HW 4 due Wed.

Recall:

If $H, K \leq G$ with $K \trianglelefteq G$ and $H \cap K = \{1\}$,

we say $HK = H \ltimes K$
semi-direct product.

Direct $\Leftrightarrow$ $hk = kh$ $\forall h \in H, k \in K$.

[In abelian groups $\ltimes = \times$]

eg The Dihedral group

$$D_n = \left\langle \underset{r}{\underset{\parallel}{\begin{pmatrix} 1 & \\ & -1 \end{pmatrix}}}, \underset{\rho}{\underset{\parallel}{\begin{pmatrix} c & -s \\ s & c \end{pmatrix}}} ; c = \cos\left(\frac{2\pi}{n}\right), s = \sin\left(\frac{2\pi}{n}\right) \right\rangle$$

$\langle r \rangle, \langle \rho \rangle \leq D_n$, $\langle \rho \rangle \trianglelefteq D_n$.
$\langle r \rangle \cap \langle \rho \rangle = \left\{ \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \right\}$

$\Longrightarrow D_n = \langle r \rangle \ltimes \langle \rho \rangle$
$\approx \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/n\mathbb{Z}$

D_n = symmetries of regular n-gon

$D_n \leq O(2)$ = symmetries of a
finite infinite circle.

$O(2) := \{ A \in M_{2\times 2}(\mathbb{R}) : A^T A = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \}$

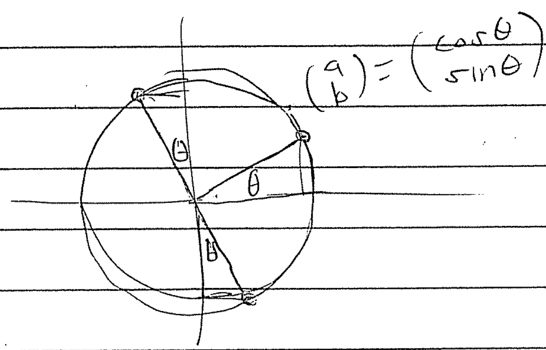
If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O(2)$. Then

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\Longrightarrow \quad a^2 + b^2 = 1 = c^2 + d^2$$
$$\& \quad ac + bd = 0$$

$\Longrightarrow \quad \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix}$ orthogonal unit vectors.

Say $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$



Then $\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$ OR $\begin{pmatrix} \sin\theta \\ -\cos\theta \end{pmatrix}$.

only 2 choices.

Conclusion: $O(2)$ consists of matrices of the form

$$A_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \quad \& \quad \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} = B_\theta$$

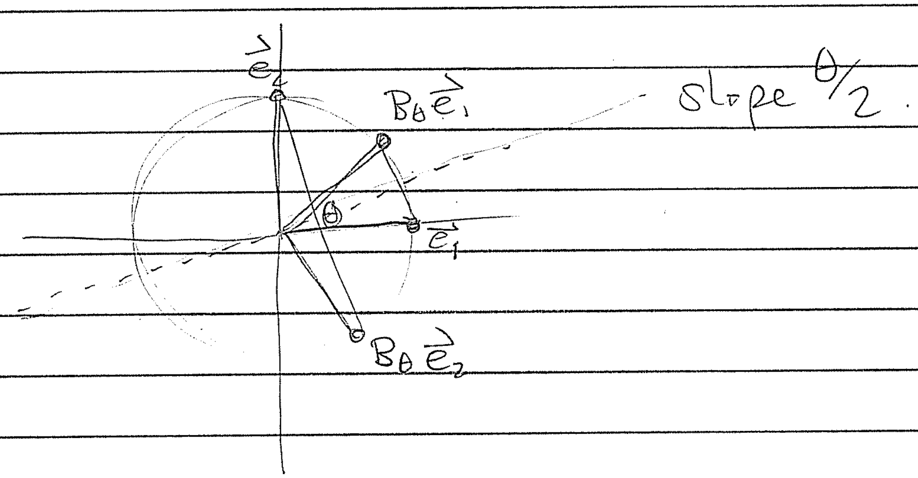
Rotation by θ counterclockwise.

$\det = -\cos^2\theta - \sin^2\theta$
$= -1$

$\det = \cos^2\theta + \sin^2\theta$
$= 1$

Q: What does it do?

A:



B_θ is reflection in line of slope $\theta/2$

$$O(2) = \{ A_\theta, B_\theta : \theta \in \mathbb{R} \}$$

= rotations & reflections of $\mathbb{R}^2$ fixing $\vec{0}$

= symmetries of a circle.

$SO(2) := \{ A \in O(2) : \det A = 1 \}$

$= \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R} \right\}$

$=$ rotations of $\mathbb{R}^2$ about $\vec{0}$

$SO(2) \leq O(2)$.

"orientation-preserving" symmetries

symmetries.

- D_n = dihedral $\leq O(2)$
- C_n = cyclic $\leq SO(2)$.

Q: $\underbrace{\{\text{reflections}\}}_{\det = -1} \leq O(2)$? NO!

Recall:

$SO(2) \approx U(1)$ = unit complex numbers.

$U(1) = \{ z \in \mathbb{C} : z\bar{z} = |z|^2 = 1 \}$

$= \{ e^{i\theta} : \theta \in \mathbb{R} \}$

$= \{ a + ib : a, b \in \mathbb{R},\ a^2 + b^2 = 1 \}$

Isomorphism $U(1) \to SO(2)$.

$a\mathbb{1} + b\,i \longmapsto a\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} + b\begin{pmatrix} & -1 \\ 1 & \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

i.e. let $\mathbb{1} = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$ $\quad i = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$.

$$i^2 = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix} = -\mathbb{1}$$

Next: $SO(3) = \{ A \in M_{3\times 3}(\mathbb{R}) : A^TA = I, \ \det A = 1 \}$

Geometry?
Algebra? (in terms of $\mathbb{C}$?)

Hamilton $\rightsquigarrow$ Quaternions (Oct 16, 1843).

$$\mathbb{H} := \{ a\mathbb{1} + bi + cj + dk : a, b, c, d \in \mathbb{R} \}$$

with $i^2 = j^2 = k^2 = ijk = -\mathbb{1}$.

Think:

$$\mathbb{1} = \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \quad i = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}, \quad j = \begin{pmatrix} & -i \\ -i & \end{pmatrix}, \quad k = \begin{pmatrix} i & \\ & -i \end{pmatrix}$$

So:

$$\mathbb{H} = \left\{ \begin{pmatrix} a+id & -b-ic \\ b-ic & a-id \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

$$\mathbb{H} \leq M_2(\mathbb{C})$$

sub ring.

$$\mathbb{H}^\times \leq GL_2(\mathbb{C}).$$

sub group.

