Math 210A Lecture 15 Notes

Daniel Raban

October 31, 2018

1 Simple Groups, Burnside's Formula, and p-Groups

1.1 Simple groups

Theorem 1.1. *A_n is simple for $n \geq 5$.*

Proof. Proceed by induction on n. We know this for $n = 5$. Assume it for $n-1$ with $n \geq 6$. The intersection of the stabilizer of i and A_n is $G_i = (S_n)_i \cap A_n \cong A_{n-1}$ for $1 \leq i \leq n$, so G_i is simple. Let $N \trianglelefteq A_n$ with $N \neq \{e\}$. If there exists $i \in X_n = \{1, \dots, n\}$ and $\tau \in N \setminus \{e\}$ with $\tau(i) = i$, then $N \cap G_i \neq \{e\}$ and $N \cap G_1 \trianglelefteq G_i$. So $N \cap G_i = G_i$; i.e. $G_i \leq N$.

For any $\sigma \in A_n$ with $\sigma(i) = j$, we have $\sigma G_i \sigma^{-1} = G_j$. Then $\sigma = \begin{pmatrix} i & j \end{pmatrix} \begin{pmatrix} k & \ell \end{pmatrix}$ works for some $\{k, \ell\} \cap \{i, j\} = \varnothing$ since $n \geq 4$. So $G_j \leq N$ since $N \trianglelefteq A_n$. So every product of 2 transpositions is in N since $n \geq 5$, so $A_n = N$.

Take $\tau \in N$. If there exists $\tau' \in N$ and $i \in X_n$ such that $\tau(i) = \tau'(i)$, then $\tau(\tau')^{-1}(i) = i$. Then $\tau = \tau'$, or $N = A_n$. Write τ as a product of disjoint cycles. There are 2 cases:

1. $\tau = \begin{pmatrix} a_1 & \cdots & a_k \end{pmatrix} \cdots$ where $k \geq 3$: Pick $\sigma \in A_k$ such that $\sigma(a_1) = a_1, \sigma(a_2) = a_2, \sigma(a_3) \neq a_3$. Take $\tau' := \sigma \tau \sigma^{-1}$. This works.
2. $\tau = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \cdots \begin{pmatrix} a_{m-1} & a_m \end{pmatrix}$: Take $\sigma = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \begin{pmatrix} a_3 & a_5 \end{pmatrix}$. Then $\tau' = \sigma \tau \sigma^{-1}$ works as well. So $\tau'(a_1) = \tau(a_1)$ but $\tau' \neq \tau$. □

In general, the following theorem is true. We will not prove it.[1]

Theorem 1.2 (classification of finite simple groups)**.** *Every finite simple group is isomorphic to one of*

1. *$\mathbb{Z}/p\mathbb{Z}$ with p prime*
2. *(simple) group of Lie type*
3. *A_n for $n \geq 5$*
4. *one of 26 sporadic simple groups*
5. *the Tits group*

[1] The proof is thousands of pages long.

1.2 Burnside's formula

For $g \in G$ and X a G-set, denote the set of fixed points of g as $X^g = \{x \in X : g \cdot x = x\}$. If $S \subseteq G$, let $X^S = \{x \in X : g \cdot x = x \, \forall g \in S\} = \bigcap_{g \in S} X^g$. Recall that the stabilizer of x is $G_x = \{g \in G : g \cdot x = x\} \subseteq G$. Then $g \in G_x \iff x \in X^g$.

Theorem 1.3 (Burnside's formula)**.** *Suppose G is finite, and X is a finite G-set. The number r of G-orbits in X is*

$$r = \frac{1}{|G|} \sum_{g \in G} |X^g|.$$

Proof. Let $S = \{(g, x) : g \in G, x \in X, g \cdot x = x\}$. On one hand,

$$S = \coprod_{g \in G} \{(g, x) : x \in X^g\},$$

which is in bijection with X^g. On the other hand,

$$S = \coprod_{x \in X} \{(g, zx) : g \in G_x\},$$

which is in bijection with G_x. So

$$\sum_{g \in G} |X^g| = |S| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|G \cdot x|} = |G| \sum_{x \in X} \frac{1}{|G \cdot x|}.$$

