Math 322, lecture 11, 12/10/17

Last time: (1) Some thems
(2) $A_n$ simple ($n \geq 5$)

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 $\sigma \in N$ of minimal support.
where $\text{supp}(\sigma) = \{2, 3, \ldots, k\}$.

1. $k \neq 1$ ($\sigma \neq \text{id}$)
2. $k \neq 2$ (transpositions are odd)
3. If $k = 3$, $\sigma$ is a 3-cycle, then $N$ contains all 3-cycles
   (New Lemma: if $\sigma, \sigma'$ 3-cycles if $\sigma \in A_n$, then $\sigma \sigma' \sigma^{-1} = \sigma'$
   then $A_n \times N \cong (3\text{-}cycles) = A_n$ two
4. If $k = 4$, $\sigma$ is a 4-cycle or product of 2-cycles
   but 4-cycles are odd, so $\sigma$ is product 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) \( k \geq 3 \), and \( \sigma \) has a cycle of length \( \geq 3 \) with \( \sigma(1) = 2, \sigma(2) = 3 \). \( \sigma \) moves 9,5 as well. Let \( \gamma = (345) \sigma (345)^{-1} \).

If \( \sigma(i) = 1 \), then \( i > 5 \). Then \( \sigma'(i) = i \) as well.

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

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

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

Now \( (345) \sigma (345)^{-1} \in N \) since \( N \) is normal, so \( \gamma \in N \) has smaller support that \( \sigma \).

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

(6) \( k \geq 5 \), \( \sigma \) odd of disjoint transposition, wlog.

\[ \sigma = (12)(34)(56)(78) \ldots \] (at least 4 such since \( \sigma \) is even)

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

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

But \( \gamma(3) = 8 \), \( \gamma(8) = 7 \) so \( \gamma \neq \text{id} \), again a contradiction.
Chapter 3: Group Actions

Def: An action \( \textbf{of} \) the group \( G \) on the set \( X \) is a binary operation \( \cdot : G \times X \rightarrow X \) s.t.,

(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 \( \textbf{is} \) a pair \( (X, \cdot) \) where \( X \) is a set, \( \cdot \) is an action of \( G \) on \( X \).

Sometimes write \( GCX \)

Examples: (0) trivial action: any \( G, X \) set \( g \cdot x = x \)
(1) Key example: \( S_X \) acts on \( X \) by evaluation:
\[ \sigma \cdot i \overset{\text{def}}{=} \sigma(i) \]
(\( \text{def} \ \sigma \) \( \in S_X \) was that \( (\sigma \cdot x) (i) \overset{\text{def}}{=} \sigma(x(i)) \)
(2) \( F \) field, \( V \) vector space \( /F \), then scalar multiplication is an action \( \cdot : C V \times C V \)
(also \( GL(V) C V \))
\[ \tau \cdot v = \tau(v) \]
(3) \( X \) set with "structure", \( \text{Aut}(X) = \{ \sigma \in X : \sigma \text{ is \textit{preserves the structure}} \} \)
- Eq. \( V \) vsp, \( G = \text{invertible} \) maps
- \( D_{2n} \) acting on \( X = \text{vertices of } \bigcirc \)
(4) $G \to \text{Aut}(G) = \{ f \in \text{Hom}(G, G) | f \text{ is an isomorphism}, f \text{ acts on } G \}.$

**Problem 56:** Induced actions: say $G$ acts on $X, Y.$

- $G$ acts on functions from $X$ to $Y.$
- $G$ acts on subsets of $X$: $g \cdot A = \{ g^{-1}a | a \in A \}.$

**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 $\sigma_g : G \to G$ by

$\sigma_g(x) = gx$

**Lemma:** $\sigma_g \in S_X$ for all $g \in G.$

More generally, let $G$ act on $X,$ define $\sigma_g : X \to X$ 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 homomorphism $G \to S_X.$

(3) The map $g \mapsto \text{actions of } g \text{ on } X$ $\to \text{Hom}(G, S_X)$ is a bijection.
First verify that \( \sigma_g \circ \sigma_h = \sigma_{gh} \).

Indeed:

\[
(\sigma_g \circ \sigma_h)(x) = \sigma_g(\sigma_h(x)) = \sigma_g(h \cdot x) = g \cdot (h \cdot x) = ((gh) \cdot x) = \sigma_{gh}(x)
\]

an action

(1) By definition of action, \( \sigma_e = \text{id}_\mathcal{X} \).

Now for any \( g \in G \), \( \sigma_g \circ \sigma_g^{-1} = \sigma_gg^{-1} = \sigma_e = \text{id}_\mathcal{X} \)

\[
\sigma_g^{-1} \circ \sigma_g = \sigma_g^{-1} \circ \sigma_g = \sigma_e = \text{id}_\mathcal{X}
\]

so \( \sigma_g \) is a bijection, i.e. \( \sigma_g \in S_\mathcal{X} \).

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

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

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

Indeed \( e \cdot x = \sigma(e)(x) = \text{id}_\mathcal{X}(x) = x \)

\[
(g \cdot (h \cdot x)) = \sigma(g)(\sigma(h)(x)) = (\sigma(g) \circ \sigma(h))(x) = (\sigma(gh))(x) = \text{def of } \sigma \quad \sigma \text{ is a hom}
\]

= (gh) \cdot x.

Clean this is indeed the inverse map. ∎

Remark 1: I will not distinguish actions of \( G \) on \( \mathcal{X} \) and homs \( G \rightarrow S_\mathcal{X} \).
Remark 2: This lemma is an important source of homomorphisms, and of normal subgroups (kernels).

1st Payoff:

Thm: (Cayley 1878): Every group \( G \) is isomorphic to a subgroup of \( S_G \). In particular, every group of order \( n \) is isomorphic to a subgroup of \( S_n \).

Pf: Consider the left-regular action of \( G \) on itself. This gives a hom \( L_G: G \to S_G \)

\( (L_G(g))(x) = gx \)

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 isomorphism onto its image.

Example: Let \( p \) be prime. Then \( C_p \) embeds in \( S_n \) iff \( p \leq n \).

Pf: If \( n > p \), \( S_n \) 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.