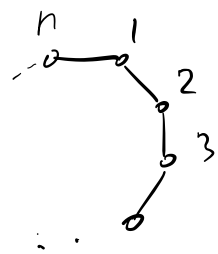
Lecture 11

Last time

- dihedral groups D_{2n}

  symmetries of

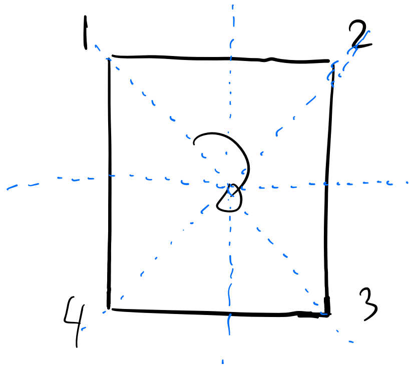


- $D_{2n} \hookrightarrow S_{2n}$

  where vertices go

- $D_6 \xrightarrow{\sim} S_3$

Example: $n=4$



← have rotation by $\frac{\pi}{2}$ and its powers:

$1, \underset{\overset{\|}{r}}{(1234)}, (13)(24), (1432)$

↑ have 4 reflections:

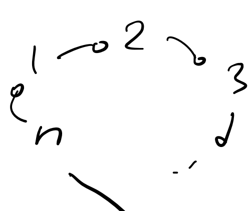
$\underset{\overset{\|}{s}}{(24)}, (12)(34), (13), (14)(23)$

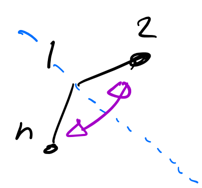
D_8 ← consists of 8 elements

← generated by <u>s, t</u>

<u>relations</u>: $r^4 = s^2 = 1$ ← clear

<u>less obvious</u>: $rs = sr^{-1} \iff rsr = s$

rotation 

reflection: 

Thm

$$D_{2n} = \langle r, s \rangle \Big/ \begin{matrix} r^n = s^2 = 1 \\ rs = sr^{-1} \end{matrix}$$

will define this carefully and prove thm

note that this presentation allows to think about D_{2n} and homomorphisms from it in very explicit terms

Claim

1) D_{2n} ← generated by s, r

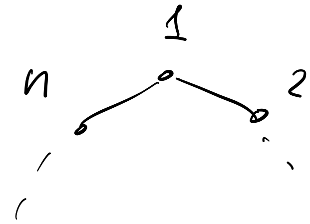
2) $|D_{2n}| = 2n$

Proof.

1) pick $\sigma \in D_{2n}$, $1 \mapsto i$ ← for some i

Composing with r^{1-i} can assume that

$\sigma : 1 \mapsto 1$



Then $n \mapsto \begin{cases} 2 \\ n \end{cases}$ ← have only these two options (σ preserves distances!)

Composing with s (if needed) can assume:

$$\sigma : \begin{array}{l} 1 \mapsto 1 \\ 2 \mapsto 2 \end{array}$$ ←

determines σ uniquely

(again use that σ preserves distances)

2) From the proof of 1) it is clear that:

$$D_{2n} = \{\underbrace{1, r, r^2, \dots, r^{n-1}, s}_{\text{all distinct}}, sr, \dots, sr^{n-1}\}$$

$\Downarrow$

$$n+1 \leq |D_{2n}| \leq 2n$$

$\Downarrow$

$$|D_{2n}| = 2n \quad (\text{use } n \mid |D_{2n}|)$$

Generators and relations: general theory

Free group

Start with S — arbitrary set.
$S = \{x_1, \dots, x_n\}$ — may be infinite in general

$\mathcal{F}(S)$ ← "free" group generated by x_i

consists of all possible products

$x_{i_1}^{\pm 1} \cdot x_{i_2}^{\pm 1} \cdot \dots$ modulo relations

(*) $\dots a \cdot x_i \cdot x_i^{-1} \cdot b \dots = \dots a \cdot b \dots$

Formal definition of $\mathcal{F}(S)$:

Let $\tilde{\mathcal{F}}(S) = \{ x_{i_1}^{\pm 1} x_{i_2}^{\pm 1} \dots \}$

define $\sim$ on $\tilde{\mathcal{F}}(S)$ as follows:

two elements of $\tilde{\mathcal{F}}(S)$ are equivalent if one can be obtain from the other via operations $(*)$.

