

Math 322, lecture 11, 12/10/17

Last time: (1) Some thms  $\leftarrow$  PSS:  $H/H \cap N \cong HN/N$   
(2)  $A_n$  simple ( $n \geq 5$ )  
if  $H \cap N = \{e\}$

Today: (1)  $A_n$  simple ( $n \geq 5$ )  
(2) Group actions

Thm: Let  $n \geq 5$  then  $A_n$  is simple.

Pf: Let  $N \triangleleft A_n$  be normal, non-trivial

Then there exists  $\sigma \in N \setminus \{e\}$  of minimal support.  
wlog  $\text{supp}(\sigma) = \{1, 2, \dots, k\}$ .

(1)  $k \neq 1$  ( $\sigma \neq \text{id}$ )

(2)  $k \neq 2$  (transpositions are odd)

(3) If  $k=3$ ,  $\sigma = 3$ -cycle, then  $N$  contains all 3-cycles

(Lemma (lemma: if  $\sigma, \sigma'$  3-cycles  $\exists \rho \in A_n: \rho \sigma \rho^{-1} = \sigma'$ )  
 $\neq N$  is normal

then  $A_n \supseteq N \supseteq \langle 3\text{-cycles} \rangle = A_n$  two

(4) If  $k=4$ ,  $\sigma = 4$ -cycle or prod of 2-cycles

but 4-cycles are odd, so  $\sigma = \text{prod of two disjoint transpositions}$ . By lemma all of those are conjugate in  $A_n$ , so  $N$  contains all of them, since they together generate  $A_n$ ,  $N = A_n$

(5)  $k \geq 5$ , and  $\sigma$  has a cycle of length  $\geq 3$

wlog  $\sigma(1)=2, \sigma(2)=3, \sigma$  moves 4,5 as well

let  $\gamma = (345)\sigma(345)^{-1}\sigma^{-1}$

if  $\sigma(i)=i$  then  $i > 5$ . Then  $\sigma^{-1}(i)=i$  as well

also  $(345)$ , and  $(345)^{-1} = (543)$  only move 3,4,5 not  $i$ .

It follows that  $\gamma(i)=i$ .

Also,  $(345)$  fixes 2,  $(345)^{-1}$  fixes 1, so  $\gamma(2)=2$ .

~~so  $\gamma \in N$~~  Now  $(345)\sigma(345)^{-1} \in N$  since  $N$  is normal,

so  $\gamma \in N$  has smaller support than  $\sigma$ .

and  $\sigma^{-1} \in N$

But  $\gamma(3)=4$  so  $\gamma \neq \text{id}$ , a contradiction

(6)  $k \geq 5$ ,  $\sigma$  prod of disjoint transposition, wlog

$$\sigma = (12)(34)(56)(78) \dots \quad (\text{at least 4 such since } \sigma \text{ is even})$$

Define  $\gamma$  same way:  $\gamma = (345)\sigma(345)^{-1}\sigma^{-1}$ . Again  $\gamma \in N$

Again  $\gamma$  fixes every fixed pt of  $\sigma$  and also 1,2.

But  $\gamma(7)=8, \gamma(8)=7$  so  $\gamma \neq \text{id}$ , again a contradiction.

□

# Chapter 3: Group Actions

Def: An action of the group  $G$  on the set  $X$  is a binary operation  $\cdot: G \times X \rightarrow X$  st.:

(1)  $e_G \cdot x = x$  for all  $x \in X$

(2)  $h \cdot (g \cdot x) = (hg) \cdot x$  for all  $h, g \in G, x \in X$ .

Def: A G-set is a pair  $(X, \cdot)$  where  $X$  is a set,  $\cdot$  is an action of  $G$  on  $X$ .

Sometimes write  $G \curvearrowright X$

Examples: (0) trivial action: any  $G, X$  set  $g \cdot x = x$

(1) Key example:  $S_X$  acts on  $X$  by evaluation:  
 $\sigma \cdot i \stackrel{\text{def}}{=} \sigma(i)$

(def of  $\cdot$  in  $S_X$  was that  $(\sigma \circ \tau)(i) \stackrel{\text{def}}{=} \sigma(\tau(i))$ )

(2)  $F$  field,  $V$  vector space  $/F$ , then scalar multiplication is an action  $F^* \curvearrowright V$

(also  $GL(V) \curvearrowright V$ )

$T \cdot \underline{v} = T(\underline{v})$

(3)  $X$  set with "structure",  $\text{Aut}(X) = \{ \sigma \in S_X \mid \sigma, \sigma^{-1} \text{ "preserve" the structure} \}$

- Eg.  $V$  vsp,  $G =$  invertible maps

-  $D_{2n}$  acting on  $X =$  vertices of   $\leftarrow C_n$

(4)  $G$  gp,  $\text{Aut}(G) = \{ f \in \text{Hom}(G, G) \mid f \text{ is an isom} \}$  acts on  $G$ .

