Groups

Sunday, January 30, 2022 11:18 AM

mod 5 $(\mathbb{Z}/5\mathbb{Z})^*$

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$(\mathbb{Z}/4\mathbb{Z})$ mod 4

+	0	1	3	2
0	0	1	3	2
1	1	2	0	3
3	3	0	2	1
2	2	3	1	0

- Any patterns?

<u>Def</u> A group $(G, *)$ is a set G w/ an operation $*: G\times G \to G$ such that the following axioms are satisfied

(1) $\forall a,b,c \in G$, $(a*b)*c = a*(b*c)$ (Assoc)

(2) $\exists$ special element $e_G \in G$ (e) s.t. $\forall y \in G$

$$e_G * y = y * e_G = y \qquad \text{(Identity)}$$

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

$$a * a^{-1} = a^{-1} * a = e_G \qquad \text{(Inverse)}$$

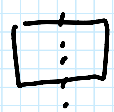
<u>Ex 1:</u> $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group, where $\mathbb{Z}/n\mathbb{Z}$ is set of integers modulo n $(1 \equiv n+1 \bmod n)$

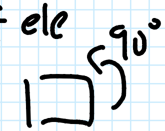
1. $+$ is associative
2. $e = 0$ is identity
3. $y + (n-y) = n \equiv 0 \bmod n$

$\Rightarrow y^{-1} = n - y$

dihedral group

<u>Ex 2:</u> $(D_4, \circ)$ is a group, where D_4 = set of symmetries of a square, $\circ$ = composition of symmetries (composing two symmetries gives you a symmetry) Here are examples of ele

reflection: $r_1 =$ 

rotation: $\theta_{\pi/2}$: 

$r_2 =$ 

Examples of Groups

Sunday, January 30, 2022 11:18 AM

Label vertices ① – ④. Two symmetries are the same if they do the same thing on the labels.

$$r_1 r_2 \left(\begin{smallmatrix} 1 & 2 \\ 4 & 3 \end{smallmatrix} \right) = r_1 \left(\begin{smallmatrix} 3 & 2 \\ 4 & 1 \end{smallmatrix} \right) = \begin{smallmatrix} 2 & 3 \\ 1 & 4 \end{smallmatrix}$$

$$= \theta_1 \left(\begin{smallmatrix} 1 & 2 \\ 4 & 3 \end{smallmatrix} \right)$$

1. Matrix multiplication is associative.
2. $e \left(\begin{smallmatrix} 1 & 2 \\ 4 & 3 \end{smallmatrix} \right) = \begin{smallmatrix} 1 & 2 \\ 4 & 3 \end{smallmatrix}$ "do-nothing"
3. Inverse of $y \in D_4$ = "reverse/undo y"

e.g. θ_1^{-1} = rotate 90° clockwise, $r_1^{-1} = r_1$

Ex 3: Symmetric group $(S_n, \circ)$, where

$S_n = \{ f : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\} \mid f \text{ is a bijection} \}$

$\circ$ = function composition

Different ways to represent ele of S_n

Two line notation:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \in S_4$$

One line notation: $\pi = \underline{2413} \in S_4$

"the top row has to be 1234 so it's redundant

Q: Is $\phi = \underline{2141} \in S_4$?

1. Function composition is assoc
2. $e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$
3. Inverse of π = reflect about horizontal axis and rearrange columns until $1, 2, \dots, n$

$$\pi^{-1} \rightsquigarrow \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

Group Tables

Sunday, January 30, 2022 11:18 AM

Hw 1: Show $|S_n| = n!$

Remark: Ex2, Ex3 are Coxeter groups

- Given a finite group, we can construct it's group table by listing out it's elements in row + column and writing result of grp multiplication

$\times$	e	g_1	g_2	$\dots$	g_k
e		$\vdots$			
g_1	$\dots$	g_3	$\dots$		
$\vdots$					
g_k					

(look back at grp tables for $\mathbb{Z}/4\mathbb{Z}$)

Lem 1: Every element of a grp appears exactly once in each row and col of it's grp table.

Ex 4: Fill out the group table using Lem 1

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$\Rightarrow$ only one grp of order 3 up to isomorphism

- In general can play same game w/ more elements, sort of like sudoku

Q: What is grp table for D_4 or S_4?

