BMC Advanced: Group Theory

Daniel Rostamloo (drostamloo@berkeley.edu)

Motivating Problem:

We have a cube, and 6 colors to assign to each face.

Q: How many colorings?

What is group theory? What is (modern) algebra?

Set theory:

Set - collection of objects, $\emptyset$

- $\{a, b\} = \{b, a\}$
- $\{a, a\} = \{a\}$
- $X = Y \iff \forall a \in X,\ a \in Y$

  also $\forall b \in Y,\ b \in X$

- φ, e.g. $x > 1$,

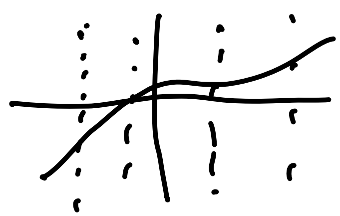
  $\{x \in \mathbb{Z} \mid x > 1\} \subset \mathbb{Z}$

- $X \cup Y$, $X \cap Y$

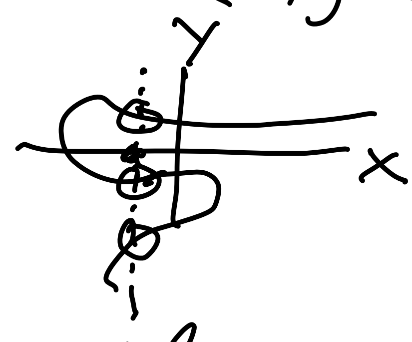
- Def: A <u>binary relation</u> R between X, Y is a subset of $\underbrace{X \times Y}$

  (Cartesian product, (x,y))

- Def: A function f from $X \longrightarrow Y$ is a b.r. s.t. $\forall x \in X$, $\exists!\, y \in Y$ s.t. $(x,y) \in f$



e.g. nonexample



- If $Z \subset X$, then $f|_Z$ is a function

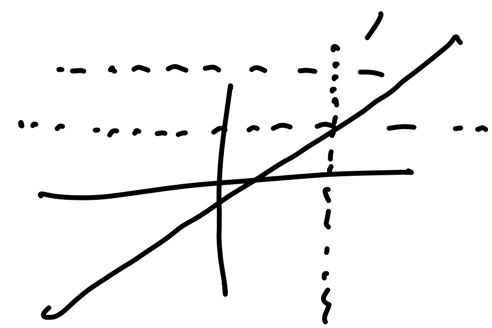
$$f|_Z = \{(x,y) \in f \mid x \in Z\}$$

- $\operatorname{img}(f) := \{ y \in Y \mid \exists x \in X, \ (x,y) \in f \}$
- Given $Z \subset Y$, $f^{-1}(Z) := \{ x \in X \mid \exists y \in Z \ (x,y) \in f \}$
- Def: $f : X \to Y$ is <u>injective</u> if $\forall x_1, x_2 \in X$,

  $f(x_1) = f(x_2) \implies x_1 = x_2$.
- Def: f is <u>surjective</u> if $\forall y \in Y$

  $\exists x \in X$ s.t. $f(x) = y$.

e.g.



- Def: f is a <u>bijection</u> $\iff$ f inj. and surj.

- Def: An <u>equivalence relation</u> R, $\sim$

$(x \sim y \iff (x,y) \in R)$

between X and X is a b.r. s.t.

1) reflexivity: $\forall x \in X$, $(x,x) \in R$

2) Symmetry: $\forall x, y \in X$ s.t. $(x,y) \in R$
$\implies (y,x) \in R$

3) Transitivity: if $(x,y), (y,z) \in R \implies (x,z) \in R$

Def: Given an équivalence rel. R on X, the <u>equivalence class</u> of $x \in X$ is

$$[x] := \{ y \in X \mid (x,y) \in R \}$$

$[y]$, we know $y \in [y]$,

Fact: $\forall (x,y) \in R$, then $[x] = [y]$

Pf: Need to show $[x] \subset [y]$, and $[y] \subset [x]$.