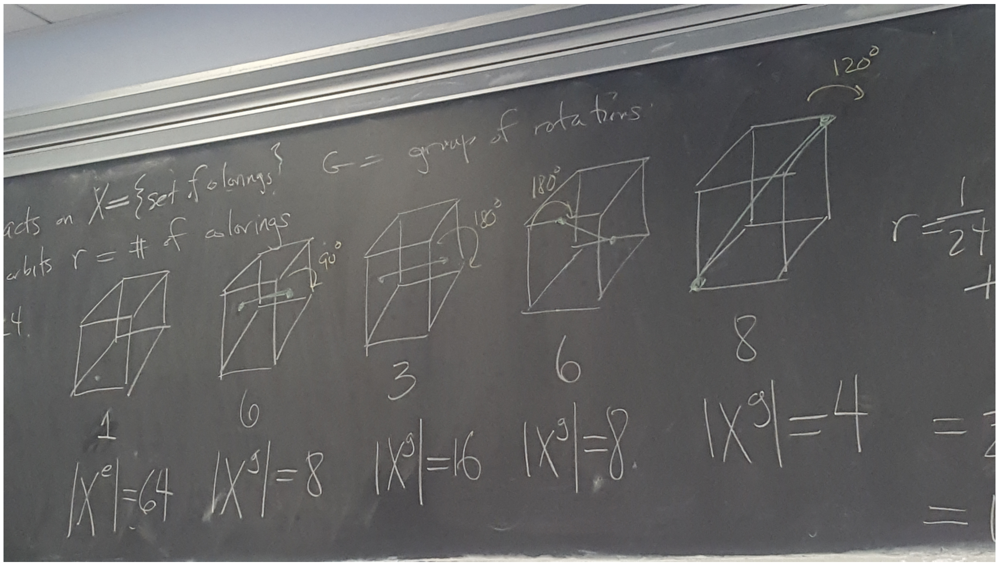
Each orbit appears $|G \cdot x|$ times in this sum. So we get

$$\sum_{g \in G} |X^g| = |G| \sum_{\text{orbit reps.}} 1 = |G| r. \qquad \square$$

This allows us to solve fun counting problems.

Example 1.1. How many ways are there to color the sides of a cube red and blue (that look different under rotations)? Let G be the group of rotations of a cube. G acts on X, the set of colorings of a cube. The number of orbits r is the number of colorings. $|G| = 24$.

Let's write out what the elements are and the number of fixed points in each case.



So, by Burnside's formula,

$$r = \frac{1}{24}(64 + 6 \cdot 8 + 3 \cdot 16 + 6 \cdot 8 + 8 \cdot 4) = 10.$$

1.3 p-groups

Let p be prime.

Definition 1.1. A group G is a p**-group** if every element of G has a p-power order.

Example 1.2. $\mathbb{Z}/p^n\mathbb{Z}$ is a p-group.

Example 1.3. Q_8 and D_4 are 2-groups.

Example 1.4. Here is an infinite p-group. $\{a/p^n : 0 \leq a \leq p^n - 1, n \geq 1\} \subseteq \mathbb{Q}/\mathbb{Z}$.

Lemma 1.1. *Let G have p-power order, and let X be a finite G-set. Then*

$$|X| \equiv |X^G| \pmod{p}.$$

Proof. Let S be a set of orbit representatives in X. Then

$$|X| = \sum_{x \in S} |G \cdot x| = \sum_{x \in S} [G : G_x] \equiv \sum_{x \in X^G} 1 = |X^G| \pmod{p},$$

where $X^G \subseteq S$ is the set of singleton orbits. □

Theorem 1.4 (Cauchy). *Let p be prime and G a finite group with $p \mid |G|$. Then G contains an element of order p.*

Proof. Let $X = \{(a_1, \dots, a_p) \in G^p : a_1 \cdots a_p = e\}$. Then $S_p \circlearrowright X$ by permuting the indices $\sigma(a_1, \dots, a_p) = (a_{\sigma(1)}, \dots, a_{\sigma(p)})$. Let $\tau = \begin{pmatrix} 1 & 2 & \cdots & p \end{pmatrix}$. Then $H = \langle \tau \rangle$ acts on X such that $X^H = X^\tau = \{(a, a, \dots, a) \mid a^p = e\}$. Note that $X^H \neq \varnothing$ since $(e, \dots, e) \in X^H$. Also, $|X| = |G|^{p-1} \equiv 0 \pmod{p}$. By the lemma, $|X^H| \equiv 0 \pmod{p}$, so since $X^H \neq \varnothing$, X^H has another element; i.e. there exists $a \neq e$ with $a^p = e$. □

Corollary 1.1. *If G is a finite p-group, then G has p-power order.*

Proposition 1.1. *If G is a nontrivial finite p-group, then $Z(G) \neq \{e\}$.*

Proof. If $Z(G) = \{e\}$, then the class equation gives

$$|G| = 1 + \sum_{x \in S} C_x = 1 + \sum_{x \in S} [G : Z_x] \equiv 1 \pmod{p},$$

where S is a set of representatives of nontrivial conjugacy classes. Since G has p-power order, we get $|G| = 1$. □

Theorem 1.5. *Every group of order p^2 is abelian.*

Proof. Let $|G| = p^2$. If G is not abelian, then $Z(G)$ has order p. Then $Z(G) = \langle a \rangle$, where a has order p. Let $b \notin \langle a \rangle$. Then b has order p, and $G = \langle a, b \rangle$. Note that b commutes with a because $a \in Z(G)$. But b commutes with itself, so $b \in Z(G)$. This is a contradiction. □