Rose-Hulman Undergraduate Mathematics Journal

Volume 17
Issue 1

Article 13

On the existence of normal subgroups of prime index

Brooklynn Szymoniak
Saginaw Valley State University

Rose-
Hulman
Undergraduate
Mathematics
Journal

On the existence of normal subgroups of prime index

Brooklynn Szymoniak [a]

Volume 17, No. 1, Spring 2016

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]Saginaw Valley State University

Rose-Hulman Undergraduate Mathematics Journal
Volume 17, No. 1, Spring 2016

On the existence of normal subgroups of prime index

Brooklynn Szymoniak

Abstract. In this article, we characterize finite groups having normal subgroups of a given prime index. Precisely, we prove that if p is a prime divisor of a finite group G, then G has no normal subgroup of index p if and only if $G = G'G^p$, where G^p is the subgroup of G generated by all elements of the form g^p for any $g \in G$ and G' is the derived subgroup of G. We also extend a characterization of finite groups with no subgroups of index 2 by J.B. Nganou to infinite groups. We display an example to show that for a prime index $p \neq 2$ the characterization does not hold.

Acknowledgements: The author is grateful to Dr. Olivier Heubo-Kwegna for initiating and supervising this project. It is due to his vision and guidance that these results were discovered.

1 Introduction

It is classical in any beginning abstract algebra class to prove that the alternating group, A_4, has no subgroups of order six, that is, no subgroups of index 2, in order to assert that the converse to Lagrange's Theorem is false. A good reference for various proofs of that fact can be found in an article by Brennan and Machale [2]. Subgroups of prime index p, where p is the smallest prime divisor of the order of the group, are interesting because they are normal. A characterization of groups having no subgroups of index p, where p is the smallest prime divisor of the order of the group, is provided in the Master's thesis of Pineda [9] in terms of the group G^p. Note that this characterization was a generalization of the same result by J.B. Nganou [8] for the case where $p = 2$. Note also that the author of the later paper obtained this characterization as a consequence of being able to compute the number of subgroups of index 2 in a finite group. Another computation of the number of subgroups of index 2 in a finite group was completed by Crawford and Wallace [3] in 1975 using Goursat's Theorem for Groups. However, the computation by Nganou [8] stands out as it uses only elementary combinatorics and linear algebra. The elementary facts from Nganou and Pineda [8, 9] suggest the problem of the characterization, in an elementary way, of the existence of normal subgroups of prime index in finite groups. Note that this characterization does not assume the prime index being the smallest prime divisor of the order of the group.

In Section 2, we establish some preliminary propositions that are necessary for later proofs. In Section 3, we give another elementary direct proof, similar to the proof by Nganou [8], of the fact that a finite group has no subgroup of index 2 if and only if the group is generated by squares (or 2-generated). We go further by extending the same result to infinite groups, that is, a group (finite or infinite) has no subgroup of index 2 if and only if the group is generated by squares. In Section 4, we display an example to show that if the finiteness condition on the group is dropped, then for a prime $p \neq 2$ it is possible to have a p-generated infinite group having a subgroup of index p. We conclude in Section 5 by providing a characterization of groups having normal subgroups of prime index p without the assumption that p is the smallest prime divisor of G.

2 Preliminaries

We now provide a series of propositions that will be used in later sections of the paper and the proofs of which many undergraduate students of abstract algebra my find quite straightforward. First recall that if S is a non-empty subset of a group G, the *subgroup of G generated* by S, denoted $\langle S \rangle$, is the smallest subgroup of G containing S. It is easily shown that

$$\langle S \rangle = \{s_1 s_2 \cdots s_n | s_i \in S, n \geq 1\}.$$

Proposition 2.1. *Let $S \subseteq G$. If S is closed under conjugation, then $\langle S \rangle$ is a normal subgroup of G.*

Proof. Let $a \in G$ and $s_1, s_2, \ldots, s_n \in S$. Then

$$a^{-1}s_1s_2\cdots s_na = (a^{-1}s_1a)(a^{-1}s_2a)\cdots(a^{-1}s_na).$$

With S closed under conjugation, meaning $a^{-1}sa \in S$ for all $a \in G$ and $s \in S$, it follows that $a^{-1}s_1s_2\cdots s_na \in \langle S\rangle$. □

