15-251: Great Theoretical Ideas in Computer Science
Fall 2018, Lecture 22

Group Theory

Group Theory

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

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

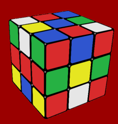
What is group theory good for?

In theoretical computer science:

- Cryptography: Fully homomorphic encryption, obfuscation…
- Quantum algorithms
- Mulmuley's approach to **P** vs. **NP**
- Checksums, error-correction schemes
- Minimizing space usage of algorithms
- Derandomization

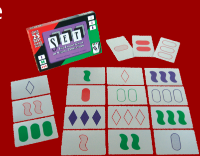
What is group theory good for?

In puzzles and games:

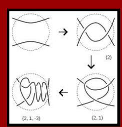


"15 Puzzle"

Rubik's Cube



SET



Tangles

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:

$$-\frac{1}{4}\frac{b}{a}+\frac{1}{2}\left(\frac{1}{4}\frac{b^2}{a^2}-\frac{2}{3}\frac{c}{a}+\frac{1}{6}\frac{\left(-288eca+108d^2a+108eb^2-36bcd+8c^3+12\sqrt{-768a^3e^3+576a^2bde^2+384a^2c^2e^2-432a^2cd^2e+81a^2d^4-432ab^2ce^2+18ab^2d^2e+240abc^2de-54abcd^3-48ac^4e+12ac^3d^2+81b^4e^2-54b^3cde+12b^3d^3+12b^2c^3e-3b^2c^2d^2}\right)^{1/3}}{a}+\frac{2}{3}\frac{12ae-3bd+c^2}{a\left(-288eca+108d^2a+108eb^2-36bcd+8c^3+12\sqrt{-768a^3e^3+576a^2bde^2+384a^2c^2e^2-432a^2cd^2e+81a^2d^4-432ab^2ce^2+18ab^2d^2e+240abc^2de-54abcd^3-48ac^4e+12ac^3d^2+81b^4e^2-54b^3cde+12b^3d^3+12b^2c^3e-3b^2c^2d^2}\right)^{1/3}}\right)^{1/2}+\frac{1}{2}\left(\frac{1}{2}\frac{b^2}{a^2}-\frac{4}{3}\frac{c}{a}-\frac{1}{6}\frac{\left(-288eca+108d^2a+108eb^2-36bcd+8c^3+12\sqrt{-768a^3e^3+576a^2bde^2+384a^2c^2e^2-432a^2cd^2e+81a^2d^4-432ab^2ce^2+18ab^2d^2e+240abc^2de-54abcd^3-48ac^4e+12ac^3d^2+81b^4e^2-54b^3cde+12b^3d^3+12b^2c^3e-3b^2c^2d^2}\right)^{1/3}}{a}-\frac{2}{3}\frac{12ae-3bd+c^2}{a\left(-288eca+108d^2a+108eb^2-36bcd+8c^3+12\sqrt{-768a^3e^3+576a^2bde^2+384a^2c^2e^2-432a^2cd^2e+81a^2d^4-432ab^2ce^2+18ab^2d^2e+240abc^2de-54abcd^3-48ac^4e+12ac^3d^2+81b^4e^2-54b^3cde+12b^3d^3+12b^2c^3e-3b^2c^2d^2}\right)^{1/3}}+\left(\frac{cb}{a^2}-\frac{2d}{a}-\frac{1}{4}\frac{b^3}{a^3}\right)\Big/\left(\frac{1}{4}\frac{b^2}{a^2}-\frac{2}{3}\frac{c}{a}+\frac{1}{6}\frac{\left(-288eca+108d^2a+108eb^2-36bcd+8c^3+12\sqrt{-768a^3e^3+576a^2bde^2+384a^2c^2e^2-432a^2cd^2e+81a^2d^4-432ab^2ce^2+18ab^2d^2e+240abc^2de-54abcd^3-48ac^4e+12ac^3d^2+81b^4e^2-54b^3cde+12b^3d^3+12b^2c^3e-3b^2c^2d^2}\right)^{1/3}}{a}+\frac{2}{3}\frac{12ae-3bd+c^2}{a\left(-288eca+108d^2a+108eb^2-36bcd+8c^3+12\sqrt{-768a^3e^3+576a^2bde^2+384a^2c^2e^2-432a^2cd^2e+81a^2d^4-432ab^2ce^2+18ab^2d^2e+240abc^2de-54abcd^3-48ac^4e+12ac^3d^2+81b^4e^2-54b^3cde+12b^3d^3+12b^2c^3e-3b^2c^2d^2}\right)^{1/3}}\right)^{1/2}\right)^{1/2}$$

(That's just the first of four roots, actually.)

