Expository Writing: Index of a Subgroup

August Liu

September 2020

We first make some easy observations.

Let G be a group. Let $H \leq G$ be a subgroup of index m. $g \in G$ has order n.

Consider the least $i \in \mathbb{N}$ for which $g^i \in H$. By division algorithm, $n = qi + r$ for some $0 \leq r \leq i - 1$. Then $g^r \in H$. This implies $r = 0$ and hence $i \mid n$.

Also notice, by Pigeonhole principle, there's a repeated coset in $H, gH, g^2H, \ldots, g^mH$. Therefore $i \leq m$.

(Here we cleverly avoided the requirement for readers to know what group actions are. Clearly this is just equivalent to considering the action of $\langle g \rangle$ on G/H, and the order of g in $Sym(G/H)$ as well as the size of the orbit containing H.)

Now we consider some special cases in which these observations imply more direct results.

(1) If G is finite, then n/i is the order of g^i in H. This implies $(n/i) \mid |H| = |G|/m$ and hence $mn \mid i|G|$. So if $mn \nmid |G|$ then $g \notin H$.

(2) If the least prime factor of n is strictly greater than m, then the only possibility for $i \mid n$ and $i \leq m$ is if $i = 1$. This implies $g \in H$.

Proposition 1.1. *$H \leq G$ has index m. g has order n. If $\gcd(m!, n) = 1$, then $g \in H$.*

Notice, in this case, the action $\phi : \langle g \rangle \to Sym(G/H)$ gives the result more directly (consider $\operatorname{Im}\phi = \{id\}$). As orders of conjugate elements are equal, all conjugates of g are also in H.

Example: An index-2 subgroup includes all elements of odd order.

(3) If m is the only number in $2, ..., m$ that divides n (hence m is prime), then $i = 1$ or m. Therefore $g^m \in H$. In particular, if m is the least prime factor of $|G|$ for G a finite group, then all mth powers are in H (also see **(4)**)

(4) If furthermore $H \trianglelefteq G$, then i is the order of gH in the quotient group. Hence $i \mid m$. This implies $i \mid \gcd(m, n)$. So

Proposition 1.2. *$H \trianglelefteq G$, $[G : H] = m$, then any mth power is in H. Hence, elements of order coprime to m is in H as they are naturally mth powers. Or, by $i \mid \gcd(m, n) = 1$.*