Proposition 2.2. *If H and K are normal subgroups of G, then $HK = \{hk | h \in H, k \in K\}$ is a normal subgroup of G.*

Proof. Since H and K are normal, we know that $ghg^{-1} \in H$ and $gkg^{-1} \in K$ for any $h \in H, k \in K$, and $g \in G$. Take any h in H and k in K. Then $g(hk)g^{-1} = gh(g^{-1}g)kg^{-1} = (ghg^{-1})(gkg^{-1})$. Since H and K are normal, it follows that $ghg^{-1} = h_1, gkg^{-1} = k_1$ where $h_1 \in H$ and $k_1 \in K$. Finally, $g(hk)g^{-1} = h_1k_1$ implies that the conjugate of any hk is in fact an element of HK, thus allowing us to conclude that HK is indeed normal. □

Proposition 2.3. *Let G be a group with identity element e and suppose $a^2 = e$ for all $a \in G$. Then G is an abelian group.*

Proof. Suppose that for every $a \in G$, $a^2 = e$. Let $a_1, a_2 \in G$. Then $(a_1a_2)^2 = (a_1a_2)(a_1a_2) = e$, by our hypothesis. Multiplying both sides of the equation $e = (a_1a_2)(a_1a_2)$ by a_2a_1 gives $(a_2a_1)e = (a_2a_1)(a_1a_2)(a_1a_2)$. So

$$\begin{aligned} a_2a_1 &= a_2(a_1a_1)a_2a_1a_2 \\ &= a_2(a_1)^2a_2a_1a_2 \\ &= (a_2)^2(a_1a_2) \\ &= a_1a_2. \end{aligned}$$

Hence, G is indeed abelian. □

3 Groups having no subgroups of index 2

As mentioned above, Nganou [8] as well as Crawford and Wallace [2] have previously characterized finite groups having no subgroups of index 2 using methods beyond the scope of most undergraduate courses. In this section, we prove their results using elementary methods which are accessible to most students of a beginning abstract algebra course. Furthermore, we extend this characterization to infinite groups. We start with a lemma that is motivated from a proof by Brennan and Machale [2].

Lemma 3.1. *Let H be a subgroup of G of index 2. Then $a^2 \in H$ for all $a \in G$.*

Proof. Let $a \in G \setminus H$. Since H has index 2, we can say $G = \{H, aH\}$. Consider a^2H. If $a^2H = aH$, then we have $aH = H$ by cancellation, which contradicts $a \notin H$. Hence, we conclude that $a^2H = H$ and so $a^2 \in H$. Since H is a subgroup, $h^2 \in H$ for any $h \in H$, which exhausts all the elements in G. Therefore, $g^2 \in H$ for any $g \in G$. □

Remark 3.2. An alternative way to prove Lemma 3.1 is to realize that, since the index of H is 2, H is a normal subgroup of G. The factor group G/H is a cyclic group of order 2 and thus $(aH)^2 = H$ for all $a \in G$ and so $a^2 \in H$ for all $a \in G$.

Given a group G, we denote by G^2 the subgroup of G generated by squares of elements in G, that is $G^2 = \langle\{a^2 | a \in G\}\rangle$. As in the article by Nganou [8], we say that G is *generated by squares* if $G = G^2$. Recall that if G_1 and G_2 are groups, the set denoted $G_1 \times G_2 = \{(g_1, g_2) | g_1 \in G_1, g_2 \in G_2\}$ under the operation $(g_1, g_2) \cdot (h_1, h_2) = (g_1h_1, g_2h_2)$ is a group, called the *direct product* of G_1 and G_2. The next proposition gives some properties of G^2.

Proposition 3.3. *Let G be a group.*

(i) The subgroup G^2 generated by squares is a normal subgroup of G.

(ii) The factor group G/G^2 is abelian.

(iii) If G_1 and G_2 are groups, then $G_1^2 \times G_2^2 = (G_1 \times G_2)^2$.

