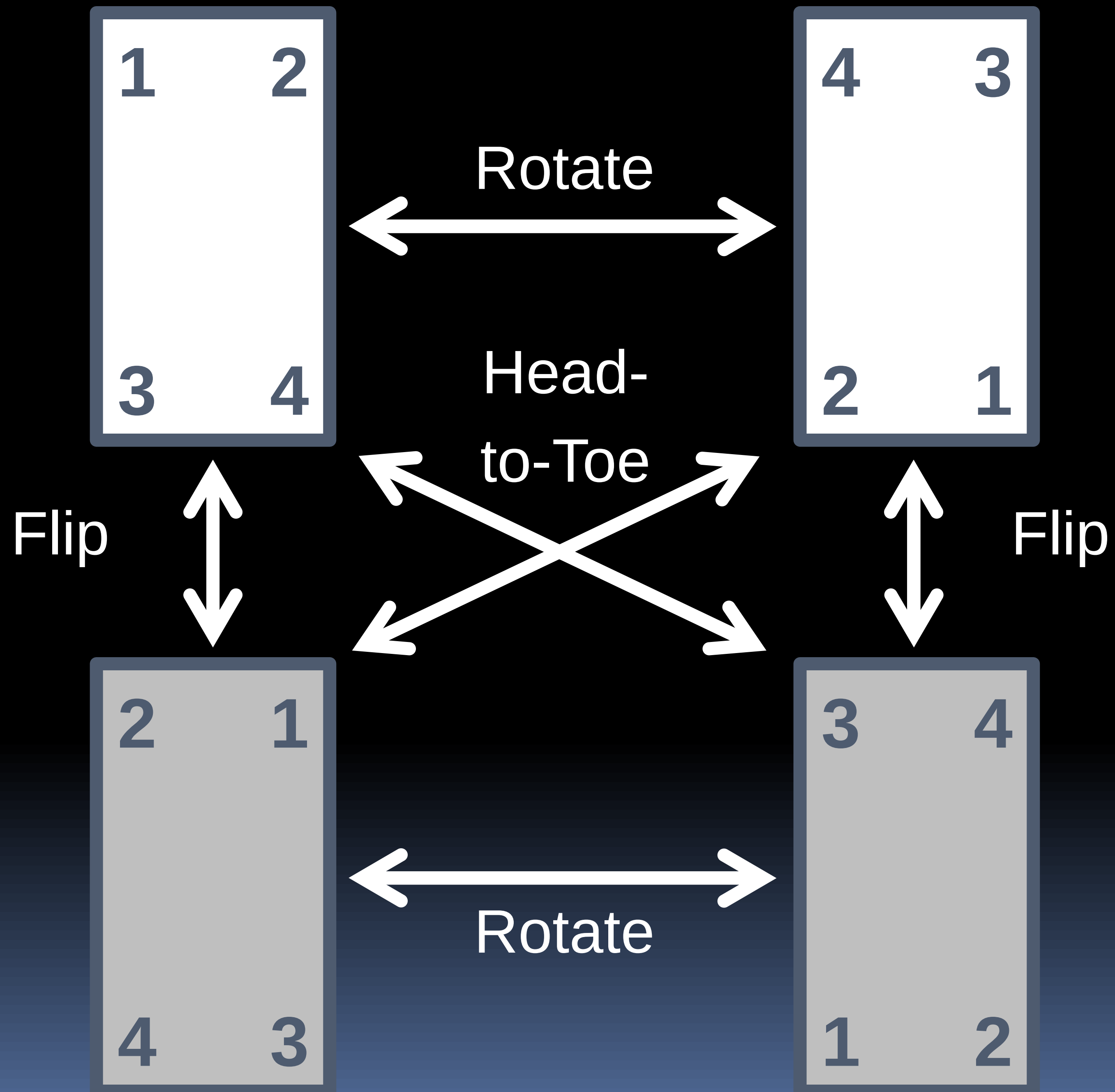
Flip

Head-to-Toe flip



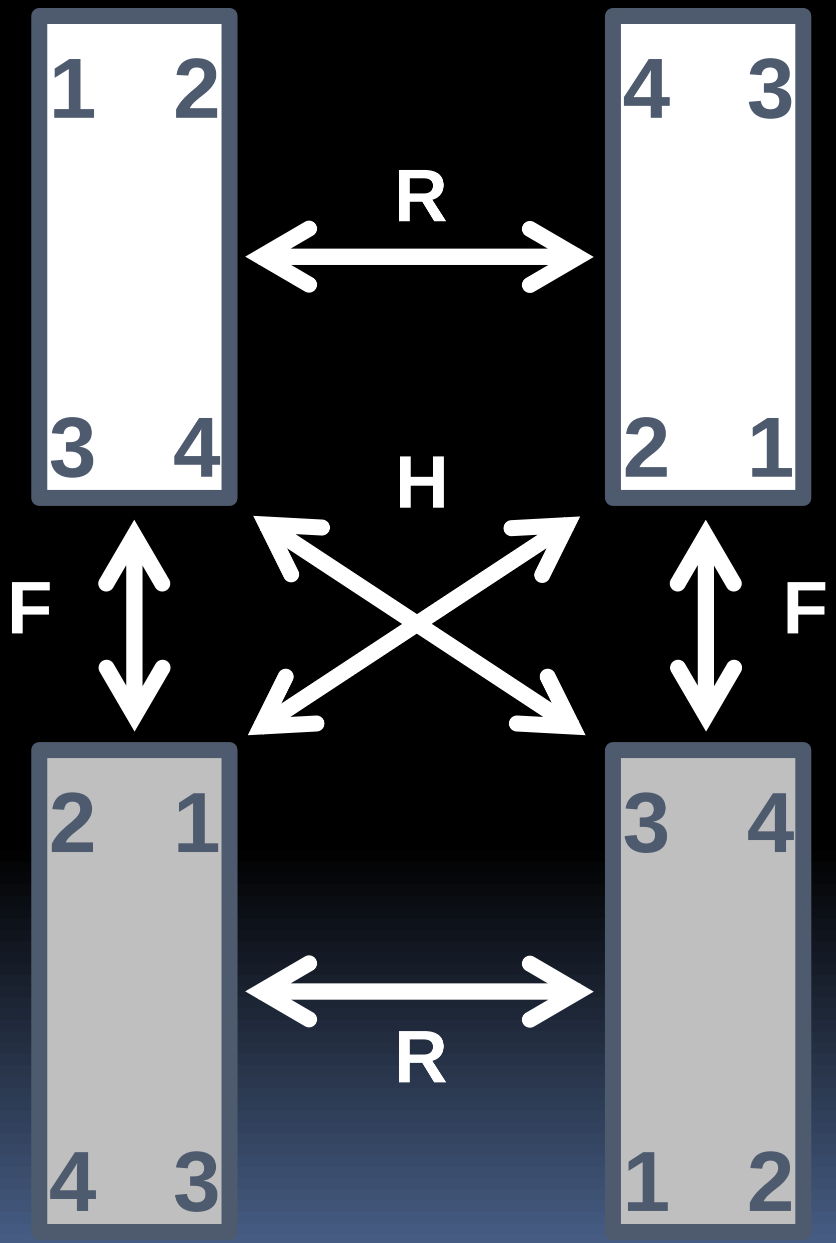
Q: How many positions can it be in?

A: Four.