For $q \in \mathbb{H}$ we define

$$\bar{q} = q^* \text{ (conjugate transpose matrix)}$$

$$q = \begin{pmatrix} a+id & -b-ic \\ b-ic & a-id \end{pmatrix} = a+bi+cj+dk.$$

$$\bar{q} = \begin{pmatrix} \overline{a+id} & \overline{b-ic} \\ \overline{-b-ic} & \overline{a-id} \end{pmatrix} = \begin{pmatrix} a-id & b+ic \\ -b+ic & a+id \end{pmatrix}$$

$$= a-bi-cj-dk.$$

quaternion <u>conjugate</u>

<u>Fact</u>: $\overline{q_1 q_2} = \bar{q}_2 \bar{q}_1$ ///

Also define

$$|q|^2 := \det(q)$$
$$= a^2+b^2+c^2+d^2$$

quaternion <u>absolute value</u>.

For all $q \in \mathbb{H}$ we have.

$$q\bar{q} = |q|^2 + 0i + 0j + 0k$$

Real part.

HW 4.1(c) says $\forall u, v \in \mathbb{H}$ we have
$|uv| = |u||v|$.

$\Longrightarrow$ unit quaternions form a group.

DEF:

$$Sp(1) := \{ q \in \mathbb{H} : |q| = 1 \}.$$

a "symplectic" group.

DEF:

conjugate transpose

$$U(n) := \{ A \in M_{n \times n}(\mathbb{C}) : A^* A = I \}$$

"unitary group"

$$SU(n) := \{ A \in U(n) : \det A = 1 \}$$

"special unitary group".

FACT: $Sp(1) \approx SU(2)$.

$$a + ib + cj + dk \longmapsto \begin{pmatrix} a+id & -b-ic \\ b-ic & a-id \end{pmatrix}$$

Analogy: $U(1) \approx SO(2)$.

$$a + ib \longmapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

Why did I mention $\mathbb{H}$?
Because $Sp(1) \approx SU(2)$ helps us understand $SO(3)$

$\exists$ special hom $SU(2) \longrightarrow SO(3)$.
2-to-1

HW 4 due NOW.

DEF: We say that $(A, +, \times, \circ)$ is an $\mathbb{R}$-algebra if

- $(A, +, \circ)$ is an $\mathbb{R}$-vector space
- $(A, +, \times)$ is a ring.

such that $\times$ respects scalar multiplication. i.e. for $a, b, c \in A$, $x, y \in \mathbb{R}$ we have.

$$(x \circ a + y \circ b)c = x \circ ac + y \circ bc.$$
$$c(x \circ a + y \circ b) = x \circ ca + y \circ cb.$$

[Say $(a,b) \mapsto ab$ is $\mathbb{R}$-bilinear]

Frobenius Theorem (1877)
If A is a finite dimensional division $\mathbb{R}$-algebra.
Then $A = \mathbb{R}$ or $\mathbb{C}$ or $\mathbb{H}$. That's All.

DEF: Given any f.d. $\mathbb{R}$-alg A we can consider the matrix $\mathbb{R}$-algebra.

$M_n(A) := \{ n \times n \text{ matrices with entries} \in A \}$

groups

$GL_n(A) := \{ \text{invertible matrices} \}$

$O_n(A) := \{ \text{orthogonal matrices} \}$
$= \{ X \in GL_n(A) : X^* X = I \}$

conjugate transpose.

For $A = \mathbb{R}, \mathbb{C}, \mathbb{H}$, these have special names.

$O_n(\mathbb{R}) = O(n)$ orthogonal
$O_n(\mathbb{C}) = U(n)$ unitary
$O_n(\mathbb{H}) = Sp(n)$ symplectic.

Big Theorem
(Lie, Killing, Cartan, Weyl).

Almost all continuous symmetry groups look like $SL(n)$, $O(n)$, $U(n)$, or $Sp(n)$
$SO(n)$, $SU(n)$

i.e. We've seen it all.

$\Longrightarrow$ implications for physics.

eg The gauge group of the standard model

$$G = \underbrace{SU(3)}_{\text{strong}} \times \underbrace{SU(2)}_{\text{weak}} \times \underbrace{U(1)}_{\text{EM}}.$$

HW 5 due next Monday.

Today: $O(3)$ & $SO(3)$.

What is a reflection?

Given $u \in \mathbb{R}^n$, let

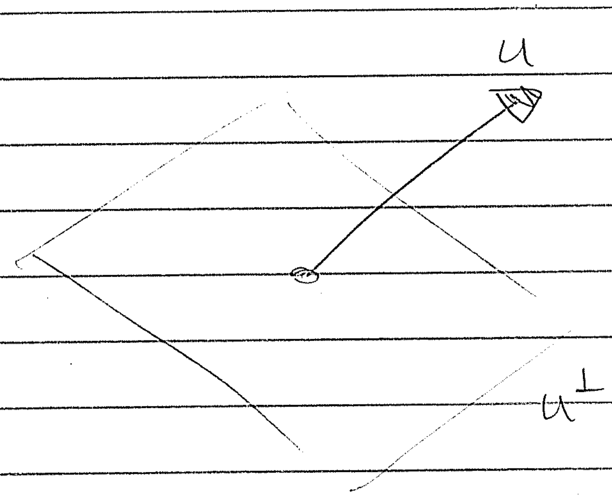
$$u^\perp := \{ x \in \mathbb{R}^n : x \cdot u = 0 \}$$

the "hyperplane" $\perp$ to u.

Orthogonal Decomposition

$$\mathbb{R}^n = \underset{\text{hyperplane}}{u^\perp} \oplus \underset{\text{line}}{\mathbb{R}u}.$$

Pic for $n=3$



DEF: Let $F_u : \mathbb{R}^n \to \mathbb{R}^n$ be the <u>unique</u> linear map that sends $F_u(\alpha \cdot u) = -\alpha \cdot u$ for all $\alpha \in \mathbb{R}$ and fixes $u^\perp$ pointwise.
i.e. $F_u(w) = w \ \forall w \in u^\perp$.

