Math 110B Homework 4

Brendan Connelly

Due Wednesday, February 11, 2026

Problem 1

Let G be a group and $N \subset G$ be a normal subgroup, finally let $f : H \to G$ be a homomorphism.
(a) Show that the subgroup

$$X := f^{-1}(N)$$

is normal in H.

We can first check X is a subgroup. It is clearly non-empty as $e \in N$ so $e \in X$. Suppose $x, y \in X$. Then, $f(x), f(y) \in N$ so $f(y)^{-1} = f(y^{-1}) \in N$. Now, consider $f(xy^{-1}) = f(x)f(y^{-1}) \in N$ so $xy^{-1} \in X$ so $f^{-1}(N)$ is a subgroup.

To check normality, suppose $x \in X$. Then, for $y \in H$,

$$f(yxy^{-1}) = f(y)f(x)f(y)^{-1} \in N$$

so $yxy^{-1} \in X$ so X is normal.

□

……

(b) Show that the index $|H/X|$ divides $|G/N|$.

We can construct the map $\varphi : H \to G/N$ defined by $\varphi(h) = \pi(f(h))$ where π is the map we defined in class $\pi : G \to G/N$ with $\pi(g) = gN$. We don't have to worry about well definedness since there is no ambiguity in the domain. We can consider the kernel of φ. We know the kernel of f is the preimage of the identity. Hence, the kernel of φ is exactly $f^{-1}(N) = X$. By the first isomorphism theorem, we then have that

$$H/X \cong \operatorname{Im}(\varphi) \leq G/N$$

Hence, by Lagrange, $|H/X|$ divides $|G/N|$.

□

Problem 2

Let X be a set with a group action $G \curvearrowright X$, where G is a finite group. For simplicity we denote the action simply by $g \cdot x$ rather than the usual $A(g, x)$. For $g \in G$, $x \in X$ we define

$$G_x = \mathrm{Stab}_x \qquad \text{and} \qquad X^g := \{x \in X \mid g \cdot x = x\}.$$

(a) Show that

$$\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|.$$

Both sides count the same fixed points in two different ways. Suppose $x \in X^g$ for some $g \in G$. Then, $A(g, x) = x$ so $g \in G_x$. Similarly, suppose $g \in G_x$ for some $x \in X$. Then, $A(g, x) = x$ so $x \in X^g$. In other words, both sides count all pairs $\{(x, g)\}$. Taking cardinalities completes the proof.

$\square$

(b) Use the orbit-stabilizer theorem to show that

$$\sum_{x \in X} |G_x| = |G| \cdot |X/G|,$$

where X/G is the set of orbits of G on X.

By Orbit Stabilizer, $|G/G_x| = |O(x)|$. We then also have $\sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|O_x|}$. We can then count over each orbit as they partition X.

$$\sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|O_x|} = \sum_{\mathcal{O} \text{ orbit}} \sum_{x \in \mathcal{O}} \frac{|G|}{|\mathcal{O}_x|}$$

In each orbit, $|\mathcal{O}|$ is constant. Hence, the inner summation is exactly $|G|$. Since we sum over all orbits, denoted $|X/G|$, we have that this sum is exactly $|G| \cdot |X/G|$.

$\square$

(c) Deduce that the average number of fixed points of an element of G is equal to the number of orbits of G on X.

Rearranging (b) gives that

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

Hence, the average number of fixed points of an element of G is equal to the number of orbits of G on X.

$\square$

Problem 3

Suppose G is a finite group which acts transitively on a set X, where $|X| > 1$. Show that there is some $g \in G$ such that $|X^g| = 0$.

Since G is transitive, it was one orbit. Hence, by question 2,

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

We know $e \in G$ and then $X^e = X$ so

$$|X| + \sum_{g \neq e} |X^g| = |G|$$

Suppose for contradiction that $|X^g| \geq 1$ for all $g \in G$. We also assume $|X| > 1$ and $n = |G|$. Then,

$$|X| + \sum_{g \neq e} |X^g| \geq 2 + (n-1) = n + 1 > n = |G|$$

which is a contradiction.

□

Problem 4

Let H be a subgroup of G, and consider the left action of G on G/H. Show that $g \in G$ is conjugate to an element of H if and only if g has a fixed point, i.e. $|(G/H)^g| \neq 0$. Deduce that G cannot be written as a union of conjugates of a subgroup $H \leq G$, as long as $H \neq G$.