1 2
3 4
Rotate
4 3
2 1
Head-
to-Toe
Flip
Flip
2 1
4 3
3 4
1 2
Rotate

Group theory is not so much
about **objects** (like mattresses).

It’s about the **transformations**
on objects and how they (inter)act.



F(**R**(mattress)) =

H(mattress)

H(**F**(mattress)) =

R(mattress)

R(**F**(**H**(mattress))) =

Id(mattress)

F•R=H

H•F=R

R•F•H=Id

R•Id•H•F•H = H

The kinds of questions asked:

What is R•Id•H•F•H ?

Do transformations **A** and **B** “commute”?

I.e., does **A•B = B•A** ?

What is the “order” of transformation **A**?

i.e., how many times do you have to

apply **A** before you get to **Id** ?

Definition of a **group of transformations**

Let X be a set.

Let G be a set of **bijections** $p : X \to X$.

We say G is a **group of transformations** if:

1. If **p** and **q** are in G then so is **p • q**.

   G is "**closed**" under composition.

2. The 'do-nothing' bijection **Id** is in G.

3. If **p** is in G then so is its inverse, $\mathbf{p}^{-1}$.

   G is "closed" under inverses.

Example: Rotations of a rectangular mattress

X = set of all physical points of the mattress

G = { **Id**, **R**otate, **F**lip, **H**ead-to-toe }

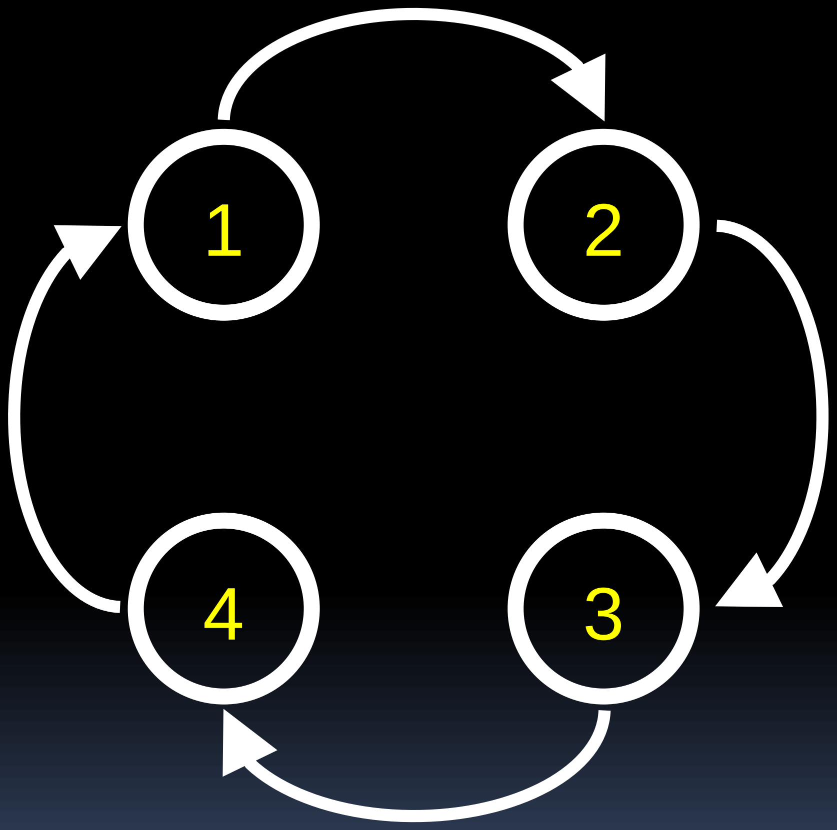
Check the 3 conditions:

1. If **p** and **q** are in G then so is **p • q**. ✓

2. The ‘do-nothing’ bijection **Id** is in G. ✓

3. If **p** is in G then so is its inverse, $\mathbf{p}^{-1}$. ✓

Example: Symmetries of a directed cycle



X = labelings of the vertices by 1,2,3,4

|X| = 24

G = permutations of the labels which don't change the graph

|G| = 4

G = { **Id**, $\mathbf{Rot_{90}}$, $\mathbf{Rot_{180}}$, $\mathbf{Rot_{270}}$ }

Example: Symmetries of a directed cycle

X = labelings of directed 4-cycle

G = { **Id**, $\mathbf{Rot_{90}}$, $\mathbf{Rot_{180}}$, $\mathbf{Rot_{270}}$ }

Check the 3 conditions:

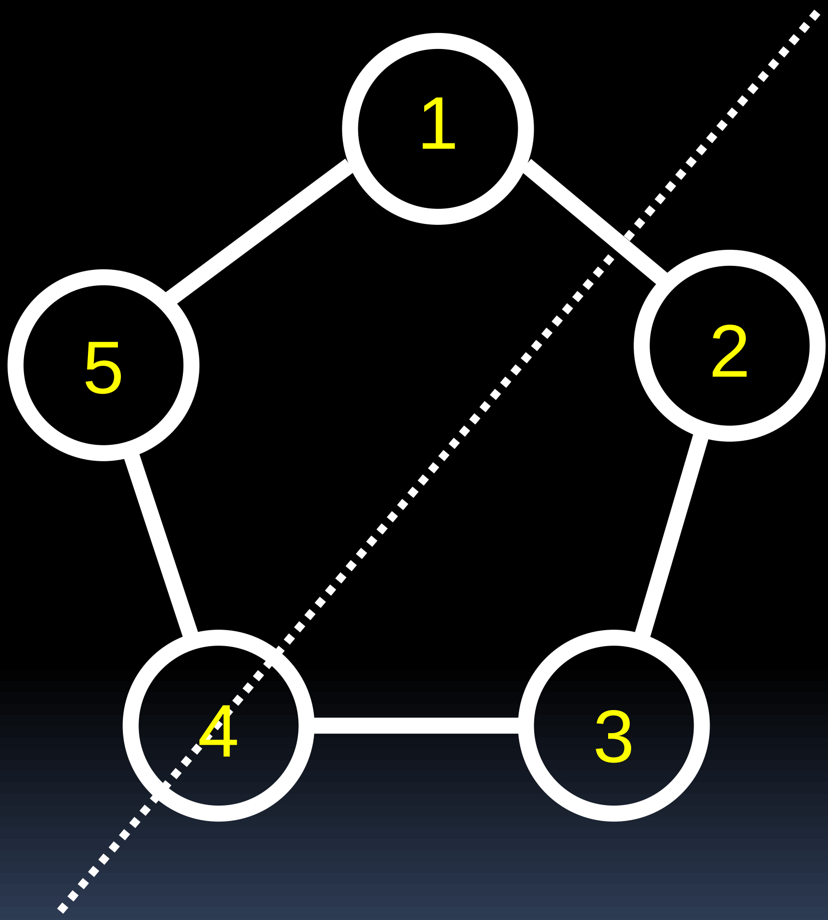
1. If **p** and **q** are in G then so is **p • q**. ✓

2. The 'do-nothing' bijection **Id** is in G. ✓

3. If **p** is in G then so is its inverse, $\mathbf{p^{-1}}$. ✓

"Cyclic group of size 4"

