MATH 171 FALL 2008: LECTURE 21

DAGAN KARP

1. Sylow theorems continued

1.1. **Normalizers.** Let

$$\mathcal{H} = \{H \leqslant G\}$$

be the set of all subgroups of a group G. Then G acts on $\mathcal{H}$ by conjugation,

$$g \cdot H = gHg^{-1}.$$

where $g \in G$.

Indeed, note that for any $g \in G$, $gHg^{-1} \leqslant G$. Let $x, y \in gHg^{-1}$. Then there exist $h_1, h_2 \in H$ such that

$$x = gh_1g^{-1} \qquad y = gh_2g^{-1}.$$

Then $y^{-1} = gh_2^{-1}g^{-1}$ and

$$xy^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = g(h_1h_2^{-1})g^{-1} \in G,$$

where the last statement follows as $h_1h_2^{-1} \in H$, because $H \leqslant G$. Therefore we have a well defined conjugation map

$$G \times \mathcal{H} \to \mathcal{H}.$$

To verify that this is a group action, note that

$$1 \cdot H = 1H1^{-1} = H$$

for any $H \leqslant G$. Further, for any $g_1, g_2 \in G$,

$$\begin{aligned}(g_1g_2) \cdot H &= (g_1g_2)H(g_1g_2)^{-1} \\ &= g_1g_2Hg_2^{-1}g_1^{-1} \\ &= g_1 \cdot (g_2Hg_2^{-1}) \\ &= g_1 \cdot (g_2 \cdot H).\end{aligned}$$

Therefore G does indeed act on $\mathcal{H}$. Thus the orbits of G form equivalence classes.

Definition 1. *The* conjugacy class *of a subgroup* H *of a group* G *is the orbit of* H *in* $\mathcal{H}$ *under the action of* G *by conjugation. It is denoted* C_H.

Date: November 20, 2008.

Definition 2. *The* normalizer $N_G(H)$ *of the subgroup* H *of the group* G *is the stabilizer of* $H \in \mathcal{H}$ *under the conjugation action of* G.

$$\begin{aligned} N_G(H) = N(H) &= \{g \in G : g \cdot H = H\} \\ &= \{g \in G : gHg^{-1} = H\}. \end{aligned}$$

Proposition 3. *The normalizer* $N_G(H)$ *of* $H \leqslant G$ *is the largest subgroup of* G *such that* $H \trianglelefteq N_G(H)$.

Proof. Suppose there is a subgroup $K \leqslant G$ such that

$$H \trianglelefteq K \leqslant G.$$

Then by definition of normal, we have, for $k \in K$,

$$kHk^{-1} = H.$$

Therefore $k \in N_G(H)$. Thus $K \subseteq N_G(H)$. □

1.2. p**-groups acting on finite sets.**

Lemma 4. *Let* H *be a* p*-group acting on a finite set* S.

(a) *The number of fixed points of* H *is congruent to* $1 \mod p$.
(b) *If* H *has exactly one fixed point, then* $|S| \equiv 1 \mod p$.

Proof. Because the orbits of S partition S, we may express S as a disjoint union of its orbits

$$S = \bigsqcup_{s_i \in S} [s_i].$$

Therefore

$$|S| = \sum_{s_i \in S} |[s_i]|.$$

But the order of the orbit is equal to the index of the stabilizer! Thus $|[s_i]| = [H : Hs_i]$. Thus we obtain what is called the *orbit equation*:

$$|S| = \sum_{s_i \in S} [H : Hs_i]. \tag{1}$$

We may split this sum into two pieces

$$|S| = \sum_{\substack{s_i \in S \\ [H:Hs_i]=1}} [H : Hs_i] + \sum_{\substack{s_i \in S \\ [H:Hs_i]\neq 1}} [H : Hs_i]. \tag{2}$$

By Lagrange's theorem, we have

$$|H| = |Hs_i| \cdot [H : Hs_i].$$

But H is a p-group, and hence $|H|$ is a multiple of p. Also the stabilizer $Hs_i \leqslant H$, and hence $|Hs_i|$ divides $|H|$, and so it is a multiple of p. Also $[H : Hs_i]$ divides $|H|$ and hence is a multiple of p.

