Recap of Prev Class:

Def^n of Group: $(G, *)$ is a grp satisfying:

(G1): If $a, b \in G$ then $a * b \in G$

(G2): For $a, b, c \in G$,

$$(a*b)*c = a*(b*c)$$

(G3): $\exists\, e \in G$ s.t.

identity element

$$a*e = e*a = a$$

notation!

(G4): $\forall a \in G$, $\exists\, a^{-1} \in G$ s.t.

$$a^{-1} * a = a * a^{-1} = e$$

"inverse of a"

Qn. Are there nice examples of grps?

Yes! Ofcourse ....

Ex: $(\mathbb{Z}_n, +)$, $\underbrace{(\mathbb{Z}_p, \times)}$, $(\mathbb{R}, +)$, ...

$(S_n, \circ)$

S_n = symmetric grp on 'n' letters.

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

$Sym(X) = S_{|X|} = S_n$ = set of "$\underline{\text{permutations}}$" of X

↳ bij fn. from $X \to X$.

So, $Sym(X) = S_n$ consists of $\underline{\text{fns}}$ from X to X.

↑ bij.

$Sym(X) = S_n = \{f_1, f_2, \ldots\}$.

$|S_n| = n! = \#(\text{bij fns on } X)$

Qn. Can we replace X by any other set of same size as X?

→ Yes! It doesn't matter.... You can take X as the set $\{a_1, a_2, \ldots, a_n\}$

Matrix Grps

→ $GL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det(A) \neq 0\}$

→ $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$

Group operation is matrix multiplication

Subgrp: $H \subseteq G$, is a subgrp of G if $(H, *)$ is a grp.

Ex: $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$

subgrp symbol.

Subgrp Criteron: $(H \neq \phi)$ $\forall\, a, b \in H$, if we have $ab^{-1} \in H$, then $H \leq G$

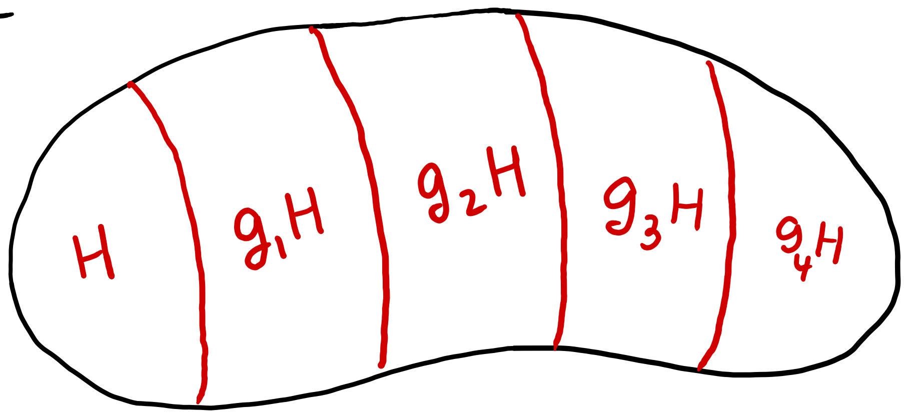
Qn. Is there any way to identify subgrps?

Partially Yes! (Lagrange)

<u>Lagrange's thm</u>: If $H \leq G$, & $|G| < \infty$, then:

$$|H| \mid |G|.$$

<u>Pf Idea</u>:



Break G into cosets, $|H| = |gH|$ $\left(\because \varphi : H \to gH,\ h \mapsto gh \text{ is bij.} \right)$

& they are also distinct (or equal)

So, $G = \coprod gH \Rightarrow |G| = \sum |gH|$

$$\Rightarrow |G| = k \cdot |H|$$

← no of distinct cosets.

$\therefore |H| \mid |G|$

Qn. Ask the most natral qstn!!

↳ Is the converse true? No!

$A_n \leftarrow$ alternating grp on n letters,

Let $n=4$, $|A_4| = \frac{4!}{2} = 12$; $6 \mid 12$ but

no subgrp of size 6.

- Normal Subgrp: let $H \leq G$, if $\forall g \in G$ we have $gHg^{-1} = H$; we say H to be normal in G.

  Notation: $H \trianglelefteq G$.

- Homomorphisms.