Example: Symmetries of **undirected** n-cycle



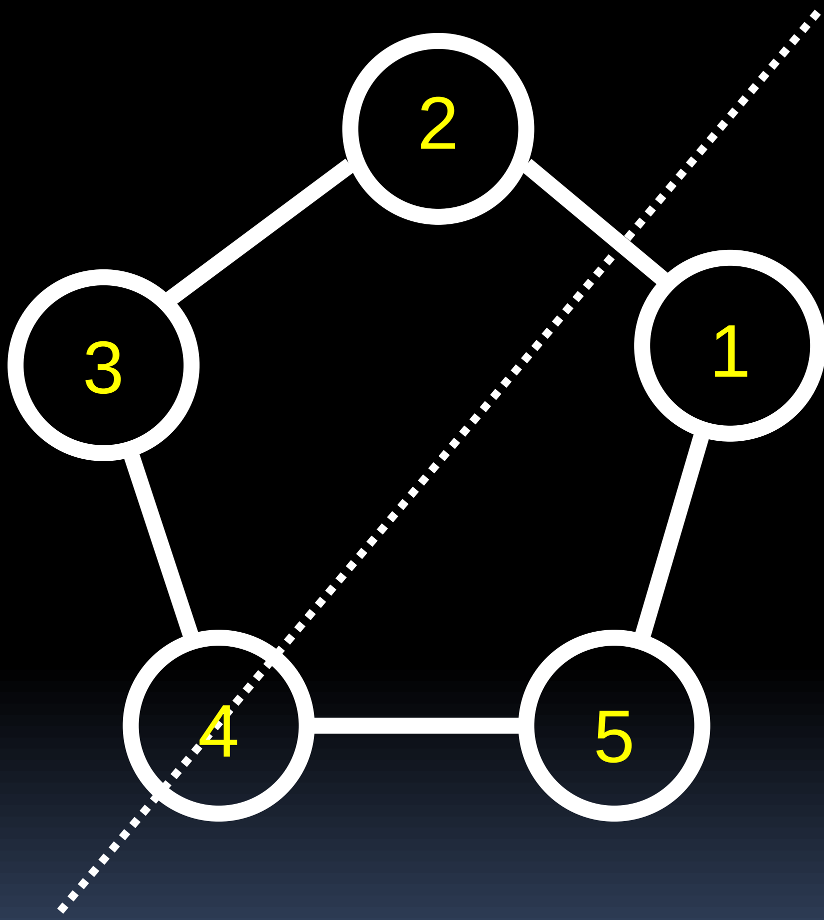
X = labelings of the vertices by 1,2, …, n

G = permutations of the labels which don't change the graph
(neighbors stay neighbors
& non-nbrs stay non-nbrs)

Poll

|G| = 2n

Example: Symmetries of **undirected** n-cycle



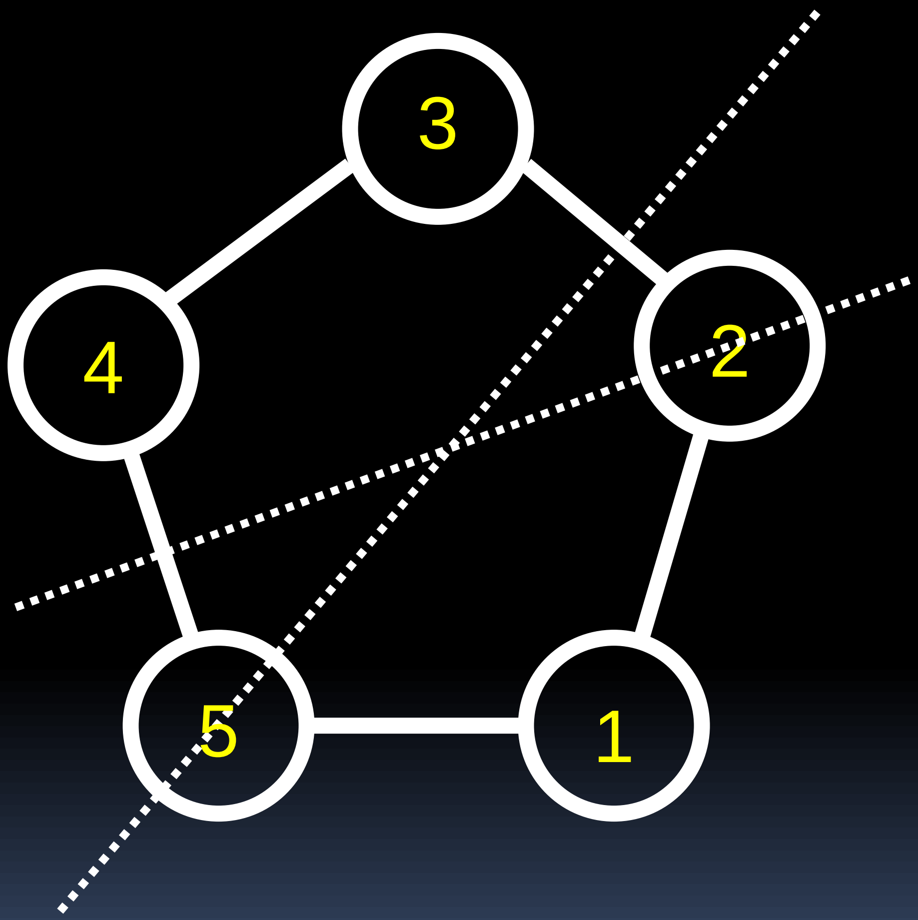
X = labelings of the vertices by 1,2, …, n

G = permutations of the labels which don't change the graph

|G| = 2n

+ one clockwise twist

Example: Symmetries of **undirected** n-cycle



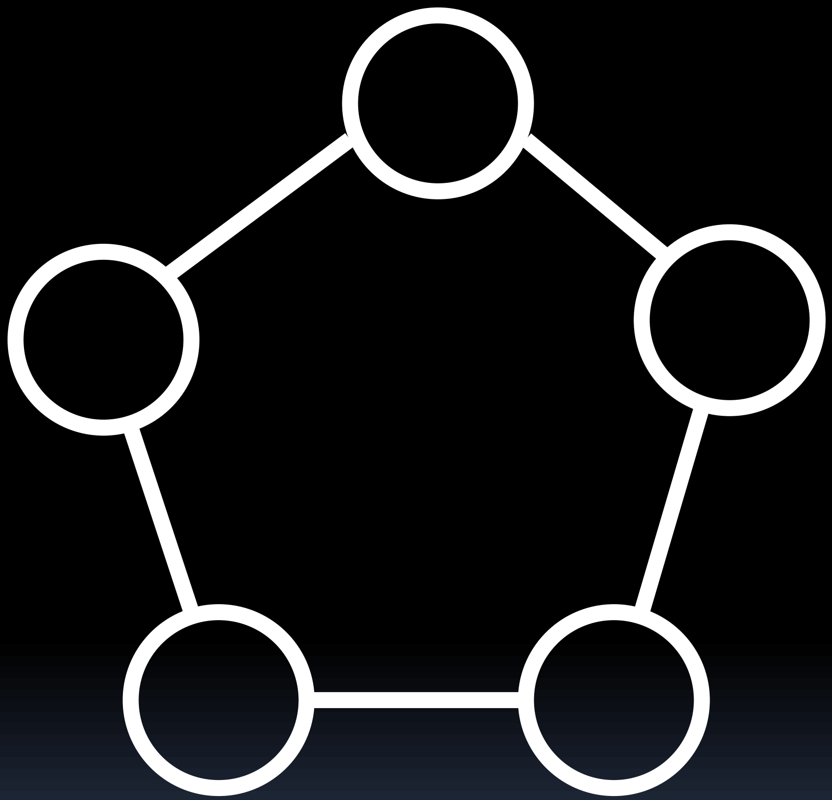
X = labelings of the vertices by 1,2, …, n

G = permutations of the labels which don’t change the graph

|G| = 2n

+ one clockwise twist =

Example: Symmetries of **undirected** n-cycle



X = labelings of the vertices by 1,2, …, n

|X| = n!

