Last time:

We were doing revision!

Last bit of revision:
Lagrange's theorem

If G is a finite group & if $H \subseteq G$ is a subgroup then obviously $|H| \leq |G|$

but, less obviously, $|H|$ divides $|G|$.

If $r = \frac{|G|}{|H|}$, then there are precisely r different right cosets of H in G

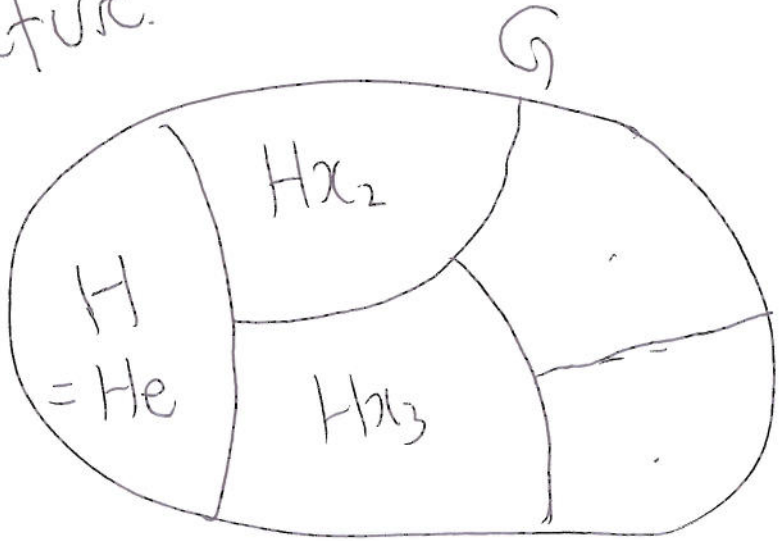
& if we call them

$Hx_1, Hx_2, \ldots Hx_r$,

then G is the disjoint union

$$G = Hx_1 \cup Hx_2 \cup \ldots \cup Hx_r.$$

Picture:



no overlaps.

Corollaries:

* If G is finite & $a \in G$, then $o(a)$ divides $|G|$ [Pf: $o(a) = |\langle a \rangle|$]
  subgroup

* If $|G| = n$ & $x \in G$ then $x^n = e$ (e = identity of G)

* If $|G| = p$ is prime then G is cyclic

  [Pf: choose $e \neq g \in G$; then $\langle g \rangle = G$]

Example: what is remainder when you divide 1000000 by 7 ?

Consider the group $\mathbb{Z}_7^*$

$= \{[1], [2], \ldots, [6]\}$

= "non-zero residues mod 7"

- a group under multiplication,

eg $[3] \times [4] = [12] = [5]$

It has order 6.

So if $[10] = [3]$ is in this group, then its order divides 6

$\therefore [10]^6 = [1]$

ie $[1000000] = [1]$

ie $1000000 \div 7 = ?$
remainder 1

Beginning of course

Chapter 1:

More examples of groups

Examples we'll see here are symmetry groups of ~~objects~~ objects in 2-dimensional space (& maybe 3-d later).

First let's define the symmetry group of $\mathbb{R}^2$ – it'll be huge – but we'll not be too bothered about it.

Start with $\mathbb{R}^2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : x, y \in \mathbb{R} \right\}$

Recall the <u>distance</u> function

$d(\underline{v}, \underline{w})$ = distance from $\underline{v}$ to $\underline{w}$, is:

if $\underline{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$, $\underline{w} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$

then $d(\underline{v}, \underline{w}) =$

$$\sqrt{(v_1 - w_1)^2 + (v_2 - w_2)^2}$$

(Pythag)

DEFINITION

An <u>isometry</u> of $\mathbb{R}^2$ is a <u>bijection</u> $f : \mathbb{R}^2 \to \mathbb{R}^2$ such that for all $\underline{v}, \underline{w} \in \mathbb{R}^2$,

$$d(f(\underline{v}), f(\underline{w})) = d(\underline{v}, \underline{w}).$$

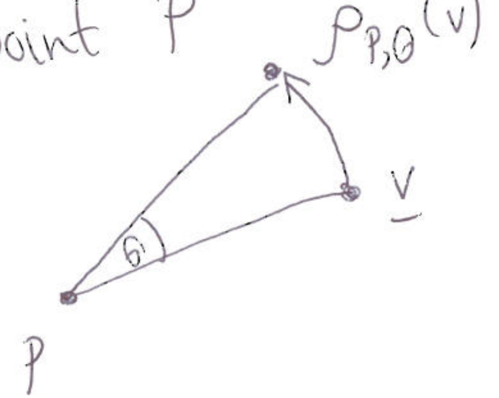
ie f "preserves distance".

