A Characterization of Cyclic Groups via Indices of Maximal Subgroups

ALAN ROCHE

Abstract. We show that cyclic groups are the only finitely generated groups with the property that distinct maximal subgroups have distinct indices.

1. Introduction

It’s well known that distinct subgroups of a cyclic group $G$ have distinct indices in $G$. It’s also well known that if a finite group of order $n$ has at most one subgroup of order $m$—and so of index $n/m$—for each divisor $m$ of $n$, then the group is cyclic (see, for example, [1, p. 192]). The property that distinct subgroups have distinct indices thus characterizes the class of finite cyclic groups. It’s less well known that the same property characterizes the infinite cyclic group: if distinct subgroups of an infinite group have distinct indices (as cardinal numbers) then the group is cyclic—see [7] which also covers the case of finite groups. The proof relies crucially on a result of Schur: if the center of a group $G$ has finite index then the commutator subgroup of $G$ is finite. Schur’s result also underpins a similar characterization of the infinite cyclic group as the only infinite group in which each nontrivial subgroup has finite index (see [2] or [8, p. 446], or the more elementary treatment in [4]).

Recall that a maximal subgroup of a group is a proper subgroup that is not strictly contained in another proper subgroup. We prove an analogous characterization of cyclic groups to that in [7] using maximal subgroups in place of arbitrary subgroups. To be precise, we establish the following.

Theorem. A finitely generated group is cyclic if and only if distinct maximal subgroups have distinct indices.

To be more precise, we take the well-known “only if” direction as given and prove the “if” direction. The result seems to be new. At least, we’ve not been able to find it in the literature. Whether the gap we (appear to) fill was much needed, you, dear reader, can decide (see [3, p. 332]). Our proof hinges on a property of the Frattini subgroup. We discuss this and other background material in Section 2. In the case of finite groups, we give a second proof of the theorem using the inclusion-exclusion principle. The result fails without the hypothesis that $G$ is finitely generated—see Section 3.

There are several characterizations of families of groups in terms of properties of maximal subgroups. For instance, a finite group is a product of its Sylow subgroups (equivalently, is nilpotent) if and only if each maximal subgroup is normal [5, Cor. 10.3.4]. Another example: a finite group is supersolvable$^1$ if and only if each maximal subgroup

---

2020 Mathematics Subject Classification. 20E34.
Key words and phrases. finitely generated group, Frattini subgroup, inclusion-exclusion principle.
Received on 29-3-2022; revised 26-5-2022.
DOI:10.33232/BIMS.0089.65.72.

$^1$A group $G$ is supersolvable if it admits a chain of normal subgroups $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = \{1\}$ (for some positive integer $r$) such that each quotient $G_i/G_{i-1}$ is cyclic.
has prime index [5, Cor. 10.5.1 and Thm. 10.5.8]. Our characterization of cyclic groups is a modest companion to these classical observations.

Acknowledgements. I am grateful to the Editor, Anthony O’Farrell, for saving me from some infelicities and to a referee for helpful suggestions.

2. Preliminaries.

For ease of reference, we collect several results which feature in the proofs of the theorem. It may be best to just skim this section, referring back to look more closely as needed.

**Finitely generated groups and maximal subgroups.** A finite group has only finitely many subgroups, and thus each proper subgroup is contained in a maximal subgroup. By the magic of Zorn’s lemma, the same conclusion holds for a finitely generated group.

**Lemma 1.** Each proper subgroup of a finitely generated group is contained in a maximal subgroup.

**Proof.** Let $G$ be a finitely generated group, say with generating set $\{g_1, \ldots, g_r\}$. For $H$ a proper subgroup of $G$, write $C$ for the collection of proper subgroups of $G$ containing $H$, ordered by inclusion. If we show that every chain in $C$ has an upper bound, then by Zorn’s lemma $C$ has a maximal element, that is, there is a maximal subgroup of $G$ containing $H$.

