On Subgroups of Prime Index

T. Y. Lam

A fixture in a beginning course in abstract algebra or group theory is the fact that any index 2 subgroup H of a group G is normal. As a generalization of this (and to show that the prime 2 is not really special in this situation), some instructors would mention the following delightful fact.

Theorem 1. *If H is a subgroup in a finite group G such that the index $[G:H]$ is the smallest prime dividing $|G|$, then H is normal in G.*

The proof of this is usually based on the fact that the transitive multiplication action of G on the left coset space of H has a kernel K given by the largest normal subgroup of G contained in H. This consideration leads to the divisibility of $[G:H]\,!$ by the index $[G:K] = [G:H]\,[H:K]$. The assumption on $[G:H]$ then implies that $[H:K] = 1$, so $H = K$ is normal in G. (See, for instance, [1, p. 123], [2, p. 44].) This proof, although short, is not suitable for beginning students since they are far from having the theory of group actions at their disposal. In teaching a beginning abstract algebra course, I found a proof for Theorem 1 that is both quick and possible for students at the level of such a course to understand. Moreover, the idea of this proof led to several criteria for the normality of subgroups of prime index (in *any* group G). Since such criteria do not seem to be available in standard textbooks or even in the general literature in group theory, I record them here. The argument is, in part, based on the usual proof that a subgroup of a cyclic group is cyclic, which the students would have just seen in the course.

Theorem 2. *For a subgroup H of prime index p in any group G, the following statements are equivalent:*
(1) *H is normal in G.*
(2) *For any $a \in G - H$, $a^p \in H$.*
(3) *For any $a \in G - H$, $a^n \in H$ for some positive integer $n = n(a)$ with no prime divisor less than p.*
(4) *For any $a \in G - H$, $a^2, \ldots, a^{p-1} \notin H$.*

If G and H are as in Theorem 1, then in view of Lagrange's theorem, the condition (3) in Theorem 2 holds by choosing $n(a) = |G|$ for each a in $G - H$. Therefore, Theorem 2 gives the normality of H. However, in Theorem 2, p need not be the smallest prime divisor of $|G|$ in case $|G|$ is finite. In fact, p can be *any* prime that is the index of some subgroup H of a group G. For instance, if G is the alternating group A_4 and H is its subgroup $\{e,\,(12)(34),\,(13)(24),\,(14)(23)\}$ of index $p = 3$, then (3) of Theorem 2 holds by choosing $n(a) = 3$ for each a in $G - H$ (since all such a are 3-cycles). Thus, we can infer the normality of H from Theorem 2. On the other hand, if G is the symmetric group S_4 and H is a copy of the dihedral group of eight elements embedded in G (with again $p = [G : H] = 3$), then (2) and (4) in the theorem clearly fail (by considering a transposition a in $G - H$), so we can infer that H is not normal in G.

Proof of Theorem 2. We show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1).

(1) $\Rightarrow$ (2). Under assumption (1), the factor group G/H makes sense and $|G/H| = p$, so (2) holds (for instance by Lagrange's theorem).

(2) $\Rightarrow$ (3). This is clear by choosing $n(a) = p$ for all a in $G - H$ (noting that p is prime).

(3) $\Rightarrow$ (4). Consider any $a \in G - H$, and let $n = n(a)$ be as in (3). Let s be the smallest positive integer such that a^s belongs to H. We can write $n = qs + r$, where q and r are integers with $0 \leq r < s$. By assumption, H contains $a^n = (a^s)^q \cdot a^r$, so $a^r \in H$. This implies that $r = 0$, so $n = qs$. Since (clearly) $s > 1$, the assumption on $n = n(a)$ in (3) implies that $s \geq p$, which proves (4).

(4) $\Rightarrow$ (1). Assume that (4) holds but that H is not normal in G. Then there exist b in G and h in H such that the conjugate $a := bhb^{-1}$ is not in H. Since $xH = yH$ if and only if $x^{-1}y \in H$, (4) implies that

$$(*) \qquad H, aH, \ldots, a^{p-1}H \text{ are the } p \text{ distinct left cosets of } H \text{ in } G.$$

From $bh = ab$, we have $bH = abH$. Clearly, b cannot be in H. Thus, by $(*)$, $bH = a^iH$ for some i such that $1 \leq i \leq p - 1$. But then $a^iH = bH = abH$, and cancellation of a gives $a^{i-1}H = bH = a^iH$, in contradiction to $(*)$. □

Remarks.

(A) It is worth pointing out that, in the proof of Theorem 2, the assumption that p is a prime is used *only* in the "clear" implication (2) $\Rightarrow$ (3). Thus, the proofs for the other three implications remain valid for *any* (finite) index $p = [G : H]$. This means that, in the case of subgroups of finite index p, (2) is still a *necessary* condition, and (3) and (4) are still *sufficient* conditions, for the normality of H in G. In the case where p is not a prime, however, neither (3) nor (4) is a necessary condition for the normality of H. This can be seen by taking G to be a cyclic group of prime-square order, and H to be $\{e\}$. Similarly, (2) is no longer a sufficient condition for the normality of H. For this, we can take G to be one of the (two) nonabelian groups of order ℓ^3 (for any odd prime ℓ), and H to be the subgroup generated by a noncentral element of order ℓ.

(B) Returning to the prime index case, Tom Dorsey has pointed out to the author that the conditions (2), (3), and (4) in Theorem 2 would have all held *automatically* if one were to replace the words "for all" there by "for some." The proof of this interesting observation is left as an exercise to the reader.

For a typical application of Theorem 2 to possibly infinite groups, we record the following (well-known) result.

Corollary. *If p is a prime and the order of each element of a group G is a power of p, then any subgroup H of index p in G is normal.*

Proof. For any a in $G - H$, we can take $n(a)$ to be the order of a, so (3) holds in Theorem 2. $\square$

ACKNOWLEDGMENT. Hearty thanks are due to the referee whose perceptive comments on the first version of this note prompted me to give a sharper formulation of the results, remarks, and examples in the present version. The referee also pointed out that the Corollary can be deduced from a slight modification of the traditional group action theoretic argument we sketched after the statement of Theorem 1.

References

[1] D. S. Dummit and R. M. Foote: *Abstract Algebra,* 2nd ed., Prentice Hall, Upper Saddle River, NJ, 1999.

[2] I. M. Isaacs: *Algebra,* Brooks-Cole, Pacific Grove, CA, 1994.

University of California
Berkeley, California 94720

Author's Email Address:
lam@math.berkeley.edu