HOW RARE ARE SUBGROUPS OF INDEX 2?

JEAN B. NGANOU

Abstract. Using elementary combinatorics and linear algebra, we compute the number of subgroups of index 2 in any finite group. This leads to necessary and sufficient conditions for groups to have no subgroups of index 2, or to have a unique subgroup of index 2. Illustrative examples and a class of counterexamples to the converse of Lagrange’s Theorem are also provided.

1. Introduction

The first and most famous counterexample to Lagrange’s Theorem is the alternating group $A_4$, which consists of the even permutations on 4 letters. The group has order 12, but it has no subgroup of order six. Equivalently, it has no subgroup of index 2. Brenan and MacHale gave a proof of this fact in this MAGAZINE [1], and then ten more proofs, for good measure. Subgroups of index 2 are of special interest because they are always normal. In fact, if $H$ has index 2 in $G$ then $H$ has only one coset other than itself. That is enough to force $H a = a H$ for every $a \in G$, which makes $H$ normal in $G$. That article motivated us to learn more about the existence of subgroups of index 2 in other groups. More precisely, we considered the questions of the essential ingredients that drive the arguments in [1] and whether they can be generalized to other groups.

In this paper we consider especially the role played by the subgroup of squares in determining whether a group has a subgroup of index 2. Using this approach we identify a larger class of groups that do not have subgroups of index 2; that is, a larger class of counterexamples to Lagrange’s Theorem.

We hope that this paper is accessible to readers with very little background. We do not use any results or concepts beyond the first part of Gallian’s textbook [3].

All groups in this article are finite.

We start by defining the subgroup of squares and verifying its main properties. Recall that if $X$ is a non-empty subset of a group $G$, the subgroup $\langle X \rangle$ of $G$ generated by $X$ is the smallest subgroup of $G$ containing $X$. It easy to verify that $\langle X \rangle$ consists

2000 Mathematics Subject Classification. Primary 06D99, 08A30.

November 27, 2011.
of the set of elements that are formed from “finite words” in the elements of $X$:

$$\langle X \rangle = \{x_1 \cdots x_n | x_i \in X; n \geq 1\}$$

In fact, it is easily seen that the set on the right is non-empty and closed under multiplication. The closure under inverses follows from $(x_1 \cdots x_n)^{-1} = x_n^{-1} \cdots x_1^{-1}$, and the fact that since $G$ is finite each $x_i^{-1}$ is equal to $x_i^{k_i}$ for some $k_i \geq 1$. Thus, by the two-step subgroup test ([3, Theorem 3.2]) the set is a subgroup of $G$.

In addition, suppose that $X$ is closed under conjugation, that is for every $x_2 X$ and $a \in G$, $axa^{-1} \in X$. Then for every $a \in G$, and $x_1, x_2, \ldots, x_n \in X$, $a(x_1x_2 \cdots x_n)a^{-1} = (ax_1a^{-1})(ax_2a^{-1}) \cdots (ax_na^{-1}) \in \langle X \rangle$. Hence $\langle X \rangle$ is normal in $G$. Therefore, if $X$ is closed under conjugation, then $\langle X \rangle$ is a normal subgroup of $G$.

A close look at some of the proofs in [1] motivates the consideration of the subgroup generated by the squares and subgroup generated by elements of odd orders.

For any group $G$, we denote by $G^2$ the subgroup of $G$ generated by squares of elements in $G$, that is $G^2 = \langle \{x^2 : x \in G\} \rangle$. We say that $G$ is generated by squares if $G = G^2$.

Note that $G^2$ is normal in $G$. In fact, from the observation above, it is enough to justify that the set of squares in $G$ is closed under conjugation. But this is clear because, for every $x, a \in G$, $axa^{-1} = (axa^{-1})^2$.

For any group $G$, we denote by $G^{\text{odd}}$ the subgroup of $G$ generated by elements of odd order in $G$. Since every element $a$ of odd order satisfies the equation $a = a^{2k}$ for some integer $k$, then $G^{\text{odd}}$ is a subgroup of $G^2$. Note that $G^{\text{odd}}$ can be a proper subgroup of $G^2$, for instance the subgroup of $\mathbb{Z}_4$ generated by elements of odd order is trivial while its subgroup of squares is $2\mathbb{Z}_4$.

