MATH 111A HOMEWORK 9 SOLUTIONS

---

8) Prove that if H has finite index n then there exists $K \lhd G$ with $K \leq H$ and $[G : K] \leq n!$.

Proof. Let $A = G/H$ be the left coset space of H in G. Let G act on G/H via multiplication, i.e.

$$g \cdot aH = gaH \quad \text{for all } g \in G \text{ and } aH \in G/H.$$

Let $f : G \to S_A$ be the homomorphism corresponding to this action, i.e.

$$f(g) = \sigma_g, \text{ where } \sigma_g(aH) = gaH.$$

Let $K = \ker(f)$. Then K is a normal subgroup of G.

(i) $K \leq H$: Let $k \in K$. Then $k \in \ker(f)$ and so $f(k) = \sigma_k$ is the identity on G/H. In particular

$$\sigma_k(H) = H \implies kH = H \implies k \in H.$$

Thus, indeed $K \leq H$.

(ii) $[G : K] \leq n!$: By the First Isomorphism Theorem, we have

$$G/K \simeq \mathrm{Im}(f)$$

and so $[G : K] = |\mathrm{Im}(f)|$. But $\mathrm{Im}(f) \leq S_A$ and S_A is isomorphic to S_n since $|A| = [G : H] = n$. Thus

$$[G : K] = |\mathrm{Im}(f)| \leq |S_A| = n!$$

as desired.

---

2) Suppose $a, b \in A$ and $g \in G$ with $b = g \cdot a$. Show that $G_b = gG_ag^{-1}$.

Proof. For any $x \in G$ we have

$$\begin{aligned}
x \in G_b &\iff x \cdot b = b \\
&\iff x \cdot (g \cdot a) = g \cdot a \qquad \text{(because } b = g \cdot a\text{)} \\
&\iff (xg) \cdot a = g \cdot a \qquad \text{(property of a group action)} \\
&\iff (g^{-1}xg) \cdot a = a \qquad \text{(property of a group action)} \\
&\iff g^{-1}xg \in G_a \\
&\iff x \in gG_ag^{-1} \qquad \text{(multiply } g \text{ on the left and } g^{-1} \text{ on the right)}
\end{aligned}$$

Thus, we have shown that $G_b = gG_ag^{-1}$.

---

4) Let $\sigma \in S_n$ non-identity and suppose $(a_1, ..., a_l)$, with $l \geq 2$, is one of the cycles in the disjoint cycle decomposition of σ. Let $G = \langle \sigma \rangle \leq S_n$, $A = \{1, ..., n\}$, and $\sigma^m \cdot a = \sigma^m(a)$ for $m \in \mathbb{Z}$ and $a \in A$. Show that $\mathcal{O}(a_1) = \{a_1, ..., a_l\}$.

Proof. By definition

$$\mathcal{O}(a_1) = \{x \cdot a_1 \mid x \in G\} = \{\sigma^m(a_1) \mid m \in \mathbb{Z}\},$$

where the second equality follows because $G = \langle \sigma \rangle$. We want to determine these images $\sigma^m(a_1)$.

Now, let $\sigma = \tau_1 \cdots \tau_s$ be the cycle decomposition of σ with $\tau_1 = (a_1 \cdots a_l)$. Since disjoint cycles commut

$$\sigma^m = (\tau_1 \cdots \tau_s)^m = \tau_1^m \cdots \tau_s^m.$$

Since the cycles $\tau_2, ..., \tau_s$ do not contain a_1, they all fix a_1 and so

$$\sigma^m(a_1) = (\tau_1^m \cdots \tau_s^m)(a_1) = \tau_1^m(a_1) = (a_1 \cdots a_l)^m(a_1).$$

Moreover, it was proved in class that

$$(a_1 \cdots a_l)^m(a_1) = a_j,$$

where $j \in \{1, ..., l\}$ is such that $j \equiv 1 + m \pmod{l}$. This shows that

$$\mathcal{O}(a_1) \subset \{a_1, ..., a_l\}.$$

But j will range over all integers $\{1, ..., l\}$ as m ranges over all $\mathbb{Z}$, we see that in fact

$$\mathcal{O}(a_1) = \{a_1, ..., a_l\}.$$