Proof. For (i), from Proposition 2.1, it is enough to see that the set of squares in G is closed under conjugation. This is clear because, for every $x, a \in G$, $a^{-1}x^2a = (a^{-1}xa)^2$.

For (ii), take any $x \in G/G^2$. Then there is an $a \in G$ such that $x = aG^2 = \{ag | g \in G^2, a \in G\}$. So $x^2 = (aG^2)^2 = (aG^2)(aG^2) = (a^2)G^2$. But $a^2 \in G^2$ implies $(a^2)G^2 = G^2$, which is the identity element in G/G^2. By Proposition 2.3, we conclude that G/G^2 is indeed abelian since all squared elements in G/G^2 equal the identity.

For (iii), we will first recall what elements the sets $G_1^2 \times G_2^2$ and $(G_1 \times G_2)^2$ consist of:

$$G_1^2 \times G_2^2 = \{(g_1, g_2) | g_1 \in G_1^2, g_2 \in G_2^2\}$$
$$(G_1 \times G_2)^2 = \langle\{(g_1, g_2)^2 | g_1 \in G_1, g_2 \in G_2\}\rangle.$$

We will begin by first proving that $(G_1 \times G_2)^2 \subseteq G_1^2 \times G_2^2$. If (x_1, x_2) is in the generating set of $(G_1 \times G_2)^2$, then we know $(x_1, x_2) = (g_1, g_2)^2 = (g_1^2, g_2^2) \in G_1^2 \times G_2^2$. Hence, $\{(g_1, g_2)^2 | g_1 \in G_1, g_2 \in G_2\}$ must be in $G_1^2 \times G_2^2$. Therefore, $(G_1 \times G_2)^2 \subseteq G_1^2 \times G_2^2$ since $(G_1 \times G_2)^2$ is the smallest subgroup containing $\{(g_1, g_2)^2 | g_1 \in G_1, g_2 \in G_2\}$.

Conversely, take any $(y_1, y_2) \in G_1^2 \times G_2^2$. Then $y_1 \in G_1^2$ and $y_2 \in G_2^2$. Hence $y_1 = j_1^2 j_2^2 \cdots j_m^2$ for some $j_1, j_2, \ldots, j_m \in G_1$ and $y_2 = k_1^2 k_2^2 \cdots k_n^2$ for some $k_1, k_2, \ldots, k_n \in G_2$. We

have

$$\begin{aligned}(y_1, y_2) &= (j_1^2 j_2^2 \cdots j_m^2, k_1^2 k_2^2 \cdots k_n^2) \\ &= (j_1^2, e)(j_2^2, e) \cdots (j_m^2, e)(e, k_1^2)(e, k_2^2) \cdots (e, k_n^2) \\ &= (j_1, e)^2 (j_2, e)^2 \cdots (j_m, e)^2 (e, k_1)^2 (e, k_2)^2 \cdots (e, k_n)^2.\end{aligned}$$

This is simply the product of elements in the set $\{(g_1, g_2)^2 | g_1 \in G_1, g_2 \in G_2\}$. Hence, this product must be in $\langle\{(g_1, g_2)^2 | g_1 \in G_1, g_2 \in G_2\}\rangle$. Therefore, $(y_1, y_2) \in (G_1 \times G_2)^2$, which implies that $G_1^2 \times G_2^2 \subseteq (G_1 \times G_2)^2$. So the two sets are indeed equal. □

In order to prove the main theorem of this section we rely on the fundamental theorem for finite abelian groups.

Theorem 3.4. *(Fundamental Theorem for Finite Abelian Group) Any finite abelian group is isomorphic to a direct sum of cyclic groups of prime power orders.*

Nganou used the number of subgroups of index 2 ([8, Theorem 2]) to show Theorem 3.5 below. Here, we instead use all the above ingredients to provide a direct proof of the theorem. The idea of this direct proof will enable us later to prove the same result for infinite groups.