Just like $G^2$, $G^{\text{odd}}$ is also normal in $G$. This follows from the observation above and the fact that orders of elements are preserved under conjugation.

2. How many subgroups of index 2?

By Lagrange’s Theorem, groups of odd order do not have subgroups of index 2, therefore only groups of even orders are relevant here. To answer our question on the existence of subgroups index 2, we consider a more general question: How many subgroups of index 2 are there in the group? The following key result shall shift the question to a question about finite vector spaces over $\mathbb{Z}_2$ where we have better tools to answer the question.

Theorem 1. The groups $G$ and $G/G^2$ have the same number of subgroups of index 2.
To see this, we start by the following observation. If $H$ is a subgroup of index 2 in $G$, then $H$ is normal in $G$ and the factor group $G/H$ has order 2. Therefore, by a consequence of the Lagrange Theorem [2, Corollary 7.4], $(xH)^2 = H$ for all $x \in G$. Hence, $x^2 \in H$ for all $x \in G$, and it follows that $G^2 \subseteq H$. Since $G^2$ is normal in $G$, then it is normal in $H$ and we can consider the factor group $\mathcal{H} := H/G^2$. This is a subgroup of $G/G^2$ and a simple calculation shows that $[G/G^2 : \mathcal{H}] = [G : H] = 2$.

We define a map $\varphi$ from the set of subgroups of $G$ of index 2 to the set of subgroups of $G/G^2$ of index 2 by $\varphi(H) = \mathcal{H}$. This is well defined and we leave it as an exercise to verify that it is a bijection by showing that its inverse is defined as follows. Given a subgroup $\mathcal{H}$ of $G/G^2$, then $\varphi^{-1}(\mathcal{H}) := \{x \in G : xH \in \mathcal{H}\}$. Since there is a bijection between the set of subgroups of index 2 in $G$ and the set of subgroups of index 2 in $G/G^2$, then these sets have the same cardinality as claimed.

Recall that the Fundamental Theorem of Finite Abelian groups states that every finite Abelian group is isomorphic to the direct product of cyclic groups of prime power order and this decomposition is unique up to reordering of the factors. Note that if $Z_n$ is a factor of such a group, then the group has elements of order $n$.

On the other hand, every group $G$ satisfying $x^2 = e$ for all $x \in G$ is Abelian. In fact, if $x^2 = e$ for all $x \in G$, then $x^{-1} = x$ for all $x \in G$. Therefore, for every $a, b \in G$, $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.

It follows from this observation that $G/G^2$ is Abelian since $(xG^2)^2 = G^2$ for all $x \in G$. Therefore, $G/G^2$ is a finite Abelian group in which every element other than the identity has order 2. Thus by the Fundamental Theorem of Finite Abelian groups, $G/G^2$ is isomorphic to a direct product of cyclic groups. But, since every non-identity in $G/G^2$ has order 2, then the only cyclic group that can show up as a factor in its direct product decomposition is $Z_2$. That means there exists an integer $n \geq 0$ such that

$$G/G^2 \cong \bigoplus_{i=1}^{n} Z_2$$

The right-hand of (I) is to be interpreted as the trivial group when $n = 0$ and this situation arises exactly when $G = G^2$.

In addition to being a group, $\bigoplus_{i=1}^{n} Z_2$ has a natural structure of a vector space over $Z_2$ with vector addition being the usual group addition and scalar multiplication defined in the natural way across components. Moreover, the subspaces and the subgroups of $\bigoplus_{i=1}^{n} Z_2$ coincide. In fact, it is clear that a subspace is a subgroup and that every subgroup is closed under addition. On the other hand, every subgroup is closed under scalar multiplication because there are only two scalars, $0, 1$. A multiplication by $0$ yields the zero vector, while a multiplication by $1$ has no effect. Finally, since a $k$-dimensional subspace has order $2^k$, we see that subgroups of index 2 (and so order $2^{n-1}$) must correspond to subspaces of dimension $n - 1$. 


