Feb1

Monday, February 1, 2021 10:29 PM

HW 2 #9 Characterize D_{2n}

Generators: r, s ← all elts come from these elts & products.

Relations:

$r^n = 1$

$s^2 = 1$ ← order of generators

$rs = sr^{-1}$ ← How Gens commute.

$$\Rightarrow D_{2n} = \langle r, s \mid r^n = s^2 = 1 \quad \underline{rs = sr^{-1}} \rangle$$

$s^i r^j$ $\left.\begin{matrix} i = 0, 1 \\ j = 0, \dots n-1 \end{matrix}\right\}$ $2n$ ←

Def$^{\underline{n}}$

A subset $S \subseteq G$ generates G if all elts of G are products of elts in S & their inverses. "$G = \langle S \rangle$"

Def$^{\underline{n}}$ A presentation of a group is

$$G = \langle g_1, g_2, g_3, \dots \mid \underbrace{R_1, R_2, R_3}_{\searrow\, *} \dots \rangle$$

s.t. ① $\{g_1, g_2, \dots\}$ generates G.

② All algebraic relations in G can be derived from the R_i

* The R_i are equation in G of relations that hold among g_i..

⇝ Order of generators

⇝ How they commute

Examples $\mathbb{Z} = \langle 1 \rangle$

$$\mathbb{Z}/n\mathbb{Z} = \langle x \mid x^n = 1 \rangle$$

$$\shortparallel$$

$$\langle \bar{1} \mid n \cdot \bar{1} = 1 \rangle$$

⚠ Generators & relations can be redundant.

Ex $$X_{2n} = \langle x, y \mid \underset{\uparrow}{x^n} = \underline{y^2 = 1} \quad \underline{xy = yx^2} \rangle$$

$y^i x^j$ $\left.\begin{matrix} i = 0, 1 \\ j = 0, 1, \dots, n-1 \end{matrix}\right\} \underline{\leq 2n}$

$$\underline{x} = x y^2 = x y y$$
$$= y x^2 y$$
$$= y x \underline{x y}$$

$$= y\,\underrightarrow{x\,y}\,x^2$$

$$= = y y x^2 x^2$$

$$= y^2 x^4$$

$$= \underline{x^4}$$

$$\Longrightarrow x^3 = 1$$

$X_{2n} = \{1, x, x^2, y, yx, yx^2\}$ order ≤ 6.

Exercise $Y = \left\langle u, v \;\middle|\; \begin{array}{l} u^4 = v^3 = 1 \\ uv = v^2u^2 \end{array} \right\rangle$

$$\Longrightarrow |Y| = 1$$

Symmetric Graps

Symmetry of Hex $\rightsquigarrow$ Bijective Function $\{1, 2, \ldots, 6\} \longrightarrow \{1, \ldots 6\}$

where do vertices go.

not every fn corresponded to such a symmetry.

Today: Let's look @ all of them.

Def^n A a set.

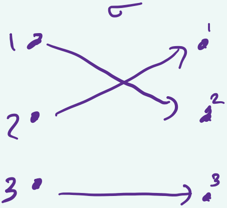
$$S_A = \{f : A \longrightarrow A \mid f \text{ bijective}\}.$$

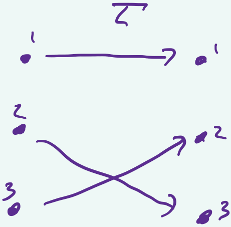
HW2 #5 $\Longrightarrow$ This is a group under $fg = f \circ g$

Defⁿ Let $A = \{1, 2, 3, \dots, n\}$ The symmetric group on n letters is

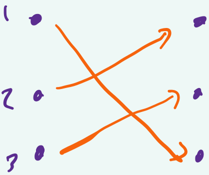
$$S_n := S_A$$

Example S_3





$\sigma = (1 \ 2)$ $\tau = (2 \ 3)$



$\tau \cdot \sigma = \tau \circ \sigma$

$(1 \ 3 \ 2)$

Prop $|S_n| = n!$

Pf/ $\sigma : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots n\}$

s.t. σ bijective. (HW1 #5 same as σ inj)

- n choices $\sigma(1)$
- $\sigma(2)$.... not $\sigma(1)$. Anything else
  $n-1$ choices
- $\sigma(3)$
  $n-2$
- $\vdots$
- $\sigma(n)$ one choice.

$$n\cdot(n-1)(n-2)\cdots(2)\cdot$$

$$\boxed{= n!}$$

Cycle Decompositions

Way to represent elements of S_n.

Def^{n} (cycle)

A cycle $(a_1\ a_2\ \cdots\ a_m) \in S_n$ is the permutation $\sigma \in S_n$ s.t.