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.

What is group theory good for?

In entertainment:

Driving the plot of S06E10 of Futurama,

“The Prisoner of Benda”

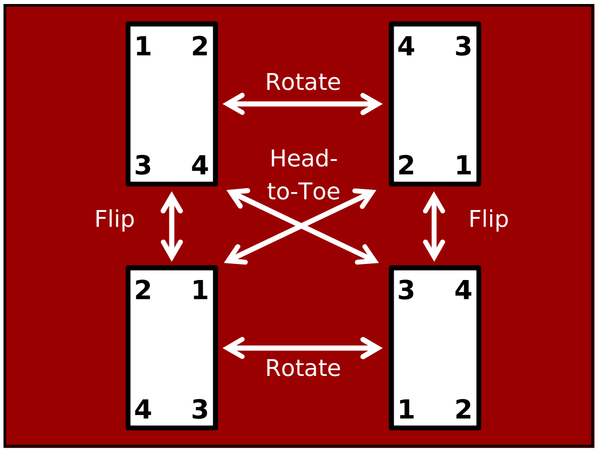
So: What **is** group theory?

Rotate


Flip

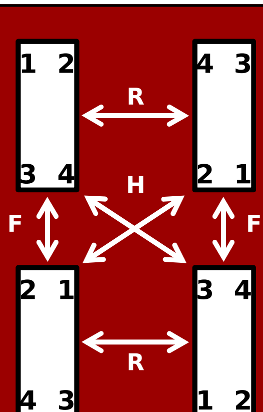

Head-to-Toe flip


Q: How many positions can it be in?
A: Four.



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)

$F \circ R = H$

$H \circ F = R$

$R \circ F \circ H = Id$

$R \circ Id \circ H \circ F \circ H = H$

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 → 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

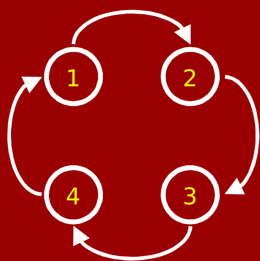
X = set of all physical points of the mattress

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

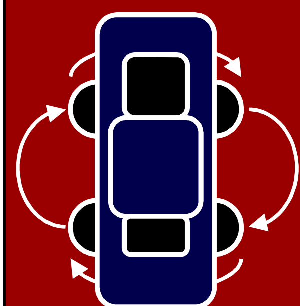
|X| = 24

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 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

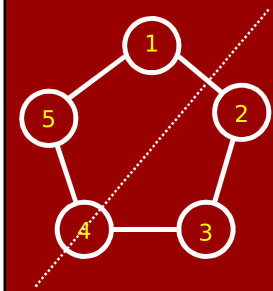
G = { **Id**, $\mathbf{Rot_{90}}$, $\mathbf{Rot_{180}}$, $\mathbf{Rot_{270}}$ }

Check the 3 conditions:

1. If **p** and **q** are in G then so is $\mathbf{p} \circ \mathbf{q}$. ✔
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



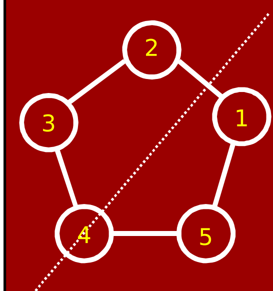
X = labelings of the vertices by 1,2, …, n

|X| = n!

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

|G| = 2n

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



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

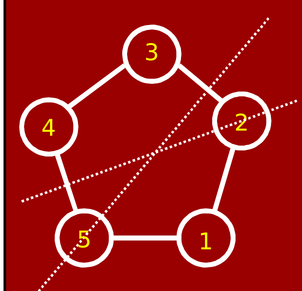
|X| = n!

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

|G| = 2n

+ one clockwise twist

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



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

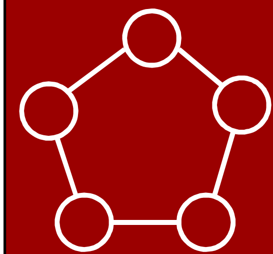
|X| = n!