A map $\varphi : G \to G'$, is a homomorphism if

$(G, *)$ $(G', \cdot)$

$$\varphi(g_1 * g_2) = \varphi(g_1) \cdot \varphi(g_2)$$

Ex: $\underbrace{\det(\cdot)}_{\text{map}} : GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$

$A \longmapsto \det(A)$

"structure preserving maps"

- $\ker \varphi := \{ g \in G : \varphi(g) = e_{G'} \} \overset{\text{Exc!}}{\trianglelefteq} G$
- $\operatorname{Im} \varphi := \{ \varphi(g) : g \in G \} \overset{\text{Exc!}}{\leq} G'$

$$\ker(\det(\cdot)) = \{ A \in GL_n(\mathbb{R}) : \det(A) = 1 \} = SL_n(\mathbb{R})$$

$\operatorname{Im}(\det(\cdot)) = \mathbb{R}^* \left(\begin{smallmatrix} \text{surj.} \\ \text{map} \end{smallmatrix} \right)$ as for any $a \in \mathbb{R}^*$ choose $\begin{bmatrix} a & & 0 \\ & 1 & \\ 0 & & 1 \end{bmatrix} \leftarrow A$, $\underset{a.}{\det(A)}$ "

- Isomorphism : "grp-th. bijections"

A map $\varphi : G \to G'$ is isomorphism if φ is a homomorphism and a bijection.

Notation: $G_1 \overset{\varphi}{\cong} G_2$ or $G_1 \cong G_2$.

- Automorphisms: (Special case of Isomorphism; when the map is b/w same grp.)

Ex: $\varphi : G \to G$ def by $\varphi(g) = x g x^{-1}$ where 'x' is arbitarily fixed.

- Quotienting of Grps :

Given a normal subgrp we can quotient G by H ($H \trianglelefteq G$), i.e.

$$G/H = \{\text{set of all left cosets of } H\}$$ ← "G mod H"

Qn. Can we make G/H to a grp?

Yes! But the operation is bit changed.

Say $(G, *)$ is a grp, $H \trianglelefteq G$, then $(G/H, \cdot)$ is a grp.

$$G/H = \{a_1 H, a_2 H, \dots\}$$

$$\rightarrow (a_1 H) \cdot (a_2 H) = (a_1 * a_2) H$$

Qn. Is there a necessary & suff condn of when we can make G/H to a grp? Yes! iff $H \trianglelefteq G$.

Idea of Building new grps ......

- Let $(G, *)$ be a grp, and $(H, *)$ & $(K, *)$ be its two subgrp

How to make bigger grps out of H & K?

Qn. Which of the const would work?

- $H \cap K$?
- $H \cup K$?
- HK ?
- $H \times K$?

If some of them doesn't work, then find some necc. & suff cond, under which it will be a subgrp.

The 1st Isomorphism Thm

(Idea of getting isomorphism out of homomorphism)

let $\varphi : G \to G'$, be a homomorphism,

then:

$$G/\ker\varphi \cong \operatorname{Im}\varphi$$

Ex: $\left|G/H\right| = \dfrac{|G|}{|H|}$

Corr. If $|G| < \infty$, then:

$$\left|G/\ker\varphi\right| = |\operatorname{Im}\varphi|$$

$$\overset{\text{Ex}}{\Longrightarrow} |G| = |\ker\varphi| \cdot |\operatorname{Im}\varphi|$$

Any similarity from lin. alg?

(Rank-Nullity Thm) let $T: V_1 \to V_2$

$$\dim V_1 = \dim(\ker(T)) + \dim(\operatorname{Im}(T))$$

Ex: $\mathbb{R}[x] = \{\text{polynomials with coeff from } \mathbb{R}\}$

$(\mathbb{R}[x], +)$ is a group wrto '$+$'.

$$\varphi : \mathbb{R}[x] \longrightarrow \mathbb{R}$$

$$\varphi(p) = p(0)$$

$$\varphi(p_1 + p_2) = (p_1 + p_2)(0)$$

$$= p_1(0) + p_2(0)$$

$$= \varphi(p_1) + \varphi(p_2)$$

φ is homomorphism!