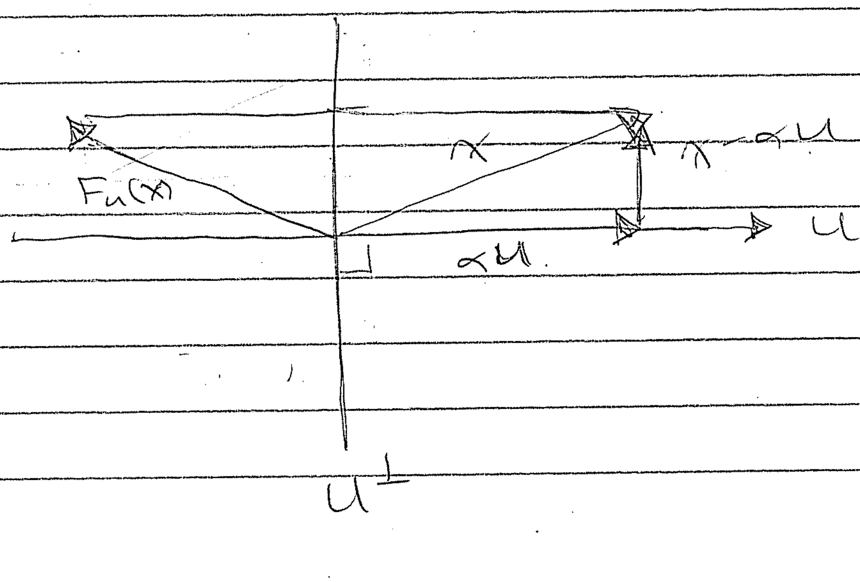
F_u is called the <u>reflection through u</u>.
(or reflection across $u^\perp$).

Let $\mathcal{B} = \{u, \underbrace{v_1, v_2, \ldots, v_{n-1}}_{\text{O.N. basis for } u^\perp}\}$

Then
$$[F_u]_{\mathcal{B}} = \left(\begin{array}{c|cccc} -1 & 0 & 0 & \cdots & 0 \\ \hline 0 & 1 & & & \\ 0 & & 1 & & 0 \\ \vdots & & & \ddots & \\ 0 & & 0 & & 1 \end{array}\right)$$

every reflection looks like this in <u>some</u> basis.

Q: What if $\mathcal{B}$ = standard basis?



$$(x-\alpha u)\circ u = 0.$$

$$x\circ u - \alpha\, u\circ u = 0$$

$$\alpha = \frac{x\circ u}{u\circ u}.$$

Then $F_u(x) = x - 2\alpha u$

$$= x - \frac{2(x\circ u)}{(u\circ u)}\, u$$

$$= x - \frac{2u}{u\circ u}(u\circ x)$$

$$= Ix - \left(\frac{2u}{u\circ u}u^T\right)x.$$

$$= \underbrace{\left(I - 2\frac{uu^T}{\|u\|^2}\right)}_{\text{The matrix of } F_u.}x$$

(a "Householder matrix").

eg. Let $u = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \in \mathbb{R}^3$.

Then $\dfrac{uu^T}{\|u\|^2} = \dfrac{1}{3}\begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}(1\ 1\ -1)$

$$= \frac{1}{3}\begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}$$

Hence

$$\underset{\substack{\uparrow \\ \text{standard} \\ \text{basis}}}{[F_u]} = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} - \frac{2}{3}\begin{pmatrix} 1 & 1 & -1 \\ 1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1/3 & -2/3 & 2/3 \\ -2/3 & 1/3 & 2/3 \\ 2/3 & 2/3 & 1/3 \end{pmatrix} = \frac{1}{3}\begin{pmatrix} 1 & -2 & 2 \\ -2 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}$$

To replace Thm 6.2.3

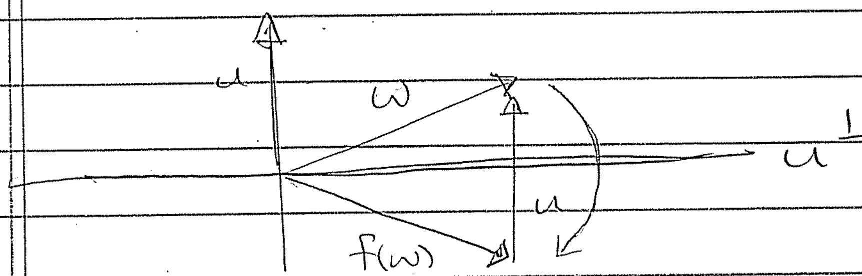
DEF: Let $\mathrm{Isom}(\mathbb{R}^n)$ = group of isometries $f: \mathbb{R}^n \to \mathbb{R}^n$. Let $\mathrm{Isom}_0(\mathbb{R}^n)$ subgroup of isometries with $f(0) = 0$.

Theorem (Cartan - Dieudonné)
Every $f \in \mathrm{Isom}_0(\mathbb{R}^n)$ is a composition of $\leq n$ reflections.

Proof by induction:
Given $f \in \mathrm{Isom}_0(\mathbb{R}^n)$, $f \neq id$.
If $n = 1$ then $f(x) = -x$. DONE.

So suppose true for $n = k-1$ and consider isom $f: \mathbb{R}^k \to \mathbb{R}^k$ with $f(0) = 0$.
Sp. $f \neq id$ so $\exists\, w \in \mathbb{R}^k$ with $f(w) \neq w$.

let $u = w - f(w) \neq 0$ and consider F_u.



Since $\|f(w)\| = \|w\|$ we have $F_u(w) = f(w)$.

Then $F_u \circ f(w) = F_u(f(w))$
$= F_u(F_u(w)) = w$.

$\Rightarrow F_u \circ f$ is an isometry that fixes w.
Let $\varphi = F_u \circ f$ and decompose

$$\mathbb{R}^k = w^\perp \oplus \mathbb{R}w.$$

Know: φ fixes $\mathbb{R}w$. i.e. $\varphi(w) = w$
Claim: $\varphi(w^\perp) \subseteq w^\perp$.
Proof: consider $v \in w^\perp$ i.e. $v \cdot w = 0$.
Then $\varphi(v) \cdot w = \varphi(v) \cdot \varphi(w) = v \cdot w = 0$

isom. preserves dot.

$\Rightarrow \varphi(v) \in w^\perp$ ///.

$\Longrightarrow \varphi : W^\perp \to W^\perp$

By induction

$$\varphi = S_1 \circ S_2 \circ \cdots \circ S_{k-1}$$

product of reflections in $W^\perp \subseteq \mathbb{R}^k$ (dim $k-1$)

Lift trivially to $\mathbb{R}^k$ to get

$$F_u \circ f = \varphi = S_1 \circ S_2 \circ \cdots \circ S_{k-1}$$

product of reflections in $\mathbb{R}^k$.

$$\Longrightarrow f = F_u \circ S_1 \circ S_2 \circ \cdots \circ S_{k-1}$$

$\blacksquare$

Cor: $\mathrm{Isom}_0(\mathbb{R}^n) = O(n)$.

Proof: $O(n) \le \mathrm{Isom}_0(\mathbb{R}^n)$ easy.

$\mathrm{Isom}_0(\mathbb{R}^n) = \langle \text{reflections} \rangle \le O(n)$.

by Theorem.

