Math 493 Lecture 13

Professor Andrew Snowden

Transcribed by Thomas Cohn

10/21/19

Group Action Summary

- Key definitions: G-set, orbit, stabilizer
- Every G-set is the disjoint union of its orbits, with each orbit a transitive G-set
- If $H \subset G$, then the set of cosets G/H is a transitive G-set, and every transitive G-set is isomorphic to one of these (up to conjugation).

Prop: (Counting Formula) If X is a finite G-set, then $\#O_X \cdot \#G_X = \#G$.

Ex: A perfect matching on a set X is an undirected graph V with vertices set X s.t. every vertex belongs to exactly 1 edge.
Question: how many perfect matchings are there on n vertices?
Well, S_n acts transitively on the vertices. Let

$$X = \left\{ \begin{matrix} 1 & 3 & 5 & \cdots & n-1 \\ 2 & 4 & 6 & & n \end{matrix} \right\}$$

So we can write $G_X = (S_2)^{n/2} \oplus S_{n/2}$, and thus

$$\#X = \frac{\#S_n}{\#G_X} = \frac{n!}{2^{n/2}(n/2)!} = (n-1)(n-3)\cdots$$

Class Formula

Let G act on X with X finite. Let $O_1, \dots, O_n$ be the orbits. Then

$$\#X = \#O_1 + \cdots + \#O_n$$

and for each $i = 1, \dots, n$, $\#O_i \mid \#G$.

Defn: A finite group G is called a ***p*-group** for prime p if $\#G$ is a prime power.

Prop: Say G is a p-group acting on a finite set X s.t. p does not divide $|X|$. Then there is a point $x \in X$ s.t. $gx = x$, $\forall g \in G$.
Proof: let $O_1, \dots, O_n$ be the orbits. Note that i is a fixed point iff $\#O_i = 1$, so we need to show $\#O_i = 1$ for some i.
Well, we know $\#O_i$ is either 1 or divides p. Well, $\#X \not\equiv 0 \bmod p$, but $\#X = \#O_1 + \cdots + \#O_n$. So one of these must be nonzero modulo p. Thus, we know that some orbit has size 1. □

Remark: $\#X \equiv \#(X^G) \bmod p$ where X^G is the set of fixed points.

Prop: Say G is a subgroup of $\mathrm{GL}_n(\mathbb{F}_p)$ s.t. G is a p-group. Then $\exists v \in \mathbb{F}_p^n \setminus \{0\}$ s.t. $gv = v$, $\forall g \in G$.
Remark: implying this proposition shows that G is conjugate to a subgroup of

$$\begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

Let G be any finite group. G acts on itself by conjugation. Say $C_1, \ldots, C_n$ are the conjugacy classes. Thus, we have the class equation:

$$\#G = \#C_1 + \cdots + \#C_n$$

This implies that if G is a group, $\#C_1 = 1$, where C_1 is the conjugacy class of the identity element. Thus, we can look at the class equation modulo p:

$$0 = 1 + (\#C_2 + \cdots + \#C_n) \bmod p$$

So $\exists i \in \{2, \ldots, n\}$ s.t. $\#C_i = 1$. Say $C_i = \{x\}$. Then $gxg^{-1} = x$, $\forall g \in G$. So we've proved if G is a nontrivial prime power, then $Z(G)$ (the center of G) is nontrivial. □

Cor: If $\#G = p^2$, then G is abelian. In fact, $G \cong \mathbb{Z}/p^2\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
Proof: let $Z = Z(G)$. We know Z is nontrivial. Say $Z \neq G$. Then pick $g \in G \setminus Z$. For cardinality reason, $G = \langle Z, g \rangle$. Thus, G is abelian. □

We consider two cases.

1. $\exists g \in G$ s.t. $\mathrm{ord}(g) = p^2$. Then $G \equiv \mathbb{Z}/p^2\mathbb{Z}$.
2. $\forall g \in G$, $g^p = 1$. Write G additively, so $px = 0$, $\forall x \in G$. Because of this, we have a well defined scalar multiplication map from $\mathbb{F}_p \times G \to G$, so G is canonically an $\mathbb{F}_p$ vector space. Since $\#G = p^2$, we have $G \equiv \mathbb{F}_p^2$.

□