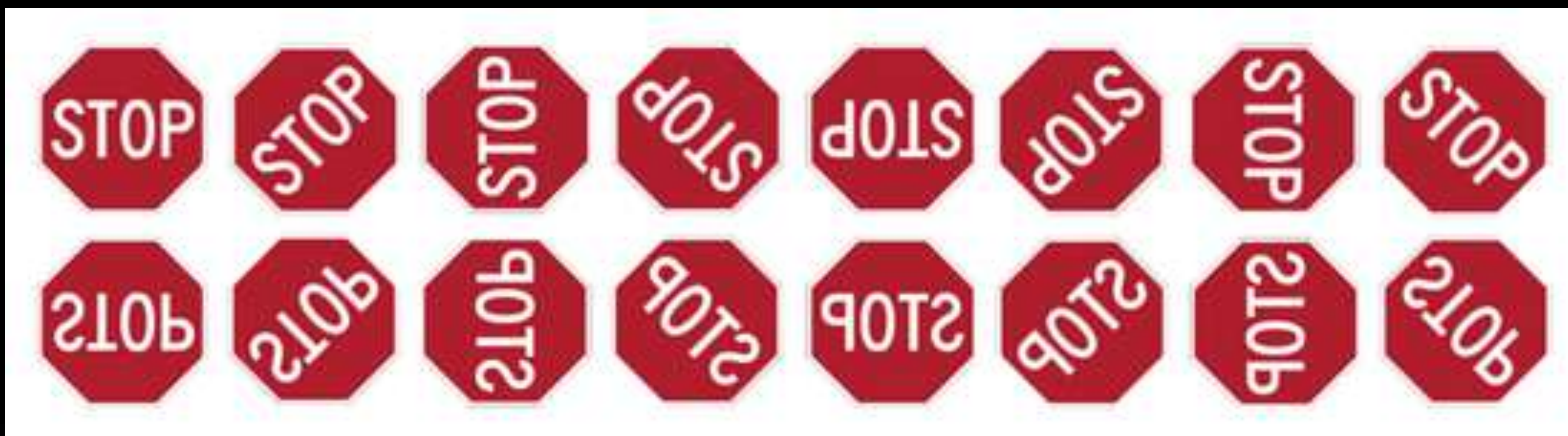
G = permutations of the labels which don't change the graph

|G| = 2n

G = { **Id**, n−1 'rotations', n 'reflections' }

"Dihedral group of size 2n"

Effect of the 16 elements of D_8 on a stop sign



Example: "All permutations"

$X = \{1, 2, \ldots, n\}$

G = all permutations of X

e.g., for n = 4, a typical element of G is:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

"Symmetric group, Sym(n) or S_n"

More groups of transformations

Motions of 3D space: translations + rotations (preserve laws of Newtonian mechanics)

Translations of 2D space by an integer amount horizontally and an integer amount vertically

Rotations which preserve an old-school soccer ball (icosahedron)

The group of mattress rotation

G = { Id, R, F, H }

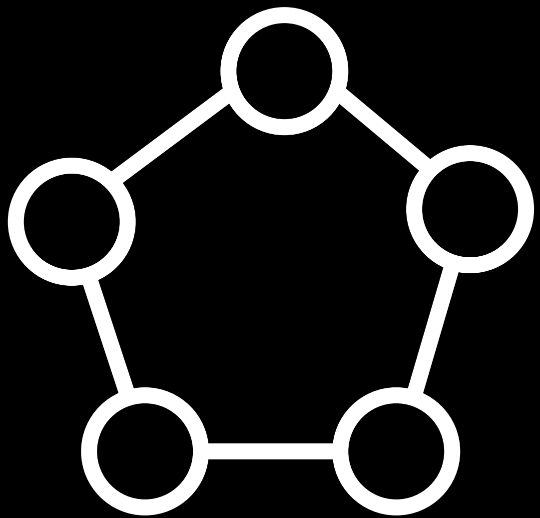
Id • Id = Id
Id • R = R
Id • F = F
Id ○ H = H
R ○ Id = R
R ○ R = Id
R ○ F = H
R ○ H = F

F • Id = F
F ○ R = H
F ○ F = Id
F ○ H = R
H ○ Id = H
H ○ R = F
H ○ F = R
H ○ H = Id

Group table

•	Id	R	F	H
Id	Id	R	F	H
R	R	Id	H	F
F	F	H	Id	R
H	H	F	R	Id

The laws of the dihedral group of size 10



G =

$\{ Id, r_1, r_2, r_3, r_4, f_1, f_2, f_3, f_4, f_5 \}$

$\circ$	Id	r_1	r_2	r_3	r_4	f_1	f_2	f_3	f_4	f_5
Id	Id	r_1	r_2	r_3	r_4	f_1	f_2	f_3	f_4	f_5
r_1	r_1	r_2	r_3	r_4	Id	f_4	f_5	f_1	f_2	f_3
r_2	r_2	r_3	r_4	Id	r_1	f_2	f_3	f_4	f_5	f_1
r_3	r_3	r_4	Id	r_1	r_2	f_5	f_1	f_2	f_3	f_4
r_4	r_4	Id	r_1	r_2	r_3	f_3	f_4	f_5	f_1	f_2
f_1	f_1	f_3	f_5	f_2	f_4	Id	r_3	r_1	r_4	r_2
f_2	f_2	f_4	f_1	f_3	f_5	r_2	Id	r_3	r_1	r_4
f_3	f_3	f_5	f_2	f_4	f_1	r_4	r_2	Id	r_3	r_1
f_4	f_4	f_1	f_3	f_5	f_2	r_1	r_4	r_2	Id	r_3
f_5	f_5	f_2	f_4	f_1	f_3	r_3	r_1	r_4	r_2	Id

God created the integers. All the rest is the work of Man.

- Leopold Kronecker

Remainders mod 5

$Z_5 = \{0,1,2,3,4\}$

$+_5$ = addition modulo 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$(a+_n b)+_n c = a+_n(b+_n c)$

$a+_n 0 = 0+_n a=a$

$a+_n (n-a) = 0$

Integers $\mathbb{Z}$

closed under +

$a+b = b+a$

$(a+b)+c = a+(b+c)$

$a+0 = 0+a=a$

$a+(-a) = 0$

The power of algebra:
Abstract away the inessential features of a problem

=

Let's define an abstract **group**.

Let G be a set.

Let ◊ be a "**binary operation**" on G;

think of it as defining a "multiplication table".

E.g., if G = { a, b, c } then…

◊	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

◊ is a binary operation.

This means that c ◊ a = b.

Definition of an (abstract) **group**

We say G is a "**group** under operation •" if:

0. [Closure] G is closed under •

i.e., $a \bullet b \in G \qquad \forall\, a,b \in G$

1. [Associativity] Operation • is associative:

i.e., $a \bullet (b \bullet c) = (a \bullet b) \bullet c \qquad \forall\, a,b,c \in G$

2. [Identity] There exists an element $e \in G$

(called the "identity element") such that

$a \bullet e = a, \ \ e \bullet a = a \qquad \forall\, a \in G$

3. [Inverse] For each $a \in G$ there is an element $a^{-1} \in G$

(called the "inverse of a") such that

$a \bullet a^{-1} = e, \ \ a^{-1} \bullet a = e$

Examples of (abstract) groups

Any group of transformations is a group.

