GROUP ACTIONS AKA PERMUTATION REPRESENTATIONS
LECTURE 2

We are going now to discuss some examples of actions.

Example 1. The symmetric group S_n acts on the set $X = \{1, 2, \dots, n\}$ as follows: $\tau * i = \tau(i)$. It is a straightforward exercise to check that this is indeed an action. Note that for every i there is a permutation σ such that $\sigma(1) = i$. It follows that this action has only one orbit (the whole set X). The stabilizer of n can be naturally identified with all permutations of the set $\{1, \dots, n-1\}$: $St(n) \cong S_{n-1}$.

Example 1 motivates the following definition.

Definition 1. *We say that the action of G on X is* **transitive***, if it has only one orbit (which then is equal to X). In other words, the action is transitive if for any two elements s, t in X there is $g \in G$ such that $gs = t$.*

Example 2. Suppose that G acts on a set X. Then G acts on the set $P(X)$ of all subsets of X as follows: if $U \in P(X)$ then $g * U = \{g * s : s \in U\}$. A straightforward verification that this is indeed an action is left as an exercise. Note that for any U we have $|U| = |g * U|$. This leads us to the next example.

Example 3. Fix an integer $k \leq |X|$ and denote by $P_k(X)$ the set of all $k-$element subsets of X. Then the action from Example 2 induces an action of G on the set $P_k(X)$. Explicitly, if $U \in P_k(X)$ then $U = \{s_1, ..., s_k\}$ and $gU = \{g * s_1, ..., g * s_k\}$.

We now apply the construction from Example 3 to the action from Example 1. Let $X = \{1, 2, ..., n\}$ and let $G = S_n$ act on X as in Example 1. Let $k \leq n$. Then we have an action of G on $P_k(X)$. We claim that this action is transitive. In fact, given k elements $s_1, ..., s_k$ of X there is a permutation f which maps i to s_i for all $i \leq k$, i.e. $f * i = s_i$. Thus $f * \{1, 2, ..., k\} = \{s_1, ..., s_k\}$. This shows that the orbit of $V = \{1, 2, ..., k\}$ is the whole $P_k(X)$, i.e. the action is transitive: $O(V) = P_k(X)$.

What is the stabilizer of V? Note that a permutation f is in $St(V)$ iff it maps the set V onto itself and then it also maps the set $S - V$ onto itself. So elements of $St(V)$ can be thought of as pairs consisting of a bijection of $V = \{1, 2, \ldots, k\}$ onto itself and a bijection of $S - V = \{k + 1, \ldots, n\}$ onto itself, i.e. $St(V) \cong S_k \times S_{n-k}$. Thus $|St(V)| = k!(n - k)!$. By the Orbit-Stabilizer Theorem,

$$|P_k(\{1, 2, \ldots, n\})| = \frac{|S_n|}{St(V)} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

In other words, we proved that a set with n elements has $\binom{n}{k}$ subsets with k elements.

Example 4. Suppose that G acts on a set X. Let H be s subgroup of G. We can restrict our attention to elements of H and we get in this way an action of H on X called **the restriction of the action of G to H**. Focusing on such a restriction can be quite useful. We illustrate it by the following result.

Suppose that $n = p^s m$ for some prime p. Let

$$f = (1, 2, 3, ..., p^s)(p^s + 1, ..., 2p^s)...((m - 1)p^s + 1, ..., mp^s)$$

be a permutation of $X = \{1, \ldots, n\}$ written as a product of disjoint cycles. All these cycles have length p^s, so f has order p^s. Let H be the cyclic subgroup of S_n generated by f: $H =< f >$. Thus H is a $p-$group of order p^s. Consider the restriction of the action of S_n on $P_{p^s}(X)$ to H. By the Orbit-Stabilizer Theorem, the size of any orbit of H divides p^s, hence it is a power of p. Thus any orbit either has size divisible by p or has size 1. Let N be the number of orbits of size 1. Since the orbits partition $P_{p^s}(X)$, we see that $|P_{p^s}(X)| - N$ is divisible by p (the set obtained from $P_{p^s}(X)$ by removing the orbits of size 1 has $|P_{p^s}(X)| - N$ elements and it is a union of orbits, each of which has size divisible by p).