Let $t \in [x]$, then $(x,t) \in R$.

But also, $(y,x) \in R$. $\Longrightarrow (y,t) \in R$.

$t \in [y]$, $[x] \subset [y]$. $\square$

Easy check: If $f: X \to Y$ is a function, then the relation $R = \{(x, x') \mid f(x) = f(x')\}$ is an eq. rel.

- $X = \mathbb{Z}$, $R = \{(x,y) \mid x - y \text{ is even}\}$.

Also an eq. rel.

Groups: Think of as symmetries

"Symmetry":

- Combining two symmetries should be a sym.
- Doing nothing is a sym.
- Any sym. should be invertible.

$\boxed{\text{Def:}}$ A group is a set G, together with a function $m : G \times G \to G$

$(a,b) \mapsto ab$

i) Associativity:

$\forall g,h,k \in G$, $m(m(g,h),k) = m(g, m(h,k))$

$(2 \cdot 3) \cdot 4 = 2 \cdot (3 \cdot 4)$

ii) Identity: $\exists e \in G$ s.t. $\forall g \in G$

$ge = g = eg$ $\quad f \circ g$

iii) $\forall g \in G$ $\exists h \in G$ s.t. $gh = hg = e$

$h = g^{-1}$

- Another def: A group (G, m) is <u>abelian</u> iff $\forall\, a, b \in G$, $a \cdot b = b \cdot a$

$$\underbrace{(G, m)}_{G,\ a \overset{m}{\cdot} b \,=\, \overbrace{ab}^{h \in G}}$$

- Klein-4 Viergrup

$$G = \{\overset{\text{identity}}{e}, \underbrace{a, b, c}_{h}\}$$

gh	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Exercise: Check group axioms for

$$G = K = K_4$$

$$(= V?)$$

- Symmetric group on a set X.

$G := \mathrm{Sym}(X) := \{\text{bijection } X \to X\}$,

and "multiplication" is function composition.

- Closure: given bijections $f, g \in \mathrm{Sym}(X)$.

$f \circ g$ is bijective. Injectivity:

$(f \circ g)(x) = (f \circ g)(x')$ WTS $x = x'$

$f(g(x)) = f(g(x')) \implies g(x) = g(x')$.

$\implies x = x'$. ✓

Surj: Suppose $x \in X$, WTS $\exists x' \in X$ s.t. $(f \circ g)(x') = x$.

$\left.\begin{aligned} &\exists a \in X \quad \text{s.t.} \quad f(a) = x. \\ &\exists x' \in X \quad \text{s.t.} \quad g(x') = a \end{aligned}\right\}$

$\Longrightarrow \quad f(g(x')) = x.$

$\Longrightarrow (f \circ g)(x') = x \longrightarrow (f \circ g)$ is surj.