For $\{H_\lambda\}_{\lambda \in \Lambda}$ a chain in $C$ (so that $H_\lambda \subseteq H_{\lambda'}$ or $H_{\lambda'} \subseteq H_\lambda$ for $\lambda, \lambda' \in \Lambda$), we set $\tilde{H} = \bigcup_{\lambda \in \Lambda} H_\lambda$. Then $\tilde{H}$ is a subgroup of $G$ containing $H$. If $\tilde{H}$ is a proper subgroup, then it’s an upper bound in $C$ for $\{H_\lambda\}_{\lambda \in \Lambda}$ and the proof is complete. Now if $\tilde{H} = G$, then $g_1 \in H_{\lambda_1}, \ldots, g_r \in H_{\lambda_r}$ for suitable $\lambda_1, \ldots, \lambda_r \in \Lambda$. As the subgroups $H_\lambda$ ($\lambda \in \Lambda$) form a chain, it follows that there is a single $\lambda_k$ such that each $H_{\lambda_i}$ is contained in $H_{\lambda_k}$. Hence each $g_i$ belongs to $H_{\lambda_k}$ and $H_{\lambda_k} = G$, a contradiction. Thus $\tilde{H}$ is a proper subgroup, and we’ve proved the lemma.

The Frattini subgroup. Next we introduce a core notion.

**Definition.** The Frattini subgroup $\Phi = \Phi(G)$ of a group $G$ is the intersection of the maximal subgroups of $G$. If $G$ has no maximal subgroups then $\Phi(G) = G$.

Since each automorphism of a group permutes the maximal subgroups in the group, $\Phi$ is characteristic in $G$ (that is, stable under each automorphism of $G$). In particular, $\Phi$ is always a normal subgroup. We set $\overline{G} = G/\Phi$. Further, for $H$ a subgroup of $G$, we write $\overline{H}$ for the image of $H$ under the canonical quotient map $g \mapsto g\Phi : G \to \overline{G}$. That is, if $H$ is a subgroup of $G$, then $\overline{H} = H\Phi/\Phi$.

We can now record the crucial property of $\Phi$ that we exploit.

**Proposition 1.** Let $G$ be a finitely generated group and let $H$ be a subgroup of $G$. Then:

(a) $G = H$ if and only if $\overline{G} = \overline{H}$;

(b) $G$ is cyclic if and only if $\overline{G}$ is cyclic.

**Proof.** It’s obvious that $G = H$ implies $\overline{G} = \overline{H}$. For the other direction in part (a), suppose $\overline{G} = \overline{H}$, so that $G = H\Phi$. Suppose also that a maximal subgroup $M$ of $G$ contains $H$. Since $\Phi \subseteq M$, we then have $G = H\Phi \subseteq M$ which is absurd. Hence $H$ is not contained in a maximal subgroup of $G$. Using Lemma 1, we see that $G = H$, as required.

Part (b) follows from part (a). In detail, $G$ is cyclic if and only if $G = \langle g \rangle$ for some $g \in G$. By part (a), this is equivalent to $\overline{G} = \langle g\Phi \rangle$ for some $g\Phi \in \overline{G}$. □
Maximal subgroups and distinct indices. We note a quick consequence of the hypothesis that distinct maximal subgroups of a group have distinct indices.

**Lemma 2.** Suppose that distinct maximal subgroups of a group $G$ have distinct indices in $G$ (as cardinal numbers). Then each maximal subgroup is normal in $G$ of prime index.

**Proof.** Let $M$ be a maximal subgroup of $G$. For $g \in G$, the conjugate $gMg^{-1}$ is again maximal and has the same index in $G$ as $M$. Thus $gMg^{-1} = M$ for all $g \in G$, that is, $M$ is normal in $G$.

We can therefore consider the quotient group $G/M$. Its subgroups have the form $H/M$ as $H$ varies through the subgroups of $G$ containing $M$. Hence $G/M$ has no nontrivial proper subgroups, and so is cyclic of prime order. Indeed, for $g \notin M$, the group $\langle gM \rangle$ is a nontrivial subgroup of $G/M$, and thus $\langle gM \rangle = G/M$; moreover, $gM$ must have prime order as otherwise $G/M$ would admit a nontrivial proper subgroup. □

**Relatively prime indices.** In the case of finite groups, our second proof of the theorem uses the index formula of the next lemma. The formula applies equally to infinite groups and is no harder to prove in this generality.