Theorem 3.5. *Let G be a finite group. A group G has no subgroups of index 2 if and only if G is generated by squares.*

Proof. Let G be a finite group not generated by squares. We show that G has a subgroup of index 2. We know the factor group G/G^2 is not trivial, hence, $|G/G^2| > 1$. Recall from Proposition 3.3 (ii), that G/G^2 is abelian. By Theorem 3.4, we can say G/G^2 is isomorphic to $Z_{p_1^{a_1}} \times Z_{p_2^{a_2}} \times \cdots \times Z_{p_n^{a_n}}$.

Recall that $x^2 = e$ for any $x \in G/G^2$ (so we say that any element in G/G^2 has order 2). Therefore any element in $Z_{p_1^{a_1}} \times Z_{p_2^{a_2}} \times \cdots \times Z_{p_n^{a_n}}$ must also be of order 2. This can only happen if each $p_i = 2$ and each $a_i = 1$ (for $i = 1, 2, \ldots, n$). Hence G/G^2 is isomorphic to the product of n copies of Z_2.

Let K be a subgroup of G such that K is isomorphic to $Z_2 \times Z_2 \times \cdots \times Z_2 \leq G/G^2$ where $|K| = 2^{n-1}$ (that is, there are $n-1$ copies of Z_2 that appear in the direct product). Then there exists some subgroup H of G where $K = H/G^2$ and $G^2 \subseteq H$ (see, for example, the text by Dummit and Foote [4]). Then $\frac{|H|}{|G^2|} = |K| = \frac{|G/G^2|}{2} = \frac{|G|}{2|G^2|}$. This is equivalent to $|H| = \frac{|G|}{2}$, which then implies that the subgroup H of G has index 2.

Now that we have established the fact that a finite group G that is not generated by squares has a subgroup of index 2, we can conclude that the contrapositive is also true. That is, if a finite group G contains no subgroup of index 2, then G must be generated by squares.

Let us now assume that a finite group G is generated by squares, that is, $G = G^2 = \langle\{x^2 | x \in G\}\rangle$. Suppose there exists a subgroup $H \leq G$ that has index 2. Then $|H| = \frac{|G|}{2}$

and so $|H| < |G|$. From Lemma 3.1, we know that $g^2 \in H$ for any $g \in G$, which implies that the generating set of G^2 is a subset of H and so $G^2 \subseteq H$. But $G = G^2$ implies $G \subseteq H$, which contradicts $|H| < |G|$. Therefore, we conclude that G does not contain any subgroups of index 2. □

We now prove Theorem 3.5 in a more general setting by dropping the finiteness condition on the group. The proof is closely related to the finite case and uses the well-known fact due to Prüfer and Baer that an (infinite) abelian group of exponent n (meaning $na = 0$ for all $a \in G$) is a direct sum of cyclic groups. Prüfer proved the theorem for countable abelian groups in 1923 [10] and Baer later in 1934 proved the same result for an arbitrary abelian group (of finite exponent) [1].

Theorem 3.6. *A group G has no subgroups of index 2 if and only if G is generated by squares.*

Proof. If G has a subgroup H of index 2, then H is normal and as in the finite case, we deduce that G is not generated by squares. If G is not generated by squares, then G/G^2 is a non trivial abelian group of exponent 2 and by the above observation G/G^2 is a direct sum of cyclic groups. Note that cyclic groups are of the form Z_m and in our case since all elements a in the cyclic group satisfy $2a = 0$ it follows that those cyclic groups are Z_2. So $G/G^2 \cong \prod_I Z_2$ and clearly has a subgroup H/G^2 of index 2, where H is a subgroup of G containing G^2. Hence $(G : H) = (G/G^2 : H/G^2) = 2$ and G has a subgroup of index 2. □

4 Groups having no subgroups of prime index

In this section, we generalize Theorem 3.5 by showing that 2 can be replaced by the smallest prime dividing the order of the group. We start with some terminology. We also display an example to show that if the finiteness condition on the group is dropped, then for a prime $p \neq 2$ it is possible to have a p-generated infinite group having a subgroup of index p. We denote $G^p = \langle \{a^p | a \in G\} \rangle$ as the subgroup of G generated by all the elements of the form a^p, $a \in G$. Note that for p a prime, G^p has some similarities with G^2. Specifically, G^p is a normal subgroup of G and $(\prod_i G_i)^p = \prod_i G_i^p$. However, G/G^p is not necessarily abelian (see Pineda [9] for an example). We say that a group G is *p-generated* if $G = G^p$. The following lemma is a generalization of Lemma 3.1.