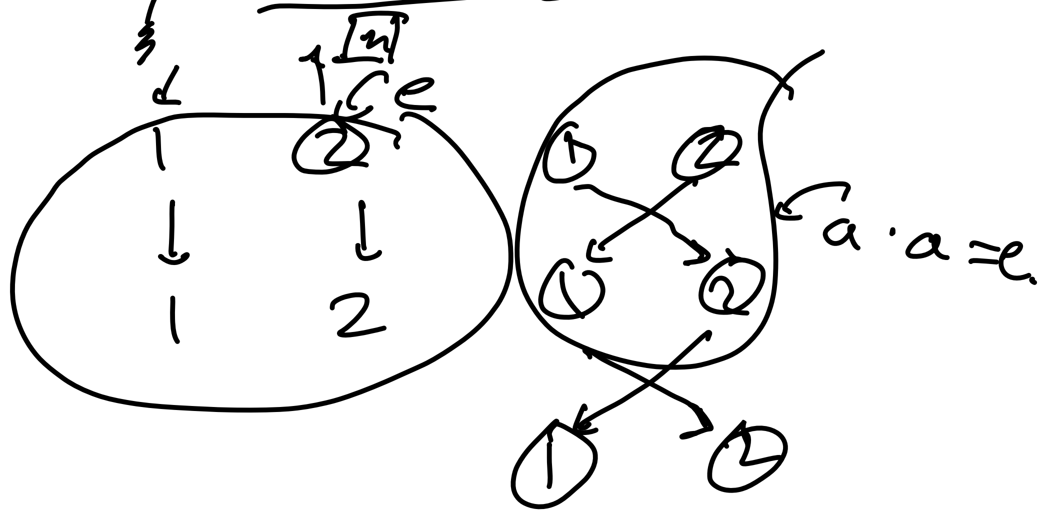
- Assoc. ✓
- Identity. ✓
- Inverses. ✓

Ex:

$\mathrm{Sym}(\{1\})$ is the trivial gp. $= \{e\}$.

$$\mathrm{Sym}(\{1,2\}) = \{e, a\}$$

where $a = a^{-1}$



Sym_n

Facts about groups:

Identity is unique:

$\exists\, e', e$ s.t. $eg = ge = g \quad \forall g \in G$

$e'g = ge' = g$

$\Longrightarrow \underline{e = ee' = e'}$

- Inverses are unique: g, $\exists\, h, h'$ s.t.

$gh = hg = e$
$gh' = h'g = e$. $\Longrightarrow h = h \cdot e = h \cdot (gh')$
$= (hg) \cdot h' = e \cdot h' = h'$

· Cancellation: $gx = gy$

$$g^{-1}(gx) = g^{-1}(gy) \Rightarrow x = y$$

$gx = yg$. ???

Subgroups:

· Facts: · $(g^{-1})^{-1} = g \longrightarrow gg^{-1} = g^{-1}g = e$

· $(ab)^{-1} = b^{-1}a^{-1} \longrightarrow (ab)(b^{-1}a^{-1})$

$$\parallel$$

$$a(bb^{-1})a^{-1} = a \cdot e \cdot a^{-1}$$
$$= a \cdot a^{-1} = e$$

Def: For G a group, a subset $H \subseteq G$ is called a <u>subgroup</u> of G if the gp. operation restricted to $H \times H \subseteq G \times G$ make H into a group. Denote $H \leq G$

$\subset \sim \subseteq$, $\subsetneq$

· Klein-4 Viergrup

$$G = \{\overset{\text{identity}}{e}, \underbrace{a, b, c}_{h}\}$$

gh	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

g

Subgps:

1-element subgp : $\{e\}$ ✓

2 — " " : $\{e,a\}$, $\{e,b\}$, $\{e,c\}$

Thm: (subgp. criterion)

A nonempty subset H of G is a subgp.

$\Longleftrightarrow \forall x, y \in H \quad x \cdot y^{-1} \in H$

Pf: ($\Longleftarrow$)

1) Let $h \in H$, let $(x, y) = (h, h)$.

$h \cdot h^{-1} = e \in H$ (identity ✓)

2) Set $(x, y) = (e, h)$. Then $x y^{-1} = e \cdot h^{-1} = h^{-1} \in H$.

$\Longrightarrow$ (inverses ✓)

3) If $h, k \in H$ $(x, y) = (h, k^{-1})$.

$\Longrightarrow h \cdot (k^{-1})^{-1} = h \cdot k \in H$.