Examples of isometries

① Rotations:

If $P \in \mathbb{R}^2$ & θ is an angle, define

$\rho_{P,\theta}$ = rotation through angle θ anticlockwise about the point P

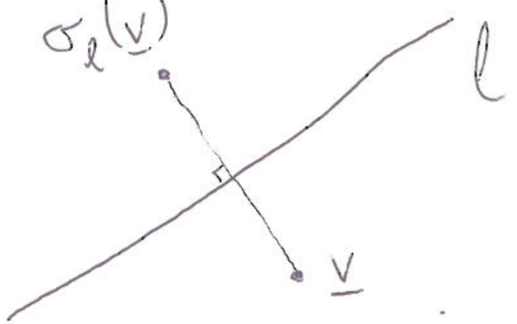


Tedious algebraic check, or "geometrically obvious":

$\rho_{P,\theta}$ is an isometry

② Reflections:

If ℓ is a line in $\mathbb{R}^2$ then define $\sigma_\ell : \mathbb{R}^2 \to \mathbb{R}^2$ to be the reflection about ℓ.

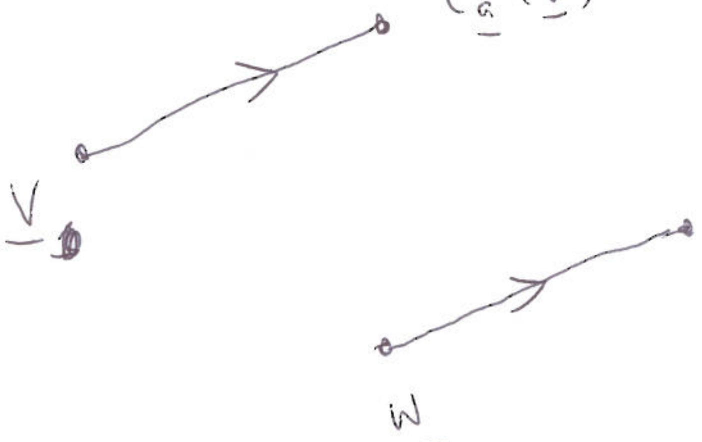


This is an isometry.

3 Translations

If $\underline{a} \in \mathbb{R}^2$, the translation $\tau_{\underline{a}} : \mathbb{R}^2 \to \mathbb{R}^2$ is simply the map defined by

$$\tau_{\underline{a}}(\underline{v}) = \underline{v} + \underline{a}$$



Then $\tau_{\underline{a}}$ is an isometry.

Remark: there are other kinds of isometries too e.g. "glide-reflection"

$f = \sigma_\ell \circ \tau_a$ is ~~often~~ sometimes not of this form

($\underline{a}$ parallel to ℓ)

<u>Definition</u> Let $I(\mathbb{R}^2)$ be the set of all isometries of $\mathbb{R}^2$.

<u>Prop^n 1.1</u> $I(\mathbb{R}^2)$ is a group, where the group law is composition of functions.

<u>Pf</u> First need to check that if $f, g \in I(\mathbb{R}^2)$ then so is $f \circ g$.

Reminder: $f \circ g$ means this function:

$(f \circ g)(v)$ means

$$f(g(v)).$$

Say $f, g \in I(\mathbb{R}^2)$.

Then $f \circ g$ is a bijection, because f & g are (M1F)

Furthermore, if $v, w \in \mathbb{R}^2$

then

$$d\big((f \circ g)(v), (f \circ g)(w)\big)$$

$$= d\big(f(g(v)), f(g(w))\big) \quad [\text{def}^n \text{ of } \circ]$$

$$= d\big(g(v), g(w)\big) \quad [f \text{ is an isometry}]$$

$$= d(v, w) \quad [g \text{ is an isometry}]$$

$\therefore$ $f \circ g$ preserves distance.

Next: check axioms