$\blacksquare$

Cor: We can describe $O(3)$

Every $A \in O(3)$ is a product of ≤ 3 reflections.

det	# reflections	geometry
$+1$	0	identity map.
-1	1	reflection.
$+1$	2	rotation (HW 5.1)
-1	3	reflection? NO. (screw reflection)

That's All.

Corollary: $SO(3)$ contains id and rotations. That's all.

Corollary (NOT OBVIOUS!) In $\mathbb{R}^3$ we have

rotation $\circ$ rotation $=$ (rotation OR id)

Not exactly true in $\mathbb{R}^n$ for $n \geq 4$.

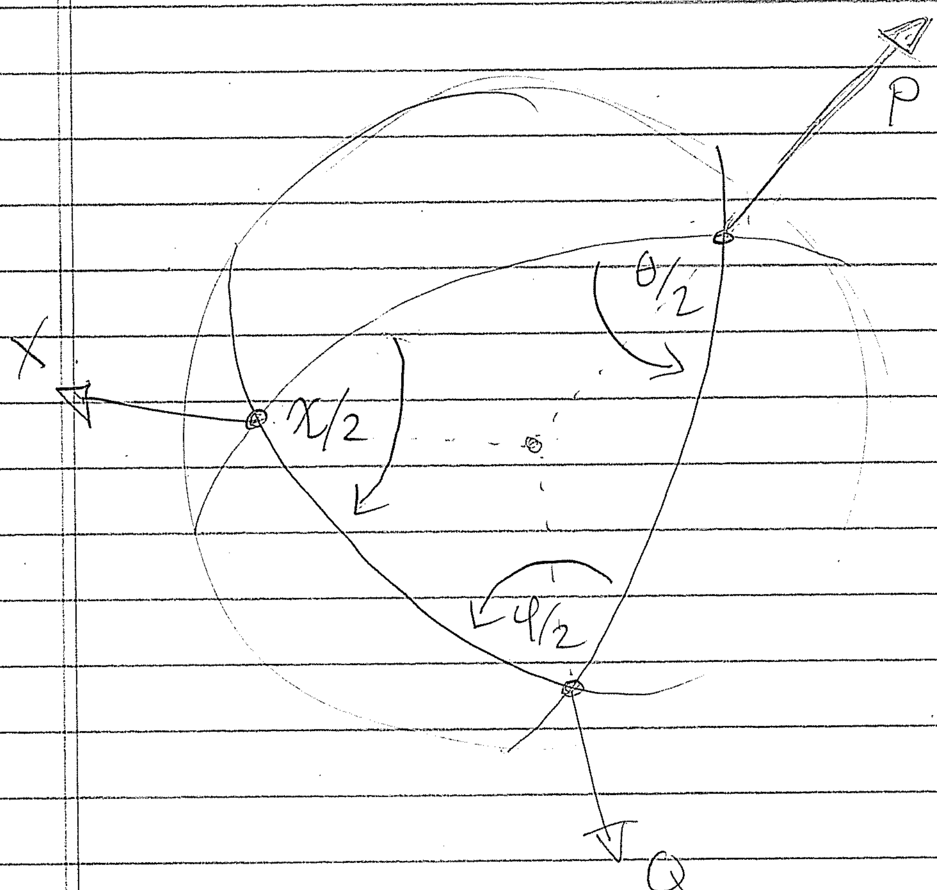
Given vector $P \in \mathbb{R}^3$ and angle $\theta \in \mathbb{R}$, let

$$R^P_\theta = \text{rotation about axis } \mathbb{R}P \text{ by } \theta \text{ counterclockwise}$$

Then

$$R^Q_\varphi \circ R^P_\theta = R^{\text{axis?}}_{\text{angle?}} = R^X_{-\chi}$$

Answer: Intersect $\mathbb{R}^3$ with a sphere.



(HW 5.2)

Q: $SO(4)$ = <u>rotations</u> of $\mathbb{R}^4$? NO.

We have

$$\left(\begin{array}{cc|cc} \cos\alpha & -\sin\beta & & \\ \sin\alpha & \cos\alpha & \multicolumn{2}{c}{\raisebox{1ex}{0}} \\ \hline & & \cos\beta & -\sin\beta \\ \multicolumn{2}{c|}{\raisebox{1ex}{0}} & \sin\beta & \cos\beta \end{array}\right) \in SO(4).$$

But I wouldn't exactly call this a "rotation".

It's a product of 4 reflections.
(Exercise: which ones?)

Say "Rotation" := product of 2 reflections.

HW 5 due Mon.

Today: "Symmetry"

Let X be a set with some structure (eg. group, ring, field, vector space, Riemannian space, etc ...)

DEF: A "symmetry" (or "automorphism") of X is a bijection $f: X \to X$ that preserves structure.

eg. $z \mapsto \bar{z}$ ($a+ib \mapsto a-ib$) is a field automorphism ("symmetry") of $\mathbb{C}$.

$$\overline{zw} = \bar{z}\,\bar{w} \quad \& \quad \overline{z+w} = \bar{z} + \bar{w}.$$

let $\mathrm{Aut}(X)$ = the group of symmetries of X under composition.

eg $\mathrm{Aut}(\text{group } \mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$\mathrm{Aut}(\text{ring } \mathbb{Z}/n\mathbb{Z}) \cong \{1\}$

$\mathrm{Aut}(\text{vector space } \mathbb{R}^n) = GL_n(\mathbb{R})$.

$\mathrm{Aut}(\text{inner product space } \mathbb{R}^n) = O(n)$

Philosophy (Representation Theory):
Given abstract group G want to study how G "acts on" nice objects. i.e.

study group homs $\varphi : G \to \mathrm{Aut}(X)$,

where X is a nice structure. Then

info about G $\longleftrightarrow$ info about X

e.g. Abstract group D_3 is more meaningful if we think D_3 = symmetries of a triangle.

Basic Example:
Let X be a set (no structure).
We say G acts on X if there is a map $G \times X \to X$ with

$$(g, x) \longmapsto g * x \in X.$$

(1) $1 * x = x \qquad \forall x \in X$

(2) $(gh) * x = g * (h * x) \qquad \forall g, h \in G, x \in X$

In other words, for each $g \in G$ we get a map $\varphi_g : X \to X$ defined by $\varphi_g(x) = g * x$.