$g \in G$ has a fixed point if and only if $A(g, g'H) = g'H$ for some $g' \in G$ by definition of a fixed point. We know this is true if and only if $gg'H = g'H$ by definition of the left action. We know this equality of cosets holds if and only if $g'^{-1}gg' \in H$, i.e. if and only if g is conjugate to an element in H.

We want to show $G \neq \bigcup_{g \in G} gHg^{-1}$. In other words, we want to show that there exists a $g \in G$ such that $g \notin \bigcup_{g \in G} gHg^{-1}$. By (3) as $H \neq G$, we know that there exists a $g \in G$ such that $|(G/H)^g| = 0$. Then, said g cannot be written as a conjugate of h.

□

Problem 5

Let S_n be the symmetric group, and let $c = (1\ 2\ \cdots\ n)$ be the n-cycle. Show that $\langle (1\ i), c \rangle = S_n$ if and only if $(i-1, n) = 1$.

Let $d := (i-1, n)$. Further, define $k := i - 1$. Assume first $d = 1$. Then, we can use what we prove the following problem. We can first consider $c^m(1i)c^{-m} = (c^m(1)c^m(i))$. Hence, we can swap any two elements separated by a distance of k mod n. However, we can see we can actually swap any two elements as if we take say any element, we can reach $1, 1+k, 1+2k, \ldots$. But, since the $\gcd(k,n) = 1$, we know that we will actually reach every element in $[n]$ from 1 via a swap. Hence, we can swap any two elements by composition. But, we also know we can create any element in S_n via the composition of swaps. We can go through any element in S_n and swap elements that are out of order. We can do this repeatedly until the elements are ordered. Said $\sigma \in S_n$ will then be exactly the inverse of the composition of these swaps. Hence, $\langle (1\ i), c\rangle = S_n$.

Now, suppose $d > 1$. We can consider the elements in S_n that are equivalent modulo d. I claim such elements will maintain their equivalence under any composition of $\langle (1\ i), c\rangle = S_n$, i.e., $x \sim y$ if $x \equiv y \mod d$. I claim $x \sim y$ under any elements generated by $(1\ i), c$. Under the swap, as $d \mid i-1$, $1 \sim i$ so the relation holds here. Under the cyclic permutation, if $x \sim y$, $x+1 \sim y+1$. Hence, any composition of swaps preserves similarity between elements. Yet, we know $(12) \in S_n$. Consider $x = 1, y = 1+d$. Then, $x \sim y$ but after the application of (12), $2 \not\sim 1+d$, which is a contradiction.

$\square$

Problem 6

Let $c = (x_1\ x_2\ \cdots\ x_k) \in S_n$ be a cycle, and let $\sigma \in S_n$ be arbitrary. Show that

$$\sigma c \sigma^{-1} = \big(\sigma(x_1)\ \sigma(x_2)\ \cdots\ \sigma(x_k)\big).$$

We want to show that the $\sigma(x_i) \mapsto \sigma(x_j)$. Further, we want to show that other elements are fixed. Consider

$$\sigma \circ c \circ \sigma^{-1}(\sigma(x_i)) = \sigma(c(x_i)) = \sigma(x_{i+1})$$

where $\sigma(c(x_k)) \mapsto \sigma(x_1)$. We also know that for $i > k$, $\sigma \circ c \circ \sigma^{-1}(\sigma^{-1} x_i) = \sigma(c(x_i)) = \sigma(x_i)$, i.e., $\sigma(x_i) \mapsto \sigma(x_i)$–all one cycles.

$\square$

Problem 7

Using the previous exercise calculate the number of conjugacy classes of S_n.

Via question 6, we see that conjugation of a cycle preserves exactly the length of the cycle. Hence, any permutation, a composition of disjoint cycles, when conjugated, will have exactly the number of cycles of said size preserved, i.e., the cycle types are preserved. Hence, the number of conjugacy classes of S_n is exactly the number of different possible cycle types that sum to n. This is exactly the number of way we can partition n, written in non-increasing order to give us uniqueness. In combinatorics, we can count this with a generating function and denote this number $p(n)$.

$\square$

Problem 8

Let $c = (x_1 \; x_2 \; \cdots \; x_n)$ be an n-cycle, and let $1 \leq d \leq n$. Find the cycle decomposition of c^d.

We know that $x_i \mapsto x_{i+d}$ modulo n. We know that if $d = 1$, this will loop around and reach every element. Otherwise, as described in question 5, $x_i \mapsto x_{i+d}$ will split into a $l = \gcd(d, n)$ cycles of length n/l, with this mapping $x_i \mapsto x_{i+d}$ modulo n in each cycle.

□