Math 322, lecture 24, 30/11/2017

Review

Problem 1: Find all subgroups of $D_{2n} = \left\langle p, r \,\middle|\, \begin{matrix} p^2 = r^n = e \\ prp = r^{-1} \end{matrix} \right\rangle$
$= \left\{ p^a r^b \,\middle|\, \begin{matrix} 0 \le a < 2 \\ 0 \le b < n \end{matrix} \right\}$

Solution: 1st idea: $R = \langle r \rangle \cong C_n$ is a large subgroup

2nd idea: we know subgps of C_n: (HW)
for each $m | n$, C_n has a unique subgp of order m,
here $\langle r^{n/m} \rangle$ has order m

3rd idea: If $H < D_{2n}$, study $H \cap R$, then H
($H \cap R$ must be one of the subgps of idea 2)

question: how many reflections can we add?

4th idea: $[D_{2n} : R] = 2$, so if $g, h \in D_{2n} \setminus R$ then $gh^{-1} \in R$

(by hand: pr^i, $p \cdot r^j$ differ by $(pr^i) \cdot (pr^j)^{-1} = pr^i r^{-j} p = pr^{i-j} p$
$= r^{j-i} \in R$)

so if $pr^i, pr^j \in H$ then their difference $(pr^i)(pr^j)^{-1} \in H \cap R$

(aside: $[H : H \cap R] \le [G : R]$ if $H, R < G$)

Conclusion: Every subgp has the form $\langle r^d \rangle$, $d | n$
or $\langle r^d, pr^b \rangle$, $d | n$

remains to determine these subgp more precisely, check for isom

First, we know: $\langle r^d \rangle = \{r^{di}\}_{i=0}^{\frac{n}{d}-1}$

Next, $\langle pr^b \rangle = \{1, pr^b\}$ normalizes rotations:

$$pr^b r^i (pr^b)^{-1} = pr^b r^i r^{-b} p = p r^i p = r^{-i}$$

so $\langle r^d, pr^b \rangle \simeq \langle r^d \rangle \rtimes \{1, pr^b\}$

<u>or:</u> our group has the elements $\{r^{di}\}_{i=0}^{\frac{n}{d}-1}$ and $\{pr^{b+\frac{n}{d}i}\}_{i=0}^{\frac{n}{d}-1}$

this is indeed a subgp: $r^{di} \cdot pr^{b+dj} = p \cdot pr^{di} p\, r^{b+dj} =$

$$= p \cdot r^{-di} r^{b+dj} = p \cdot r^{b+d(j-i)}$$

so $pr^b \cdot r^{di} pr^{b+dj} = pr^b p\, r^{b+d(j-i)} = r^{-b} r^{b+d(j-i)} = r^{d(j-i)}$

So our list of subgps is:

for $d|n$: $\{r^{di}\}_{i=0}^{\frac{n}{d}-1}$

for $d|n$, $b \bmod n$ $\{r^{di}, pr^{b+di}\}_{i=0}^{\frac{n}{d}-1}$

<u>5th idea:</u> In second type, b is only defined <u>mod d</u>.

(replacing b with $b+dk$ gives same coset $\{b+di\}_{i \bmod \frac{n}{d}}$ in $\mathbb{Z}/n\mathbb{Z} / \langle [d] \rangle$

(conversely, if $b \not\equiv b' \pmod d$ then sets

$\{b+di\}_{i \bmod \frac{n}{d}}$, $\{b'+di\}_{i \bmod \frac{n}{d}}$ disjoint cosets

So: The subgps of D_{2n} are:

(1) for each $d|n$, $\langle r^d\rangle \cong C_{n/d}$

(2) for each $d|n$, each $0\le b<d$, $\langle r^d, pr^b\rangle \cong D_{2n/d}$

Question? Let G, H be groups, let $C < \mathrm{Aut}(H)$ be a subgp. Suppose $\varphi, \psi \in \mathrm{Hom}(G,C)$, both surjective.

Are $G \ltimes_\varphi H$, $G \ltimes_\psi H$ isomorphic?

(PS 8: yes if G is cyclic)
(PS 9: yes if $G \cong V$)

Answer: no! Example: $G = C_4 \times C_2$

$H = C_n$ (n odd) $\quad C = \{1, \text{inverse}\} \subset \mathrm{Aut}(C_n)$

$\{\pm 1\} < (\mathbb{Z}/n\mathbb{Z})^\times$.

Map $G \twoheadrightarrow C$ by: $C_4 \twoheadrightarrow C$, $C_2 \to \{e\}$ or $C_4 \twoheadrightarrow \{e\}$, $C_2 \twoheadrightarrow C$

Question 3; X finite set, $\sim$ equiv rel on X, X_i = equiv classes $1\le i\le r$.

