Mathematics 122 – Lecture notes for 5 Nov. 2003

HW: 6.4.2, 6.4.3, 6.4.6, 6.4.9
Read §6.6 for Friday (Richard Taylor)
HW due Monday: 6.6.5, 6.6.6, 6.6.10, 6.6.15
Peter Green lectures Monday

Thm (Sylow Theorem): Let G be finite of order $N = p^n m$, where m is prime to p.

1) $\exists$ a Sylow p-subgroup of order p^n
2) Any two such subgroups are conjugate
3) The number ℓ of such subgroups satisfies $\ell | m$, $\ell \equiv 1 \pmod p$

Rmk: It's possible that $\ell = 1$, i.e. $H \trianglelefteq G$ is the unique Sylow p-subgroup. For if H has order p^n, so does $H' = gHg^{-1}$. If $\ell = 1$, then $gHg^{-1} = H$ for all $g \in G$. Thus $H \triangleleft G$.

Pf (review): Via groups acting on sets. G acts by translation on the set $\mathcal{J}$ of subsets $J \subset G$, $|J| = p^n$, via $g(J) = g \cdot J$. The number of subsets $J: \binom{N}{p^n}$ is prime to p, so some orbit O_J has size <u>prime to p</u>. Thus G_J has order divisible by p^n. But $|G_J| \le p^n$, for if $j \in J$, $g \in G_J$, then $gj \in J$. So in fact $|G_J| = p^n$. This gives $|G_J|$ elements in J, and $|G_J|$ is a Sylow p-subgroup.

2) Now let H be a subgroup. G acts by translation, transitively on G/H, which has order m, prime to p. The stabilizer of gH is the Sylow p-subgroup gHg^{-1}. Let H' be a Sylow p-subgroup, and restrict the action of G on G/H to H'. The orbits have size $\underset{|H'|/|\text{stabilizer}|}{\overset{\|}{p^a}}$, $0 \le a \le n$. Some orbit has size $= 1$, not divisible by p. Thus $H' \subset gHg^{-1}$.

3) Since all Sylow p-subgroups are conjugate, we have a transitive action of G, by conjugation, on the set $\mathcal{H}$ of all Sylow p-subgroups. The stabilizer of H, for this action, is $G_H = N(H)$. Hence

$$\mathcal{H} = G/N(H) \supset N(H) \supset H$$

and $|\mathcal{H}|$ divides m. Consider the action of H, by conjugation, on $\mathcal{H}$. This fixes the point H. I claim that this is the <u>unique fixed point</u>, so all other orbits have size divisible by p. If H' is fixed by conjugation by elements of H, then $\substack{H \\ H'} \subset N(H)$, hence $H' \subset H$, hence $H' = H$ (since H' and H have the same order). So H is the only one-point orbit in $\mathcal{H}$, and the number of elements in $\mathcal{H}$ is $1 + k_2 + \cdots + k_r$, where each k_i is the number of points in an orbit and so is an index $[H : \tilde{H}]$ of some proper subgroup $\tilde{H} \subset H$, hence is a positive power of p. So the number ℓ of elements in $\mathcal{H}$ is $\equiv 1 \pmod p$.

Classification theorems

$|G|=p$, then G is cyclic, $G\cong \mathbb{Z}/p\mathbb{Z}$

$|G|=p^2$, then G is abelian, $G\cong(\mathbb{Z}/p\mathbb{Z})^2$ $\forall g\neq e, g^p=e$

$\cong \mathbb{Z}/p^2\mathbb{Z}$

$|G|=p\cdot q$, $p<q$, p and q both prime

- $\exists$ subgroups H_p, H_q that are Sylow subgroups of orders p and q. Both are cyclic and isomorphic to $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Z}/q\mathbb{Z}$, respectively.
- As a set $G=H_p\cdot H_q=\{\tau^a\sigma^b,\ 0\le a\le p, 0\le b\le q\}$ // $H_p=\langle\tau\rangle$, $H_q=\langle\sigma\rangle$
- $G=\bigcup_{0\le a\le p}\tau^a H_q$. These cosets are distinct for distinct $\tau,\tau'\in H_p$. So

$\tau H_q=\tau' H_q \Rightarrow \tau(\tau')^{-1}\in H_q \Rightarrow \tau(\tau')^{-1}\in H_p\cap H_q=\{1\}$

$(\tau^a\sigma^b)(\tau^{a'}\sigma^{b'})=?$

First observation: $H_q \triangleleft G$. # of Sylow p-subgroups l divides p and $\equiv 1 \pmod q$