(2) $\Rightarrow$ $\varphi_{gh}(x) = (gh) * x = g * (h * x) = \varphi_g(\varphi_h(x))$
$= \varphi_g \circ \varphi_h(x)$

$\Rightarrow$ $\varphi_{gh} = \varphi_g \circ \varphi_h$

(1) $\Rightarrow$ $\varphi_1 = \text{id map}$

Then φ_g is a bijection $X \to X$ because it is invertible.

$$\varphi_g \circ \varphi_{g^{-1}} = \varphi_{gg^{-1}} = \varphi_1 = id \quad ///$$

Hence $\varphi : G \to \text{Aut}(X) = \{\text{bijections } X \to X\}$
$g \mapsto \varphi_g$
is a group homomorphism.

eg G acts on itself by conjugation

$\varphi : G \to \text{Aut}(G)$, $g \mapsto \varphi_g$ defined by $\varphi_g(h) = ghg^{-1}$.

eg given subgroup $H \leq G$, G acts on the cosets G/H by left multiplication

$\varphi : G \to Aut(G/H)$ defined by
$g \mapsto \varphi_g \quad \varphi_g(aH) = (ga)H$.

Warning: G/H just a set

TWO CONCEPTS: Let $G \curvearrowright X$ (G acts on X)

Given $x \in X$, let

$G(x) = Orb(x) := \{ g * x : g \in G \} \subseteq X$.
the G-orbit of $x \in X$.

Claim: $x \sim y \iff \exists g \in G, \ g * x = y$
is an equivalence. Hence X is partitioned into orbits.

Given $x \in X$, let

$G_x = Stab(x) := \{ g \in G : g * x = x \} \subseteq G$.

Claim: $Stab(x) \leq G$ is a subgroup

☆ Orbit - Stabilizer Theorem: For each $x \in X$ there exists a bijection

$$\mathrm{Orb}(x) \longleftrightarrow G/\mathrm{Stab}(x).$$

Proof: Every elt of $\mathrm{Orb}(x)$ looks like $g * x$ for some $g \in G$. Define a map $\mathrm{Orb}(x) \to G/\mathrm{Stab}(x)$ by $g * x \to g\,\mathrm{Stab}(x)$.
Surjective by definition.
Well-Defined? Injective? Note:

$$\begin{aligned} g * x = h * x &\iff x = (g^{-1}h) * x \\ &\iff g^{-1}h \in \mathrm{Stab}(x) \\ &\iff g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x). \end{aligned}$$

$\Longrightarrow$ proves well-defined
$\Longleftarrow$ proves injective ∎

eg. $G \curvearrowright G$ by conjugation.

$$\mathrm{Orb}(h) = \{ghg^{-1} : g \in G\} = C(h)$$ conjugacy class.

$$\mathrm{Stab}(h) = \{g \in G : ghg^{-1} = h,\ gh = hg\} = Z(h) \leq G.$$ centralizer.

Orbit-Stabilizer says

$$C(h) \leftrightarrow G/Z(h). \quad (\text{HW } 3.2).$$

Corollary: If $|G| < \infty$ then

$$|\mathrm{Orb}(x)| = |G| / |\mathrm{Stab}(x)|$$

$$\Longrightarrow \quad |G| = |\mathrm{Orb}(x)|\,|\mathrm{Stab}(x)|.$$

i.e. $|\mathrm{Orb}(x)|$, $|\mathrm{Stab}(x)|$ both $\mid |G|$ //.

Moreover, $\forall\, g \in G$, $x \in X$ we have

$$\mathrm{Stab}(g * x) = g\left(\mathrm{Stab}(x)\right)g^{-1}$$

Proof: Let $h \in \mathrm{Stab}(g * x)$.
i.e. $h * (g * x) = (hg) * x = g * x$.
$\Longrightarrow (g^{-1}hg) * x = x$
$\Longrightarrow g^{-1}hg \in \mathrm{Stab}(x) \Longrightarrow h \in g\,\mathrm{Stab}(x)\,g^{-1}$.

Let $h \in g\left(\mathrm{Stab}(x)\right)g^{-1}$, say $h = gag^{-1}$ with $a \in \mathrm{Stab}(x)$. Then
$h * (g * x) = (gag^{-1}) * (g * x) = (ga) * x$
$= g * (a * x) = g * x$.
$\Longrightarrow \quad h \in \mathrm{Stab}(g * x)$ ▧

In words: elements in same orbit have conjugate stabilizers ///

<u>DEF</u>: If $G \curvearrowright X$ with $\mathrm{Orb}(x) = X$ (just one orbit) we say G <u>acts</u> <u>transitively</u> on X.

i.e. $\forall x, y \in X \ \exists g \in G, \ g * x = y$.

Application: The Dodecahedron D.

Let $G = \mathrm{Aut}(D) = $ rotational symmetries $\leq SO(3)$.

$G \curvearrowright \{\text{faces of } D\}$ transitively.

Hence, given a face F, $\mathrm{Orb}(F) = \{\text{all faces}\}$
$\mathrm{Stab}(F) = $ cyclic of size 5.

$$\Rightarrow |G| = |\mathrm{Orb}(F)|\,|\mathrm{Stab}(F)| = \#\text{faces} \cdot 5 = 12 \cdot 5 = 60$$

Also $G \curvearrowright \{\text{vertices}\}$ transitively.
Let $v = $ some vertex. $\mathrm{Orb}(v) = \{\text{all vertices}\}$
$\mathrm{Stab}(v) = $ cyclic size 3.

$\Rightarrow$ $|G| = |\mathrm{orb}(v)|\,|\mathrm{stab}(v)|$

$60 = \#\text{vertices} \cdot 3$

$\Rightarrow$ $\#\text{vertices} = 60/3 = 20$.

How many edges? Let e = an edge.

$\mathrm{orb}(e) = \{\text{all edges}\}$

$\mathrm{stab}(e)$ = cyclic size 2.

$\Rightarrow$ $|G| = |\mathrm{orb}(e)|\,|\mathrm{stab}(e)|$

$60 = \#\text{edges} \cdot 2$

$\Rightarrow$ $\#\text{edges} = 60/2 = 30$ ✓.

Now let $G \curvearrowright G$ by conjugation

Recall: $g \sim h$ (conjugate) if they do the same thing.

Describe the conjugacy classes.

(1) $\{1\}$ size 1

(2) $\{\text{rotate } \pm 2\pi/3 \text{ around a vertex}\}$ size 20.

(3) $\{\text{rotate } \pm 2\pi/5 \text{ around a face}\}$ size 12

(4) $\{\text{rotate } \pm 2(2\pi/5) \text{ around face}\}$ size 12.

(5) $\{\text{rotate } \pm \pi \text{ around edge}\}$ size 15.

Class Equation:

$$60 = \underbrace{1 + 20 + 12 + 12 + 15}_{\text{partition into conj. classes.}}$$

Final observation:

If $N \trianglelefteq G$ then

① $|N| \mid |G|$

② N = union of conj. classes.

so $|N|$ = sum of $\{1, 20, 12, 12, 15\}$

Impossible unless $N = \{1\}$ OR $N = G$.

$\Longrightarrow$ G is a SIMPLE group.

(the smallest nonabelian simple group)

HW 5 due this Wed.
Exam 3 Wed Nov 3.