Therefore, reducing equation (2) modulo p yields

$$\sum_{\substack{s_i \in S \\ [H:Hs_i]=1}} [H : Hs_i] \equiv |S| - 0 \mod p.$$

But $[H : Hs_i] = 1$ implies $|H| = |Hs_i|$, and so $Hs_i = H$. Therefore every element of H is in the stabilizer of s_i, i.e.

$$h \cdot s_i = s_i$$

for all $h \in H$. Therefore s_i is a fixed point of H if and only if $[H : Hs_i] = 1$. Thus we have

$$\#\text{ fixed points of } H = \sum_{\substack{s_i \in S \\ [H:Hs_i]=1}} 1 = \sum_{\substack{s_i \in S \\ [H:Hs_i]=1}} [H : Hs_i] \equiv |S| \mod p.$$

Part (b) is a special case of part (a). □

1.3. **Sylow theorems continued.** In Lecture 20, we established Sylow's First Theorem, which proves the existence of Sylow p-subgroups. We couple the remaining Sylow theorems together in the following result.

Theorem 5. *Let G be a finite group.*

(i) *Any p-subgroup $H \leqslant G$ is contained in a Sylow p-subgroup of G.*
(ii) *All Sylow p-subgroups of G are conjugate.*
(iii) *The number of Sylow p-subgroups of G is congruent to 1 modulo p.*

Proof. [After S. Lang] Let H by a p-subgroup of the finite group G. Further, let P be a Sylow p-subgroup of G, the existence of which is guaranteed by Sylow's first theorem. We first show that if H is contained in the normalizer of P, $H \leqslant N_G(P)$, then $H \subseteq P$.

So, suppose $H \subseteq N_G(P)$. Then we have

$$P \trianglelefteq HP \leqslant N_G(P).$$

To see this, note that for $hx \in HP$, we have

$$(hx)P(hx)^{-1} = h(xPx^{-1})h^{-1} = hPh^{-1} = P,$$

where the second equality holds as $x \in P$ and the third holds by assumption $H \subseteq N_G(P)$. Thus $HP \subseteq N_G(P)$. Further, the above computation immediately implies that P is normal in HP.

We now show

$$[HP : P] = [H : H \cap P]$$

and use this to show that $H \subseteq P$. By Lagrange's theorem we have

$$|HP| = |P| \cdot [HP : P] \tag{3}$$

$$|H| = |H \cap P| \cdot [H : H \cap P]. \tag{4}$$

Further, we have

$$|HP| = \frac{|H||P|}{|H \cap P|}.$$

Thus

$$[HP : H] = \frac{|HP|}{|P|} = \frac{|H|}{|H \cap P|} = |H| \cdot \frac{[H : H \cap P]}{|H|} = [H : H \cap P].$$

Now we use this to show $H \subseteq P$. Indeed, suppose otherwise. Then

$$|H \cap P| < |H|.$$

Therefore, by (4), $[H : H \cap P] > 1$. Hence $[HP : P] > 1$, and therefore

$$|HP| > |P|.$$

But $|HP|$ is a power of p, as H is a p-subgroup of G and P is a Sylow p-subgroup of G. But HP can not have larger order than P, as P is a Sylow p-subgroup of G! This contradiction shows that our assumption was false, and hence $H \subset P$.

We now consider the general case. Let $\mathcal{S}$ be the set of all conjugates of P,

$$\mathcal{S} = \{gPg^{-1} : g \in G\}.$$

Note that G acts on $\mathcal{S}$ by conjugation. Since $P \leqslant N_G(P)$ and indeed $P \subsetneqq N_G(P)$, we have $|N_G(P)| > |P|$. Since P is a Sylow p-subgroup, the order of $N_G(P)$ must not be a power of p. We have $|N_g(P) = |P|[N_g(P) : P]$. Hence $[N_G(P) : P]$ must be prime to p. Therefore, by the orbit equation (1) applied to the finite group $\mathcal{S}$, it follows that $|\mathcal{S}|$ is not divisible by p.

Now, let H by any p-subgroup of G. Then H acts on $\mathcal{S}$ by conjugation. Then by Lemma 4 (a), $\mathcal{S}$ can not have zero fixed points under the action of H. Let Q be such a fixed point. Then by definition $H \subset N_G(Q)$. Note that $|Q| = |P|$, and hence Q is a Sylow p-subgroup of G, as are all elements of $\mathcal{S}$. Thus by the first part of this proof, $H \subset Q$. This proves the first part of the theorem.

Now suppose H is a Sylow p-subgroup of G. Then $|H| = |Q|$, and therefore $H = Q$. This proves part (ii).

Thus, when H is a Sylow p-subgroup, H has only one fixed point (as we just showed that any fixed point of $Q \in \mathcal{S}$ of H is equal to H). Hence part (iii) follows from Lemma 4 (b), and this proves the theorem. $\square$