PS6: Induced actions: say  $G$  acts on  $X, Y$ .

$\Rightarrow G$  acts on functions from  $X$  to  $Y$ .

$\Rightarrow G$  acts on subsets of  $X$ :  $g \cdot A = \{ g \cdot a \}_{a \in A}$  if  $A \subset X$ .

:

The Regular action

Claim left multiplication is an action of  $G$  on itself:

set  $g \cdot x = gx$

New point of view: fix  $g \in G$  define  $\sigma_g: G \rightarrow G$  by

$$\sigma_g(x) = gx$$

Lemma  $(1) \sigma_g \in S_G$  for

More generally, let  $G$  act on  $X$ , define  $\sigma_g: X \rightarrow X$

by  $\sigma_g(x) = g \cdot x$

Lemma: (1)  $\sigma_g \in S_X$  for all  $g \in G$ .

(2) The map  $g \mapsto \sigma_g$  is a hom  $G \rightarrow S_X$ .

(3) The map  $\{ \text{actions of } G \text{ on } X \} \rightarrow \text{Hom}(G, S_X)$

$\mapsto \sigma$ .

is a bijection.

Pfs First verify that  $\sigma_g \circ \sigma_h = \sigma_{gh}$ .

Indeed:  $(\sigma_g \circ \sigma_h)(x) \stackrel{\text{def of } \circ}{=} \sigma_g(\sigma_h(x)) \stackrel{\text{def of } \sigma_g, \sigma_h}{=} \sigma_g(h \cdot x) = g \cdot (h \cdot x) = (gh) \cdot x \stackrel{\text{an action}}{=} \sigma_{gh}(x)$

(1) By definition of action,  $\sigma_{e_G} = \text{id}_X$ .

Now for any  $g \in G$ ,  $\sigma_g \circ \sigma_{g^{-1}} = \sigma_{gg^{-1}} = \sigma_{e_G} = \text{id}_X$

$$\sigma_{g^{-1}} \circ \sigma_g = \sigma_{g^{-1}g} = \sigma_{e_G} = \text{id}_X$$

so  $\sigma_g$  is a bijection, i.e.  $\sigma_g \in S_X$ .

(2) We already checked  $\sigma_g \circ \sigma_h = \sigma_{gh}$ .

(3) How map  $\{ \text{actions} \} \rightarrow \{ \text{homs} \}$ ?

need inverse. Given  $\sigma \in \text{Hom}(G, S_X)$  define an action of  $G$  on  $X$  by  $g \cdot x = (\sigma(g))(x)$ .

Indeed  $e_G \cdot x = (\sigma(e_G))(x) = \text{id}_X(x) = x$ .

$$g \cdot (h \cdot x) \stackrel{\text{def}}{=} (\sigma(g))((\sigma(h))(x)) \stackrel{\text{def of } \sigma}{=} (\sigma(g) \circ \sigma(h))(x) \stackrel{\sigma \text{ is a hom}}{=} (\sigma(gh))(x) = (gh) \cdot x.$$

Clear this is indeed the inverse map.  $\square$

Remark 1: I will not distinguish actions of  $G$  on  $X$  and homs  $G \rightarrow S_X$ .

Remark 2: This lemma is an important source of homomorphisms, ~~and~~ <sup>and</sup> of normal subgs (kernels)

1st Payoff:

Thm: (Cayley 1878): Every ~~subgp~~ <sup>group</sup>  $G$  is isomorphic to a subgp of  $S_G$ . In particular, every gp of order  $n$  is isom to a subgp of  $S_n$ .

Pf: Consider the left-regular action of  $G$  on itself.

This gives a hom  $L_G: G \rightarrow S_G$

$$(L_G(g))(x) = gx$$

Say  $g \in \text{Ker}(L_G)$  then  $L_G(g) = \text{id}_G$  i.e.  $g \cdot x = x$  for all  $x \in G$

so  $g = e_G$ , i.e.  $\text{Ker } L_G = \{e_G\}$  and  $L_G$  is injective,

i.e. an isom onto its image  $\square$

Example: let  $p$  be prime then  $C_p$  embeds in  $S_n$

iff  $p \leq n$

Pf: If  $n \geq p$ ,  $S_n$  contains a  $p$ -cycle,

and if  $C_p$  embeds in  $S_n$  then by Lagrange  $p \mid n!$

but if  $n < p$  all prime factors of  $n!$  are less than  $p$  so  $p \nmid n!$  and no embedding is possible