Summing up ...

1 Let $I \leq SO(3)$
= rotational symmetries of icosahedron/dodecahedron.

$I \curvearrowright I$ by conjugation.

Given $a, b, c \in I$ with $a = cbc^{-1}$,

Let $e_1, e_2, e_3 \in \mathbb{R}^3$ be standard basis.

Let $c = (c_1\ c_2\ c_3)$, c_i column vectors.

Let $\mathcal{B}_1 = \{e_1, e_2, e_3\}$, $\mathcal{B}_2 = \{c_1, c_2, c_3\}$

Then C = change of basis from $\mathcal{B}_1$ to $\mathcal{B}_2$.
C^{-1} = change from $\mathcal{B}_2$ to $\mathcal{B}_1$.

If $a = cbc^{-1}$ then

$$[a]_{\mathcal{B}_2} = [b]_{\mathcal{B}_1}$$

~~DO THE "SAME THING"~~.

Corollary: The conj classes of I are:

(1) $\{1\}$ size 1

(2) $\{$rotate $\pm 2\pi/3$ around vertex$\}$ size 20.

(3) $\{$rotate $\pm 2\pi/5$ around face$\}$ size 12

(4) $\{$rotate $\pm 4\pi/5$ around face$\}$ size 12

(5) $\{$rotate π around edge.$\}$ size 15.

Class Equation of I:

$$60 = 1 + 20 + 12 + 12 + 15$$

So what?

DEF: We say group G is simple if every group hom. $\varphi : G \to G'$ is injective or 0

(G cannot "collapse")

Equivalently G has no normal subgroup except $\{1\}$ and G.

"simple" $\approx$ "prime" $\approx$ "building blocks"

Fundamental Theorem Arithmetic. ($- \infty$)

$\mathbb{Z}$ has unique prime factorization.

Jordan-Hölder Theorem (1870 →)

Finite groups have "unique simple factorization"

Note: J-H $\Longrightarrow$ FTArith.
cyclic groups.
(Next Semester ....)

eg. - $\mathbb{Z}/p\mathbb{Z}$ is simple since it has No subgroups except $\{0\}$ & itself.

- no other abelian group is simple.

- non-abelian simple groups ?

Theorem: I is simple.

Proof: suppose $N \trianglelefteq I$ with $1 < |N| < 60$.

Then $|N| \in \{2, 3, 4, 5, 6, 10, 12, 15, 20, 30\}$

by Lagrange.

Also since $aNa^{-1} = N \ \forall a \in I$,

$N =$ union of conj. classes of I.

$\Rightarrow |N| = 1 +$ numbers from $\{12, 12, 15, 20\}$.

Contradiction. $\boxtimes$

I is smallest non-abelian simple group.

Also

$$A_5 \approx I \approx PSL_2(\mathbb{F}_5)$$

alternating permutations of $\{1,2,3,4,5\}$

$$= \frac{SL_2(\mathbb{F}_5)}{Z(SL_2(\mathbb{F}_5))}$$

Huge Theorem (Class. of Finite Simple groups).
Every fin. simp. gp. is one of.

(1) $\mathbb{Z}/p\mathbb{Z}$. ∞

really the same

(2) Groups like A_5. ∞

(3) Groups like $PSL_2(\mathbb{F}_5)$. ∞

(4) one of 26 "sporadic" groups.

3×10^9 base pairs in human genome.

eg. The Monster. $|M| \approx 8 \times 10^{53}$

10^{57} hydrogen atoms in a star

Recall Orbit-Stabilizer:

Let $G \curvearrowright X$. Then $\forall x \in X$,

$$\mathrm{Orb}(x) \longleftrightarrow G/\mathrm{Stab}(x).$$
$$g * x \longleftrightarrow g\,\mathrm{Stab}(x).$$

$G(x) = \mathrm{Orb}(x) = \{g * x : g \in G\} \subseteq X$

$G_x = \mathrm{Stab}(x) = \{g \in G : g * x = x\} \leq G.$

But more is true ...

DEF Call $(G, X, G \curvearrowright X)$ a G-set

Given two G-sets $G \curvearrowright X$ and $G \curvearrowright Y$, we say

$$X \cong_G Y$$

if $\exists$ bijection $\varphi : X \to Y$ such that

$$\varphi(g * x) = g * \varphi(x) \quad \forall\, g \in G, x \in X.$$

(preserves G-action).

Theorem: Given $G \curvearrowright X$ with $x \in X$,

$$\mathrm{Orb}(x) \cong_G G/\mathrm{Stab}(x).$$

as G-sets.

where $G \curvearrowright \mathrm{Orb}(x)$ by $g*(h*x) = (gh)*x$

and $G \curvearrowright G/\mathrm{Stab}(x)$ by $g*(h\,\mathrm{Stab}(x)) = (gh)\,\mathrm{Stab}(x)$.

If $G \curvearrowright X$ transitively (only one orbit)
i.e. $\mathrm{Orb}(x) = X \ \forall x \in X$ then

$$X \approx_G G/\mathrm{Stab}(x) \quad \text{for any } x \in X.$$

Philosophy (Klein's Erlangen Program, 1872)

- too many geometries!
- need to systematize.

Let X = a "geometry". (transitive).
$G = \mathrm{Aut}(X)$ its "symmetries"

Then $X \approx_G G/\mathrm{Stab}(x)$.

Replace X with cosets of G.

Say $G \curvearrowright X$ acts simply-transitively if

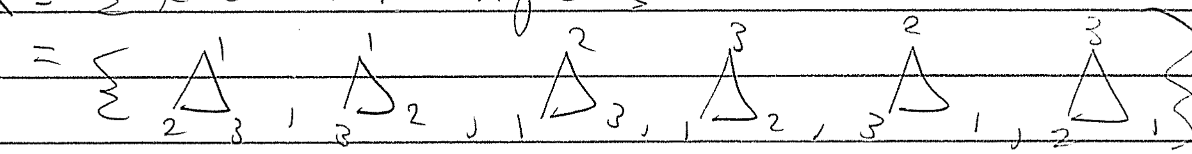
$\mathrm{Orb}(x) = X \quad \forall x \in X$ transitive
$\mathrm{Stab}(x) = \{1\} \quad \forall x \in X$ simple.

Then

$$\mathrm{Orb}(x) = \boxed{X \approx_G G} = G/\mathrm{Stab}(x) = G/\{1\}$$

Replace X with G !

