LECTURE 20 Nov. 3/2003

Last time:

Used class equation to show that any group of order p^2 is abelian (& only two such groups, up to iso)

We already knew a group of order p is cyclic ($\simeq \mathbb{Z}/p\mathbb{Z}$).

Q What about G of order pq (e.g. S_3, of order 6) or of order p^3?

Rmk on groups of order p^2:

Here are the two possibilities...

① There is an element $g \in G$ of order p^2. Then G is cyclic

$$G \xrightarrow{\sim} \mathbb{Z}/p^2\mathbb{Z}$$

$$g \longmapsto 1 \pmod{p^2}$$

$$(\Rightarrow g^a \longmapsto a \pmod{p^2})$$

② There is no element of order p^2. So every $g \neq e$ has order p

Then the field $\mathbb{Z}/p\mathbb{Z}$ acts on G by

$$a \cdot g = g^a = \underbrace{g \cdots g}_{a \text{ times}}$$

$$0 \cdot g = e$$

So G is a vectorspace $/(\mathbb{Z}/p\mathbb{Z})$ of dimension 2

$$G \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$$
$$g_1^{a_1} \cdot g_2^{a_2} \longmapsto (a_1, a_2)$$

Notation $n \geq 1$ $G = (\mathbb{Z}/p\mathbb{Z})^n \leftarrow$ n-dim'l v.sp. $/(\mathbb{Z}/p\mathbb{Z})$
order p^n; every $g \neq e$ of order p
is called $\boxed{\text{"elementary abelian } p\text{-group"}}$

---

§ Sylow theorems

- we've already seen:
  G acts on $S = G$ by conjugation
  $$g \cdot s = g s g^{-1}$$
  O_s = Orbits = conjugacy classes of elts. s
  G_s = centralizer of s = $\{g : gsg^{-1} = s\}$

- G also acts by conjugation on the set $S = \{H \subset G \text{ subgroups}\} =: \mathcal{H}$
  $$g \cdot H = gHg^{-1} = \text{another subgroup of } G \in \mathcal{H}$$

O_H = the set of subgroups conjugate to H
$G_H = \{g : gHg^{-1} = H\}$
= "normalizer of H"
=: "$N(H)$"

Note:

$$H \triangleleft N(H) \subset G$$

H is normal in $N(H)$ &
$N(H)$ is in fact the largest subgroup of G in which H is normal

Ex: In S_3:

$$A_3 = \{e, (123), (132)\} \triangleleft S_3$$
$$\Rightarrow N(A_3) = S_3$$

$$H = \{e, (12)\} \subset S_3$$
$$\Rightarrow N(H) = H$$

Ex: In $GL_2(F)$

$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in F \right\} \subset G := GL_2(F)$$

$$\Rightarrow \underset{H \triangleleft}{N(H)} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in F \right\} \subset G$$

Theorem (Sylow)

Assume G is a finite group of order $N = p^m \cdot n$ (with $p \nmid n$). Then:

① • there is a subgroup H of G of order p^m (called a Sylow p-subgroup) (not necessarily unique!)

② • if K is a subgroup of order p^a $(a \leq m)$ then K is contained in a conjugate of H

($\Rightarrow$ in particular, any two p-Sylow subgroups H and H' are conjugate)

③ • the number ℓ of Sylow p-subgroups of G (i.e the size of the "conjugacy class") divides n and satisfies $\ell \equiv 1 \pmod{p}$.

WARNING

If d divides $N = \# G$, there need not be a subgroup of order d

Ex $G = A4$ has order 12

There is no subgroup of order $6 = pq$

Sylow only implies $\exists H$ of order 3 & H' of order 4.

Pf) of ①

FACT $\binom{N}{p^m}$ is prime to p

(Verify by considering power of p dividing numerator & denominator of $\frac{N(N-1)(N-2)\cdots(N-p^m+1)}{p^m(p^m-1)\cdots 1}$.)

(<u>Notation</u>: $\mathrm{ord}_p(a)$ = power of p dividing a)

(In general $\mathrm{ord}_p(N-k) = \mathrm{ord}_p(p^m - k)$ $\quad k < p^m$
where N is as in Sylow thm statement)

Let G act on the set
$S = \{$ <u>subsets</u> of G of order $p^m \}$
by translation: $g \cdot J = \{gx : x \in J\}$
$\# S$ is prime to p (by $\binom{N}{p^m}$ being prime to p)
We will find a Sylow p-subgroup H as a stabilizer G_S for this action

Break S up into G-orbits:
$$\# S = \# O_{S_1} + \# O_{S_2} + \cdots + \# O_{S_n}$$
$$= |G|/|G_{S_1}| + |G|/|G_{S_2}| + \cdots + |G|/|G_{S_n}|$$

Since $\# S$ is prime to p, at least one $\#(\text{orbit})$ must also be prime to p, say $\# O_{S_i}$
But $\# O_{S_i} = p^m \cdot n / |G_{S_i}|$ is prime to p

$$\Rightarrow \quad p^m \text{ divides } \# G_{S_i}$$

<u>Claim</u> $\# G_{S_i} \le p^m$
$S_i =$ some subset J of G order p^m
For $g \in G_{S_i}$, $g \cdot J = J$.
This implies that J = a union of left cosets for G_J.

Thus $|G_S| \leq |J| = p^m$
& it follows that $|G_s| = p^m$, as desired

(In fact: J has stabilizer of order p^s
$\iff J = H$ is a Sylow p-subgroup,
in which case $J = G_S = H$)

(so this J isn't just a ~~set~~ subset but
a subgroup)

Pf) of ②
H Sylow p-subgroup found in part ①

G acts transitively on $S = G/H$.
(which has order n)
(by translation)
$\uparrow$ prime to p.
Stabilizer of $sH \in S$ is $G_{sH} = sHs^{-1}$,
So $\{G_{sH} : sH \in S\}$ is the set of
conjugates of H

Let K be another p-subgroup &
let K act on S by restriction
of G-action.

There must be an orbit, say the orbit
of sH, of order prime to p
So $|K| / |\text{stabilizer}|$ is prime to p.

But $|K| = p^a$, so we must have

$$\left. \begin{array}{l} |\underline{\text{Stab}_{sH}}| = |K| \\ \text{Stab}_{sH} = K \cap G_s = K \cap sHs^{-1} \end{array} \right\} \Rightarrow K \subset sHs^{-1}$$ as desired!

Pf) of ③ $\#\{\text{Sylow } p\text{-subgps}\} = \ell = |G| / |N(H)|$

normalizer of H.

as G acts transitively on set of Sylow p-subgroups by conjugation (part ②) and (stab. of H) $= N(H)$.

Since $H \subset N(H)$, $N(H)$ has order divisible by p^m. So ℓ divides $n = N/p^m$.

Restrict action of conjugation on the Sylows to the subgroup H.

Recall, there are ℓ Sylows.

The orbit of H has 1 element

All other orbits have p^a elements ($m \geq a \geq 1$)

If H' were in an orbit of size 1, then H normalizes H'

$$\begin{matrix} H, \\ H' \end{matrix} \subset \underbrace{N(H')}_{p^m \cdot n'} < G$$

Sylow-p subgps of

$\therefore$ conj in $N(H') \Rightarrow H = H'$. $\boxtimes$