**Lemma 3.** Let $G$ be a group and let $H_1, \ldots, H_r$ be finite index subgroups of $G$ whose indices are pairwise relatively prime, that is, $\gcd([G: H_i],[G: H_j]) = 1$, for $i \neq j$. Then $H_1 \cap \cdots \cap H_r$ has finite index in $G$ and

$$[G : H_1 \cap \cdots \cap H_r] = [G : H_1] \cdots [G : H_r]. \quad (1)$$

**Proof.** To simplify the notation, we set $K = H_1 \cap \cdots \cap H_r$. Consider the map of left coset spaces

$$gK \mapsto (gH_1, \ldots, gH_r) : G/K \to G/H_1 \times \cdots \times G/H_r.$$

Observe that this map is injective. Indeed, if $gH_i = g'H_i$ for each $i$, then $g^{-1}g' \in H_i$ for each $i$, and so $g^{-1}g \in K$ and $gK = g'K$. Thus $K$ has finite index in $G$ and

$$[G : K] \leq [G : H_1] \cdots [G : H_r]. \quad (2)$$

On the other hand,

$$[G : K] = [G : H_i][H_i : K] \quad (for \ i = 1, \ldots, r).$$

As the indices $[G : H_i]$ are pairwise relatively prime, the product $[G : H_1] \cdots [G : H_r]$ divides $[G : K]$. In particular,

$$[G : H_1] \cdots [G : H_r] \leq [G : K]. \quad (3)$$

Comparing (2) and (3), we’ve proved (1). □

**The Inclusion-Exclusion Principle.** We recall the statement and give a short proof.

**Proposition 2.** For finite sets $S_1, \ldots, S_r$,

$$\left| \bigcup_{i=1}^r S_i \right| = \sum_i |S_i| - \sum_{j<k} |S_j \cap S_k| + \cdots + (-1)^{r-1}|S_1 \cap \cdots \cap S_r|. \quad (4)$$

**Proof.** Let $S = \bigcup_{i=1}^r S_i$. Given $T \subseteq S$, we write $1_T$ for the characteristic function of $T$. In this notation, we’ll establish the equality of functions

$$1_{\bigcup_{i=1}^r S_i} = \sum_i 1_{S_i} - \sum_{j<k} 1_{S_j \cap S_k} + \cdots + (-1)^{r-1}1_{S_1 \cap \cdots \cap S_r}. \quad (5)$$

The identity (4) then follows by taking the integral of each side with respect to the counting measure on $S$ (the one that gives each element of $S$ measure 1).
We set $\mathbb{1} = \mathbb{1}_S$. For $T \subseteq S$, we also write $T^c$ for the complement of $T$ in $S$, so that
\[ \mathbb{1}_{T^c} = \mathbb{1} - \mathbb{1}_T. \] (6)
Further, for $T_i \subseteq S$ (for $i = 1, 2$), we have
\[ \mathbb{1}_{T_1 \cap T_2} = \mathbb{1}_{T_1} \mathbb{1}_{T_2}. \] (7)
Now, taking $T = \left( \bigcup_{i=1}^r S_i \right)^c$ in (6) gives
\[ \mathbb{1}_{\bigcup_{i=1}^r S_i} = \mathbb{1} - \mathbb{1}_{\bigcap_{i=1}^r S_i}^c \]
\[ = \mathbb{1} - \mathbb{1}_{S_1} \cdots \mathbb{1}_{S_r} \] (by (7))
\[ = \mathbb{1} - (\mathbb{1} - \mathbb{1}_{S_1}) \cdots (\mathbb{1} - \mathbb{1}_{S_r}) \] (by (6)).
Expanding the product on the last line, we see that
\[ \mathbb{1}_{\bigcup_{i=1}^r S_i} = \sum_i \mathbb{1}_{S_i} - \sum_{j<k} \mathbb{1}_{S_j} \mathbb{1}_{S_k} + \cdots + (-1)^{r-1} \mathbb{1}_{S_1} \cdots \mathbb{1}_{S_r} \]
\[ = \sum_i \mathbb{1}_{S_i} - \sum_{j<k} \mathbb{1}_{S_j \cap S_k} + \cdots + (-1)^{r-1} \mathbb{1}_{S_1 \cap \cdots \cap S_r}. \]
We’ve shown that (5) holds and hence also (4). \(\square\)

3. Two Examples.

We prove the theorem in Sections 4 (finite groups) and 5 (infinite groups). In this section, we give two examples of groups that are not finitely generated, and so certainly not cyclic, but have the property that distinct maximal subgroups have distinct indices. Thus the theorem fails if we drop the hypothesis that our groups are finitely generated.