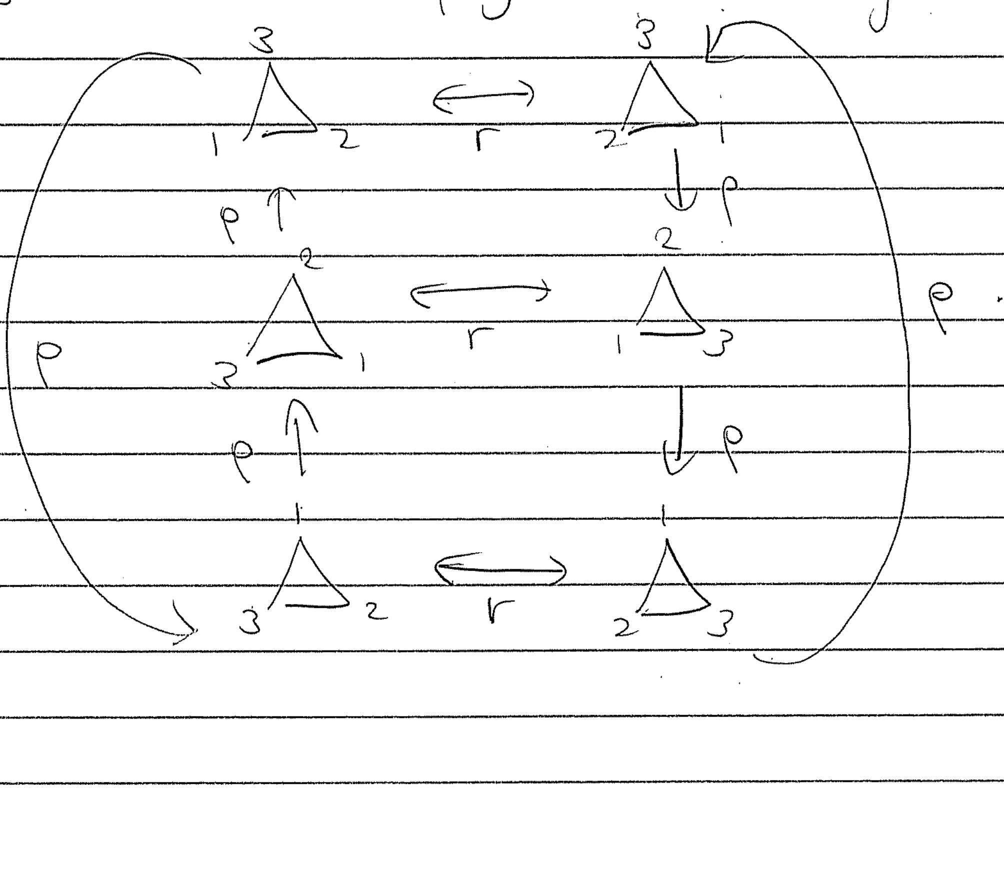
Let $X = \{$ labeled triangles $\}$

$=$ 

Let $D_3 = \langle r, \rho : r^2 = \rho^3 = 1,\ r\rho = \rho^{-1} r \rangle$

$=$ dihedral group.

$D_3 \curvearrowright X$ simply-transitively.



But $X \approx_{D_3} D_3$. so: replace X by D_3.

One choice: where to put $1 \in D_3$?

$$\begin{tikzcd}
r\rho^2 \arrow[r, leftrightarrow, "r"'] \arrow[dd, bend right=60, "\rho"'] & \rho^2 \arrow[d, "\rho"] \\
r \arrow[u, "\rho"] \arrow[r, leftrightarrow, "r"'] & 1 \arrow[d, "\rho"] \\
r\rho \arrow[u, "\rho"] \arrow[r, leftrightarrow, "r"'] & \rho \arrow[uu, bend right=60, "\rho"']
\end{tikzcd}$$

Klein: triagles are unnecessary
D_3 is enough by itself.

HW 5 due now.

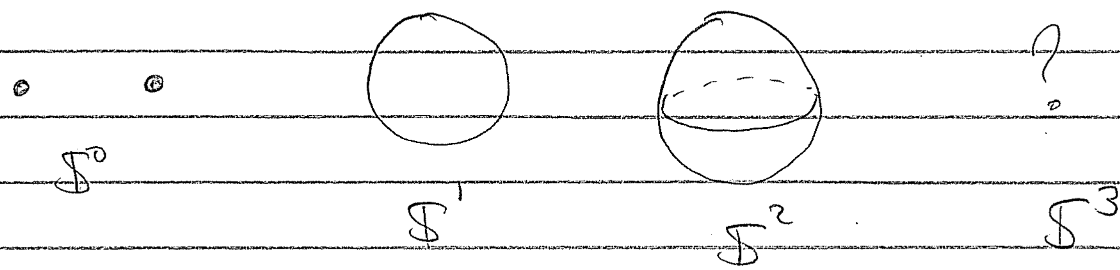
Exam 3 next Wed Nov 30

Wrapping up . . .

$\mathbb{H}$ & $SO(3)$.

<u>DEF</u>: the n-dimensional sphere is

$$\mathbb{S}^n := \{ x \in \mathbb{R}^{n+1} : \|x\| = 1 \} \subseteq \mathbb{R}^{n+1}.$$



$\{\pm 1\} \curvearrowright \mathbb{S}^0$ simply-transitively,
hence $\mathbb{S}^0 \approx \{\pm 1\}$

$U(1) \approx SO(2) \curvearrowright \mathbb{S}^1$ simply-transitively
hence $\mathbb{S}^1 \approx U(1)$ "the <u>circle</u> group"

$\mathbb{S}^2$ is <u>not</u> a group
("hairy ball" theorem)

But $\mathbb{S}^3$ <u>IS</u> a group.

Recall: Frobenius Theorem

$$\begin{array}{ccccc} \mathbb{R}, & & \mathbb{C}, & & \mathbb{H} \\ \swarrow & & \downarrow & & \searrow \\ \mathbb{S}^0 & & \mathbb{S}^1 & & \mathbb{S}^3 \end{array}$$

Let $\mathbb{H} = \{ a + bi + cj + dk : a, b, c, d \in \mathbb{R} \}$
$= \mathbb{R}^4$ (topologically).

Let $Sp(1) = \{ u \in \mathbb{H} : |u| = 1 \}$
$= \mathbb{S}^3$ (topologically).

Note that $Sp(1) \curvearrowright \mathbb{S}^3$ $(= Sp(1))$
by left multiplication, simply-trans.

$\Longrightarrow$ $\mathbb{S}^3 \approx Sp(1)$.

Moreover, this action is <u>isometric</u>:

$$v \longmapsto uv$$

and $|uv| = \underbrace{|u|}_{1}|v| = |v|$.

Hence $Sp(1) \xrightarrow{\text{hom}} O(4)$.

Moreover, since $|u|^2 = \det(u) = 1$ we have

$$Sp(1) \xrightarrow{\text{hom}} SO(4).$$

But what about $SO(3)$?

