Week 5: Group actions and the class formula

Practice Problems

1. Show that any group with class formula $60 = 1 + 12 + 12 + 15 + 20$ has no nontrivial normal subgroups.

2. Let $\mathrm{SL}_2(\mathbb{Z})$ denote the set of 2×2 matrices M with integer entries such that $\det(M) = 1$. Show that $\mathrm{SL}_2(\mathbb{Z})$ is a group. Verify that we have an action of $\mathrm{SL}_2(\mathbb{Z})$ on the set $\mathbb{R} \setminus \mathbb{Q}$ of irrational reals given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot r = \frac{ar + b}{cr + d}.$$

   If we allow a, b, c, d to be complex valued, then a function of the form $f(z) = \frac{az+b}{cz+d}$ is called a Möbius transformation, or fractional linear transformation.

3. Determine the center $Z(\mathrm{SL}_2(\mathbb{Z}))$ of $\mathrm{SL}_2(\mathbb{Z})$. We define the modular group to be the quotient

$$\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/Z(\mathrm{SL}_2(\mathbb{Z})).$$

   Show that if $A \in Z(\mathrm{SL}_2(\mathbb{Z}))$, then $A \cdot r = r$ for all $r \in \mathbb{R} \setminus \mathbb{Q}$, and deduce that the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{R} \setminus \mathbb{Q}$ induces an action of $\mathrm{PSL}_2(\mathbb{Z})$ on $\mathbb{R} \setminus \mathbb{Q}$.

Presentation Problems

1. Let G be a finite group and let H be a proper subgroup of G. Show that $G \neq \bigcup_{g \in G} gHg^{-1}$.

2. Let G be a finite group acting on a set X. For each $g \in G$, let $X^g = \{x \in X : gx = x\}$ be the set of the elements in X fixed by g. Let X/G denote the set of orbits of X under the action of g. Show that

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

   by counting the set $\{(g, x) \in G \times X : gx = x\}$ in 2 different ways. This is known as Burnside's lemma.

3. Let G be a finite p-group and let H be a nontrivial normal subgroup of G. Show that $H \cap Z(G) \neq 1$. Give a counterexample if H is not a normal subgroup of G.

4. Let H and K be finite subgroups of a group G.
   (a) Construct a transitive group action of $H \times K$ on HK.
   (b) Use the orbit-stabilizer theorem to show that $|HK| = |H||K|/|H \cap K|$.

Bonus: Frobenius' Theorem

Let G be a finite group and let n be a divisor of $|G|$. Frobenius' theorem states that the number of solutions to $g^n = 1$ is a multiple of n. A proof of this result using Burnside's lemma and some combinatorics can be found at `https://sbseminar.wordpress.com/2015/09/05/a-counting-argument-for-frobenius-theorem/`. By "d-torsion" elements, the post means elements g such that $g^d = 1$. Here are a couple applications of Frobenius' theorem:

1. Let G be a finite group of order $p^k m$ where p is a prime not dividing m. Show that the number of elements of G of order a power of p is congruent to $p^k \pmod{p^{k+1}}$.

2. Show that if p is a prime then p divides $(p-1)! + 1$.

This last result is known as Wilson's theorem (2/4).

Tricky Problems

1. Let G be a finite group of order $p^k m$ where p is a prime possibly dividing m. Let X be the collection of subsets of G of order p^k. Let G act on X by left multiplication. For each $0 \leq j \leq k$, let n_j count the number of orbits of cardinality $p^j m$.

   (a) Show that if $S \in X$ then S is a (disjoint) union of right cosets of the stabilizer subgroup $\mathrm{Stab}_G(S)$.

   (b) Show that every orbit of X has cardinality $p^j m$ for some $0 \leq j \leq k$.

   (c) Show that n_0 counts the number of subgroups of G of order p^k.

   (d) Show that
   $$\binom{p^k m - 1}{p^k - 1} = \frac{1}{m}|X| = \sum_{j=0}^{k} n_j p^j \equiv n_0 \pmod{p}.$$

   (e) Show that the number of subgroups of G of order p^k is congruent to 1 modulo p by applying parts (c) and (d) to both G and $\mathbb{Z}/p^k m\mathbb{Z}$. In particular, G contains a subgroup of order p^k.

   Here are a couple applications of this result:

   (f) Let $2^p - 1$ be a Mersenne prime and let G be a finite group of order $2^p(2^p - 1)$. Show that G contains a normal subgroup of order $2^p - 1$ or 2^p.

   (g) Show that if p is a prime then p divides $(p-1)! + 1$.

   This last result is known as Wilson's theorem (3/4).

2. Let $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/Z(\mathrm{SL}_2(\mathbb{Z}))$ be the modular group defined in practice problem 3.

   (a) Consider the matrices
   $$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$
   in $\mathrm{SL}_2(\mathbb{Z})$. Let x be the coset of A in $\mathrm{PSL}_2(\mathbb{Z})$ and let y be the coset of B in $\mathrm{PSL}_2(\mathbb{Z})$. Show that $|x| = 2$ and $|y| = 3$ but $|xy| = \infty$.

   (b) Show that A and B generate $\mathrm{SL}_2(\mathbb{Z})$. *Hint*: Use the matrix AB^{-1} to perform row operations.

   (c) Deduce that x and y generate $\mathrm{PSL}_2(\mathbb{Z})$.

   (d) Show that
   - x takes negative irrationals to positive irrationals,
   - y takes positive irrationals to negative irrationals less than -1,
   - y^2 takes positive irrationals to negative irrationals larger than -1.

   (e) Show that no nonempty product that alternates between x and y or y^2 can act trivially on $\mathbb{R} \setminus \mathbb{Q}$.

   (f) Show that $\mathrm{PSL}_2(\mathbb{Z})$ is presented by $(x, y \mid x^2, y^3)$.

   (g) Conclude that $\mathrm{PSL}_2(\mathbb{Z}) \cong C_2 * C_3$.