Lemma 4.1. *Let G be a finite group and H a subgroup of G of index p, where p is the smallest prime divisor of the order of G. Then $a^p \in H$ for all $a \in H$.*

Proof. Since p is the smallest prime divisor of the order of G, any subgroup of G of prime index is normal in G (see, for example, the article by Lam [7]). So G/H is a group of prime order p and is therefore cyclic. For any $a \in G$, we can say $(aH)^p = H$ and thus $a^p \in H$ for all $a \in G$. □

For the case $p = 2$, we use the fact that G/G^2 is abelian. Given G/G^p is not necessarily abelian when $p \geq 3$, instead of the Fundamental Theorem for abelian groups, we instead use Cauchy's Theorem.

Theorem 4.2. *(Cauchy's Theorem) Let p be a prime divisor of the order of a finite group G. Then there exists $x \in G$ of order p.*

Recall that a group G is a p-group if the order of G is a power of p. It is a common exercise in graduate textbooks to show that p-groups satisfy the converse to Lagrange's Theorem, that is, for any divisor m of the order of G, there is a subgroup of G of order m (see, for example, Exercise 29 in Section 4.3 of Dummit and Foote [4]). We provide a proof here using induction.

Proposition 4.3. *Let G be a finite group such that $a^p = e$ for all $a \in G$. Then G is a p-group and consequently G has a subgroup of order p^k for each positive integer k with $p^k/|G|$.*

Proof. Let q be another prime divisor of the order of G. Then by Cauchy's Theorem, there exists $a \in G$ of order q. By assumption $a^p = e$, so q divides p and it follows that $p = q$ as both p and q are prime. Hence the order of G is a power of p.

Thus $|G| = p^n$ for some positive integer n. First consider the subset $Z(G) = \{g \in G : gx = xg, \forall x \in G\}$ of G. Recall that $Z(G)$ is called the center of G and we leave it up to the reader to verify that $Z(G)$ is a normal subgroup of G. If $Z(G) = G$, then this simply means G is abelian and has a subgroup of order p^j for each positive integer j with $0 \leq j \leq n$ (all finite abelian groups satisfy the converse of Lagrange's Theorem).

If $Z(G) \neq G$, then Dummit and Foote [4, Theorem 8] assure us that $Z(G)$ is not trivial. By induction, let us assume that any group of order p^α with $\alpha < n$ has a subgroup of order p^β where $\beta \leq \alpha$. Hence, our goal is to prove that G satisfies the converse of Lagrange's Theorem. Since the order of $Z(G)$ must divide p^n, then $|Z(G)| = p^{\alpha_1}$ for an integer α_1 with $1 \leq \alpha_1 < n$. The factor group $G/Z(G)$ must have order of p^{α_2} with $\alpha_2 = n - \alpha_1$. Using our induction hypothesis on $Z(G)$ and on $G/Z(G)$ (as both are p-groups with orders p^{α_1} and p^{α_2} respectively with $\alpha_1 < n$ and $\alpha_2 < n$), there exists a subgroup H of $Z(G)$ of order p^{β_1} with $0 \leq \beta_1 \leq \alpha_1$ and also there exists a subgroup K of G with $Z(G) \leq K$ where $|K/Z(G)| = p^{\beta_2}$ and $0 \leq \beta_2 \leq \alpha_2$. So $|K| = p^{\alpha_1+\beta_2}$, and $\alpha_1 \leq \alpha_1 + \beta_2 \leq \alpha_1 + \alpha_2 = n$. This leads us to conclude that, there exists a subgroup of G of any order p^α with $0 \leq \alpha \leq n$. Hence G satisfies the converse of Lagrange's Theorem. □

The next result is in Pineda's article [9, Proposition 20], but we reprove it here for easy reading and to justify the remark that follows.