(Only need to check that composition of functions is associative.)

E.g., the ‘mattress group’ (AKA Klein 4-group)

•	Id	R	F	H
Id	Id	R	F	H
R	R	Id	H	F
F	F	H	Id	R
H	H	F	R	Id

identity element is Id

$R^{-1} = R$

$F^{-1} = F$

$H^{-1} = H$

Examples of (abstract) groups

Any group of transformations is a group.

$\mathbb{Z}$ (the integers) is a group under operation +

Check:

0. + really is a binary operation on $\mathbb{Z}$
1. + is associative: $a+(b+c) = (a+b)+c$
2. "e" is 0: $a+0 = a$, $0+a = a$
3. "a^{-1}" is $-a$: $a+(-a) = 0$, $(-a)+a = 0$

Examples of (abstract) groups

Any group of transformations is a group.

$\mathbb{Z}$ (the integers) is a group under operation $+$

$\mathbb{R}$ (the reals) is a group under operation $+$

$\mathbb{R}^+$ (the positive reals) is a group under $\times$

$Q \setminus \{0\}$ (non-zero rationals) is a group under $\times$

Z_n (the integers mod n) is a group under $+$ modulo n

NONEXAMPLES of groups

G = {all odd integers}, operation $+$

$+$ is not a binary operation on G!

(Natural numbers, +)

No inverses !

$\mathbb{Z}$, operation $-$

$-$ is not associative! & No identity!

$\mathbb{Z} \setminus \{0\}$, operation $\times$

1 is the only possible identity element;

but then most elements don't have inverses!

Permutation property

In a group table,
every row and
every column
is a permutation
of the group elements

Follows from
"cancellation
property"
(which we will
prove shortly)

Dihedral group of size 10

∘	Id	r_1	r_2	r_3	r_4	f_1	f_2	f_3	f_4	f_5
Id	Id	r_1	r_2	r_3	r_4	f_1	f_2	f_3	f_4	f_5
r_1	r_1	r_2	r_3	r_4	Id	f_4	f_5	f_1	f_2	f_3
r_2	r_2	r_3	r_4	Id	r_1	f_2	f_3	f_4	f_5	f_1
r_3	r_3	r_4	Id	r_1	r_2	f_5	f_1	f_2	f_3	f_4
r_4	r_4	Id	r_1	r_2	r_3	f_3	f_4	f_5	f_1	f_2
f_1	f_1	f_3	f_5	f_2	f_4	Id	r_3	r_1	r_4	r_2
f_2	f_2	f_4	f_1	f_3	f_5	r_2	Id	r_3	r_1	r_4
f_3	f_3	f_5	f_2	f_4	f_1	r_4	r_2	Id	r_3	r_1
f_4	f_4	f_1	f_3	f_5	f_2	r_1	r_4	r_2	Id	r_3
f_5	f_5	f_2	f_4	f_1	f_3	r_3	r_1	r_4	r_2	Id

Let’s connect back to Modular arithmetic

Modular arithmetic

Defn: For integers a,b, and positive integer n,
a ≡ b (mod n)   (read: "*a congruent to b modulo n*") means
  (a-b) is divisible by n, or equivalently
  a mod n = b mod n   (x mod n is remainder of x when divided by n, and belongs to {0,1,…,n-1})

Suppose x ≡ y (mod n) and a ≡ b (mod n). Then

1) x + a ≡ y + b (mod n)
2) x * a ≡ y * b (mod n)
3) x - a ≡ y – b (mod n)

So instead of doing +,,- and taking remainders, we can first take remainders and then do arithmetic.*

Modular arithmetic

$(Z_n, +)$ is group (understood that + is $+_n$)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

What about $(Z_5, *)$?
(* = multiplication modulo n)

NOT a group.
1 = candidate for identity, but
0 has no inverse.

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

Okay, what about
$(Z_5^*, *)$ where

$Z_5^* = Z_5 \setminus \{0\} = \{1,2,3,4\}$

Turns out, it *is* a group.

Multiplication table mod 6 for $Z_6 \setminus \{0\} = \{1,2,3,4,5\}$

*	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

2,3,4 have no inverse

NOT a group !

Multiplicative inverse in $Z_n \setminus \{0\}$

Theorem: For $a \in \{1,2,\ldots,n-1\}$, there exists $x \in \{1,2,\ldots,n-1\}$ such that $ax \equiv 1 \pmod{n}$

if and only if

$\gcd(a,n) = 1$

Proof (if) : Suppose $\gcd(a,n)=1$

There exist integers r,s such that

$r\,a + s\,n = 1$ (Extended Euclid)

So $ar \equiv 1 \pmod{n}$.

Take $x = r \bmod n$, $ax \equiv 1 \pmod{n}$ as well.

Multiplicative inverse in $Z_n \setminus \{0\}$

Theorem: For $a \in \{1,2,\ldots,n-1\}$, there exists $x \in \{1,2,\ldots,n-1\}$ such that $ax \equiv 1 \pmod{n}$

<u>if and only if</u>

$\gcd(a,n) = 1$

Proof (only if) : Suppose $\exists x$, $ax \equiv 1 \pmod{n}$

So $ax-1 = nk$ for some integer k.

If $\gcd(a,n)=c$, then c divides $ax-nk$

Since $ax-nk=1$, this means $c=1$.

Recall:

$Z_6 = \{0, 1,2,3,4,5\}$

$Z_6^* = \{1,5\}$

$Z_n^* = \{x \in Z_n \mid \gcd(x,n) =1\}$

Elements in Z_n^* have multiplicative inverses

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Exercise:

Check $(Z_n^*, *)$ is a group

(* is multiplication modulo n)

$Z_{12}^* = \{0 \le x < 12 \mid \gcd(x,12) = 1\}$
$= \{1,5,7,11\}$

$*_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Z_{15}^{*}

*	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Fact:
For prime p, the set $Z_p^* = Z_p \setminus \{0\}$

Proof:
It just follows from the definition!

For prime p, all $0 < x < p$ satisfy $\gcd(x,p) = 1$

Euler Phi Function $\phi(n)$

$\phi(n)$ = size of Z_n^*

= number of integers $1 \leq k < n$ that are relatively prime to n.

p prime

$\Leftrightarrow Z_p^* = \{1,2,3,\ldots,p-1\}$

$\Leftrightarrow \phi(p) = p-1$

Back to abstract groups

Abstract algebra on groups

Theorem 1:

If $(G, \bullet)$ is a group, identity element is unique.

Proof:

Suppose f and g are both identity elements.

Since g is identity, $f \bullet g = f$.

Since f is identity, $f \bullet g = g$.

Therefore $f = g$. ■

Abstract algebra on groups

Theorem 2:

In any group $(G,\bullet)$, inverses are unique.

Proof:

Given $a \in G$, suppose b, c are both inverses of a.

Let e be ***the*** identity element.

By assumption, $a \bullet b = e$ and $c \bullet a = e$.

Now: $c = c \bullet e = c \bullet (a \bullet b)$

$= (c \bullet a) \bullet b = e \bullet b = b$ ∎

Theorem 3 (Cancellation): If a ♦ b = a ♦ c, then b = c

Proof: Multiply on left by a^{-1}

Similarly, b ♦ a = c ♦ a implies b = c

So each row and each column of a group table are permutations of the group elements.