$\Longrightarrow H \leq G$

Def: A group is:

A set G with m an operation

(a function $G \times G \to G$)

1) identity e s.t.

$$\forall g \quad m(e,g) = m(g,e) = g$$

$$e \cdot g = g \cdot e = g$$

2) inverses

$$\forall g \in G \ \exists g^{-1} \text{ s.t. } g g^{-1} = g^{-1} g = e$$

3) Associativity

$$\forall g, h, k \in G \quad (g \cdot h) \cdot k = g \cdot (h \cdot k)$$

e.g. $\mathrm{Sym}_n :=$ { the set of bijections on $\{1, 2, 3, \dots, n\}$ }.

$$\{1, 2, 3, \dots, n\}$$
$$\{1, 2, 3, \dots, n\}$$

f : Bijection $\iff$ Inj., Surj.

f Inj $\iff \big(f(a) = f(b) \implies a = b \big)$

f Surj. iff. $\big(\forall b \in \{1, 2, \dots, n\},\ \exists a \in$ s.t. $f(a) = b \big)$.

Def: A homomorphism $\varphi : G \to H$ is a function $G \to H$ s.t.

$$\forall g, h \in G, \quad \varphi(\underset{\substack{\uparrow \\ \text{mult.} \\ \text{in } G}}{gh}) = \underbrace{\varphi(g) \cdot \varphi(h)}_{\substack{\uparrow \\ \text{mult. in } H.}}.$$

Note: $\varphi(e_G) = e_H$.

$$\varphi(g) = \varphi(e_G \cdot g) = \varphi(e_G) \cdot \varphi(g)$$

$$\Rightarrow \quad \varphi(g) = \varphi(e_G) \cdot \varphi(g) \qquad \forall g \in G$$

$$\varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) = \varphi(e_G).$$

$$\underbrace{(\varphi(e_G))^{-1} \cdot \varphi(e_G)}_{e_H} \cdot \varphi(e_G) = \underbrace{(\varphi(e_G)^{-1}) \cdot \varphi(e_G)}_{e_H}$$

$$\Longrightarrow \varphi(e_G) = e_H.$$

Similarly,

$$\varphi(g^{-1}) = (\varphi(g))^{-1}.$$

Exercise in proofs.

$\varphi : G \to \{e\}$ is a homorphism for ANY function $\varphi : G \to \{e\}$.

Thm: If $\varphi : G \to H$ is a hom. and $K \leq H$, then $\varphi^{-1}(K) \leq G$

$$\varphi^{-1}(K) = \{g \in G \mid \varphi(g) \in K\}.$$

Pf: $\varphi^{-1}(K)$ is nonempty b.c. $e_H \in K$; so since $\varphi(e_G) = e_H$, $e_G \in \varphi^{-1}(K)$.

Now use subgp. criterion.

Reminder: If $A \subset G$, G a group, then $A \leq G \iff \forall a, b \in A$, $ab^{-1} \in A$.

Let $x, y \in \varphi^{-1}(K)$. WTS that $xy^{-1} \in \varphi^{-1}(K)$.

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \underbrace{\varphi(x)}_{\in K}\underbrace{\varphi(y)}_{\in K}{}^{-1} \in K.$$

$$\implies \varphi(xy^{-1}) \in K \implies xy^{-1} \in \varphi^{-1}(K).$$

So, $\varphi^{-1}(K) \leq G$.

Def: The <u>kernel</u> of a hom. $\varphi: G \to H$ is $\varphi^{-1}(\{e_H\})$

Def: the <u>image</u> of φ is

$$\varphi(G) := \{\varphi(g) \mid \forall g \in G\}.$$

Thm: $\varphi: G \to H$ is injective

$\iff \ker \varphi = \{e_G\}$, i.e. $\ker \varphi$ is trivial.

Pf: ($\Leftarrow$) If $\varphi(x) = \varphi(y)$, $x \neq y$.

Then $\varphi(x)\varphi(y)^{-1} = \varphi(x)\varphi(y^{-1}) = \varphi(xy^{-1}) = e_H$.

In particular, $xy^{-1} \neq e_G$ and $xy^{-1} \in \ker \varphi$.

Suppose $\ker \varphi$ is nontrivial.

$(\Rightarrow)$ $\exists\, xy^{-1} \in \ker \varphi$, $x \neq y$.