Theorem 4.4. *Let p be the smallest prime divisor of the order a finite group G. Then G has no subgroups of index p if and only if G is p-generated.*

Proof. Assume that $G^p \neq G$. We will show that, as a result of our previous proposition, that G must have a subgroup of index p. First recall that G^p is normal, so G/G^p is a factor group

with order $\frac{|G|}{|G^p|}$. Notice that any $x \in G/G^p$ has the property $x^p = e$. By Proposition 4.3, G/G^p is a p-group and so $|G/G^p| = p^n$ for some integer n. Again by Proposition 4.3, there exists a subgroup $K \leq G$ with $G^p \subseteq K$, such that K/G^p has an order of p^{n-1}. Consequently, we have $(G : K) = \frac{|G|}{|K|} = \frac{|G/G^p|}{|K/G^p|} = \frac{p^n}{p^{n-1}} = p$.

We will assume that G is p-generated. Contrary to what we are to prove, suppose there exists a subgroup $H \leq G$ with index p. Then $|H| = \frac{|G|}{p}$ and so $|H| < |G|$. As shown previously, we know that this assumption leads us to the fact that $a^p \in H$ for any $a \in G$. Take any element g in $G = G^p$ and notice that $g^p \in H$ and so $G^p \subseteq H$. This contradicts $|H| < |G|$. Therefore, the assumption that $(G : H) = p$ is false and so we have reached our desired conclusion that G has no subgroup of index p. □

Remark 4.5. (i) Note that for the sufficiency of Theorem 4.4, we do need p to be the smallest prime divisor of the order of the group. In fact note that the dihedral group $D_3 = \{e, r, r^2, s, rs, r^2s | r^3 = s^2 = e, srs = r^2\}$ is 3-generated, since $e^3 = e$, $s^3 = s$, $(rs)^3 = rs$, and $(r^2s)^3 = r^2s$; and the subgroup generated by these four elements e, s, rs, and r^2s must be the whole group D_3 by Lagrange's Theorem. However, D_3 possesses a subgroup of index 3, namely the subgroup generated by s.

(ii) As for the necessity of Theorem 4.4, we do not use in the proof the fact that p is the smallest prime divisor of the order of the group. One application of this is the fact that, for instance, the alternating group A_6 is 3-generated and is also 5-generated. In fact it is well known that if G is a simple group and if m is the index of a subgroup H of G, then m divides the order of G (Lagrange's Theorem) and the order of G divides $m!$ (as G is simple, G can be embedded in the symmetry group S_m on the m cosets of the subgroup H). Since A_n is simple for all $n \geq 5$, A_n has a subgroup of prime index p if $\frac{n!}{2}$ divides $p!$, which can happen only if $n = p$. For $n \geq 6$, and n not a prime, A_n has no subgroup of prime index. For instance A_6 has no subgroup of index 2, 3, 5. Therefore A_6 is 3-generated, 5-generated.

(iii) For $p = 2$, we were able to drop the finiteness condition in Theorem 3.6. However in Theorem 4.4, if we drop G being finite, then the smallest prime is automatically dropped in the theorem as the order of G is infinite and the theorem would be false. In fact, it is enough to pick an arbitrary direct sum of D_3 defined in (i) of this remark. Since $(\prod_i D_3)^3 = \prod_i D_3^3$ and D_3 is 3-generated, it follows that $\prod_i D_3$ is 3-generated. If we choose the subgroup of $\prod_i D_3$ consisting of replacing only one copy of D_3 by the subgroup generated by s, we obtain a subgroup of $\prod_i D_3$ of index 3.

