Quiz Friday: def of a group

MATH 417

HW#1 posted

08/29/2018 Wed

Last time Defined a group G as a set with
a binary operation $G \times G \to G$, $(a,b) \mapsto ab$
a unary operation $G \to G$, $a \mapsto a^{-1}$
and a distinguished element $e \in G$ so that
(i) $ea = a = ae$ for all $a \in G$
(ii) $aa^{-1} = e = a^{-1}a$ —//—
(iii) $a(bc) = (ab)c$ for all $a,b,c \in G$

stated without proof:
Theorem Suppose $f: \mathbb{R}^2 \to \mathbb{R}^2$ is an isometry. Then there is a 2×2 matrix A with $\underbrace{A^T A = AA^T = I}_{\text{i.e. } A \text{ is orthogonal}}$ and $\vec{b} \in \mathbb{R}^2$ so that

$$f(\vec{v}) = A\vec{v} + \vec{b} \quad \text{for all } \vec{v} \in \mathbb{R}^2.$$

We need this theorem to prove:
Theorem 1.1 The group

$$Euc(2) = \{f: \mathbb{R}^2 \to \mathbb{R}^2 \mid f \text{ is an isometry}\}$$

is a group with the group operation = composition.

Proof. The identity element of $Euc(2)$ is the identity map $I: \mathbb{R}^2 \to \mathbb{R}^2$, $I(\vec{v}) = \vec{v}$

- the composition of two isometries is an isometry, so we have a well-defined "multiplication"

$$Euc(2) \times Euc(2) \to Euc(2), \quad (g, f) \mapsto g \circ f$$

- Remains to show the existence of inverses.

Suppose $f: \mathbb{R}^2 \to \mathbb{R}^2$ is an isometry. Then there is a 2×2 orthogonal matrix A and $\vec{b} \in \mathbb{R}^2$ so that $f(\vec{v}) = A\vec{v} + \vec{b}$.
To find f^{-1} we need to solve

$$\vec{w} = A\vec{v} + \vec{b} \quad \text{for } \vec{w} \text{ in terms of } \vec{v}.$$

Since $\vec{w} = A\vec{v} + \vec{b}$, $\quad A^T\vec{w} = A^TA\vec{v} + A^T\vec{b}$.

But $A^TA\vec{v} = I\vec{v} = \vec{v}$. $\quad \Rightarrow \quad A^T\vec{w} = \vec{v} + A^T\vec{b}$

$$\Rightarrow \quad \vec{v} = A^T\vec{w} - A^T\vec{b}.$$

So we set $f^{-1}(\vec{w}) := A^T\vec{w} - A^Tb$ if $f(\vec{v}) = A\vec{v} + \vec{b}$.

It's easy to check that

$f(f^{-1}(\vec{w})) = \vec{w}$ and $f^{-1}(f(\vec{v})) = \vec{v}$

for all $\vec{v}, \vec{w} \in \mathbb{R}^2$.

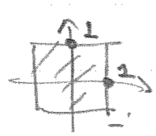
$$\Rightarrow \quad f \circ f^{-1} = I = f^{-1} \circ f.$$

We conclude that Euc(2) is a group.

<u>Def</u> A <u>geometric figure</u> is a subset R of $\mathbb{R}^2$.

<u>Ex</u> The <u>unit circle</u> $S^1 = \{(x,y) \in \mathbb{R}^2 \mid x^2+y^2=1\}$ is a geometric figure.

The unit square



$R = \{(x,y) \in \mathbb{R}^2 \mid |x| \le 1, |y| \le 1\}$ is a geometric figure.

<u>Definition</u> The <u>group of symmetries</u> $Aut(R)$ of a geometric figure R is the set

$$Aut(R) = \{ f \text{ is an isometry} \mid f(R) \subseteq R \}.$$

<u>Lemma 2.1</u> $Aut(R)$ is a group under composition with the unit element I = identity map.