(a) show: $G = \{\sigma \in S_X : x\sim y \text{ iff } \sigma x \sim \sigma y\} < S_X$

(b) when is $G \cong \prod_i S_{X_i}$?

S_{X_i} embeds in S_X as the permutations supported in X_i

these commute with each other (permutations with disjoint support commute). so $\langle \bigcup_i S_{X_i} \rangle \cong \prod_i S_{X_i}$

~~Also~~ (isom is: if $\sigma_i \in S_{X_i}$ define $\sigma = \bigcup_i \sigma_i$

i.e. $\sigma(x) = \sigma_i(x)$ if $x \in X_i$)

This is a subgp of G: for any $x, y \in X$, $\sigma \in \prod_i S_{X_i}$,

$\sigma x \sim x$, $\sigma y \sim y$ so $\sigma x \sim \sigma y$ iff $x \sim y$

Question: does G contain anything else?

(note: $G \supset \prod_{i \in I} S_{X_i}$ both finite so either have equality or G is bigger, certainly not isomorphic)

Question: can we have $\sigma \in G$ s.t. $\sigma x \not\sim x$?

suppose $\sigma x = x' \not\sim x$. Then σ maps the equivalence class of x to that of x' (this is what $\sigma \in G$ means)

and conversely so $\sigma\restriction_{[x]}$ is a bijection of $[x]$, $[x']$,

In particular they have same size

Conversely, if $\# X_i = \# X_j$, Define σ s.t. $\sigma\restriction_{X_i}$ is any bijection with X_j, $\sigma\restriction_{X_j}$ any bijection with X_i, say $\sigma = \mathrm{id}$ outside X_i, X_j.

$\sigma \in G$ since it maps equivalence classes to equivalence classes

So $G \neq \prod_i S_{X_i}$ iff two X_i have same size, $G = \prod_i S_{X_i}$ iff all equiv classes of $\sim$ have distinct sizes

Question: ~~w~~ How many elements of order m are there in C_n?

Solution: let $H < C_n$ be the unique subgp of order m $(m|n)$ $(H \cong C_m)$. Then ~~as~~ H is cyclic, so any generator of H has order m. Conversely, if $a \in C_n$ has order m, $\langle a \rangle \subset C_n$ is a subgp of order m, i.e $\langle a \rangle = H$, and a generates H.

So: $\#\{a \in C_n \mid a \text{ has order } m\} = \#\{a \in H \mid a \text{ generates } H\}$

$$\underset{\substack{\uparrow \\ H \cong \mathbb{Z}/m\mathbb{Z}}}{=} \#\{a \in \mathbb{Z}/m\mathbb{Z} \mid a \text{ is a generator}\} = \#\{a \in \mathbb{Z}/m\mathbb{Z} \mid a \text{ is prime to } m\}$$

$$= \#(\mathbb{Z}/m\mathbb{Z})^\times.$$

Eg. elements of order 5 is $C_{5^{100}}$: are 4 of them

in $(C_5)^{100}$ every element has order dividing 5, and $5^{100}-1$ of them have order 5

Question: G gp of order $351 = 27 \cdot 13$

~~either~~ G either $P_3 \rtimes P_{13}$ or $P_{13} \rtimes P_3$

suppose $P_3 \cong C_9 \times C_3$ ~~want to~~ classify G.

Solution: suppose P_3 is normal. To classify products $P_{13} \ltimes P_3$ need to study subgps of order 13 of $\mathrm{Aut}(C_9 \times C_3)$

Any element of order 9 in $C_9 \times C_3$ belongs to a "basis" with an element of order 3

~~If~~ So: if $g, h \in P_3$ have order 9, ~~have~~ $\exists\, \alpha \in Aut(P_3)$: $\alpha(g) = h$

~~So~~ Let $H < Aut(P_3)$ be the stabilizer of g. Then:

$$\# Aut(P_3) = \# H \cdot \# \text{orbit}$$

How many elements of order 9 in $C_9 \times C_3$?

$= \left\{ (a,b) \,\middle|\, \begin{matrix} a \bmod 9 \text{ generator} \\ b \bmod 3 \text{ arbitrary} \end{matrix} \right\} \longleftrightarrow (\mathbb{Z}/9\mathbb{Z})^\times \cdot \mathbb{Z}/3\mathbb{Z}$

are $6 \cdot 3 = 18$ of them

So $\# Aut(P_3) = 18 \cdot \# H$

$\# H = ?$