$\sigma(a_1) = a_2$

$\sigma(a_2) = a_3$

$\vdots$

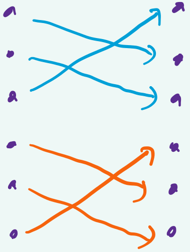
$\sigma(a_m) = a_1$

$\sigma(x) = x \quad \forall\ x \neq a_i$

Ex $\overset{\tau}{(2\ 3)}\overset{\sigma}{(1\ 2)} = (1\ 3\ 2)$

In general a permutation may have multiple cycles.

Ex



$$\begin{tikzcd}(1 \arrow[r, bend right] & 2 \arrow[r, bend right] & 3) \arrow[ll, bend right] & (4 & 5 & 6)\end{tikzcd}$$

2 cycles

observe

① Share no elts

② They commute

$$(1\ \underline{2}\ 3)(4\ \underline{5}\ 6)$$
$$= (\underline{4\ 5}\ 6)(\underline{1\ 2}\ 3)$$

Defⁿ $\sigma \in S_n$. The cycle decomposition of σ is

$$\sigma = (a_1\ a_2 \cdots a_{n_1})(b_1\ b_2 \cdots b_{n_2}) \cdots (z_1\ z_2 \cdots z_{n_z})$$

s.t All disjoint.

$$\begin{tikzcd}a_1 \arrow[r] & a_2 \arrow[r] & \cdots \arrow[r] & a_{n_1} \arrow[lll, bend left]\end{tikzcd}$$

$$\begin{tikzcd}b_1 \arrow[r] & b_2 \arrow[r] & \cdots \arrow[r] & b_{n_2} \arrow[lll, bend left]\end{tikzcd}$$

$$\vdots$$

$$\begin{tikzcd} z_1 \arrow[r] & z_2 \arrow[r] & \cdots \arrow[r] & z_{n_3} \arrow[lll, bend left] \end{tikzcd}$$

These always exist.

Proof by algorithm

First $|\sigma| \le |S_n| = n!$ (HW2 7?)

$\rightsquigarrow \sigma^k = id$ some k.

$a_1 \in S_n$ $a_2 = \sigma(a_1)$

$a_3 = \sigma(a_2) = \sigma^2(a_1)$

$\vdots$

$a_1 = \sigma(a_{n_1}) = \overset{id}{\sigma^k}(a_1)$

$\rightsquigarrow (a_1\ a_2 \cdots a_{n_1})$.

Choose $b_1 \neq a_i$. rinse repeat until exhaust set $\{1, \dots, n\}$.

Rmk [DF Page 30 do it for a $\sigma \in S_{13}$]

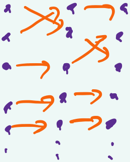
Observation

$(2\ 3)(1\ 2) = (1\ 3\ \underset{*}{2})$

$(1\ 2)(2\ 3) = (1\ 2\ 3)$

$(1\ 2), (2\ 3) \in S_n$ any & Don't commute.

Ex/



$n \geq 3$.

Theorem S_n not abelian for any $n \geq 3$.

Exercise

$$(1\ 2\ 3)\underbrace{(3\ 5)(2\ 3\ 4)} \leftarrow$$

$$\underbrace{(1\ 2\ 3)(2\ 5\ 3\ 4)}$$

$$(1\ 2\ 5)(3\ 4) \leftarrow$$

Facts / Upshots

① Cycle decomp is unique.... up 2

i) Reordr Cycles

ii) Rotating cycles.

(Pf later)

$$(1\ 2\ 5) = (2\ 5\ 1)$$

② $\sigma = (a_1 \cdots a_{n_1}) \cdots (z_1 \cdots z_{n_z})$ cycle decomp

$$|\sigma| = \mathrm{lcm}(n_1, n_2, \ldots, n_z).$$

Pf/ HW. $(1\ 2\ 3)^3 = id$

§ Homomorphisms & Isomorphisms

Ex

$$(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z}) = \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{0}),(\bar{1},\bar{1})\}$$

$$(\bar{1},\bar{1})+(\bar{0},\bar{1})$$

$$=(\bar{1}+\bar{0},\ \bar{1}+\bar{1}) = (\bar{1},\bar{0})$$

Ex

$$(\mathbb{Z}/12\mathbb{Z})^{\times} = \{\bar{1},\bar{5},\bar{7},\overline{11}\}$$

$$\bar{7}\cdot\overline{11} = \overline{77} = \bar{5}$$

$$\bar{7}\cdot\bar{7} = \overline{49} = \bar{1}$$

Ex $G = \{e, x, y, z\}$

$$x^2 = y^2 = z^2 = e$$

$xy = z$

$xz = y$

$yz = x$

abelian

Observe Same group up to relabelling elements.

Exercise Show also true for Group from HW2 #4.

Goal Develop a good notion of same-ness for groups.

Recall For sets, this notion of sameness was capture by notion of bijection.

Observe

Bijection not enough to capture sameness of groups.

Ex

① $\mathbb{Z}/4\mathbb{Z}$ not like 3 gps above.
(e.g. above all elts order ≤ 2
$|3| = 4$ in $\mathbb{Z}/4\mathbb{Z}$.)