So $\varphi(xy^{-1}) = e_H$

$\parallel$

$\varphi(x)\,\varphi(y)^{-1}$

$$\Rightarrow \varphi(x)\,\underbrace{\varphi(y)^{-1} \cdot \varphi(y)} = e_H \cdot \varphi(y)$$

$$\varphi(x) = \varphi(y).$$

$\square$

- Def: An $\underline{\text{isomorphism}}$ is a bijective homomorphism.

$\underbrace{\text{isomorph}}$ "same shape"

- Two groups are "isomorphic" if $\exists\ \varphi : G \to H$ an isomorphism.

- Exercise: Composition of isomorphisms is an isomorphism.

$$\text{iso.} \begin{cases} \varphi : G \to H \\ \psi : H \to P \end{cases} \implies \psi\varphi : G \to P \text{ is an iso.}$$

E.g. $\mathrm{Aut}(G) := \{\text{isomorphism } G \to G\}$ is a group. (Aut means automorphism)

$$(\mathbb{Z}/4\mathbb{Z})_+ \to (\mathbb{Z}/4\mathbb{Z})_+$$

$$1 \bmod 4 \mapsto 3 \bmod 4.$$

$\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$

Check: This is a nontrivial isomorphism.

Rmk: If $G = \langle g \rangle = \{ g^n \mid n \in \mathbb{Z} \}$,

then G is called <u>cyclic</u>,

and any hom: $\varphi : G \to H$ is

determined by $\varphi(g)$.

If $G = \langle g_1, g_2, \dots \rangle$

it suffices to define $\varphi(g_i)$ $\forall i$.

- In an abelian gp, generators for

$G = \langle g_1, \dots, g_n \rangle$ behave "like a basis" of vec. spc.

$\forall g \in G$, $g = \sum_i c_i g_i = c_1 g_1 + c_2 g_2 + \dots + c_n g_n$.

$$\underbrace{(g_1+g_1+\cdots)}_{c_1}+\underbrace{(g_2+g_2+\cdots)}_{c_2}+\cdots$$

Going back: $\mathrm{Aut}(G)$ is a group.

Associativity: $\forall f, g, h \in \mathrm{Aut}(G)$

Why is $(fg)h = f(gh)$?

Identity: $id_G : g \mapsto g$ is the identity.

Inverses: $\forall \varphi \in \mathrm{Aut}(G)$, $\exists \varphi^{-1}$ a function

s.t. $\varphi\varphi^{-1} = \varphi^{-1}\varphi = id_G$,

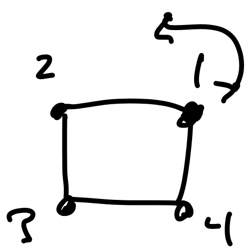
and φ^{-1} is indeed a homorphism.

Group actions:

Def: A group action (left) of a group G on a set X is a homorphism

$$\varphi : G \to \mathrm{Sym}(X).$$

- X is called a G-set.



$= X$, $\quad \{1,2,3,4\} = X$, $\quad G = C_4 = \{e, g, g^2, g^3\}$

$g^4 = e$

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

$x \in X$

$$\varphi(g)(x) =: g \cdot x$$

e.g. above, $\varphi(g)(1) = 2$.

φ can also be thought of as a function

$$G \times X \longrightarrow X \qquad \varphi(e) = id_X = e_{Sym(X)}$$

$$(g, x) \longmapsto g \cdot x \quad \text{s.t.} \quad \overbrace{e \cdot x = x}$$

and $(gh) \cdot x = g \cdot (h \cdot x)$

$$\varphi(gh)(x) = \varphi(g)(\varphi(h)(x))$$

$$\varphi(gh) = \varphi(g)\varphi(h)$$

Right action.

$$X \times G \longrightarrow X$$

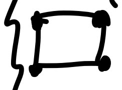
$$(x, g) \longrightarrow X. \qquad \text{s.t.} \quad x \cdot e = x$$

$$x \cdot (gh) = (x \cdot g) \cdot h$$

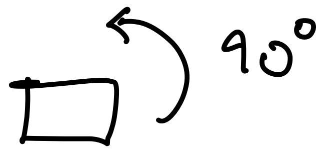
e.g. Left action $G \circlearrowleft G$ (generally, denote gp. action by $G \circlearrowleft G$)

Indeed, groups can be thought of as symmetries of an object!

