# Tutorial 8

Let $G$ be a group of order $n = p^e p_1^{e_1} \dots p_k^{e_k}$, where $p < p_1 < \cdots < p_k$ are primes. Suppose $G$ has a subgroup $H$ of index $p$.

**Problem 1.** Let $G$ act on the $p$ cosets of $H$ by left multiplication [see Tutorial 3 Q3.], namely

$$g \,.\, g'H = (gg')H.$$

In other words, for each $g \in G$, we can define the map

$$f_g : G/H \to G/H, g'H \mapsto (gg')H.$$

a) Show that $f_g$ is a permutation.

b) Consider the map

$$\Phi : G \to S_p, g \mapsto f_g.$$

Show that $\Phi$ is a homomorphism.

**Remark.** $\Phi$ is the *permutation representation* of the action by $G$. We will talk more about this soon.

**Solution**

a) For injectivity, note that for $g', g'' \in G$, $f_g(g'H) = f_g(g''H)$ tells us $gg'H = gg''H$ which implies $g''^{-1}g^{-1}gg' = g''^{-1}g' \in H$. This is only true if $g'H = g''H$, so $f_g$ is injectivity. Surjectivity follows from the fact that $f_g$ is an injective self-map on a finite set.

b) We have

$$\Phi(gg')(g''H) = f_{gg'}(g''H) = gg'g''H = f_g(f_{g'}(g''H)) = (\Phi(g) \circ \Phi(g'))(g''H).$$

**Problem 2.** Continuing with the notation of the previous problem, with the homomorphism $\Phi : G \to S_p$. Let $K = \ker \Phi$.

a) Show that $K \subseteq H$. [*Hint*: Tutorial 7 Q3.]

b) Use the first isomorphism theorem to show that $o(G/K) \mid o(S_p)$.

c) Let $r = [H : K]$. Show that $r = 1$. Conclude that $H \trianglelefteq G$.

That is, if $G$ is a finite group and $H \leq G$ is of the smallest possible prime index, then $H \trianglelefteq G$.

**Solution**

a) $K$ contains the $g \in G$ such that $f_g = \mathrm{id}$. Now $f_g = \mathrm{id}$ exactly when $g'H = gg'H$ for all $g' \in G$, or equivalently, $g'^{-1}gg' \in H$ for all $g' \in G$.

This is true if and only if $g \in g'Hg'^{-1}$ for all $g' \in G$, and so $f_g = \mathrm{id}$ is equivalent to

$$g \in \bigcap_{g' \in G} g'Hg'^{-1}.$$

Now since one of the components of the intersection is $eHe^{-1} = H$, this intersection sits inside $H$.

Tutorial 7 Question 3 tells us $K \subseteq H$ and $K \trianglelefteq G$. [You can also show the last one using the normality of the kernel.]

b) Since $\Phi$ is a homomorphism, first isomorphism theorem tells us that $G/K \cong \Phi(G)$. Thus, $o(G/K) = o(\Phi(G))$. We also know that $\Phi(G) \leq S_p$ and Lagrange theorem gives us $o(G/K) = o(\Phi(G)) \mid o(S_p) = p!$.

c) We have from a) that $K \leq H$. Tower law of indices gives us

$$o(G/K) = [G : K] = [G : H][H : K] = p \cdot [H : K] = pr.$$

We note that $[H : K] \mid o(H) \mid o(G)$. Thus all prime factors of $r = [H : K]$ are $\geq p$.

However, b) gives us $pr \mid p!$ which forces $r \mid (p-1)!$. If $r > 1$ then it must have a prime factor, say $q$, and $q \mid (p-1)!$. Since $q$ is a prime it must divide one of $1, 2, 3, ..., p-1$. This cannot happen as $q \geq p$.

Thus, $r = 1$ and so $H = K$. Thus $H \trianglelefteq G$.

**Remark.** This is a generalization of Exercise 100.