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

|G| = 2n

+ 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"

Example: "All permutations"

X = {1, 2, …, n}

G = all permutations of X

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

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

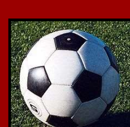
"Symmetric group, Sym(n)"

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.



|G| = 60

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

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

$$F \circ R = H$$

$$H \circ F = R$$

$$R \circ F \circ H = Id$$

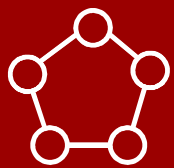
$$R \circ Id \circ H \circ F \circ H = H$$

The laws of mattress rotation

G = { Id, R, F, H }

$Id \circ Id = Id$	$F \circ Id = F$
$Id \circ R = R$	$F \circ R = H$
$Id \circ F = F$	$F \circ F = Id$
$Id \circ H = H$	$F \circ H = R$
$R \circ Id = R$	$H \circ Id = H$
$R \circ R = Id$	$H \circ R = F$
$R \circ F = H$	$H \circ F = R$
$R \circ H = F$	$H \circ H = Id$

The laws of the dihedral group of size 10



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

∘	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 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 $c \circ a = b$.

Definition of an (abstract) **group**

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

1. Operation ∘ is **associative**:

   i.e., $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall\, a,b,c \in G$

2. There exists an element $e \in G$

   (called the "identity element") such that

   $a \circ e = a, \; e \circ a = a \quad \forall\, a \in G$

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

   (called the "inverse of a") such that

   $a \circ a^{-1} = e, \; a^{-1} \circ a = e$

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 ×

$\mathbb{R} \setminus \{0\}$ is a group under ×

$\mathbb{Z}_n$ (the integers mod n) is a group under +

NONEXAMPLES of groups

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

$+$ is not a binary operation on G!

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

$-$ is not associative!

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

1 is the only possible identity element;
but then most elements don't have inverses!

Abstract algebra on groups

Theorem 1:
If $(G, \circ)$ is a group, identity element is unique.

Proof:
Suppose f and g are both identity elements.
Since g is identity, $f \circ g = f$.
Since f is identity, $f \circ g = g$.
Therefore $f = g$. ■

Abstract algebra on groups

Theorem 2:
In any group $(G, \circ)$, inverses are unique.

Proof:
Given $a \in G$, suppose b, c are both inverses of a.
Let e be **the** identity element.
By assumption, $a \circ b = e$ and $c \circ a = e$.
Now: $c = c \circ e = c \circ (a \circ b)$

$= (c \circ a) \circ b = e \circ b = b$ ■

Abstract algebra on groups

Theorem 3:
For all a in group G we have $(a^{-1})^{-1} = a$.

Theorem 4:
For $a,b \in G$ we have $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Theorem 5:
In group $(G,\circ)$, it doesn't matter how you put parentheses in an expression like

$$a_1 \circ a_2 \circ a_3 \circ \cdots \circ a_k$$

("generalized associativity").

Notation

In abstract groups, it's tiring to always write $\circ$. So we often write ab rather than $a \circ b$.

Sometimes write 1 instead of e for the identity.

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.

Then $a^j a^k = a^{j+k}$ holds for all $j,k \in \mathbb{Z}$.

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 ∘ b = b ∘ 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 duel ☹

One of the main inventors of group theory.

Some abelian groups:

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

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

($\mathbb{R}$, +)

Some nonabelian groups:

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

Motions of 3D space

Sym(n) ("symmetric group on n elements")

Another fun group: Quaternion group

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

Multiplication defined by:

1 is the identity

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

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

$ij = k$, $ji = -k$

$jk = i$, $kj = -i$

$ki = j$, $ik = -j$

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

Application to computer graphics

"Quaternions": expressions like

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

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

Suppose we store points (x,y,z) in 3D space as quaternions $xi + yj + zk$.

To rotate point p an angle of θ around an axis defined by unit vector (u,v,w), let

$q = \cos(\theta/2) + \sin(\theta/2)u\,i + \sin(\theta/2)v\,j + \sin(\theta/2)w\,k.$

Then the rotated point is qpq^{-1}.

Isomorphism

Here's a group: V = { 00, 01, 10, 11 }
⊕ (bitwise XOR) 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

∘	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,∘) and (H,•) are "**isomorphic**" if there is a way to rename elements so that they have the same multiplication table.