The only such possibility is $l=1$ (since $q>p$). Thus $\tau\sigma\tau^{-1}=\sigma^a\in H_q$

$\Rightarrow \tau\sigma=\sigma^a\tau$, and we now turn to finding a

ex: $p\cdot q=6$ $H_q=\langle 1,\sigma,\sigma^2\rangle$ $H_p=\langle 1,\tau\rangle$

$$\tau\sigma\tau^{-1}=\begin{cases}\sigma \Rightarrow \tau\sigma=\sigma\tau \Rightarrow G \text{ is abelian}, \cong\mathbb{Z}/6\mathbb{Z}, \text{ generated by } (\sigma\tau)\\ \sigma^2=\sigma^{-1}\Rightarrow G\cong D_6 \text{ (also } S_3)\end{cases}$$

ex: $|G|=2\cdot q$ $H_q=\langle 1,\sigma,\sigma^2,\dots,\sigma^{q-1}=\sigma^{-1}\rangle$ $H_2=\langle 1,\tau\rangle$ $\tau\sigma\tau^{-1}=\sigma^a$

Claim: $a\equiv\pm 1 \pmod q$. $\tau^2\sigma\tau^{-2}=\tau(\tau\sigma\tau^{-1})\tau^{-1}=\tau(\sigma^a)\tau^{-1}=\overbrace{\sigma^a\cdots\sigma^a}^{a \text{ times}}=\sigma^{a^2}$

$\overset{\shortparallel}{\sigma}$, since $\tau^2=e$.

Thus $\sigma^{a^2}=\sigma \Rightarrow a^2\equiv 1 \pmod q \Rightarrow a\equiv\pm1 \pmod q$

- In general, we have $\boxed{a^p\equiv 1 \pmod q}$ and $a=1$ gives $G\cong\mathbb{Z}/pq\mathbb{Z}$, gen. by $\sigma\tau$
- In this case, we have

$$\tau\sigma\tau^{-1}=\begin{cases}\sigma\Rightarrow\sigma\tau=\tau\sigma,\ G\cong\mathbb{Z}/2q\mathbb{Z} \text{ generated by } (\tau\sigma)\\ \sigma^{-1}\Rightarrow G\cong D_{2q}\end{cases}$$

ex: $|G|=15=3\cdot5$. $\langle\sigma\rangle=H_5\triangleleft G$, $H_3=\langle 1,\tau,\tau^2\rangle$

In fact, in this case, $H_3\triangleleft G$ as well, as the number of Sylow 3-subgroups divides 5, $\equiv 1 \pmod 3$, hence equals 1.

- $\tau\sigma\tau^{-1}=\sigma^a$, with $a^3\equiv 1 \pmod 5$ $\Rightarrow a\equiv 1 \pmod 5$ (Compute this explicitly).

The only possibility is $a=1$, so $\tau\sigma=\sigma\tau$ and $G\cong\mathbb{Z}/15\mathbb{Z}$.

ex: $|G|=21=3\cdot7$. H_7 is normal, H_3 may not be normal (there can be 1 or 7 Sylow 3-subgroups). $a^3\equiv 1(7)\Rightarrow a\equiv 1,2,4 \pmod 7$. So

$$\tau\sigma\tau^{-1}=\begin{cases}\sigma & \tau\sigma=\sigma\tau,\ G\cong\mathbb{Z}/21\mathbb{Z}\\ \left.\begin{matrix}\sigma^2\\ \sigma^4\end{matrix}\right\} & \text{give isomorphic nonabelian groups of order 21, with 7 Sylow 3-subgroups.}\end{cases}$$

Rmk: The subgroups we've written down so far actually exist — see Coxeter presentation

Rmk: Classification quickly becomes more complicated for $|G|$ taking forms other than the ones listed above...

Groups of order $12 = 2^2 \cdot 3$

There are 5 distinct groups, two of which are abelian, namely $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

H_4 in G has order 4 and is either isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$

H_3 in G has order 3, $H_3 = \langle 1, \sigma, \sigma^2 \rangle$

#ℓ of Sylow 2-subgroups is 1 or 3

#ℓ of Sylow 3-subgroups is 1 or 4

<u>One or the other of these is normal</u>

Imagine we have 4 Sylow 3-subgroups. Then we have 8 elements of order 3, 1 elements of order 1, and $\{e\} \cup \{3 \text{ remaining elements}\} = H_4$.

Thus of the remaining possibilities,

one is A_4 (Sylow 2-subgroup is normal)

one is D_{12} (Sylow 3-subgroup is normal)

one is new.

(see Artin for a full treatment)