ARE SUBGROUPS OF PRIME INDEX NORMAL?

LEO GOLDMAKHER

1. INTRODUCTION

A classical result in group theory is that any subgroup of index 2 must be normal. But what about subgroups of a more general index? Such questions play a role in applications, e.g. to solvability of groups of prime-power order.

Even the case of general prime index isn’t as straightforward as one might guess. For example, one might be tempted to conjecture that if \( H \leq G \) has prime index, then \( H \) must be a normal subgroup of \( G \). This is not the case:

**Example 1.** Let \( D_8 \) denote the dihedral group of order 8. A copy of \( D_8 \) sits inside \( S_4 \) and has index 3; however, \( D_8 \not\triangleleft S_4 \). (Exercise!)

However, if we impose additional conditions on the index, we can prove normality. Here’s a famous example of this. Let \( P^- (n) \) denote the smallest prime factor of \( n \).

**Proposition 1.1.** Suppose \( H \leq G \) and \( |G/H| = P^-(|G|) \). Then \( H \triangleleft G \).

We give two proofs of this result. In both, let \( p := P^-(|G|) \).

**Proof 1 (via group actions).** The natural action of \( G \) on \( G/H \) by left multiplication induces a homomorphism \( \varphi : G \to S_p \). I claim that \( \ker \varphi = H \). (This will conclude the proof, since \( \ker \varphi \triangleleft G \).)

First observe that \( \ker \varphi \leq H \leq G \), so it suffices to prove that \( |G/\ker \varphi| = p \). Since \( G/\ker \varphi \) embeds in \( S_p \), it has order dividing \( p! \). But also, the order of \( G/\ker \varphi \) divides \( |G| \). These two conditions force \( |G/\ker \varphi| = p \).

**Remark.** This proof seems to be folklore – if anyone knows a reference, I’d be grateful!

**Proof 2 (via induction on \( |G| \)).** In order to induct on \( |G| \), we’d like to produce a subgroup \( K \leq H \) with \( |H/K| = p \). But how do we find such a \( K \)? The key observation in this proof is that one can take \( K \) to be the intersection of any two subgroups which satisfy the hypotheses of Proposition 1.1.

First note that if \( H \) happens to be the only subgroup of index \( p \) in \( G \), then the proof is already over (since in this case \( H \) is fixed under conjugation, hence must be normal). Thus we may assume \( G \) has two subgroups \( H \) and \( H' \), both of index \( p \) in \( G \). Let

\[
K := H \cap H',
\]

and observe that

\[
|HH'| = \frac{|H||H'|}{|K|}.
\]

(This is most easily seen by applying the first isomorphism theorem to the map \( H \times H' \to G \) defined by \( (x, y) \mapsto xy \).) I claim that \( K \) is our desired subgroup of index \( p \) in \( H \), and that \( HH' = G \). Indeed, \( (*) \) gives

\[
1 < |H/K| \leq |G/H'| = p,
\]

while Lagrange’s theorem implies \( |H/K| \mid |G| \). Since \( p \) is the smallest nontrivial divisor of \( |G| \), we immediately deduce that

\[
|H/K| = p = |H'/K|.
\]

Date: May 24, 2018.

1The author.
Combining this with (\ast) shows that
\[ HH' = G. \]
By induction we know that \( K \triangleleft H \) and \( K \triangleleft H' \), whence \( K \triangleleft HH' = G \). Moreover, \( |G/K| = p^2 \), whence the group \( G/K \) must be abelian. (Exercise!) Thus every subgroup of \( G/K \) is normal; in particular, \( H/K \triangleleft G/K \).
The fourth isomorphism theorem now implies that \( H \triangleleft G \).
\[ \square \]

Remark. I learned this proof thanks to a post by Tobias Kildetoft on math stackexchange.

2. Lam’s theorem

In view of Example 1 and Proposition 1.1, it’s natural to wonder about sufficient conditions on \( |G/H| \) to guarantee that \( H \triangleleft G \). In 2004, T. Y. Lam (On Subgroups of Prime Index, Amer. Math. Monthly) discovered a lovely elementary proof of Proposition 1.1 which has the added benefit of producing a more general result.

**Proposition 2.1.** Given \( H \leq G \), set \( n := |G/H| \). Consider the following statements:

1. If \( g \notin H \), then \( g^k \in H \) for some \( k \in \mathbb{N} \) satisfying \( P^-(k) \geq n \).
2. If \( g \notin H \), then \( g^2, g^3, \ldots, g^{n-1} \notin H \).
3. If \( g \notin H \), then \( g^n \in H \).

Then \( (1) \implies (2) \implies H \triangleleft G \implies (3) \).

**Exercise 1.** Note that if \( n \) is prime, then \( (3) \implies (1) \) and the above proposition becomes the equivalence of all three assertions with the normality of \( H \) in \( G \). We explore this special case of the proposition in this exercise.

(a) Prove that Proposition 2.1 implies Proposition 1.1. (Your proof should be very short.)

(b) Use Proposition 2.1 to give a very short proof that (the embedding of) \( D_8 \) isn’t normal in \( S_4 \).

(c) Use Proposition 2.1 to give a very short proof that (the embedding of) \( \mathbb{Z}_2 \times \mathbb{Z}_2 \) is normal in \( A_4 \).

**Proof of Proposition 2.1.** We only prove that \( (2) \implies H \triangleleft G \), leaving the other implications as exercises. Assume (2) holds. It suffices to show that \( xHx^{-1} \subseteq H \) for all \( x \in G \). This is automatically true for \( x \in H \), so we henceforth assume \( x \notin H \).

Pick any \( g \in (xHx^{-1}) \setminus H \). Thus (2) implies \( H, gH, \ldots, g^{n-1}H \) are pairwise disjoint. Moreover, since \( |G/H| = n \), this is a complete list of cosets, i.e.
\[ G/H = \bigsqcup_{0 \leq \ell \leq n-1} g^\ell H. \]
It follows that \( xH = g^i H \) for some \( i \leq n - 1 \). Since \( x \notin H \) by hypothesis, \( i \neq 0 \). But now observe that \( gxH = xH = g^iH \), whence
\[ g^iH = xH = g^{i-1}H. \]
This is impossible, which means that we couldn’t have picked \( g \) the way we wanted to, i.e. that \( xHx^{-1} \subseteq H \). Since \( x \) is arbitrary, we conclude that \( H \triangleleft G \).
\[ \square \]

**Exercise 2.** When \( n \) is composite, the assertions of Proposition 2.1 aren’t equivalent. We explore this here.

(a) Construct \( H \triangleleft G \) such that both assertions (1) and (2) fail to hold.

(b) Construct \( H \ntriangleleft G \) for which assertion (3) holds.