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** of G.

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

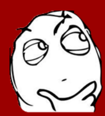
$|C_4| = 4$

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 a, denoted $|a|$, is the smallest $m \geq 1$ such that $a^m = 1$.

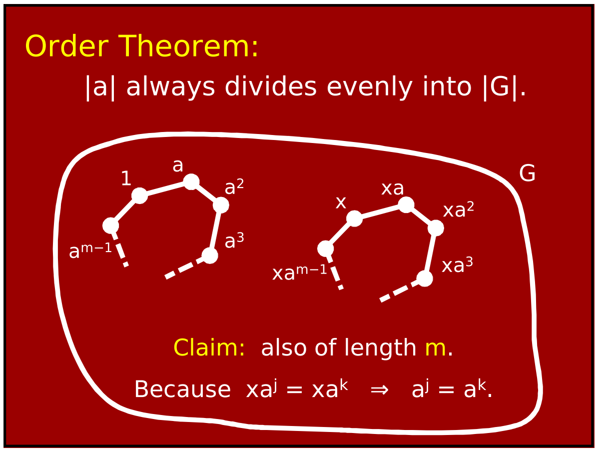
Note that $a, a^2, a^3, \ldots, a^{m-1}, a^m=1$ all distinct.

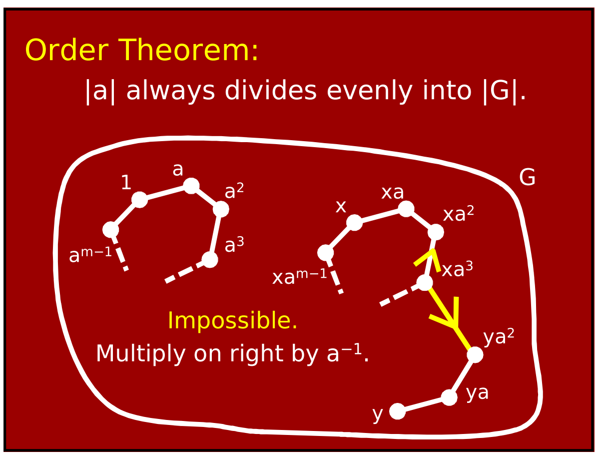
Examples:

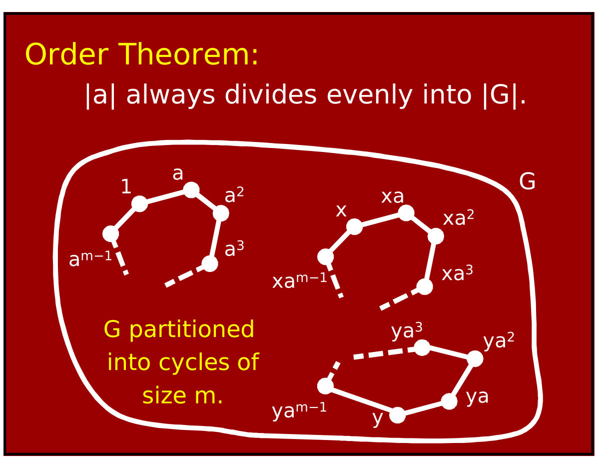
In mattress group (order 4),
$|Id| = 1$, $|R| = |F| = |H| = 2$.

In directed-4-cycle group (order 4),
$|Id| = 1$, $|Rot_{180}| = 2$, $|Rot_{90}| = |Rot_{270}| = 4$.

In dihedral group of order 10
(symmetries of undirected 5-cycle)
$|Id| = 1$, $|\text{any rotation}| = 5$, $|\text{any reflection}| = 2$.


Order Theorem:
|a| always divides evenly into |G|.
G
1
a
a²
a³
aᵐ⁻¹
x
xa
xa²
xa³
xaᵐ⁻¹
Claim: also of length m.
Because xaʲ = xaᵏ ⇒ aʲ = aᵏ.


Order Theorem:
|a| always divides evenly into |G|.
G
1
a
a²
a³
aᵐ⁻¹
x
xa
xa²
xa³
xaᵐ⁻¹
ya²
ya
y
Impossible.
Multiply on right by a⁻¹.