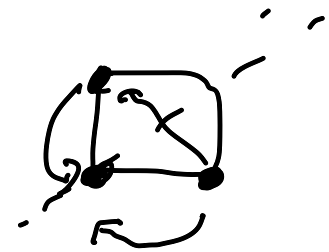
e.g. The <u>dihedral group</u> D_n can be thought of as the group of symmetries of the regular n-gon under rotation and reflection across an axis.

e.g. $D_4 \circlearrowright \{$  $\}$

as follows: $D = \langle g, h \rangle$

$g \mapsto$ 

$h \mapsto$ 



Note: $h^2 = 1$

$g^4 = 1$, $gh = hg^{-1}$

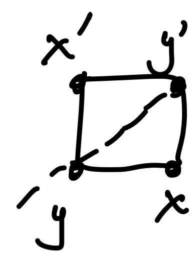
$$D_4 = \{1, g, g^2, g^3, h, gh, g^2h, g^3h\}$$

$|D_4| = 2 \cdot 4 \rightsquigarrow$ more gen. $|D_n| = 2n$

• Def: For $G \curvearrowright X$ and $x \in X$; the <u>orbit</u> of x under G is the set

$$Gx := \{ g \cdot x \mid \forall g \in G \}$$

Morally: "Everything we get by acting on x with G

e.g. $C_2 \curvearrowright \square$ by reflection across 

$C_2 = \{1, g\}$

$$Gx = \{x, x'\} \neq X$$

$$Gy = \{y\}, \quad Gy' = \{y'\}$$

If $Gx = X$ $\forall x \in X$, then $G \circlearrowright X$ is called <u>transitive</u>.

Claim: $x \sim y$ iff $Gx = Gy$ is an equivalence relation.

Pf: Reflexive, WTS $x \sim x$ $\forall x$

$Gx = Gx$

$\Rightarrow x \sim x$

Sym. WTS if $x \sim y$ Then $y \sim x$

$Gx = Gy$

$Gy = Gx$

Trans. WTS if $x \sim y$, $y \sim z$, then $x \sim z$.

Let $x' \in Gx$.

WTS that $x' \in Gz$.

$x' = g \cdot x = g' \cdot y$

since $Gy = Gz$, then $y \in Gz$

so $y = g'' \cdot z$ for some $g'' \in G$.

$$x' = g' \cdot (g'' \cdot z) = g'g''(z) \Rightarrow x' \in Gz.$$

$$\Rightarrow Gx \subset Gz$$

Similarly, $Gz \subset Gx$.

Since orbits form equivalence classes, we can consider el'ts of X as being "partitioned" into orbits.

Burnside's Lemma:

Let G a finite group that acts on X.

$\forall g \in G$, let $X^g := \{ x \in X \mid g \cdot x = x \}$.

$$\underbrace{|X/G|}_{\text{partition of } X \text{ by orbit}} = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

~~ie~~ for $H \trianglelefteq G$, we consider $g \sim g'$ if $g' = gh$ for some $h \in H$.

Coloring the cube!

3 colors, and how many distinct colorings of the cube?

"up to rotation".

$|X| = 3^6$

$|G| = 24$. = # of rotations

$X^g \ \forall g$:

$|X^e| = 3^6$, $|X^{90°}| = 3^3$, $|X^{180°}| = 3^4$

$$|X^{120^\circ}| = 3^2, \quad |X^{180^\circ}| = 3^3$$

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

$$= \frac{1}{24}(\dots)$$

$$= 57$$