MATH 171 FALL 2008: LECTURE 20

DAGAN KARP

1. SYLOW THEOREMS

The first Sylow theorem is a partial converse to Lagrange's theorem. For a group G of order n, the order of every subgroup divides n. It is not the case that every divisor of n is the order of a subgroup of G. But this is the case if the divisor is the power of a prime.

Definition 1. *For a prime number* p*, a finite group* G *is a* p-group *if the order of* G *is a power of* p*.*

Definition 2. *A* p-subgroup *of a finite group* G *is a subgroup of order* p^k *for some* k *where* p *is prime.*

Definition 3. *Let* G *be a finite group of order* n *and* p *be prime. A* Sylow p-subgroup *of* G *is a* p*-subgroup of order* p^k *such that* $p^k | n$ *and* $p^{k+1} \nmid n$*.*

Theorem 4 (Sylow's first theorem)**.** *Let* G *be a finite group and* p *a prime number. If* p^k *divides* $|G|$*, then* G *contains a subgroup of order* p^k*. In particular,* G *contains a Sylow* p*-subgroup.*

In our proof of this theorem, we'll use the following lemma, presented as a proposition in our study of the classification of groups.

Proposition 5. *Let* G *be a finite Abelian group and* p *a prime number. If* p *divides* $|G|$*, then* G *contains an element of order* p*.*

Proof. We induce on the order of G. If $|G| = 1$, then the theorem holds trivially.

Now assume the theorem holds for all groups of order less than $|G|$. If G contains a proper subgroup H such that p^k divides $|H|$, then H has a subgroup of order p^k and we are done.

Otherwise, p^k does not divide the order of any proper subgroup of G. In this case, consider the class equation

$$|G| = |Z(G)| + \sum_{|C_x|>1} |C_x|.$$

Since $|G| = |C_G(x)| \cdot [G : C_G(x)]$ and p^k divides $|G|$ and not $|C_G(x)|$, it must be the case that p^k divides $[G : C_G(x)] = |C_x|$.

Therefore p divides $|Z(G)|$, and by the above proposition $Z(G)$ has an element x of order p. Then $\langle x \rangle \trianglelefteq G$. But p^{k-1} divides $|G/\langle x \rangle|$, and hence by the induction hypothesis $G/\langle x \rangle$

Date: November 17, 2008.

has a subgroup of order p^{k-1}. This subgroup is of the form $H/\langle x\rangle$ where $H \leqslant G$. But we have $|H| = p^k$. □

Corollary 6 (Cauchy's theorem)**.** *Let* G *be a finite group and* p *a prime number. If* p *divides* $|G|$*, then* G *contains an element of order* p*.*

The following are also called Sylow theorems.

Theorem 7. *The number of Sylow* p*-subgroups of a finite group* G *divides* $|G|$ *and is congruent to* 1 *modulo* p*.*

Theorem 8. *All Sylow* p*-subgroups of a finite group are conjugate.*

Corollary 9. *A Sylow* p*-subgroup of* G *is a normal subgroup of* G *if and only if it is the only Sylow* p*-subgroup of* G*.*

Example 10. *The Sylow 2-subgroups of* S_3 *are* $\{(1),(12)\},\{(1),(13)\}$ *and* $\{(1),(23)\}$*.*

$$(13)\{(1),(12)\}(13)^{-1} = \{(1),(23)\}$$
$$(23)\{(1),(12)\}(23)^{-1} = \{(1),(13)\}$$

Proposition 11. *Let* $|G| = 2p$ *where* p *is prime. Then* G *is cyclic or dihedral.*

Proof. By Cauchy's theorem, G has elements a, b of order 2 and p, respectively. Then G is generated by $\{a, b\}$. Now $\langle b\rangle$ has index 2 and hence is normal. Therefore

$$aba^{-1} = b^k$$

for some $k < p$. Therefore

$$b^{k^2} = (b^k)^k = (aba^{-1})^k = ab^ka^{-1} = a(aba^{-1})a^{-1} = a^2ba^{-2}.$$

But $a^2 = 1$. Thus $b^{k^2} - 1 = 1$. Therefore p divides $k^2 - 1$.

$$k^2 = (k-1)(k+1).$$

But $k < p$. So $k - 1 = 0$ or $p = (k + 1)$. In the first case,

$$aba^{-1} = b$$

and G is Abelian, as a, b generate G. Then $|ab| = 2p$.

Otherwise the elements of G may be written a^ib^j where $i = 0$ or $i = 1$ and $0 \leqslant j < p$. Also,

$$a^ib^jab^l = a^{i+1}b^{l-j}.$$

□

Proposition 12. *Let* $p > q$ *be prime. If* q *does not divide* $p - 1$*, then every group of order* pq *is cyclic.*

Exercise.

(1) Show that every group of order 30 has a nontrivial proper normal subgroup.
(2) Do the same for groups of order 56.
(3) Prove that a group of order 175 is Abelian.
(4) Prove that a group of order 105 has a subgroup of order 35.
(5) Find a Sylow 2-subgroup of S_4, and show that it is isomorphic to D_4. ($|D_4| = 8$)