For readers that are not familiar with vector spaces over fields other than \( \mathbb{R} \) or \( \mathbb{C} \), it should be noted that the axioms remain the same. For instance, if we require the same axioms of vector spaces over \( \mathbb{R} \), but use \( \mathbb{Z}_2 \) as the set of scalars, we obtain the notion of vector spaces over \( \mathbb{Z}_2 \). The definitions of concepts such as basis, dimension and subspace are the same. Moreover, every \( n \)-dimensional vector space \( V \) over \( \mathbb{Z}_2 \) is isomorphic to \( \bigoplus_{i=1}^{n} \mathbb{Z}_2 \) where the isomorphism is obtained by taking coordinates with respect to some fixed basis; from which it follows that \( V \) is finite as a set and \( |V| = 2^n \).

Recall that an \((n - 1)\)-dimensional subspace of an \( n \)-dimensional vector space \( V \) is called a hyperplane of \( V \). We now count the hyperplanes of finite dimensional vector spaces over \( \mathbb{Z}_2 \).

**Theorem 2.** Every \( n \)-dimensional vector space over \( \mathbb{Z}_2 \) has \( 2^n - 1 \) hyperplanes.

Without loss of generality, we may assume that \( V = \bigoplus_{i=1}^{n} \mathbb{Z}_2 = \mathbb{Z}_2^n \). Using simple combinatorics and elementary linear algebra, we show that there are \( 2^n - 1 \) hyperplane(s) in \( V \).

First we count the ordered linearly independent sets of \( n - 1 \) vectors in \( \mathbb{Z}_2^n \). To construct such a set, we need to carefully choose \( n - 1 \) vectors \( v_1, \ldots, v_{n-1} \).

For the choice of \( v_1 \), the only vector to avoid is the zero vector of \( \mathbb{Z}_2^n \), leaving us with \( 2^n - 1 \) ways of choosing \( v_1 \). Once \( v_1 \) is chosen, we must choose \( v_2 \notin \text{Span}\{v_1\} = \{0, v_1\} \), and there are \( 2^n - 2 \) such choices. Suppose we have chosen \( v_1 \) through \( v_k \), then we need to choose \( v_{k+1} \notin \text{Span}\{v_1, \ldots, v_k\} \). An ordered linearly independent set of \( k \) vectors spans a subspace containing \( 2^k \) vectors and these must all be avoided if one wants to extend the ordered set and preserve linear independence. It follows that there are \( 2^n - 2^k \) choices for the \((k + 1)\)st vector, thus there are \( 2^n - 2^k \) possibilities. In total, we have \((2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-2})\) linearly independent subsets of \( n - 1 \) vectors. Similarly, since each hyperplane of \( \mathbb{Z}_2^n \) contains \( 2^{n-1} \) vectors, the same argument above shows that each hyperplane of \( \mathbb{Z}_2^n \) has \((2^{n-1} - 1)(2^{n-1} - 2) \cdots (2^{n-1} - 2^{n-2})\) linearly independent subsets with \( n - 1 \) vectors. Each of these sets is the basis of a hyperplane, but different bases may give rise to the same hyperplane. In fact, the argument above shows that each hyperplane in \( \mathbb{Z}_2^n \) has \((2^n - 1)(2^{n-1} - 2) \cdots (2^{n-1} - 2^{n-2})\) distinct bases. Therefore, the number of hyperplanes in \( \mathbb{Z}_2^n \) is:

\[
\frac{(2^n - 1)(2^n - 2) \cdots (2^n - 2^{n-2})}{(2^{n-1} - 1)(2^{n-1} - 2) \cdots (2^{n-1} - 2^{n-2})}
\]

Which simplifies to \( 2^n - 1 \) as we needed.

Combining Theorem 1 and Theorem 2 we now obtain a formula for the number of subgroups of index 2 in a group \( G \).

**Corollary.** There are \( 2^n - 1 \) subgroups of index 2 in \( G \) where \( n \) is the integer in the isomorphism \((I)\).
By the isomorphism (I), subgroups of $G/G^2$ are of the same number as subgroups of $\mathbb{Z}_2^n$. From the discussion preceding 2, subgroups of $G/G^2$ correspond to subspaces of $\mathbb{Z}_2^n$ and subgroups of index 2 in $G/G^2$ correspond to subspaces of $\mathbb{Z}_2^n$ of dimension $n - 1$ (the hyperplanes). By Theorem 2, $\mathbb{Z}_2^n$ has $2^n - 1$ hyperplanes. Therefore, there are $2^n - 1$ subgroup(s) of index 2 in $G/G^2$, and by Theorem 1, we conclude that there are $2^n - 1$ subgroups of index 2 in $G$. It is worth pointing out that an alternate proof of the preceding result that uses more advanced tools can be found in [2]. In addition, readers interested in more details on counting subspaces of a fixed dimension can consult [6], [7]. The following results are easy consequences of the preceding Corollary.