Theorem 3 (Cancellation): If $a \blacklozenge b = a \blacklozenge c$, then $b = c$

Theorem 4:

For all a in group G we have $(a^{-1})^{-1} = a$.

Theorem 5:

For $a,b \in G$ we have $(a \bullet b)^{-1} = b^{-1} \bullet a^{-1}$.

Theorem 6:

In group $(G,\bullet)$, it doesn't matter how you put parentheses in an expression like $a_1 \bullet a_2 \bullet a_3 \bullet \cdot \cdot \cdot \bullet a_k$ ("generalized associativity").

Notation

In abstract groups, it's tiring to always write $\bullet$.

So we often write ab rather than $a \bullet b$.

Sometimes write 1 instead of e for the identity

(When operation is “addition”, write 0 in place of e)

For $n \in \mathbb{N}^+$, write a^n instead of $aaa \cdots a$ (n times).

Also a^{-n} instead of $a^{-1}a^{-1} \cdots a^{-1}$, and a^0 means 1.

(again denote a+ a+ … + a by na for additive groups)

Algebra practice

Problem: In the mattress group {1, R, F, H}, simplify the element $R^2 (H^3 R^{-1})^{-1}$

One (slightly roundabout) solution:

$H^3 = H H^2 = H 1 = H$, so we reach $R^2 (H R^{-1})^{-1}$.

$(H R^{-1})^{-1} = (R^{-1})^{-1} H^{-1} = R H$, so we get $R^2 R H$.

But $R^2 = 1$, so we get $1 R H = R H = F$.

Moral: the usual rules of multiplication, **except**…

Commutativity?

In a group we do NOT NECESSARILY have

$$a \bullet b = b \bullet a$$

Actually, in the mattress group we do have this for all elements; e.g., RF = FR (=H).

Definition:

"a,b∈G commute" means ab = ba.

"G is commutative" means **all** pairs commute.

In group theory, “commutative groups” are usually called **abelian** groups.

Niels Henrik Abel (1802−1829)

Norwegian

Died at 26 of tuberculosis ☹

Age 22: proved there is no quintic formula.

Evariste Galois (1811−1832)

French

Died at 20 in a dual ☹

Laid the foundations
of group theory and Galois theory

Some abelian groups:

"Mattress group" ("Klein 4-group")

Symmetries of a **directed** cycle ("cyclic group")

$(\mathbb{R}, +)$, $(Z_n^*, \times)$

Some nonabelian groups:

Symmetries of an **undirected** cycle ("dihedral group")

Permutation group S_n ("symmetric group on n elements")

Invertible n x n real matrices (under matrix product)

More fun groups:

Matrix groups

$SL_2(\mathbb{Z})$: Set of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

where $a,b,c,d \in \mathbb{Z}$ and $ad-bc=1$.

Operation: matrix mult. Inverses: $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

Application: constructing **expander graphs**, 'magical' graphs crucial for derandomization.

Isomorphism

Here's a group: V = { (0,0), (0,1), (1,0), (1,1) }

+ modulo 2 is the operation

There's something familiar about this group…

V

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

same after renaming:

00↔Id

01↔R

10↔F

11↔H

The mattress group

•	Id	R	F	H
Id	Id	R	F	H
R	R	Id	H	F
F	F	H	Id	R
H	H	F	R	Id

Isomorphism

Groups $(G,\bullet)$ and $(H,\Diamond)$ are "**isomorphic**" if there is a way to rename elements so that they have the same multiplication table.

Formally, bijection $\sigma : G \to H$ such that

$\sigma(a \bullet b) = \sigma(a) \Diamond \sigma(b) \quad \forall a,b \in G$

Fundamentally,
they're the "same" abstract group.

Isomorphism and orders

Obviously, if G and H are isomorphic
we must have $|G| = |H|$.

$|G|$ is called the **order / size** of G.

E.g.: Let C_4 be the group of transformations
preserving the directed 4-cycle.

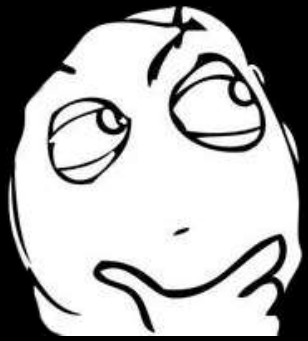
$|C_4| = 4$

Q: Is C_4 isomorphic to the mattress group V ?

Isomorphism and orders

Q: Is C_4 isomorphic to the mattress group V ?

A: No!



$a^2 = 1$ for every element $a \in V$.

But in C_4, $Rot_{90}{}^2 = Rot_{270}{}^2 \neq Rot_{180}{}^2 = Id^2$

Motivates studying powers of elements.

Order of a group element

Let G be a ***finite*** group. Let $a \in G$.

Look at $1, a, a^2, a^3, \ldots$ till you get some repeat.

Say $a^k = a^j$ for some $k > j$.

Multiply this equation by a^{-j} to get $a^{k-j} = 1$.

So the first repeat is always 1.

Definition: The order of x, denoted ord(a), is the smallest $m \geq 1$ such that $a^m = 1$.

Note that $a, a^2, a^3, \ldots, a^{m-1}, a^m=1$ all distinct.

Examples:

In mattress group (order 4),

ord(Id) = 1,   ord(R) = ord(F) = ord(H) = 2.

In directed-4-cycle group (order 4),

ord(Id) = 1, ord(Rot_{180}) = 2, ord(Rot_{90}) = ord(Rot_{270}) = 4.

In dihedral group of order 10

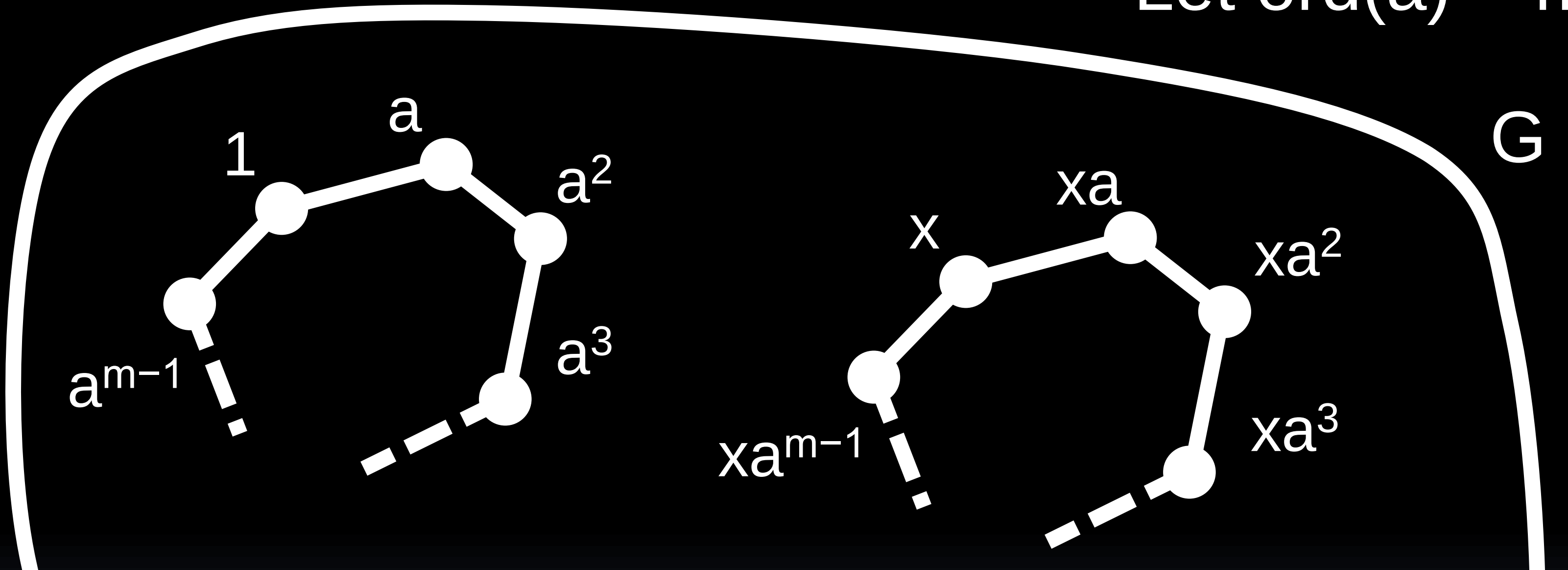
(symmetries of undirected 5-cycle)