First, let $M$ be a maximal subgroup of an abelian group $A$, so that the quotient $A/M$ has no proper nontrivial subgroups. As noted in the proof of Lemma 2, it follows that $A/M \cong \mathbb{Z}/p\mathbb{Z}$ for some prime $p$.

**Example 1.** Suppose an abelian group $A$ is such that $nA = A$ for all nonzero integers $n$ (using additive notation). Abelian groups with this property are called divisible. For example, the additive group $\mathbb{Q}$ is divisible. Further, a quotient of a divisible group is divisible. In particular, $A$ can never have $\mathbb{Z}/p\mathbb{Z}$ as a quotient (for $p$ a prime), and so $A$ has no maximal subgroups. Thus the maximal subgroups of $A$ have distinct indices—vacuously. By Lemma 1, if $A$ is nontrivial then it is not finitely generated.

**Example 2.** Consider the additive group $A = \bigoplus_p \mathbb{Z}/p\mathbb{Z}$ where the sum is over all primes. By construction, $A$ is not finitely generated.

Its maximal subgroups are the subgroups $lA$ as $l$ varies through the primes. Indeed, for $l$ prime, multiplication by $l$ is an isomorphism on $\mathbb{Z}/p\mathbb{Z}$ for $p \neq l$ and is the zero map on $\mathbb{Z}/l\mathbb{Z}$. Thus $lA = \bigoplus_{p\neq l} \mathbb{Z}/p\mathbb{Z}$. The projection map from $A$ to $\mathbb{Z}/l\mathbb{Z}$ therefore induces an isomorphism
\[ A/lA \cong \mathbb{Z}/l\mathbb{Z}, \] (8)
whence $lA$ is a maximal subgroup of $A$. On the other hand, say $M$ is a maximal subgroup of $A$. Then $A/M \cong \mathbb{Z}/l\mathbb{Z}$ for some prime $l$, so that $lA \subseteq M$. Maximality of $lA$ now implies that $lA = M$.

By (8), distinct maximal subgroups of $A$ have distinct indices in $A$. 
4. Finite Groups.

We now prove the theorem for finite groups—in two ways.

Let \( G \) be a nontrivial finite group and write \( M_1, \ldots, M_r \) for the maximal subgroups of \( G \). By hypothesis, the indices \( [G : M_1], \ldots, [G : M_r] \) are distinct. By Lemma 2, each \( M_i \) is normal in \( G \) and there exist primes \( p_1, \ldots, p_r \) such that \( G/M_i \cong \mathbb{Z}/p_i\mathbb{Z} \) (for \( i = 1, \ldots, r \)).

First proof. Consider the homomorphism

\[
g \mapsto (gM_i)_{i=1,\ldots,r} : G \to \prod_{i=1}^r G/M_i.
\]

Its kernel is \( M_1 \cap \cdots \cap M_r = \Phi \), and thus \( \bar{G} = G/\Phi \) embeds in \( \prod_{i=1}^r G/M_i \). Now

\[
\prod_{i=1}^r G/M_i \cong \prod_{i=1}^r \mathbb{Z}/p_i\mathbb{Z} \cong \mathbb{Z}/p_1 \cdots p_r\mathbb{Z}.
\]

Hence \( \bar{G} \) embeds in a cyclic group, and so is cyclic. Using Proposition 1 (b), we conclude that \( G \) is cyclic.