② $\underset{\substack{\uparrow \\ \text{abelian}}}{\mathbb{Z}/6\mathbb{Z}}$ & $\underset{\substack{\uparrow \\ \text{not.}}}{S_3}$ have 6 elts.

Want bijection that respects group law.

$$\begin{tikzcd} G \arrow[rr, leftrightarrow, "\text{bijection}"] & & H \\ g_1 \arrow[rr, leftrightarrow, "\text{lines up}"] & & h_1 \\ g_2 \arrow[rr, leftrightarrow, "\text{lines up}"] & & h_2 \\ g_1 \cdot g_2 \arrow[rr, leftrightarrow] & & h_1 \cdot h_2. \end{tikzcd}$$

*

Exercise

Fails
$$\underline{(\mathbb{Z}/12\mathbb{Z})^\times \longleftrightarrow \mathbb{Z}/4\mathbb{Z}}$$

$$x \longleftrightarrow 3$$

$$1 = x^2 \longleftrightarrow 3+3 = 2$$

$$1 \longleftrightarrow 2$$

$$1 = 1^2 \longleftrightarrow 2+2 = 0$$

Right type of functions btwn groups

Defn Let $(G, *)$, $(H, \star)$ be groups. A (group) homomorphism is a function

$$\phi : G \longrightarrow H$$

s.t.

$$\phi(x * y) = \phi(x) \star \phi(y)$$

$\forall\ x, y \in G$.

Notation $\phi(xy) = \phi(x)\phi(y)$

Defn Let $\phi : G \longrightarrow H$ be a homomorphism. If ϕ is bijective, the we call ϕ an isomorphism.

We say G & H are isomorphic.

Notation

$$G \cong H$$

$$G \simeq H$$

$$\phi : G \xrightarrow{\sim} H$$

Examples

1) All graps ①, ②, ③ from before are isomorphic.

2) $\mathrm{id}_G : G \longrightarrow G$ is an isomorphism

$\mathrm{id}(x+y) = x+y = \mathrm{id}(x) + \mathrm{id}(y)$ ✓

bijective ✓

3) $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/n\mathbb{Z}$

$a \longmapsto \bar{a}$

surjective homomorphism

$\phi(a+b)$
$= \overline{a+b}$
$= \bar{a} + \bar{b}$
$= \phi(a) + \phi(b)$ ✓

4) $\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}_{>0}, \times)$

$x \longmapsto e^x$

$e^{x+y} = e^x e^y$ homom.

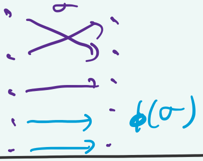
log an inverse.

So $(\mathbb{R}, +) \simeq (\mathbb{R}_{>0}, \times)$

5) $S_3 \xrightarrow{\phi} S_5$

$(1\ 2) \longmapsto (1\ 2)$

$(1\ 2\ 3) \longmapsto (1\ 2\ 3)$



Exercise

Injective homom.

All $n \leq m$ exist injective hom

$\phi : S_n \longrightarrow S_m$

Properties of homomorphisms & isomorphisms

① Let $\phi : G \longrightarrow H$ & $\psi : H \longrightarrow K$ be homomorphisms. Then

$$\psi \circ \phi : G \longrightarrow K$$ is too.

Exercise.

② Let $\phi : G \longrightarrow H$ be an isomorphism.

↗ HW1 $\Longrightarrow$ $\exists$ unique $\phi^{-1} : H \longrightarrow G$ of sets.

Exercise

Show ϕ^{-1} is an isomorphism. ←

③ ϕ, ψ from ① are isos.

Then so is $\psi \circ \phi$.

Consequence

"Isomorphic" is an equivalence relation!

i) Reflexive $G \simeq G$

ii) Symmetric ②

iii) Transitive ③

The equivalence classes are called isomorphism classes of groups.

The algebraic properties of a group should all be captured by its isomorphism class.

Prop $\phi : G \xrightarrow{\sim} H$ an iso.

G & H share many properties

1) G abelian $\Longleftrightarrow$ H is abelian.

2) $|G| = |H|$

3) $x \in G$, $\Rightarrow$ $|x| = |\phi(x)|$

Pf/ G abelian $\Longrightarrow$ H is.

Let $h_1, h_2 \in H$.

ϕ surjective, $\exists$ g_i s.t. $\phi(g_i) = h_i$ $\leftarrow$ $i = 1, 2$.

$$\begin{aligned} h_1 h_2 = \phi(g_1)\phi(g_2) &= \phi(g_1 g_2) \\ &= \phi(g_2 g_1) \\ &= \phi(g_2)\phi(g_1) \\ &= h_2 h_1 \end{aligned}$$

✓

Other direction same using ϕ^{-1}. $\varnothing$

2) True for any bijection.

3) Exercise.