φ is onto, as for $a \in \mathbb{R}$, let $p(x) = a$, then $\varphi(p) = p(0) = a \in \mathbb{R}$

$$\ker \varphi = \{ p \in \mathbb{R}[x] : p(0) = 0 \}$$

$= \{\text{all poly with const. term } 0\}$

$$\mathbb{R}[x] \big/ \ker \varphi \cong \mathbb{R}$$

Quotienting in some sense means adding more zeros to the abmient space. For ex: Here we are adding more zeros (treating more elements as zero poly (apart from 0 poly) in $\mathbb{R}[x]$), for ex: (x^2+3x) is a zero element; (treated as)

$$3x^2+4x+2 = \underbrace{(3x^2+4x)}_{\text{equiv. to } 0}+2$$

equivalent in new quot.

~ 2

(this is a non rigorous, but intuitive idea.)

[So, here what matters is just the const terms; so it is $\cong \mathbb{R}$]

Ex: $\mathbb{R}[x,y] = \{$all poly in formal vars. 'x' & 'y' with coeff in $\mathbb{R}\}$

$\mathbb{R}[x,y]\big|_{S^1} = \{$all poly. in '$x$' & '$y$' which was orginally def in $\mathbb{R}^2$ but now restricted to $S^1\}$

$$\varphi : \mathbb{R}[x,y] \longrightarrow \mathbb{R}[x,y]\big|_{S^1}.$$

$$\varphi(p) = p\big|_{S^1}.$$

$$p(x,y) = 3x^2y + 2$$

$$p(x,y) : \mathbb{R}^2 \to \mathbb{R}$$

$$p(x,y)\big|_{S^1} : S^1 \longrightarrow \mathbb{R}.$$

$$\ker \varphi = \{ p \in \mathbb{R}[x,y] : p(S^1) = 0 \}$$

Clearly $(x^2+y^2-1) \in \ker \varphi$.

Let $p(x,y) : \mathbb{R}^2 \to \mathbb{R}$ def by:

$$p(x,y) = x^2+y^2+5.$$

Now, restrict it to S^1.

So, $p(x,y)|_{S^1} : S^1 \longrightarrow \mathbb{R}$,

$$p(x,y)|_{S^1} = x^2+y^2+5.$$

Any point on S^1 is $(\cos\theta, \sin\theta)$

So, $p((\cos\theta, \sin\theta)) = \cos^2\theta + \sin^2\theta + 5$
$= 6$

By 1st Iso Thm:

$$G/\underbrace{\operatorname{Ker}\varphi}_{\text{(all poly which are zero on } S^1)} \cong \mathbb{R}[x,y]\Big|_{S^1}$$

Here $(x^2+y^2-1) \in \operatorname{Ker}\varphi$, so,

$$p(x,y) = x^2+y^2+5 = \underbrace{(x^2+y^2-1)}_{\text{equiv. to } 0} + 6 \overset{\text{equiv.}}{\sim} 6$$

Ex: $\mathbb{R}/\mathbb{Z} \cong S^1$.

$$x = \underbrace{[x]}_{\text{equiv. to zero.}} + \{x\}$$

$$x \underset{\substack{\uparrow \\ \text{equiv}}}{\sim} \{x\} \in [0,1)$$

$$\begin{tikzcd}
\mathbb{R}/\mathbb{Z} \arrow[r, "\sim"] \arrow[dr, "\wr"'] & {[0,1)} \arrow[d, "\wr"] \\
 & S^1
\end{tikzcd}$$

$\varphi : [0,1) \to S^1$

$x \mapsto (\cos\theta, \sin\theta)$

$\theta = 2\pi x$.

Group Action:

Motivation? Scalar Multiplication

$$1 \cdot \vec{x} = \vec{x}$$

$$a \cdot (b \cdot \vec{x}) = (ab) \cdot \vec{x}$$

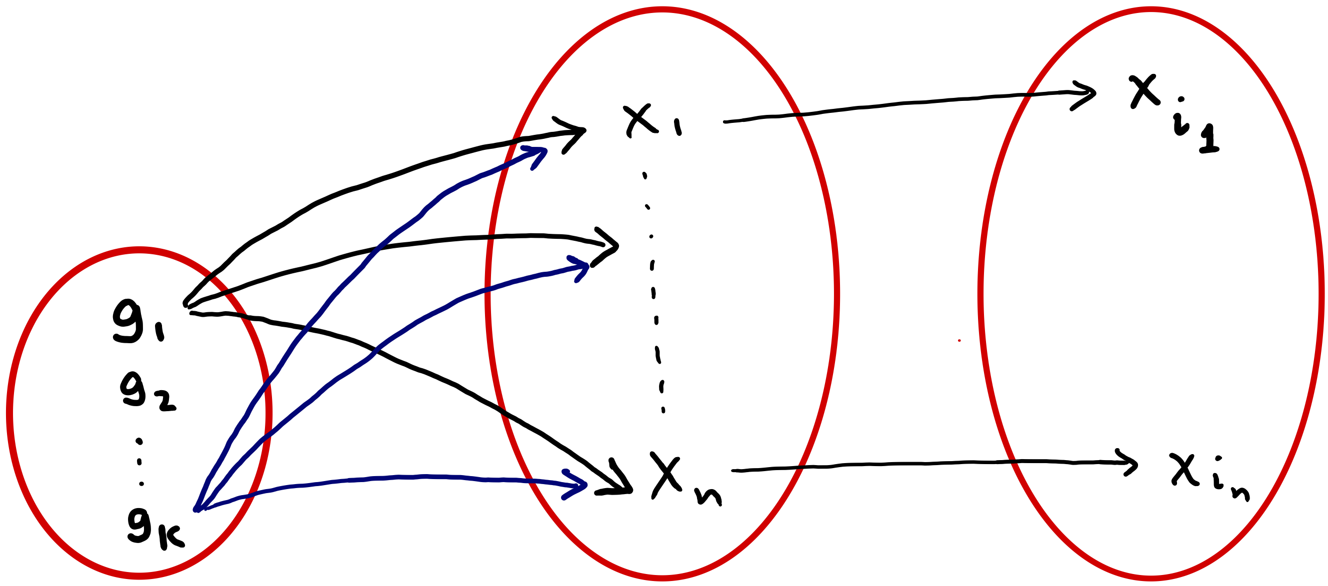
An action of G on X denoted by $G \curvearrowright X$ is a map from $G \times X \longrightarrow X$ satisfying:

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

(here $a \cdot b$) action of 'a' on 'b'.

For finite case of X, we can see it as:

Using elements of G to permute the elements of X.



- $e \cdot x = x$, says the identity shudn't permute elements of X.

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

Say h permute x to x'

& g permute x' to $\tilde{x}'$

then what we have is:

$$\begin{tikzcd} x \arrow[rr, "gh"] \arrow[dr, "h"'] & & \tilde{x}' \\ & x' \arrow[ur, "g"'] \arrow[u, phantom, "\circlearrowleft"] & \end{tikzcd}$$

Given a action we define:

First fix $x \in X$, then:

$$\operatorname{orb}(x) = \{ g \cdot x : g \in G \} \subseteq X$$

$$\operatorname{stab}(x) = \{ g \in G : g \cdot x = x \} \overset{\text{Ex.}}{\leq} G.$$

<u>Exc</u>: let $H \leq G$, then:

1. $g_1 H = g_2 H \iff g_2^{-1} g_1 H = H$
2. $g_1 H = g_2 H \iff g_2^{-1} g_1 \in H$.

The Orbit - Stabilizer Thm.

Theorem: let $G \curvearrowright X$, & $|G| < \infty$, then for any $x \in X$, we have:

$$|G| = |orb(x)| \cdot |stab(x)|$$

Proof: Define; $\varphi : G/_{stab(x)} \longrightarrow orb(x)$

where $\varphi(g\, stab(x)) = g \cdot x$

Claim: φ is well-defined.

Proof: To show φ is well def, we need to show:

if $g_1 stab(x) = g_2 stab(x)$

then $g_1 \cdot x = g_2 \cdot x$

But, $g_1 stab(x) = g_2 stab(x)$

$\overset{Ex}{\Rightarrow}$ $g_2^{-1} g_1 stab(x) = stab(x)$

$\overset{Ex}{\Longrightarrow} \quad g_2^{-1} g_1 \in \text{stab}(x)$

But any element $g \in \text{Stab}(x)$ means by def^n: $g \cdot x = x$.