A: Quite tedious to compute, is there a more compact way to present the grp? Yes

Generators and Relations

Sunday, January 30, 2022 11:18 AM

Notation: When grp mult is given write

$$a^n = \underbrace{a * a * \cdots * a}_{n \text{ times}}, \quad ab := a*b$$

Def A relation in a grp G is a product of elements of the grp s.t. the product $= e$

Ex 4: In $\mathbb{Z}/4\mathbb{Z}$, notice

$$1^1 = 1, \quad 1^2 = 2, \quad 1^3 = 3, \quad 1^4 = 0$$

all ele can be obtained as powers of 1 and $1^4 = 0$ is a relation. This actually completely describes the grp $\mathbb{Z}/4\mathbb{Z}$

$$\mathbb{Z}/4\mathbb{Z} = \langle a \mid a^4 = e \rangle$$

Ex 5: $(\mathbb{Z}, +)$ is a grp. Powers of 1 only gives positive integers, but what if we also included non-positive powers? Let $a = 1$, then as a set $\mathbb{Z} = \langle a^n \mid n \in \mathbb{Z} \rangle$

$$(\mathbb{Z}, +) = \langle a \mid \quad \rangle$$

no relations!

Def A grp G is said to be generated by a subset $S = \{g_1, \dots, g_k\} \subseteq G$ if every element of G can be written as

$$a_1^{\varepsilon_1} \cdots a_\ell^{\varepsilon_\ell}, \quad a_i \in K, \ \varepsilon_i = \{\pm 1\}$$

Remark: The generators are sort of a "basis" for the grp.

Remark: Clearly $S = G$ generates G but the point is that frequently you can get away with much smaller subset

Presentation

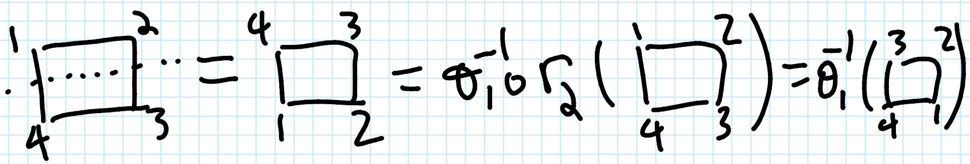
Sunday, January 30, 2022 11:18 AM

Def A presentation of a grp G, is a set S of generators for G along with a set R of minimal generating relations $\leftarrow$ all other relations in G can be derived from these

$$G = \langle S \mid R \rangle$$

Ex 5: Claim $D_4 = \langle r_1, r_2 \mid r_1^2 = e,\ r_2^2 = e,\ (r_1 r_2)^4 = e \rangle$

- $r_1 r_2 = \theta_1$



Remark: Can think of S = alphabet

R = rules that alphabet follows

Linear Algebra

Def: A map $T: \mathbb{R}^n \to \mathbb{R}^m$ is linear if

(a) $T(\vec{v} + \vec{w}) = T(\vec{v}) + T(\vec{w})$, $\vec{v}, \vec{w} \in \mathbb{R}^n$

(b) $T(c\vec{v}) = c\,T(\vec{v})$, $c \in \mathbb{R}$

- By fixing a basis $B_n = \{\vec{v_1}, \dots, \vec{v_n}\}$ of $\mathbb{R}^n$ and a basis $B_m = \{w_1, \dots, w_m\}$ of $\mathbb{R}^m$

$$\left\{ \begin{matrix} \text{linear maps} \\ \mathbb{R}^n \to \mathbb{R}^m \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} m \times n \text{ matrices} \\ M_{m\times n}(\mathbb{R}) \end{matrix} \right\}$$

$$T \longleftrightarrow \begin{array}{c} \begin{matrix} T(v_1) & \cdots & T(v_n) \end{matrix} \\ \begin{pmatrix} a_{11} & & \\ & \ddots & \\ a_{1n} & & a_{nn} \end{pmatrix} \end{array}$$