Decompose into "imaginary" and "real" parts.

$$\mathbb{H} = \mathbb{R} \oplus \mathbb{R}^3.$$

where $\mathbb{R}^3 = \{ai + bj + dk : a, b, c \in \mathbb{R}\}$
$= \operatorname{Im}(\mathbb{H})$.

$\operatorname{Im}(\mathbb{H})$ is <u>not</u> a group (not closed) but it is quite interesting.

Let $u, v \in \mathbb{R}^3 = \operatorname{Im}(\mathbb{H})$.

$u = u_1 i + u_2 j + u_3 k$

$v = v_1 i + v_2 j + v_3 k$.

Then $uv = -(u_1v_1 + u_2v_2 + u_3v_3)\,1$

$+ \left[(u_2v_3 - u_3v_2)i - (u_1v_3 - u_3v_1)j + (u_1v_2 - u_2v_1)k\right]$

i.e. $\underbrace{uv = -u \cdot v}_{\substack{\text{real} \\ \text{part} \in \mathbb{R}}} + \underbrace{u \times v}_{\substack{\text{imaginary} \\ \text{part} \in \mathbb{R}^3}} \notin \mathrm{Im}(\mathbb{H})$.

Cor: Given $u \in \mathrm{Im}(\mathbb{H})$ we have

$$u^2 = -u \cdot u + \overset{0}{\cancel{u \times u}} = -|u|^2$$

Unit imaginaries satisfy $u^2 = -1$
(LOTS of roots of -1).
~~a whole S^2 of them~~

Polar Form of $Sp(1)$.

Given $t \in Sp(1)$ we can write

$$t = a + ub \quad \text{where} \quad \begin{cases} a, b \in \mathbb{R} \\ u \text{ is } \underline{\text{unit}} \text{ imaginary} \end{cases}$$

$$|t|^2 = a^2 + b^2 = 1$$

$$\Longrightarrow \quad \begin{aligned} a &= \cos\theta \\ b &= \sin\theta \end{aligned} \quad \text{for some } \theta \in \mathbb{R}.$$

$\Rightarrow \; t = \cos\theta + u\sin\theta$.

Parameters: $\theta \in \mathbb{R}$

$u \in S^2 \subseteq \mathbb{R}^3 = \mathrm{Im}(\mathbb{H})$.

Euler's Formula

$$e^{u\theta} = \cos\theta + u\sin\theta$$

Still True! Proof only needs $u^2 = -1$. ///

Cor: De Moivre's Formula.

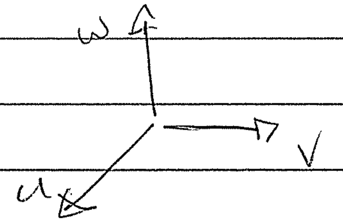
$$(\cos\theta + u\sin\theta)^n = (e^{u\theta})^n = e^{u(n\theta)}$$
$$= \cos(n\theta) + u\sin(n\theta). \checkmark$$

But WHY??

Theorem: $Sp(1) \curvearrowright \mathbb{R}^3 \; (= \mathrm{Im}(\mathbb{H}))$
by conjugation. $t \mapsto \varphi_t(u) = t^{-1}ut$.

Moreover if $t = \cos\theta + u\sin\theta$ then
$\varphi_t : \mathbb{R}^3 \to \mathbb{R}^3$ is ROTATION around
axis u by angle 2θ

Proof: Fix an orthonormal basis $\{u, v, w\}$ for $\mathbb{R}^3 (= \mathrm{Im}(\mathbb{H}))$ where



$$uv = -\overset{0}{\cancel{u \cdot v}} + \overset{w}{\cancel{u \times v}} = w$$

$$\left.\begin{array}{l} vw = u \\ wu = v \end{array}\right\} \text{similarly.}$$

Let $c = \cos\theta$, $s = \sin\theta$.
How does $t = c + us$ act on basis $\{u, v, w\}$?

$$\begin{aligned} t^{-1} u t &= (c - us) u (c + us) \\ &= (cu - u^2 s)(c + us) && u^2 = -1. \\ &= (cu + s)(c + us) \\ &= (\cancel{c^2 + s^2}) u + \cancel{sc} + \cancel{u^2 sc} && u^2 = -1 \\ &= u && c^2 + s^2 = 1. \end{aligned}$$

Fixes u ✓.

$$\begin{aligned} t^{-1} v t &= (c - us) v (c + us) \\ &= (cv - suv)(c + us) && uv = w \\ &= (cv - sw)(c + us) \\ &= c^2 v - scw + scvu - s^2 wu && \cancel{vu = -w} \\ & && wu = v. \\ &= (c^2 - s^2) v - 2sc\, w \\ &= \cos 2\theta\, v - \sin 2\theta\, w \end{aligned}$$

Similarly, $t^{-1} w t = \sin 2\theta\, v + \cos 2\theta\, w$.

5

So t acts on $\mathbb{R}^3 = \langle u, v, w \rangle$ as.

$$[t]_{\{u,v,w\}} = \begin{pmatrix} 1 & & \\ & \cos 2\theta & -\sin 2\theta \\ & \sin 2\theta & \cos 2\theta \end{pmatrix}$$

~~rotate 2θ in (v,w) plane~~
~~(around u-axis)~~

Corollary (Euler's Rotation Theorem)

In $\mathbb{R}^3$, rotation $\circ$ rotation = rotation

Proof: $\forall\, t \in Sp(1)$ we know that $\varphi_t(x) = t^{-1} x t$ is a rotation. But given $a, b \in Sp(1)$

$$\varphi_a \circ \varphi_b = \varphi_{ab}$$

Since $ab \in Sp(1)$ (it's a group), $\varphi_a \circ \varphi_b$ is a rotation

Hence we have a hom $\varphi : Sp(1) \to SO(3)$

Kernel?

$$1^{-1} x 1 = x$$

$$(-1)^{-1} x 1 = x.$$

$\ker \varphi = \{\pm 1\}$

1st Iso. Theorem

$$\Longrightarrow \quad \frac{S^3}{\{\pm 1\}} = \frac{Sp(1)}{\{\pm 1\}} \approx SO(3).$$

$$SO(3) = S^3 / \{\pm 1\} \quad \text{antipodal points identified}$$

$$= \mathbb{RP}^3 \quad \text{real projective 3-space}$$

$$\begin{tikzcd}
\begin{array}{c}\text{simply connected } S^3 \\ Sp(1) = SU(2)\end{array} \arrow[dr, "2\text{ to }1"'] & & \begin{array}{c}\text{NOT connected} \\ O(3)\end{array} \arrow[dl, "2\text{ to }1"] \\
& \begin{array}{c}SO(3) \\ \mathbb{RP}^3\end{array} &
\end{tikzcd}$$

THE END.