<u>Proof</u> We really need to check two things:

1) for any $f, g \in Aut(R)$, $\quad g \circ f \in Aut(R)$ (So we have a map $Aut(R) \times Aut(R) \to Aut(R)$)

2) If $f \in Aut(R)$ then $f^{-1} \in Aut(R)$ as well.

Check 1) if $f(R) = R$ and $g(R) = R$ then

$$(g \circ f)(R) = g(f(R)) = g(R) \quad (\text{since } f(R) = R)$$
$$= R \quad (\text{since } g(R) = R)$$

2) If $f(R) = R$ then

$$R = I(R) = f^{-1}(f(R)) = f^{-1}(R)$$
$$\Rightarrow f^{-1} \in Aut(R)$$

So the map $Euc(2) \to Euc(2)$, $f \mapsto f^{-1}$

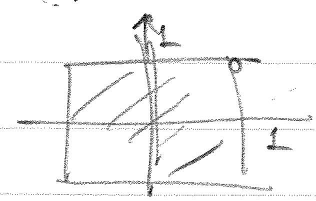
takes any $f \in Aut(R)$ to $f^{-1} \in Aut(R)$.

Ex $R = S^1$. $f(\vec{v}) = A\vec{v} + \vec{b} \in Aut(S^1)$

$\Leftrightarrow \vec{b} = 0$ (since S^1 = vectors distance 1 from $\vec{0}$)

So $Aut(S^1)$ = the group of 2x2 orthogonal matrices.

Ex R = unit square



$Aut(R)$ has 8 elements:

4 reflections, 3 rotations and I.

In terms of matrices

$$Aut(R) = \Big\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}_{90^\circ \text{ rotation}}, \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}_{180^\circ \text{ rotation}}, \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{270^\circ \text{ rotation}},$$

$$\underbrace{\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}}_{\text{reflexions}} \Big\}$$

One can work out the multiplication table ...

Permutations

Let X be a set. We define (see p18 of Goodman)

$$Sym(X) = \{ f : X \to X \mid f \text{ is invertible} \}$$

Note: If $f: X \to X$, $g: X \to X$ are invertible, then so is $g \circ f$.

Reason $(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ (g^{-1} \circ g) \circ f$
$= f^{-1} \circ I \circ f = f^{-1} \circ f = I.$

Similarly $(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ f^{-1}) \circ g^{-1}$
$= g \circ g^{-1} = I.$

$\Rightarrow$ The inverse of $g \circ f$ is $f^{-1} \circ g^{-1}$.

Lemma 2.2 $Sym(X)$ is a group with "multiplication" = composition and unity = $I = Id_X : X \to X$.

Proof
1. composition is associative
2. For any $f \in Sym(X)$, $f^{-1} \in Sym(X)$ and $f \circ f^{-1} = I = f^{-1} \circ f$.
3. For any $f \in Sym(X)$
   $f \circ I = f = I \circ f$.

Ex $X = \{1, 2\}$

$Sym(X)$ has exactly two maps: I and
$f: \{1,2\} \to \{1,2\}$, $f(1) = 2$, $f(2) = 1$.

Notation / definition

$S_n = Sym(\{1, 2, \dots n\})$ the group of permutations on n letters.

Any element $\sigma \in S_n$ is called a permutation

"Claim S_n" has $n!$ elements.

<u>Proof.</u> Given $f \in S_n$ there are

n ways to choose $f(1)$

$n-1$ ways to choose $f(2)$

$\vdots$

1 way to choose $f(n)$

$\Rightarrow$ total # of choices is $n \cdot (n-1) \cdots 2 \cdot 1 = n!$

<u>Notation</u> if $f \in S_n$ we can picture it as a table

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & & f(n) \end{pmatrix}$$

<u>Ex</u> $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$

This is combersome for larger n. Better way.

<u>Ex</u> $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 3 & 2 & 7 & 1 & 5 \end{pmatrix} \in S_7.$

What does it do?

$$1 \to 4 \to 2 \to 6 \qquad 3 \circlearrowleft \qquad 5 \to 7$$

A decomposition of σ into "cycles"!