ord(Id) = 1, ord(any rotation) = 5, ord(any reflection) = 2.

Order Theorem: For a finite group G & a $\in$ G

ord(a) always divides |G|.

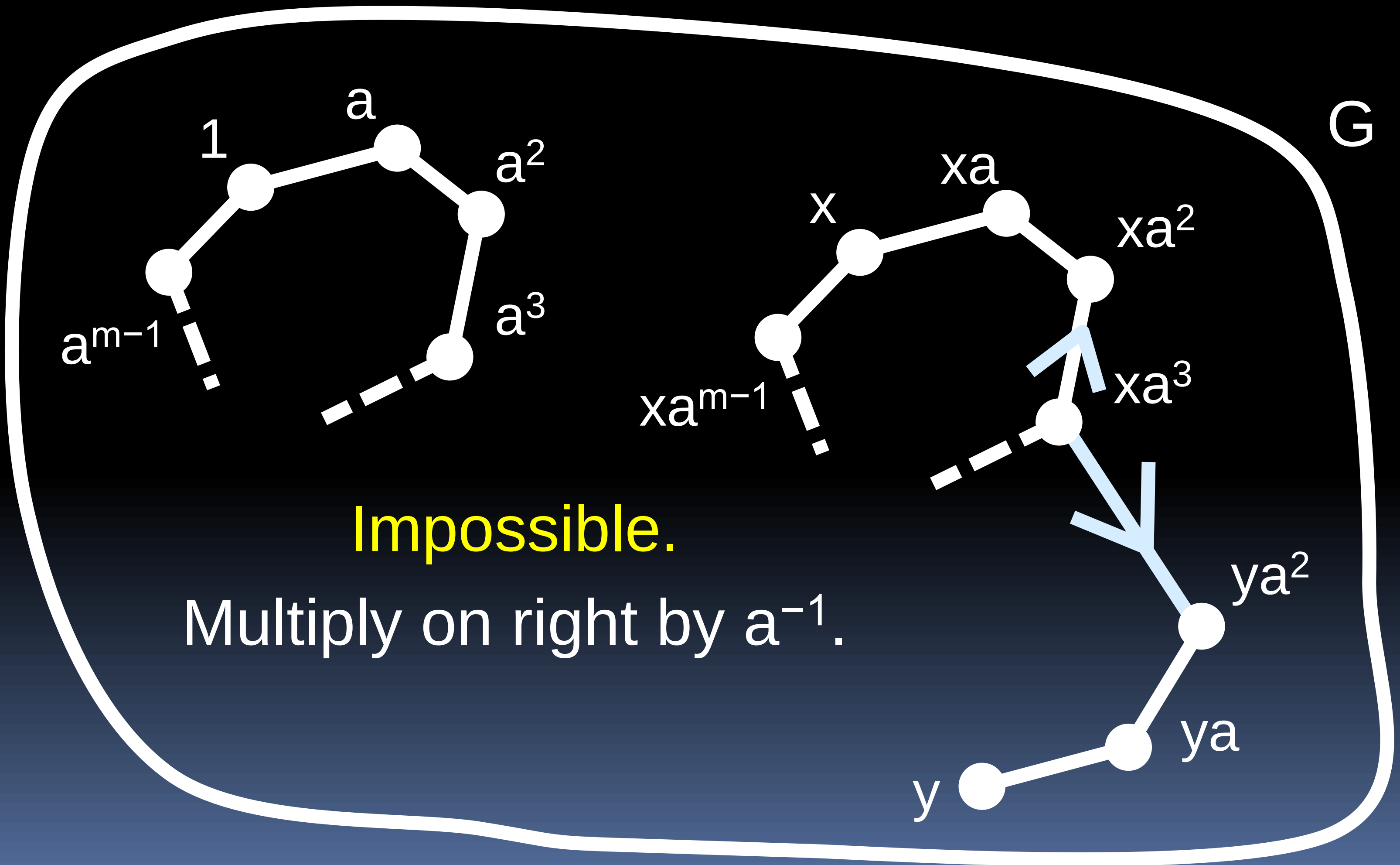
Let ord(a) = m.



Claim: also of length m.

Because $xa^j = xa^k \Rightarrow a^j = a^k$.

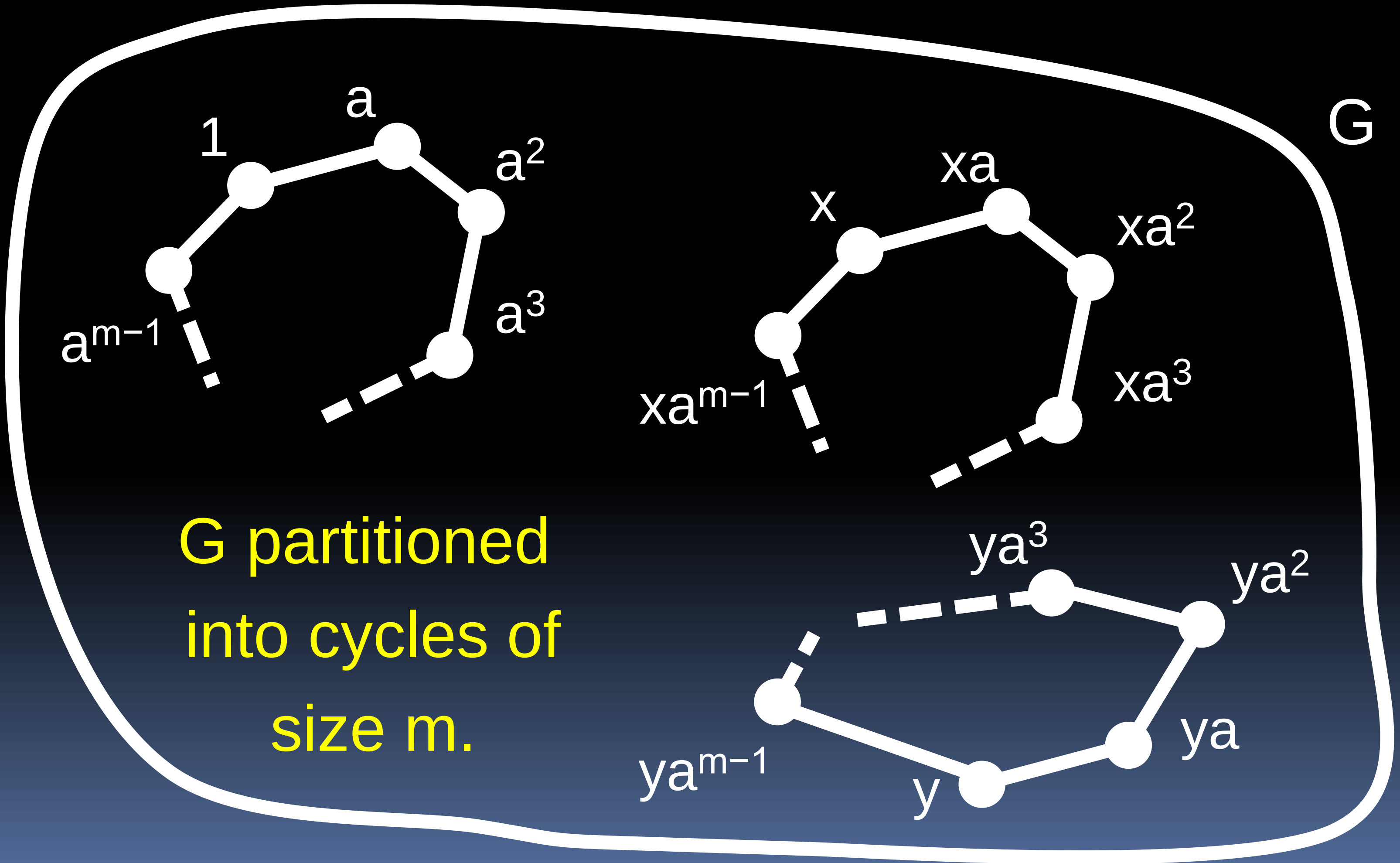
Order Theorem: ord(a) always divides |G|.



