M7210 Lecture 38 Monday, November 26, 2012

Sylow Theorems

Review. Suppose X is a G-set, and $x \in X$. Recall:

- $G_x := \{ g \in G \mid gx = x \}$ is called the *isotropy group of x*, or *stabilizer of x*.
- $Gx := \{ gx \mid g \in G \}$ is called the *orbit of x*.

Counting Formula. *For any $x \in X$, $|G| = |Gx|\,|G_x|$.* (Be able to prove this!)

Action of G on the set of elements of G by conjugation

Suppose G is a finite group that acts on $X = G$ by conjugation according to the rule:

$$(g, x) \mapsto gxg^{-1}.$$

Let $x \in G$. Then G_x is the so-called *centralizer of x*, $Z_G(x) := \{g \in G \mid gxg^{-1} = x\}$. The intersection of all centralizers is called the *center of G* and is denoted Z_G. It contains the elements of G that commute with all $x \in G$. The orbit of x under conjugation, $\{ gxg^{-1} \mid g \in G \}$, is called the *congugacy class of x* and is denoted $\mathcal{C}\ell(x)$. From the Counting Formula:

$$|\mathcal{C}\ell(x)| = \frac{|G|}{|Z_G(x)|}. \tag{2}$$

Any two different congugacy classes are disjoint. Therefore, the order of G is the sum of the orders of the congugacy classes. Now $|\mathcal{C}\ell(x)| = 1$ if and only if $x \in Z_G$. This gives us

Class Equation. *If R contains one representative from each non-singleton conjugacy class of G, then*

$$|G| = |Z_G| + \sum_{x \in R} |\mathcal{C}\ell x| = |Z_G| + \sum_{x \in R} \frac{|G|}{|Z_G(x)|}.$$

In the remainder of this lecture, we will assume that G is a finite group of order $p^m r$, where p is prime and $(p, r) = 1$.

Sylow Theorem 1. *G contains a subgroup of order p^m.*

Remark. A subgroup of G whose order is a power of p is called a *p-subgroup*. A subgroup of order p^m is called a *Sylow p-subgroup*.

Proof. The proof is by induction on the order of G, the case $|G| = 1$ being obvious. Suppose the theorem is known for all groups of order $< n$ and $|G| = n$. If $|Z_G|$ is divisible by p, then by the structure theorem for abelian groups, Z_G has a subgroup H of order p. H is normal in G, and the theorem follows by the induction hypothesis and the Isomorphism Theorem. If $|Z_G|$ is not divisible by p then (by the Class Equation) $\frac{|G|}{|Z_G(x)|}$ is *not* divisible by p for some $x \in G$. For any such x, $Z_G(x)$ has order $p^m s$ for some $s < r$. The induction hypothesis tells us that $Z_G(x)$ has a subgroup of order p^m. /////

In general, we cannot expect a Sylow p-subgroup of G to be normal in G. If G has normal Sylow p-subgroup, there are very strong consequences, due to the following:

Lemma. *Suppose that G is a group of order nr, where $(n, r) = 1$ and that $N \subseteq G$ is a normal subgroup of order n. Let $H \subseteq G$ be a subgroup of order m, where $(m, r) = 1$. Then $H \subseteq N$.*

Proof. Let $\pi : G \to G/N$ be the canonical homomorphism, and let k be the order of $\phi(H)$. Then k divides m since k is the order of a homomorphic image of a group of order m. Also, k divides r, since k is the order of a subgroup of a group of order r. Therefore $k = 1$. Since $\phi(H)$ has only one element, $H \subseteq N$. /////

Let P be a Sylow p-subgroup of G. The lemma shows that if P is *normal*, then any p-subgroup of G is contained in P. In particular, if P is *normal* then it is the *only* Sylow p-subgroup of G.

Action of G on the set of subgroups of G by conjugation

Suppose G is a finite group. Let X be the set of subgroups of G. G acts on X by conjugation according to the rule:

$$(g, H) \mapsto gHg^{-1},$$

where H is a subgroup of G. Note that gHg^{-1} has the same number of elements as H.

The stabilizer of a subgroup H is called the *normalizer of H*:

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}.$$

This is a subgroup of G, and it is the largest subgroup of G in which H is normal (hence the name). By the Counting Formula, the number of distinct conjugates of H is the index of $N_G(H)$ in G:

$$|\{ gHg^{-1} \mid g \in G \}| = |G/N_G(H)|.$$

The Lemma above implies that if P is a Sylow p-subgroup of G (not necessarily normal in G) and H is a p-subgroup of $N_G(P)$, then $H \subseteq P$.

Sylow Theorem 2. *With the same hypotheses as Sylow Theorem 1, let Π be the set of Sylow p-subgroups of G. Then: (a) $|\Pi| \equiv 1$ mod p; (b) any two subgroups in Π are conjugate; (c) $|\Pi|$ divides r and (d) any p-subgroup of G is contained in a Sylow p-subgroup*

Proof. G acts on Π by conjugation. Let $P \in \Pi$. Then P also acts on Π by conjugation. The P-orbit of P itself is the singleton $\{P\}$, since $pPp^{-1} = P$ for all $p \in P$. We will show that P is the *only* element of Π with a singleton P-orbit. Let Q be any element of Π. If the P-orbit of Q has only one element, then $pQp^{-1} = Q$ for all $p \in P$, and this means that $P \subseteq N_G(Q)$, so $P = Q$ by the lemma. On the other hand, if the orbit of Q under the action of P is not a singleton, then it has $|P|/|P_Q| = p^\ell$ elements, for some $\ell \geq 1$. This proves (a). Notice that the same argument used to prove (a) shows that any union U of G-orbits within Π has order congruent to 1 mod p, for if $P' \in U$, then U is a union of P'-orbits of which exactly one is a singleton. Now, we will show that Π consists of a single G-orbit. If this is not the case, then Π is the disjoint union of a (non-empty) G-orbit and another set consisting of one or more non-empty G-orbits. But this implies $|\Pi| \equiv 2$ mod p, contradicting (a). This proves (b). Since Π is an orbit of a G-action and the stabilizer of $P \in \Pi$ is $N_G(P)$, we get $|\Pi| = |G|/|N_G(P)|$, from which (c) follows. Finally, suppose H is a p-subgroup of G. Let H act on Π by conjugation. Since the orbits of H have cardinality a power of p, there must be a singleton orbit, say $\{P\}$. Then $H \subseteq N_G(P)$, so $H \subseteq P$, by the lemma, and this proves (d). /////