So, here $(g_2^{-1} g_1) \cdot x = x$

$$\Rightarrow \quad g_2 \cdot ((g_2^{-1} g_1) \cdot x) = g_2 \cdot x$$

$$\Rightarrow \quad (g_2 g_2^{-1} g_1) \cdot x = g_2 \cdot x$$

$$\Rightarrow \quad g_1 \cdot x = g_2 \cdot x \text{, as required.}$$

Check φ is one-one & onto. (Exc)

$$G/\mathrm{Stab}(x) \xrightarrow[\sim]{\text{bij}} \mathrm{orb}(x) \subseteq X$$

$$\Rightarrow \left| G/\mathrm{Stab}(x) \right| = |\mathrm{orb}(x)|$$

$$\Rightarrow \frac{|G|}{|\mathrm{stab}(x)|} = |\mathrm{orb}(x)|$$

$$\Rightarrow |G| = |\mathrm{orb}(x)| \cdot |\mathrm{stab}(x)| .$$

thus, the theorem.

let, $SO_2 := \{A \in GL_n(\mathbb{R}) : AA^t = I\}$

any $A \in SO_2$ is of the form

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

We let $SO_2 \curvearrowright \mathbb{R}^2$ via:

$$A \cdot v = Av, \quad \text{where}$$

$v = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ is a (2×1) matrix.

Check its a valid action! (Exc)

let's pick $(1,0) \in \mathbb{R}^2$, & look at its' orbit;

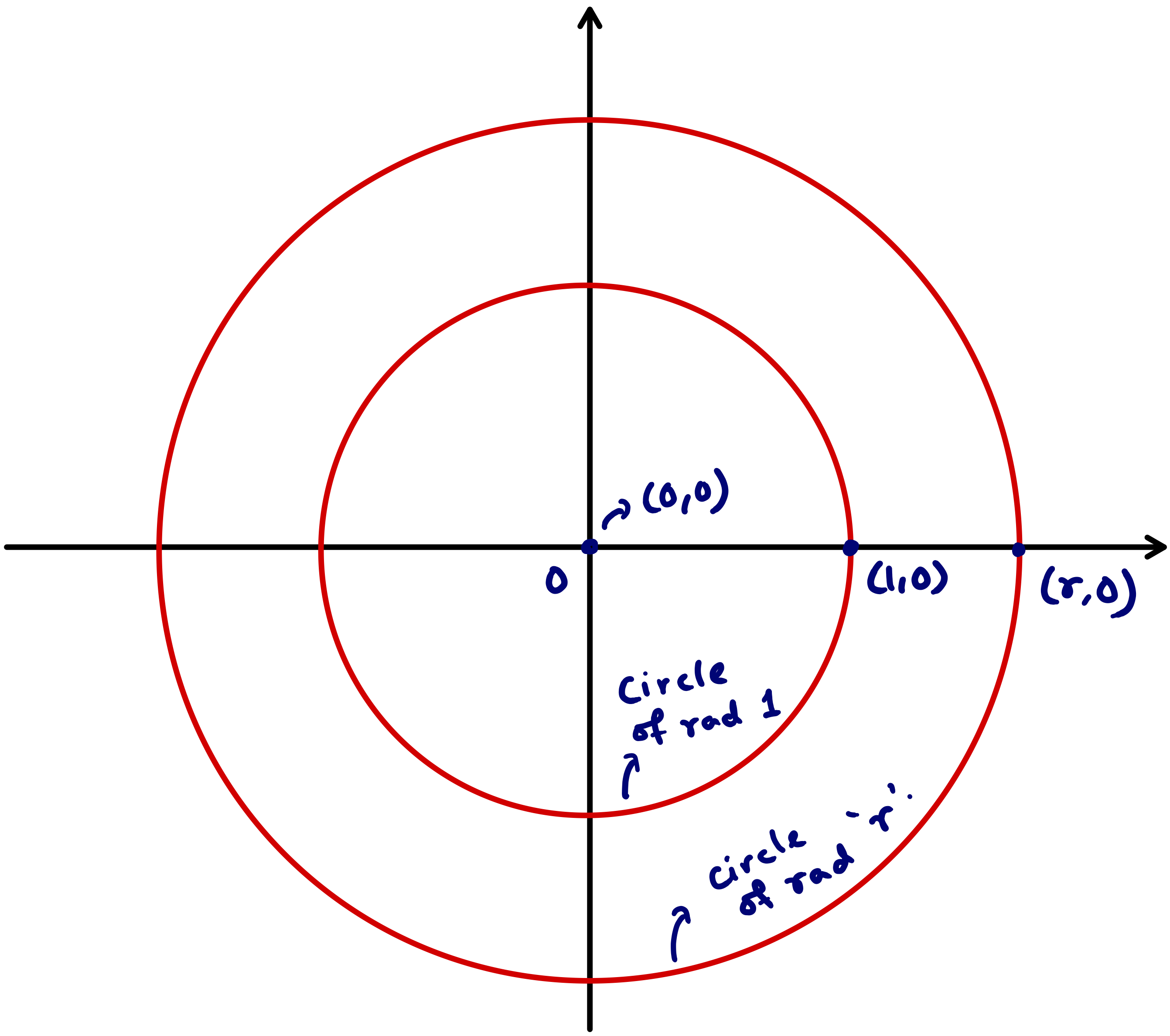
$$\operatorname{orb}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \left\{A \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} : A \in SO_2\right\}$$

