GROUP ACTIONS AKA PERMUTATION REPRESENTATIONS
LECTURE 3

In the previous lecture we considered several group actions and we used them to derived some interesting results. Now we will identify three basic observations, which we used implicitly in some of our arguments. We state them below as three fundamental rules of counting associated to a group action of a finite group G on a finite set X.

Rule 1. *If O is an orbit of the action, then $|O| = |G|/|St(s)|$ for any $s \in O$.*

This rule follows immediately from the Orbit-Stabilizer theorem.

Rule 2. *Let p be a prime number which does not divide $|X|$. Then there is an element $s \in X$ such that $|O(s)|$ is not divisible by p.*

In fact, if the number of elements in every orbit is divisible by p then the number of elements in X, which is the sum of the numbers of elements in each orbit, is also divisible by p. But we assumed that this is not the case, so the number of elements in at least one orbit is not divisible by p.

Rule 3. *Suppose that G is a finite p-group, p a prime number. Let r denote the number of fixed points for this action. Then $|X| \equiv r \pmod{p}$. In particular,*
(i) if $|X|$ is not divisible by p then $r > 0$, i.e. there is at least one fixed point.
(ii) if $p||X|$ and $r > 0$ then $r \geq p$, i.e. if there is a fixed point, then the are at least p of them.

In order to justify Rule 3 recall that the number of elements in X is equal to the sum of the numbers of elements in each orbit. Note that by Rule 1, the number of elements in each orbit divides $|G|$. Since $|G|$ is a power of the prime p, the number of elements in each orbit is a power of p as well. We have r orbits which consist of $1\ (= p^0)$ element and in all other orbits the number of elements is a multiple of p (being a positive power of p). So the sum of the numbers of elements in the orbits (which is $|X|$) equals $r +$ a multiple of p. Consequently, $|X| \equiv r \pmod{p}$. If $|X|$ is

not divisible by p then we immediately get that $r \neq 0$, which justifies (i). If $p||X|$ then also $p|r$. In particular, if $r \neq 0$ then r is at least p, which proves (ii).

In the previous lecture we have seen that a group G acts on itself by left multiplication. There is another very important action of G on itself, **the action by conjugation**. It is defined by $g * a = gag^{-1}$ for any $a, g \in G$. The verification that this is indeed an action is straightforward and is left as an exercise. Note the orbit of any h in G under the action by conjugation is exactly the conjugacy class of h: $O(h) = \{ghg^{-1} : g \in G\}$. The stabilizer $St(h)$ of h is precisely the centralizer $C(h)$ of h (see problem 7 in homework 5). Note that problem 7 of homework 6 studies some properties of this action. Recall the two fundamental result obtained in this problem:

Theorem A. If G is a finite p-group then the center of G is a non-trivial subgroup.

Theorem B. If p is a prime then any finite group of order p^2 is abelian.

Theorem B is a simple consequence of Theorem A (see part 5. of problem 7). Theorem A can be now derived as a consequence of our rules applied to the conjugation action. In fact, G acts on itself by conjugation and the identity element e is a fixed point. Since $p||G|$, Rule 3 tells us that there are at least p fixed points. Fixed points of the conjugation action are precisely the elements of the center. Thus $|Z(G)| \geq p$.

Theorem A is a fundamental tool in the study of finite p-groups. We illustrate its use by proving the following theorem.

Theorem. Let P be a finite group of order p^n, p a prime. Then P has a normal subgroup of order p^k for $k = 0, 1, \ldots, n$.

We prove the theorem by induction on n. In $n = 1$ then P has order p and the result is clear: P has subgroup $\{e\}$ of order $1 = p^0$ and the subgroup P of order p and both are normal subgroups.

Assume now that the result is true for p-groups of order less than p^n and consider a p-group P of order p^n. Since P has non trivial center, there is an element $a \in Z(P)$ of order p. Let $B =< a >$, so B is a normal subgroup of order p in P. Consider the

quotient group $Q = P/B$ and the quotient homomorphism $\pi : P \longrightarrow Q$. Since Q has order $p^{n-1} < p^n$, our inductive assumption tells us that Q has normal subgroups Q_i of order p^i, $i = 0, \ldots, n-1$. By the correspondence theorem, $P_i = \pi^{-1}(Q_i)$ is a normal subgroup of P which contains B and $P_i/B = Q_i$. It follows that P_i has p^{i+1} elements. Thus P has normal subgroups of order $p, p^2, \ldots, p^n$. Clearly the trivial subgroup is normal of order p^0. This completes our proof of the Theorem.

Let us now look at the induced action of G on the set $P(G)$ of all subsets of G as discussed in the previous lecture. Since conjugation by any element is an automorphism of G, this action takes subgroups of G to subgroups of the same size. Thus the conjugation action induces an action of G on the set of all subgroups of G of any given order, where g moves a subgroup H to its conjugate gHg^{-1}.

Suppose now that $|G| = p^k m$, where p is a prime, $k > 0$ and $p \nmid m$. Let Syl_p be the set of all Sylow $p-$subgroups of G, i.e. all subgroups of order p^k (we proved that this set is not empty). Thus G acts by conjugation on Syl_p. In the next lecture we are going to analyze this action more closely and derive several fundamental facts about Sylow subgroups.