$$T(\vec{v_1}) = a_{11}\vec{w_1} + \dots + a_{1n} w_m$$

$\vdots$

Linear Algebra

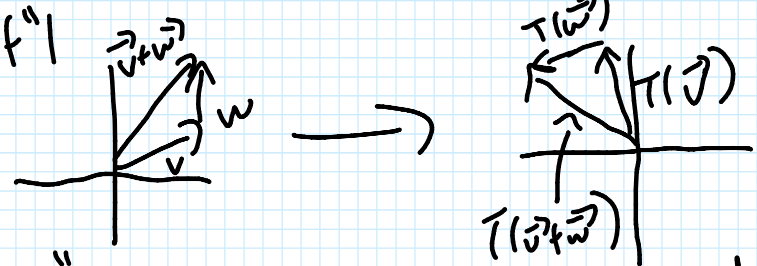
Sunday, January 30, 2022 11:18 AM

Remark: Usually people let

$$B_n = \left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix} \right\}$$

Ex 6: Rotation in $\mathbb{R}^2$ ($\mathbb{R}^n$) is a linear map

"pf"1



taught in high school

"pf"2: rotation preserves angles and lengths

Pf3: rotation by angle $\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$

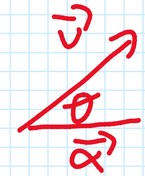
Ex 7: Reflection across a hyperplane in $\mathbb{R}^n$ is a linear map. Explicitly,

let $\alpha \in \mathbb{R}^n$. Then reflection in hyperplane orthogonal to α denoted S_α is

$$S_\alpha(\vec{v}) = \vec{v} - \frac{2\langle \vec{v}, \vec{\alpha} \rangle}{\langle \vec{\alpha}, \vec{\alpha} \rangle} \vec{\alpha}$$ ← dot product

$-\dfrac{\langle \vec{v}, \vec{\alpha} \rangle}{\langle \vec{\alpha}, \vec{\alpha} \rangle} \vec{\alpha}$ = projection of $\vec{v}$ onto line spanned by $\vec{\alpha}$

Pf:

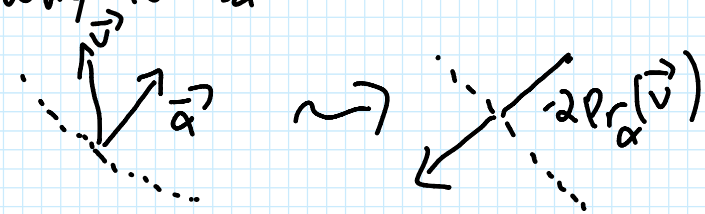


$$Pr_{\vec{\alpha}}(\vec{v}) = \|\vec{v}\| \cos\theta \frac{\vec{\alpha}}{\|\vec{\alpha}\|}$$

$$= \|\vec{v}\| \frac{\langle v, \alpha \rangle}{\|\vec{v}\| \, \|\alpha\|} \frac{\vec{\alpha}}{\|\vec{\alpha}\|}$$

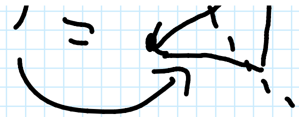
$$= \frac{\langle v, \alpha \rangle}{\langle \alpha, \alpha \rangle} \vec{\alpha}$$

Why is S_α reflection? Let $\alpha = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$



$\Rightarrow \vec{v} - 2Pr_\alpha(\vec{v}) =$

$v = \alpha f_{\alpha}(v) =$



Representations

Sunday, January 30, 2022 11:18 AM

- S_α is linear by direct computation

$$S_\alpha(v+w) = v+w - \frac{2\langle v+w, \alpha\rangle}{\langle \alpha,\alpha\rangle}\alpha$$

$$= v - \frac{2\langle v,\alpha\rangle}{\langle \alpha,\alpha\rangle}\alpha + w - \frac{2\langle w,\alpha\rangle}{\langle \alpha,\alpha\rangle}\alpha$$

$$= S_\alpha(v) + S_\alpha(w)$$

Remark: We just showed that all ele of D_4 are linear maps. Instead of thinking of elements of D_4 abstractly, can think of them as concrete matrices. Formally,

Def A representation (V,ρ) of a group G is a vector space V along with a group homomorphism

$$\rho : G \to GL(V)$$

can talk about trace, e.v., your problem is now linear

Ex 8: The map

$$D_4 \longrightarrow GL(\mathbb{R}^2)$$

$$r_1 \longrightarrow S_{\binom{1}{0}}$$

$$r_2 \longrightarrow S_{\binom{1}{-1}}$$

$$\theta_1 \longrightarrow \begin{pmatrix} \cos \pi/4 & -\sin \pi/4 \\ \sin \pi/4 & \cos \pi/4 \end{pmatrix}$$

is called the geometric representation of D_4.