5 Existence of normal subgroups of prime index

In this section we turn our attention on the existence of normal subgroups of prime index for a finite group. Note that in Remark 4.5 (ii), we state that A_n, $n \geq 5$, is a simple group and therefore has no normal subgroups. In particular, A_n has no normal subgroups of prime

index p. For instance A_5 has no normal subgroup of index 2, 3 or 5. We want to produce a class of groups that will always possess a normal subgroup of prime index for any prime divisor of the order of the group (in other words, any prime allowed by Lagrange's Theorem). We start with the following recollection on commutators of a group which can be found in the textbook by Dummit and Foote [4, page 171]. Recall that if G is a group, and $x, y \in G$, then the *commutator* of x and y is $[x, y] = xyx^{-1}y^{-1}$. Note that $[x, y] = e$ if and only if $xy = yx$ (since $x^{-1}y^{-1} = (yx)^{-1}$). We launch here a series of propositions to be used later.

Proposition 5.1. *Let H be a normal subgroup of G. Then G/H is abelian if and only if $[x, y] \in H$ for all $x, y \in G$.*

Proof. First assume that G/H is abelian and take any x, y in G. Then the product of the factor groups xH and yH can be written as $(xy)H = (xH)(yH) = (yH)(xH) = (yx)H$. The factor group containing $[x, y]$ can be written as

$$\begin{aligned}(xyx^{-1}y^{-1})H &= ((xy)(yx)^{-1})H \\ &= (xy)H(yx)^{-1}H \\ &= (yx)H(yx)^{-1}H \\ &= ((yx)(yx)^{-1})H \\ &= H.\end{aligned}$$

Therefore, we conclude that $xyx^{-1}y^{-1} = [x, y]$ must be in H.

Assume that $[x, y] \in H$ for any $x, y \in G$. Since H is normal, then G/H is defined and $[y^{-1}, x^{-1}]H = H$. Recall this is the identity element, so $(xy)H = (xy)H[y^{-1}, x^{-1}]H = ((xy)[y^{-1}, x^{-1}])H = ((xy)(y^{-1}x^{-1})(yx))H = (yx)H$. Hence, $(xH)(yH) = (xy)H = (yx)H = (yH)(xH)$. Therefore, G/H is abelian. □

Let H and K be subgroups of G. We write $[H, K]$ for the subgroup of G generated by the commutators $\{[h, k] | h \in H, k \in K\}$. We write G' for $[G, G]$, and G' is called the *derived subgroup* of G. The following proposition can be found as Theorem 5.12 in the textbook by Fraleigh [5].

Proposition 5.2. *Let G be a group.*

(i) The derived subgroup G' is normal in G.

(ii) The derived subgroup G' is the smallest normal subgroup of G such that G/G' is abelian, or more precisely, if H is a normal subgroup of G, then G/H is abelian if and only if $G' \subseteq H$.

Proof. For (i), it will suffice to show that any element $x' = [x, y] \in G'$ and $g \in G$ exhibits $g^{-1}x'g\ G'$. Since we have $x' = [x, y] = xyx^{-1}y^{-1}$, then we will insert $e = g^{-1}g$ between each

element of $xyx^{-1}y^{-1}$ to obtain $xyx^{-1}y^{-1} = x(gg^{-1})y(gg^{-1})x^{-1}(gg^{-1})y^{-1}$. From the product $g^{-1}[x,y]g$ we obtain

$$\begin{aligned} g^{-1}[x,y]g &= g^{-1}(xgg^{-1}ygg^{-1}x^{-1}gg^{-1}y^{-1})g \\ &= (g^{-1}xg)(g^{-1}yg)(g^{-1}x^{-1}g)(g^{-1}y^{-1}g) \\ &= (g^{-1}xg)(g^{-1}yg)(g^{-1}xg)^{-1}(g^{-1}yg)^{-1} \\ &= [g^{-1}xg, g^{-1}yg]. \end{aligned}$$

Therefore, $g^{-1}x'g \in G'$.

For (ii), first note that if $G' \subseteq H$, then any element $[x,y] \in G'$ is also in H. From here, we can directly apply Proposition 5.1 to justify the claim that G/H is abelian if and only if $G' \subseteq H$. □

Before we state the main theorem of this paper, let us establish the following lemma that motivates our result:

Lemma 5.3. *The factor group $G/G'G^p$ is abelian*

Proof. Note that G' and G^p are both normal in G (see Proposition 5.2 and the introduction to Section 4) and so is the subgroup $G'G^p$ by Proposition 2.2. Since $G' \subseteq G'G^p$, it follows from Proposition 5.2 (ii) that $G/G'G^p$ is abelian. □

This lemma is promising as it allows us to use the Fundamental Theorem of Finitely Generated Abelian Groups to give the structure of $G/G'G^p$. The subgroup $G'G^p$ is often called the p-Frattini subgroup of G.

