Lecture 10

Last time: - $H \subset G$ normal $\Leftrightarrow$ G/H group.

- in general, G/H set.

- for G finite, $[G:H] := |G/H|$

- $aH \xrightarrow{\sim} H$ (inverse a.)
  $a \mapsto a^{-1}$.

Corollary G finite

$$|G| = |H| \cdot [G:H]$$

Proof. $G = \bigsqcup aH$

number of cosets is $|G/H|$

$|aH| = |H|$

$$|G| = \sum_{|G/H|}' |H| = |G/H| \cdot |H| \quad \checkmark$$

Theorem (Lagrange's thm)

Let $H \subset G$. The order of H

(H a subgroup)

divides the order of G.

Corollary The order of an element of a finite group divides the order of the group.

proof Take $a \in G \rightsquigarrow \langle a \rangle \subset G$.

Recall that $\text{ord}(a) = |\langle a \rangle|$ divides $|G|$ by Lagrange's thm applied to $H = \langle a \rangle$

Corollary Suppose G has prime order

$\Leftarrow$

$G \simeq \mathbb{Z}/p\mathbb{Z}$ or $G = \{1\}$

proof:

Assume $G \neq \{1\}$. Take $a \in G \setminus \{1\}$.

$ord(a) > 1$, $ord(a) \mid p \Rightarrow ord(a) = p$

It follows that $\langle a \rangle = G$

is

$\mathbb{Z}/p\mathbb{Z}$

Corollary G - finite, $a \in G$.

Then $a^{|G|} = 1$.

proof. $a^{ord(a)} = 1$, $ord(a) \mid |G|$

$$a^{|G|} = \left(a^{ord(a)}\right)^{\frac{|G|}{ord(a)}} = 1 \checkmark$$

Example of application of Lagrange's thm

(1)

If $H, K \subset G$ ← subgroups of a finite group G

and $\gcd(|H|, |K|) = 1 \Rightarrow H \cap K = \{1\}$

proof $|H \cap K| \mid |H|$ & $|H \cap K| \mid |G|$

use $\gcd(|H|, |K|) = 1$

$\Rightarrow |H \cap K| = 1$ ✓

(2) Let G a finite, abelian of order $2n$ with n odd.

Show that G contains a unique element of order 2.

Proof. 1) pair elements $g \mapsto g^{-1}$

element 1 will be paired with itself $\Rightarrow$ $\exists$ another element g s.t.

$$g^{-1} = g$$

$$g^2 = 1$$

Remains to show that this g is unique.

Consider $H := \langle g \rangle \subset G$

H: normal

Take G/H - group of odd order.

If $x \in G$ - has order $2 \Rightarrow x^2 = 1$

$\Rightarrow (xH)^2 = 1 \Rightarrow xH = H \Rightarrow x \in \{1, g\}$

$\Rightarrow x = g$ ✓

Important comment

Lagrange's thm tells us that if $a \in G$

$$\text{ord}(a) \mid |G|$$

Is the converse true?

In general NO!

take $(\mathbb{Z}/12\mathbb{Z})^\times$ — it has order 4 but no element of order 4

The converse is true for prime divisors of $|G|$.

will prove later

Theorem (Cauchy) Let G be a finite group, $p \mid |G|$ (p prime).

Then $\exists\, a \in G$ s.t. $\text{order}(a) = p$

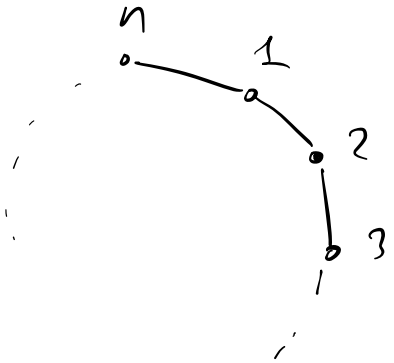
try to prove this Thm. for G commutative

Dihedral groups

An important family of examples of groups is the class of groups whose elements are symmetries of geometric objects.

The simplest subclass of symmetries of regular planar figures

Def. for $n \geq 3$, let D_{2n} be the set of symmetries of a regular n-gon:

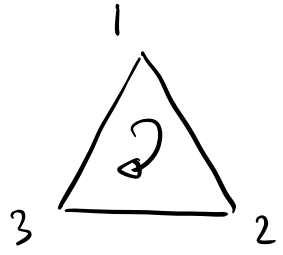


Each symmetry can be described uniquely by the corresponding permutation of $\{1, 2, \ldots, n\}$.

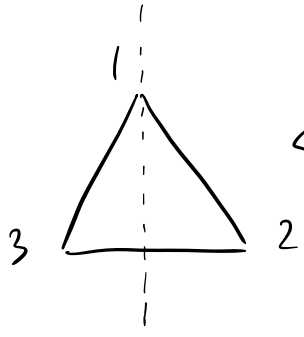
In other words, we have an embedding:

$$D_{2n} \hookrightarrow S_n$$

Example: $n = 3$



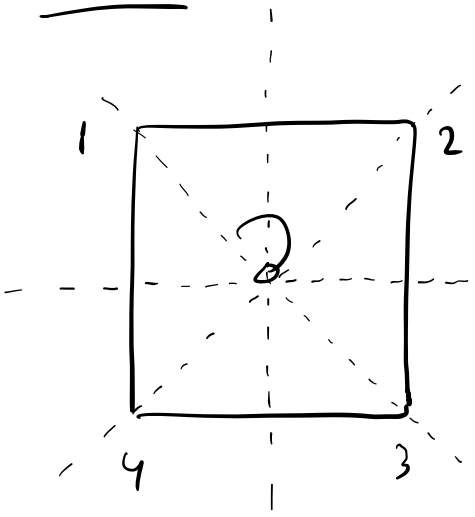
$\curvearrowleft$ rotation 2 by $\frac{2\pi}{3}$ $\leftrightarrow$ $(123) \in S_3$



$\curvearrowleft$ reflection $\leftrightarrow$ $(23) \in S_3$

$(123), (23)$ generate $S_3 \Rightarrow D_6 = S_3$

$n = 4$



have rotation by $\frac{\pi}{2}$

and its powers:

$$1, \underbrace{(1234)}_{r}, (13)(24), (1432)$$

have 4 reflections:

$$\underbrace{(24)}_{s}, (12)(34), (13), (14)(23)$$

D_8 consists of $\underline{8}$ elements

generated by $\underline{s, t}$

Relations: $r^4 = s^2 = 1$ clear

Less obvious: $rs = sr^{-1} \iff rsr = s$

Thm: $D_{2n} = \langle r, s \rangle \,/\, r^n = s^2 = 1,\ rs = sr^{-1}$

will make sense of this and prove thm

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

First step:

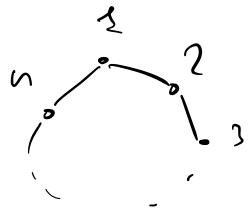
1) D_{2n} is generated by s, r

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

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

Composing with r^{-i} can assume that

$\sigma : 1 \longmapsto 1$



Then $2 \longmapsto \begin{cases} 2 \\ n \end{cases}$

two options
(σ preserves distances!)

Composing with s (if needed) can assume: $\sigma : 1 \longmapsto 1$

$2 \longmapsto 2$

this determines σ uniquely
(use that σ preserves distances!)

understand, why?

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

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

$$\Downarrow$$

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

$$\Downarrow$$

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

Next time: careful definition of

$G = \langle x_1, \dots, x_n \rangle /$ relations + how to construct homomorphisms from G

Identification $D_{2n} \simeq \langle r, s \rangle / \langle r^n = s^2 = 1, srs = r \rangle$