**Corollary.** A group has no subgroup of index 2 if and only if it is generated by squares.

**Corollary.** A group $G$ has a unique subgroup of index 2 if and only if $G^2$ has index 2 in $G$.

Since $G^{odd} \subseteq G^2$, it follows from the above Corollaries and Lagrange’s Theorem that if more than half of the elements in $G$ have odd order, then $G$ has no subgroups of index 2 which is [1, Theorem]. It is worth pointing out that this condition on elements of odd order is not a necessary condition for a group with no subgroups of index 2. For instance, the linear group $SL(2,3)$ of $2 \times 2$ matrices in $\mathbb{Z}_3$ with determinant 1 is a group of order 24 that has no subgroups of index 2, but has only nine elements of odd order [5].

We would like to point out that the above results for index 2 can easily be generalized to index $p$ for any prime number $p$. In this case, one would use the $p$-Frattini subgroup $[G,G][G^p]$ (which coincides with $G^2$ when $p = 2$ as $[G,G] \subseteq G^2$). Here $[G,G]$ denotes the subgroup of $G$ generated by the commutators of $G$ (a commutator of $G$ is an element of the form $xyx^{-1}y^{-1}$ with $x, y \in G$). Note that since the set of commutators and the set of $p^{th}$ powers of elements in $G$ are closed under conjugation, it follows as observed earlier that $[G,G]$ and $G^p$ are normal subgroups of $G$. Recall that if $N,H$ are subgroups of a group $G$ with $N$ normal in $G$, then $NH := \{nh : n \in N, h \in H\}$ is a subgroup of $G$. In addition if $H$ is also normal in $G$, then $NH$ is normal in $G$. Therefore, $[G,G][G^p]$ is a normal subgroup of $G$.

The same counting argument approach used in the proof of Theorem 2 would show that there are $(p^n - 1)/(p - 1)$ subgroups in $G$ of index $p$ where $n$ is the dimension of $G/[G,G][G^p]$ viewed as a vector space over $\mathbb{Z}_p$. We leave the details of the general case as an exercise.

3. **Applications**

We present a few applications of the results from the previous section.

**Example.** For every $n \geq 2$, the alternating group $A_n$ on $n$ symbols has no subgroups of index 2.
Note that a quick way to argue this is to observe that the result is trivially true for $A_2$, $A_3$ and for $A_4$ [1], and for $n \geq 5$, appeal to the fact that $A_n$ is a simple group. But we want to get this as an application of the Corollaries above which is more elementary.

By these Corollaries, it is enough to show that $A_n$ is generated by squares. For this, recall that every even permutation is a product of 3-cycles [2, Ex. 5.47]. Therefore, it is enough to show that every 3-cycle is in $A_{2n}$, but this is clear because if $\alpha$ is a 3-cycle, then $\alpha = \alpha^{-2} = (\alpha^{-1})^2$ and $\alpha^{-1} \in A_n$.

As another application of the Corollaries, we prove that the alternating group $A_n$ is the only subgroup of index 2 in the symmetry groups $S_n$.

**Example.** $S_n$ has a unique subgroup of index 2: $A_n$.

By one of the Corollaries, it is enough to show that $A_n = S_{2n}^2$.

As seen in the previous Example, $A_n = A_{2n}^2$ and since $A_{2n}^2 \subseteq S_{2n}$, then $A_n \subseteq S_{2n}^2$.

Conversely, since the square of every permutation is an even permutation, then $S_{2n}^2 \subseteq A_n$. Therefore, $A_n = S_{2n}^2$ as required.

