11.3.2025: Math 122 Lecture 16 Notes

Vasily Krylov

1 Last Time

Last time we established that $G \curvearrowright X$ partitions X into G orbits, so that $X = \sqcup \mathcal{O}$. Note that x and y are in the same orbit if $y = gx$ for some $g \in G$. The main proposition was that there exists an explicit bijection between the orbit O_i and G/G_{x_i} (where G_{x_i} is the stabilizer of x_i). This bijection is given by $gG_{x_i} \mapsto gx_i$ (as a map from $G/G_{X_i} \to O_i$).

As an example, consider $S_3 \curvearrowright S_3$ via conjugation. We have $S_3 = \{1\} \sqcup \{(12), (13), (23)\} \sqcup \{(123), (132)\}$. Consider $O_3 = \{(123), (132)\}$ and let $x_3 = (123)$. The stabilizer is $G_{x_3} = \{1, (123), (132)\}$. We have $|G_{x_3}| = 6/2 = 3$, and by the main result, $O_{x_3} \cong S_3/G_{x_3}$. We note that O_{x_3} has 2 elements and S_3 has 6 elements, which checks out. Explicitly, $S_3/\langle(123)\rangle \to \{(123), (132)\}$ has two conjugacy classes; there is $\langle(123)\rangle \mapsto (123)$ and $(12)\langle(123)\rangle \mapsto (132)$.

2 Counting Formulas

Counting Formula 1. Let $G \curvearrowright X$, with each finite. Then for any $x \in O \subset X$ (with O an orbit), we have that $|G| = |O||G_x|$, i.e. $|O| = [G : G_x]$.

Proof. We have that $O \cong G/G_x \implies |O| = |G/G_x| = [G : G_x] = |G|/|G_x| \implies |O||G_x| = |G|$. □

One application is that this lets us compute the number of elements of G_x (useful in the pset).

Counting Formula 2. Let $G \curvearrowright X$. Then $X = O_1 \sqcup \cdots \sqcup O_k$, with $x_i \in O_i$ some representative of each orbit. Then $|X| = |O_1| + \cdots + |O_k| = [G : G_{x_1}] + \cdots + [G : G_{x_k}]$.

As an example, consider $S_3 \curvearrowright S_3$ via conjugation. Let $O_1 = \{1\}, O_2 = \{(12), (23), (13)\}, O_3 = \{(123), (132)\}$. Then we have $G_1 = S_3, G_{(12)} = \{1, (12)\}, G_{(123)} = \{(1), (123), (132)\}$. We have $6 = |S_3| = [S_3 : S_3] + [S_3 : \langle(12)\rangle] + [S_3 : \langle(123)\rangle] = 6/6 + 6/2 + 6/3 = 1 + 3 + 2 = 6$.

Prop. Let G be a finite group of order p^k, where p is prime and $k \in \mathbb{Z}_{\geq 1}$. Such G is a called a p-group (e.g. $G = D_8$). Recall that the center $Z \subset G$ consists of all $g \in G$ such that $\forall h \in G, gh = hg$. In this case, the center $Z \subset G$ is nontrivial. (E.g. in D_8, the center is $\{1, r^2\}$.) Further, Z is a p-group, and $|Z| \geq p$ by Lagrange's theorem.

Proof. Consider $G \curvearrowright G$ by conjugation. Then $G = O_1 \sqcup \cdots \sqcup O_k$, where these represent conjugacy classes. An element $g \in G$ lives in Z if and only if $O_g = \{g\}$, as if G is central, then the stabilizer is $G_g = G$, so G/G_g must have size 1. This shows that $g \in Z \implies O_g = \{g\}$. Conversely, if $O_g = \{g\}$, then $\forall h \in G, hgh^{-1} = g \implies hg = gh$, so $g \in Z$.

We have $G = Z \sqcup (\sqcup O_i)$, where the O_i are orbits of noncentral elements. We know that $|O_i| > 1$. We also know that $|O_i|||G| = p^k \implies |O_i| = p^{k_i}, k_i \geq 1 \implies p||O_i|$. We have $|Z| = |G| - \sum |O_i| \implies p||Z|$, as the right hand side is divisible by p. This completes the proof. $\square$

Thm. (Cauchy's). Let G be a finite group with $p||G|$, p prime. Then G has an element of order p.

Proof. First, let G be a p-group, so $|G| = p^k$. Then take $g \in G$ any non-identity element with order $m > 1$. We know by Lagrange that $m||G| \implies m|p^k \implies m = p^l$ for some $l > 0$, so $p|m$. Then $g^{m/p}$ has order p. We note that whenever $g \in G$ has order m and $n|m$ with $1 \leq n \leq m$, then $g^{m/n}$ has order n.

Next, assume G is commutative. We use strong induction on $|G|$. Assume the theorem holds for arbitrary H such that $|H| < |G|$. For the base case $|G| = 2$, we have $G \cong \mathbb{Z}/2\mathbb{Z}$, and $1 \in \mathbb{Z}/2\mathbb{Z}$ has order 2. Take $g \in G$ an arbitrary non-identity element. Let $H = \langle g \rangle \subset G$. We have two cases: first, when $p||H|$, and second, when p does not divide $|H|$.

First, consider when $p||H|$. In this case, p divides the order of g, so $g^{|H|/p}$ has order p.

Next, consider when $p \not| |H|$. then $p||G/H| = |G|/|H|$. Since $|G/H| < |G|$, by induction, we can find some coset $xH \in G/H$ with order p. We have $(xH)^p = H$. Let m be the order of $x \in G$. We know $x^m = 1$ in G. This implies $(xH)^m = H$, so $p|m$, and again, $x^{m/p}$ has order p.

Finally, let G be an arbitrary group. We claim that it suffices to prove there is a nontrivial p-subgroup $H \subset G$. We have $|G| = p^k n$; we claim there is always a subgroup $H \subset G$ with $|H| = p^k$. We will prove this next time. $\square$

Thm. (First Sylow Theorem). Let G be a finite group of order $|G| = p^k n$, with p, n coprime. Then $\exists H \subset G$ such that $|H| = p^k$.