Claim (see Section 7.9 of Artin's book for details)

1) $\sim$ = equivalence relation

2) every equivalence class has unique shortest representative (called reduced word)

↑ check this!

Example:

sts ⤳ reduced

$sttt^{-1}s$ ⤳ not reduced

Definition $\mathcal{F}(S) := \tilde{\mathcal{F}}(S)/\sim$

↗ set of **equivalence classes**

Claim: $\mathcal{F}(S)$ has a **group structure**

given by: if $A, B \in \mathcal{F}(S)$, then

to define $A \cdot B$ pick any $a \in A$, $b \in B$

then $A \cdot B$ ⤳ equivalence class of ab

↗ Check that this operation is well-defined

is it clear what you need to check here?

Relations

Start with $\mathcal{F}(S)$, want to impose some relations $R \subset \mathcal{F}(S)$

↳ want all of these elements to be equal to 1

How to define $\mathcal{F}(S) / \langle R \rangle$?

Ex: $\langle r, s \rangle / \langle r^4, s^2, srsr^{-1} \rangle$

↳ what this quotient means?

Note: $\left.\begin{matrix} r^4 = 1 \\ s^2 = 1 \end{matrix}\right\} \Rightarrow r^4 s^2 = 1 \Rightarrow$ the whole subgroup of $\mathcal{F}(S)$ generated by R

must be in <R>

Naively: can try $\mathcal{F}(S) / \langle R \rangle$ — subgroup generated by R

this is not a group in general (may not be normal!)

Correct thing to do:

$\langle R \rangle \subset \mathcal{F}(S)$

$\langle R \rangle$: minimal normal subgroup that contains R

And then $\mathcal{F}(S) / \langle R \rangle$ ← makes sense and has group structure

How to think about $\langle R \rangle$:

$\langle R \rangle \leftarrow$ elements of G that can be obtained from R using a finite sequence of the operations of multiplication, inversion, and <u>conjugation</u>.

<u>Ex:</u> $\langle r^4, s^2, srsr^{-1} \rangle_R$ contains $\underline{rsr^{-1}s}$

$$rsr^{-1}s = s^{-1} \cdot srsr^{-1} \cdot s$$

<u>The most important property of $\mathcal{F}(S)/\langle R \rangle$</u>

<u>Thm</u> $G \leftarrow$ arbitrary group, then

$\varphi : \mathcal{F}(S)/\langle R \rangle \to G$

is **the same** as:

1) $y_i \in G \quad \forall x_i \in S$

↑ collection of elements in G

2) $\forall x_{i_1} \cdots x_{i_k} \in R, \quad y_{i_1} \cdots y_{i_k} = 1$

<u>proof.</u>

(1) given y_i, we can define

$$\begin{array}{ccc} F(S) & \xrightarrow{\tilde{\varphi}} & G \\ \cup & & \cup \\ x_i & \longmapsto & y_i \end{array}$$

it extends to a homomorphism ← why?

② We have:

$$\begin{array}{ccc} \mathcal{F}(S) & \xrightarrow{\tilde{\psi}} & G \\ & {\scriptstyle\varphi}\searrow & \nearrow {\scriptstyle\Psi} \\ & & \mathcal{F}(S)/\langle R \rangle \end{array}$$

← want Ψ s.t. this diagram is commutative

General theorem that implies ②

<u>Thm</u> Let $f: S \to S'$ ← group homom. with kernel K

Let $N \subset S$ normal contained in K.

Then there is a <u>unique</u> map $S/N \xrightarrow{h} S'$ s.t.

$$\begin{array}{ccc} S & \xrightarrow{f} & S' \\ & \searrow & \nearrow {\scriptstyle h} \\ & S/N & \end{array}$$

← is commutative

← will prove next time