We are going to find N. Suppose that the orbit of U has size 1. This means that $f^i * U = U$ for every i. Let $a \in U$. Note that we may write $a = lp^s + b$ for some $0 \leq l < m$ and $0 < b \leq p^s$ and then the orbit of a under H is $\{lp^s + 1, ..., (l + 1)p^s\}$. Since $a \in V$, we have $f^i * a \in f^i * V = V$, so V contains $\{lp^s + 1, ..., (l + 1)p^s\}$. Since $|V| = p^s$, we conclude that $V = \{lp^s + 1, ..., (l + 1)p^s\}$. Conversely, for every $l \in \{0, \ldots, m - 1\}$ the orbit of $V_l = \{lp^s + 1, ..., (l + 1)p^s\}$ has 1 element since $f * V_l = V_l$. Thus we see that there are exactly m orbits of size 1, i.e. $N = m$.

We summarize the above considerations in the following theorem.

Theorem 1. *The number of $k-$element subsets of an $n-$element set is equal to $\binom{n}{k} = n!/k!(n-k)!$. If $n = p^s m$, where p is a prime then $p|\binom{n}{p^s} - m$. In particular, if $p \nmid m$ then $p \nmid \binom{n}{p^s}$.*

Counting the orbits of size 1 for a given action is needed in many applications of group actions. Therefore we introduce the following notion.

Definition 2. *An element $s \in X$ is called a* **fixed point** *of the action of G on X if the orbit of s equals to $\{s\}$. Equivalently, s is a fixed point iff $St(s) = G$, i.e. if $gs = s$ for every $g \in G$.*

Fixed points should be thought of as elements having many symmetries, so they are of special interest.

Example 5. Every group G acts on itself (i.e. $X = G$) as follows: $g * h = gh$. The verification that this is an action is straightforward. This action is usually called **the action of G on itself by left translations**.

We combine the action from Example 5 with the construction in Example 3. Let G be a finite group and p a prime divisor of $|G|$. Thus we may write $|G| = p^s m$ for some integers m not divisible by p and $s > 0$. Let X be the set of all subsets of G of size p^s, i.e. $X = P_{p^s}(G)$. The group G acts on itself by left multiplication (see Example 5) so it acts on X according to Example 3. Explicitly, if $A = \{a_1, ..., a_{p^s}\}$ is an element of X (i.e. a subset of G of size p^s) and $g \in G$ then we have $g * A = \{ga_1, ..., ga_{p^s}\}$. By Theorem 1, $|X| = \binom{p^s m}{p^s}$ and $p \nmid |X|$ (since $p \nmid m$). Since X is partitioned into orbits, at least one orbit of G on X has size not divisible by p, i.e. there exists an element $T \in X$ whose orbit $O(T)$ has cardinality not divisible by p. Recall that $|O(T)| = |G|/|St(T)|$. It follows that the stabilizer $St(T)$ has order $|G|/|O(T)|$ divisible by p^s. On the other hand, for any $A \in X$ the stabilizer of A has at most p^s elements. In fact, let $a \in A$. If $g \in St(A)$ then $ga \in A$ so we have a function $St(A) \longrightarrow A$, $g \mapsto ga$ which is injective. Thus the number of elements in $St(T)$ is both divisible by p^s and not larger than p^s, i.e. $|St(T)| = p^s$. In other words, we

found a subgroup $St(T)$ of G which has p^s elements. The existence of such subgroup is a very important theorem:

Theorem 2. *(Sylow) If G is a finite group such that $|G| = p^s m$, where p is a prime and $\gcd(p, m) = 1$ then G has a subgroup of order p^s.*

Subgroups whose existence we just established are very important in group theory and we introduce the following definition

Definition 3. *Let G be a finite group such that $|G| = p^s m$ where p is a prime and $\gcd(p, m) = 1$. Any subgroup of G of order p^s is called a* **Sylow $p-$subgroup** *of G*

As a corollary of Theorem 2 we get the following result due to Cauchy:

Theorem 3. *(Cauchy) Let G be a finite group and p a prime divisor of $|G|$. Then G has an element of order p.*

Proof: Let P be a Sylow $p-$subgroup of G, so $|P| = p^s$ for some $s > 0$. Let $a \in P$, $a \neq e$. The order of a divides p^s, so it equals p^k for some $0 < k \leq s$. Now $a^{p^{k-1}}$ has order p. $\square$

A different proof of Cauchy's theorem is given in Problem 4 of homework 7.