Impossible.

Multiply on right by a^{-1}.

Order Theorem: $\forall a \in G$, ord(a) divides |G|.



Order Theorem: ord(a) always divides |G|.

Corollary: If |G| = n, then $a^n=1$ for all $a \in G$.

Proof: Let ord(a) = m. Write n = mk.

Then $a^n = (a^m)^k = 1^k = 1$.

Corollary: Euler's Theorem: For $a \in Z_n^*$, $a^{\phi(n)} = 1$

That is, if gcd(a,n)=1, then $a^{\phi(n)} \equiv 1 \pmod{n}$

Corollary (Fermat's little theorem):

For prime p, if gcd(a,p)=1, then

$a^{p-1} \equiv 1 \pmod{p}$

Cyclic groups

A finite group G of order n is cyclic if
G= $\{e,b,b^2,\ldots,b^{n-1}\}$ for some group element b

In such a case, we say the element b ***"generates"*** G,
or b is a *"generator"* of G.

Examples:

- $(Z_n, +)$ What is a generator?
- C_4 (Symmetries of directed 4-cycle)

Non-examples: Mattress group;
any non-abelian group.

How many generators does $(Z_n, +)$ have?

Answer: $\phi(n)$

b generates $Z_n \Leftrightarrow \exists$ a s.t. ba $\equiv$ 1 (mod n)

(ba = b+b+…+b (a times))

Same holds for *any* cyclic group with n elements

Subgroups

Q: Is (Even integers, +) a group?

A: Yes. It is a "subgroup" of $(\mathbb{Z},+)$

Definition: Suppose $(G, \bullet)$ is a group.

If $H \subseteq G$, and if $(H,\bullet)$ is also a group,

then H is called a subgroup of G.

To check H is a subgroup of G, check:

1. H is closed under $\bullet$
2. $e \in H$
3. If $h \in H$ then $h^{-1} \in H$
   - (3^{rd} condition follows from 1,2 if H is finite)

Examples

Every G has two trivial subgroups: {e}, G

Rest are called "proper" subgroups

Suppose k, $1 < k < n$, divides n.

Q1. Is ({0, k, 2k, 3k, …, (n/k-1)k}, $+_n$) subgroup of (Z_n,$+_n$) ?

Yes!

Q2. Is (Z_k, $+_k$) a subgroup of (Z_n, $+_n$)?

No! it doesn't even have the same operation

Q3. Is (Z_k, $+_n$) a subgroup of (Z_n, $+_n$)?

No! Z_k is not closed under $+_n$

Lagrange's Theorem

Theorem: If G is a finite group, and H is a subgroup then

$|H|$ divides $|G|$.

Proof similar to order theorem.

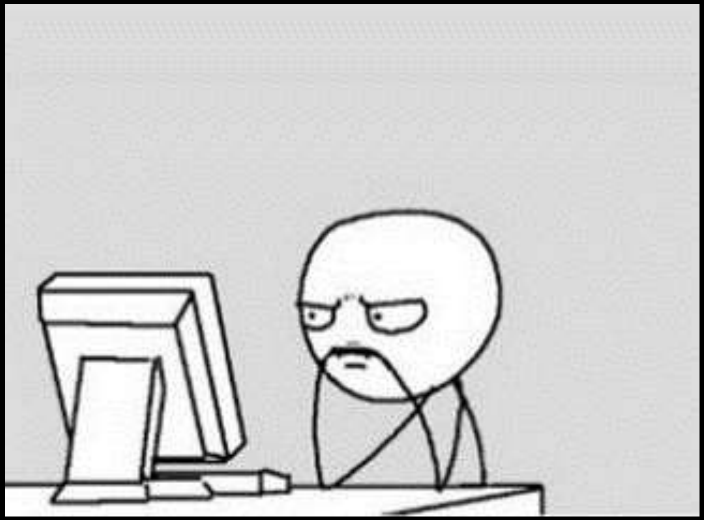
Corollary (order theorem): If $x \in G$, then ord(x) divides $|G|$.

Proof of Corollary:

Consider the set $T_x = (x, x^2, x^3, \ldots)$

(i) $\text{ord}(x) = |T_x|$

(ii) $(T_x, \bullet)$ is a subgroup of $(G, \bullet)$ (check!)



Study Guide

Definitions:

Groups; Commutative/abelian

Isomorphism ; order of elements; subgroups

Specific Groups:

Klein 4-, cyclic, dihedral, symmetric, number-theoretic.

Doing:

Checking for "groupness"

Computations in groups

Theorem/proof:

Order Theorem; Lagrange Thm

Modular arithmetic

Euler theorem

More fun groups:

Quaternion group

$Q_8 = \{ 1, -1, i, -i, j, -j, k, -k \}$

Multiplication defined by: 1 is the identity

$(-1)^2 = 1, \quad (-1)a = a(-1) = -a$

$i^2 = j^2 = k^2 = -1$

$ij = k, \quad ji = -k$

$jk = i, \quad kj = -i$

$ki = j, \quad ik = -j$

Exercise: valid defn. of a (nonabelian) group.

Application to computer graphics

"Quaternions": expressions like

$$3.2 + 1.4i - .5j + 1.1k$$

which generalize complex numbers ($\mathbb{C}$).

Let (x,y,z) be a unit vector, θ an angle, let

$$q = \cos(\theta/2) + \sin(\theta/2)x\, i + \sin(\theta/2)y\, j + \sin(\theta/2)z\, k$$

Represent **p=**(a,b,c) in 3D space by quaternion P= a i + b j + c k

Then qPq^{-1} is its rotation by angle θ around axis (x,y,z).