Theorem 5.4. *Let p be a prime divisor of the order of a finite group G. Then G has no normal subgroups of index p if and only if $G = G'G^p$.*

Proof. Let H be a normal subgroup of G of index p. Then $a^p \in H$ for all $a \in G$ and so $G^p \subseteq H$. Note also that G/H is a group of prime order so it is cyclic and therefore abelian. Thus $G' \subseteq H$ by Proposition 5.2 (ii). Hence $G'G^p \subseteq H$ and $G \neq G'G^p$.

Conversely, suppose that $G \neq G'G^p$. Then the factor group $G/G'G^p$ is nontrivial and abelian by the above observation. Using the Fundamental Theorem of Finitely Generated Abelian Groups, we can find a subgroup H of G containing $G'G^p$ of index p. Note that since $G/G'G^p$ is abelian the subgroup $H/G'G^p$ is normal and H is a normal subgroup of G by the fourth isomorphism theorem [4, Theorem 20]. □

Remark 5.5. (i) Note that if $p = 2$, we have $G'G^2 = G^2$. In fact, since G^2 is normal in G and G/G^2 is abelian, it follows that $G' \subseteq G^2$. Since every subgroup of index 2 is automatically normal, in Theorem 5.4, if $p = 2$, we recover the statement of Theorem 3.5.

(ii) The fact that the factor group $G/G'G^p$ is abelian is crucial in the proof of Theorem 5.4. In fact, it is the reason why the subgroup H in the proof is normal. This differs from the case of Theorem 4.4 where G/G^p is just a p-group (not necessarily abelian) allowing the existence of subgroups of prime index that are not necessarily normal.

(iii) We provide an application of Theorem 5.4. Let us reconsider the dihedral group D_3 of Remark 4.5. We have $\langle s \rangle$ is a subgroup of index 3 and $D_3 = D_3^3$, so $D_3 = D_3' D_3^3$. By Theorem 5.4, D_3 has no normal subgroups of index 3. In particular, the subgroup $\langle s \rangle$ is not normal.

References

[1] R. Baer, Erweiterung von Gruppen und ihn Isomorphismen, Math. Zeitschrift 38(1934), 375-416.

[2] M. Brennan, D. Machale, Variations on a Theme: A_4 Definitely has no subgroup of Order six!, Math. Magazine 73, No.1, 36-40 (Feb. 2000).

[3] R. R. Crawford, K. D.Wallace, On the Number of Subgroups of Index Two - An Application of Goursats Theorem for Groups, Mathematics Magazine 48, No. 3, (1975), 172-174.

[4] D. S. Dummit, R. M. Foote, *Abstract Algebra*, 3rd Edition, Hoboken, NJ: John Wiley & Sons, 2004

[5] J. B. Fraleigh, *A first course in Abstract Algebra*, Seventh Edition, Addison Wesley, Pearson Education, 2003.

[6] J. A. Gallian, *Contemporary Abstract Algebra*, Fifth Edition, Houghton Mifflin Company, Boston, MA, 2002.

[7] T.Y. Lam, On subgroups of prime index, The American Mathematical Monthly, Vol. 111, No. 3 (Mar., 2004), pp. 256-258.

[8] J. B. Nganou, How rare are the subgroups of index 2?, Mathematics Magazine, Vol. 85, No. 3 (June 2012), pp. 215-220.

[9] M. L. Pineda, *Characterizing the number of subgroups of prime index*, Master Thesis in Mathematics, California State Polytechnic University, Pomona, 2014.

[10] H. Prüfer, Untersuchungen über die Zerlegbarkeit der abählbaren primren Abelschen Gruppen, Math. Zeitsch 17 (1923), 35-61.