We need a preparatory observation for the second proof. Let \( i_1, \ldots, i_k \) be distinct indices between 1 and \( r \). Since the various (group) indices \( [G : M_{i_j}] \) are (pairwise) relatively prime (for \( j = 1, \ldots, k \)), it follows from Lemma 3 that

\[
[G : M_{i_1} \cap \cdots \cap M_{i_k}] = [G : M_{i_1}] \cdots [G : M_{i_k}] = p_{i_1} \cdots p_{i_k}.
\]

We set \( n = |G| \) and rewrite (9) as

\[
|M_{i_1} \cap \cdots \cap M_{i_k}| = \frac{n}{p_{i_1} \cdots p_{i_k}}.
\]

Second proof. The strategy of the proof is to show that there are elements of \( G \) that lie outside each maximal subgroup. For any such \( g \in G \), the cyclic subgroup \( \langle g \rangle \) cannot be proper, so that \( G \) is cyclic with generator \( g \). To implement the strategy, we count the number of elements in \( \bigcup_{i=1}^r M_i \). A trivial estimate then shows that this number is less than \( n = |G| \), whence \( G \) is cyclic.

Using the inclusion-exclusion principle and (10), we have

\[
\left| \bigcup_{i=1}^r M_i \right| = \sum_i |M_i| - \sum_{j<k} |M_j \cap M_k| + \cdots + (-1)^{r-1} |M_1 \cap \cdots \cap M_r| = \sum_i \frac{n}{p_i} - \sum_{j<k} \frac{n}{p_j p_k} + \cdots + (-1)^{r-1} \frac{n}{p_1 \cdots p_r} = n \left( \sum_i \frac{1}{p_i} - \sum_{j<k} \frac{1}{p_j p_k} + \cdots + (-1)^{r-1} \frac{1}{p_1 \cdots p_r} \right) = n \left[ 1 - \left( 1 - \frac{1}{p_1} \right) \cdots \left( 1 - \frac{1}{p_r} \right) \right] < n.
\]

We’ve proved (again) that \( G \) is cyclic.

Remark 1. For \( n \) a positive integer, let \( p_1, \ldots, p_r \) be the distinct prime divisors of \( n \). Recall that \( \phi(n) \) is the number of integers between 1 and \( n \) that are relatively prime to
n. Applying the above proof to a cyclic group of order $n$ gives the well-known formula

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

(11)

The inclusion-exclusion principle also yields the formula directly—without an appeal to group theory. To spell this out, write $n$ for the set of integers between 1 and $n$ and $n/p_i$ for the set of elements of $n$ that are divisible by $p_i$, so that $|n/p_i| = n/p_i$ (for $i = 1, \ldots, r$). Then the union $\bigcup_{i=1}^r n/p_i$ consists of the integers between 1 and $n$ that are divisible by some prime divisor of $n$—that is, the integers between 1 and $n$ that are not relatively prime to $n$. Thus

$$\left|\bigcup_{i=1}^r n/p_i\right| = n - \phi(n).$$

Counting $|\bigcup_{i=1}^r n/p_i|$ via the inclusion-exclusion principle (exactly as above), we obtain (11) once more.

5. Infinite Groups.

Next we prove the theorem for infinite groups. We treat abelian groups first (finite and infinite) and then reduce to this case.

To start, note that if distinct maximal subgroups of a group $G$ have distinct indices then each quotient of $G$ inherits the property. Indeed, for $N$ a normal subgroup of $G$, a maximal subgroup of $G/N$ has the form $M/N$ for a unique maximal subgroup $M$ of $G$ containing $N$ and $[G/N : M/N] = [G : M]$.

Lemma 4. Let $A$ be a finitely generated abelian group such that distinct maximal subgroups of $A$ have distinct indices in $A$. Then $A$ is cyclic.

Proof. By (a part of) the fundamental theorem of finitely generated abelian groups, there is a nonnegative integer $r$ and a finite abelian group $T$ such that $A \cong \mathbb{Z}^r \times T$. As quotients of $A$, the groups $\mathbb{Z}^r$ and $T$ have the property that distinct maximal subgroups have distinct indices.

If $r = 0$, then $A$ is finite and hence cyclic (since we’ve proved the theorem for finite groups).