We want to apply the results of the previous section to the dihedral groups $D_n$ ($n > 2$). For the convenience of the reader, we recall the definition of the dihedral groups. Let $Isom(\mathbb{R}^2)$ be the set of isometries of $\mathbb{R}^2$ (also thought of as the $xy$-plane), then $Isom(\mathbb{R}^2)$ is a group under the composition of maps. Let $R$ be the rotation counter-clockwise in $\mathbb{R}^2$ of $\frac{360^\circ}{n}$ about the origin and $S$ be the reflection about the $x$-axis. Then $D_n$ is the subgroup of $Isom(\mathbb{R}^2)$ generated by $\{R, S\}$ in the sense discussed in the introductory paragraph of section 1. Since $R^n = id$ and $RS = SR^{n-1}$, it is easy to see that $D_n = \{S^iR^j : i = 0, 1; j = 0, 1, \ldots, n - 1\}$, in particular $D_n$ has order $2n$. We know that the subgroup $\langle R \rangle$ of rotations has index 2 in $D_n$. Therefore, we are interested in knowing if there are other subgroups of index 2 or if this is the only one. We have the following result.

**Theorem 3.** $D_n$ has a unique subgroup of index 2 if $n$ is odd and three subgroups of index 2 when $n$ is even.

With the description of $D_n$ preceding the theorem, one sees that $D_{2n}^2 = \langle R^2 \rangle$. In fact the elements outside of $\langle R \rangle$ have the form $SR^i$ and are reflections of order 2 which means that when they are squared they do not contribute any non-trivial elements to the subgroup $D_{2n}^2$.

On the other hand, recall that in every group, if $a$ is an element of order $o(a) = m$, then for every integer $k > 0$, $o(a^k) = m/gcd(m, k)$ [3, Thm. 4.2]. Therefore since $o(R) = n$, then

$$o(R^2) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ n & \text{if } n \text{ is odd} \end{cases}$$
Thus, 
\[ |D_n/D_n^2| = |D_n/\langle R^2 \rangle| = \frac{2n}{\phi(R^2)} = \begin{cases} 4 & \text{if } n \text{ is even} \\ 2 & \text{if } n \text{ is odd} \end{cases} \]
And the isomorphism \((I)\) for the group \(D_n\) corresponds to:
\[ D_n/D_n^2 \cong \begin{cases} \mathbb{Z}_2 \oplus \mathbb{Z}_2 & \text{if } n \text{ is even} \\ \mathbb{Z}_2 & \text{if } n \text{ is odd} \end{cases} \]
The result is then clear from either Theorem 1 or Theorem 2. The following result the proof of which is left as an easy exercise, leads to a large class of counterexamples to the converse of the Lagrange’s Theorem.

**Theorem 4.** For every groups \(G_1\) and \(G_2\),
\[ (G_1 \bigoplus G_2)^2 = G_1^2 \bigoplus G_2^2 \]

It follows from Corollary 2 and Theorem 4 that if neither \(G_1\) nor \(G_2\) has a subgroup of index 2, then \(G_1 \bigoplus G_2\) does not have a subgroup of index 2. In particular, for every \(n \geq 4\) and every odd natural number \(m\), the group \(A_n \bigoplus \mathbb{Z}_m\) does not have a subgroup of index 2. This provides a counterexample of order \(\frac{nm}{2}\) (\(n \geq 4\) and \(m \geq 1\) odd) to the converse of Lagrange’s Theorem. Other counterexamples are \(SL(2,3) \bigoplus A_n\) with \(n \geq 4\) and \(SL(2,3) \bigoplus \mathbb{Z}_n\) with \(n\) odd.

Note that using the fact that more than half the elements of \(A_4\) have odd order, the authors of [1] were able to conclude that there are counterexamples of order \(12m\) with \(m\) odd to the Lagrange’s Theorem. Unfortunately, it is not true in general that more than half the elements of \(A_n\) have odd order. For instance, \(A_{10}\) has only 893025 elements of odd orders while \(A_{10}\) has 1814400 elements. Therefore, our approach produces a new class of counterexamples.

**Acknowledgements:** I would like to thank the editor and the referees as their remarks led to a considerable improvement of both the presentation and the content of this article.

**References**


Department of Mathematics, University of Oregon, Eugene, OR 97403, OR 48710-0001

E-mail address: nganou@uoregon.edu