Order Theorem:
|a| always divides evenly into |G|.
G
1
a
a²
a³
aᵐ⁻¹
x
xa
xa²
xa³
xaᵐ⁻¹
ya³
ya²
ya
y
yaᵐ⁻¹
G partitioned
into cycles of
size m.

Order Theorem:

|a| always divides evenly into |G|.

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

Proof: Let |a| = m. Write n = mk.

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

A Group Theory Application

Check Digits

Say you have important strings of digits:

credit card numbers
EFT routing numbers
UPC numbers
money serial numbers
book ISBNs

People screw up when transcribing them.

Check Digits

Most common human screwups:

single digit wrong (e.g., 6→8):	60-90%
omitting/adding digit:	10-20%
transposition (e.g., 35→53):	10-20%
other screwups:	≤ 5%

Instead of making them n random digits, make them n random digits + a 'check digit'.

Check Digits

Example: Book ISBNs before 2007.

Desired id#: 1 3 6 0 4 2 9 9 4 **7**

10 9 8 7 6 5 4 3 2

dot-prod mod 11: $1\times10+3\times9+6\times8+0\times7+4\times6+2\times5+9\times4+9\times3+8\times2 = 4$

check digit: top it off to get 0 mod 11

Pros: You can detect any single-digit or transposition error.

Check Digits

Example: Book ISBNs before 2007.

Desired id#: 1 3 6 0 4 2 9 9 4 **7**

10 9 8 7 6 5 4 3 2

dot-prod mod 11: $1\times10+3\times9+6\times8+0\times7+4\times6+2\times5+9\times4+9\times3+8\times2 = 4$

check digit: top it off to get 0 mod 11

Cons: Um, check digit should be 10? "Write X"!
Doesn't scale if you want longer id#'s.

Verhoeff Check Digit Method

Encode digits by elements of dihedral group of order 10.

Let σ be the permutation $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix}$

Given a desired id# $a_0\, a_1\, a_2 \cdots a_{n-1}$,
choose unique check digit a_n satisfying group equation

$$enc(\sigma^0(a_0)) \circ enc(\sigma^1(a_1)) \circ enc(\sigma^2(a_2)) \circ \cdots \circ enc(\sigma^n(a_n)) = e$$

Pros: Detects single-digit & transposition errors.
Uses just digits 0, 1, 2, …, 9.
Scales to any length of id#.

Verhoeff Check Digit Method

Encode digits by elements of dihedral group of order 10.

Let σ be the permutation $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix}$

Given a desired id# $a_0\, a_1\, a_2 \cdots a_{n-1}$,
choose unique check digit a_n satisfying group equation

$$enc(\sigma^0(a_0)) \circ enc(\sigma^1(a_1)) \circ enc(\sigma^2(a_2)) \circ \cdots \circ enc(\sigma^2(a_n)) = e$$

Cons: Can’t really be done by a human.

Verhoeff Check Digit Method

Encode digits by elements of dihedral group of order 10.

Let σ be the permutation $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix}$

Given a desired id# $a_0\, a_1\, a_2 \cdots a_{n-1}$,
choose unique check digit a_n satisfying group equation

$$enc(\sigma^0(a_0)) \circ enc(\sigma^1(a_1)) \circ enc(\sigma^2(a_2)) \circ \cdots \circ enc(\sigma^2(a_n)) = e$$

Is this really a con?
What human manually checksums credit cards?
We have computers, you know.

Verhoeff Check Digit Method

Nevertheless, it's like the Dvorak keyboard of check digit methods. ☹

German federal bank started using it for Deutsche Marks (with some letters?) in 1990.

Then they went and got the euro (which uses a different scheme).

The 10 is a good denomination for mathematicians.

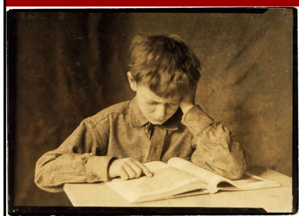
Leonhard Euler on the back of the old 10 Swiss franc note.

The 10 is a good denomination for mathematicians.

I do not know how this works.

Cahit Arf and an equation in the group $\mathbb{Z}_2$ starring on the back of a Turkish 10 lira.

Study Guide



Definitions:
- Groups
- Commutative/abelian
- Isomorphism
- Order

Groups:
- Klein 4-, cyclic, dihedral, symmetric, quaternions

Doing:
- Checking for groupness
- Computations in groups

Theorem/proof:
- Order Theorem