Suppose $r > 0$. We need to show that $T$ is trivial and $r = 1$. If $T$ is nontrivial, then it admits a maximal subgroup, say $T_{\text{max}}$, and $[T : T_{\text{max}}] = p$ for some prime $p$. In this case, the subgroups $\mathbb{Z}^r \times T_{\text{max}}$ and $p\mathbb{Z} \times \mathbb{Z}^{r-1} \times T$ would each have index $p$ in $\mathbb{Z}^r \times T$. We conclude that $T$ is trivial, so that $A \cong \mathbb{Z}^r$. In the same way, we have $r = 1$: for $r > 1$ and $p$ a prime, the subgroups $p\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}^{r-2}$ and $\mathbb{Z} \times p\mathbb{Z} \times \mathbb{Z}^{r-2}$ each have index $p$ in $\mathbb{Z}^r$. □

Combining Lemma 4 and earlier arguments, the theorem for infinite groups follows readily.

Proof. Let $G$ be a finitely generated infinite group such that distinct maximal subgroups of $G$ have distinct indices in $G$. We want to show that $G$ is cyclic.

Write $\{M_i\}_{i \in I}$ for the family of maximal subgroups of $G$. By Lemma 2, each $M_i$ is normal in $G$ and each quotient $G/M_i$ is cyclic, hence abelian. As in the first proof for finite groups, we consider the homomorphism

$$g \mapsto (gM_i)_{i \in I} : G \rightarrow \prod_{i \in I} G/M_i.$$ 

Since the kernel is $\Phi$, we see that $\overline{G} = G/\Phi$ embeds in the abelian group $\prod_{i \in I} G/M_i$, and so $\overline{G}$ is abelian. Moreover, $\overline{G}$ is finitely generated and distinct maximal subgroups of $\overline{G}$. 

have distinct indices. Hence, by Lemma 4, \( G \) is cyclic. Appealing to Proposition 1 (b), we conclude that \( G \) is cyclic. \( \square \)

6. A Comment on Cyclic \( p \)-groups.

The maximal subgroups of a finite cyclic group \( G \) are the subgroups of prime index, one for each prime divisor of \( |G| \). In particular, a nontrivial finite cyclic \( p \)-group (\( p \) a prime) has a unique maximal subgroup. Conversely, if a finite group \( G \) has a unique maximal subgroup \( M \), then any element of \( G \) that is not in \( M \) is a generator, so \( G \) is cyclic, and the order of \( G \) is a \( p \)-power for \( p = [G : M] \). That is, the nontrivial cyclic groups of prime-power order are precisely the finite groups that have a single maximal subgroup. This characterization of cyclic groups of prime-power order can be slightly augmented as follows.

(\( \alpha \)) Suppose the maximal subgroups of a finite group \( G \) form a single conjugacy class. Then \( G \) is cyclic of prime-power order.

**Proof.** Let \( M \) be a maximal subgroup of \( G \). By hypothesis, the union of the maximal subgroups of \( G \) is \( \bigcup_{g \in G} gMg^{-1} \). Now, an elementary counting argument shows that a finite group is never a union of conjugates of a proper subgroup (see, for example, [9, Lemma 6.1]). Thus there is an element of \( G \) that is not contained in a maximal subgroup, whence \( G \) is cyclic. Moreover, \( M \) must be the unique maximal subgroup of \( G \), and so \( G \) has prime-power order. \( \square \)

**Remark 2.** What happens if you replace “finite” in (\( \alpha \)) by “finitely generated”? The statement is then false—in spectacular fashion. In fact, for each sufficiently large prime \( p \), there is an infinite group \( G \) such that

(a) each nontrivial proper subgroup has order \( p \) and so is maximal,

(b) the maximal subgroups (that is, the nontrivial proper subgroups) form a single conjugacy class.

Note that any such \( G \) is generated by two elements: for \( h \neq 1 \) and \( g \notin \langle h \rangle \), the subgroup \( \langle h, g \rangle \) has more than \( p \) elements, and hence \( G = \langle h, g \rangle \).

An infinite group that satisfies (a) is called a **Tarski monster**. These ghoulish groups were shown to exist by A. Y. Olshanskii and independently by E. Rips (for details, see Chap. 9 of Olshanskii’s bestiary [6]). Among them are ones that also satisfy (b).

**References**


Alan Roche can remember studying at University College Dublin and the University of Chicago when he was a young and callow fellow. He has worked at the University of Oklahoma
since 2001. His principal mathematical interests are in number theory and related parts of representation theory.

Department of Mathematics, University of Oklahoma, Norman, OK 73019, USA.
E-mail address: aroche@ou.edu