$$= \left\{\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} : \theta \in [0, 2\pi)\right\}$$

$$\therefore \ \mathrm{orb}\left(\begin{pmatrix}1\\0\end{pmatrix}\right) = \left\{ \begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix} : \theta \in [0, 2\pi) \right\}$$

$$\text{lly}, \ \mathrm{orb}\left(\begin{pmatrix}r\\0\end{pmatrix}\right) = \left\{ \begin{pmatrix}r\cos\theta\\ r\sin\theta\end{pmatrix} : \theta \in [0, 2\pi) \right\}$$

So, we have the following geometry:



$$\operatorname{orb}\left(\begin{pmatrix}0\\0\end{pmatrix}\right) = \left\{ A\begin{pmatrix}0\\0\end{pmatrix} : A \in SO_2 \right\}$$

$$= \left\{ \begin{pmatrix}0\\0\end{pmatrix} \right\}.$$

Clearly, $\mathbb{R}^2$ is being partitioned by orbits.

Qn. Is it true in general?

Yes!

<u>Claim</u>: orbits partition the acting space X (Exc)

then by Exc:

circle of radius 'r' in $\mathbb{R}^2$.

$$\mathbb{R}^2 = \{(0,0)\} \coprod_{0<r<\infty} S^1_r$$

(A Beautiful App.) Use this action to show $\sin\theta$ & $\cos\theta$ can't have simul. roots. (Complete it ....)

[Was done in class, see recording]

Theorem: let $H, K \leq G$, with $|G| < \infty$, then:

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Proof: We let:

$H \times K \curvearrowright HK$ by:

$$(h,k) \cdot \tilde{h}\tilde{k} = h\tilde{h}\tilde{k}k^{-1}$$

Check it's a valid action.

We will use the orbit stabilizer thm.

$$|G| = |orb(e)| \cdot |stab(e)|$$

$$orb(e) = \{(h,k) \cdot e : (h,k) \in H \times K\}$$

$$= \{hk^{-1} : h \in H, k \in K\}$$

$$\overset{\text{bij.}}{\cong} HK$$

$$\therefore |\mathrm{orb}(e)| = |HK|$$

$$\begin{aligned}
\mathrm{stab}(e) &= \{(h,k) \in H \times K : (h,k)\cdot e = e\} \\
&= \{(h,k) \in H \times K : hek^{-1} = e\} \\
&= \{(h,k) \in H \times K : h = k\} \\
&\overset{\text{bij}}{\cong} H \cap K
\end{aligned}$$

$$\therefore |\mathrm{stab}(e)| = |H \cap K|$$

$$\therefore \text{By OST} : |G| = |H \cap K| \cdot |HK|$$

$$\Rightarrow \frac{|H \times K|}{|H \cap K|} = |HK|$$

$$\Rightarrow \boxed{|HK| = \frac{|H||K|}{|H \cap K|}}$$

Some Valid Actions: ($G \curvearrowright G$)

- Left Mul.
- Right Mul.
- Conjugation.

Left Mul.

$$G \curvearrowright G$$

$$g \cdot a = \underbrace{ga}_{\text{grp op.}}$$

Check its a valid action! (Exc)

[Was done in class, .. see recording]

Right Mul.

$$G \curvearrowright G$$

$$g \cdot a = ag^{-1}$$

Check its a valid action! (Exc)

[Was done in class, .. see recording]

• Conjugation.

$$G \curvearrowright G$$

$$g \cdot a = gag^{-1}$$

Check its a valid action! (Exc)
[was done in class, .. see recording]

<u>Cayley's Thm:</u> Let G be a finite grp then $G \cong K \leq S_n$, where $n = |G|$.

<u>Proof:</u> Let $G \curvearrowright G$ via left mul.

(solve it if you can...)

Exc: (Application of Cayley) Show that given any 'n', there exists finitely many non-isomorphic groups.