A characterization of the cyclic groups by subgroup indexes

Let G be a group. Then G is *cyclic* if there exists some $g \in G$ such that $G = \langle g \rangle := \{g^m : m \in \mathbb{Z}\}$. For every positive integer n, $\mathbb{Z}/\langle n \rangle$ (the additive group of integers modulo n) is the unique cyclic group on n elements, and $\mathbb{Z}$ is the unique infinite cyclic group (up to isomorphism). The cyclic groups play a nontrivial role in abelian group theory. For instance, The Fundamental Theorem of Finitely Generated Abelian Groups states that every finitely generated abelian group is a finite direct sum of cyclic groups (see Hungerford [**7**], Theorem 2.1). Further, every abelian group G for which there is a finite bound on the orders of the elements of G is a (possibly infinite) direct sum of cyclic groups (cf. Fuchs [**6**], Theorem 11.2).

Given the fundamental role the cyclic groups play in group theory, it is hardly a surprise that many characterizations of these groups have appeared in the literature over the years; see the bibliography for a sample of such papers. The purpose of this note is to present a new characterization via subgroup indexes. Recall that if G is a group and $H < G$ (that is, H is a subgroup of G), then the *index* $(G : H)$ of H in G is simply the cardinality of the set of right cosets of H in G; more compactly, $(G : H) = |\{Hg : g \in G\}|$ (equivalently, $(G : H)$ is the cardinality of the set of left cosets of H in G).

It is not hard to show that distinct subgroups of a finite cyclic group have distinct cardinalities (we will shortly present a proof of this assertion). It then follows immediately that distinct subgroups of a finite cyclic group G have distinct indexes in G. The same property is enjoyed by the infinite cyclic group $\mathbb{Z}$ of integers. To wit, every subgroup of $\mathbb{Z}$ is of the form $\langle m \rangle$ for some integer $m \geq 0$. Note that if m and n are distinct positive integers, then $m = (\mathbb{Z} : \langle m \rangle) \neq n = (\mathbb{Z} : \langle n \rangle)$. Further, $(\mathbb{Z} : \{0\}) = \aleph_0$. Hence distinct subgroups of $\mathbb{Z}$ have distinct indexes in $\mathbb{Z}$.

In this paper, we show that the previous property enjoyed by the cyclic groups completely distinguishes them within the class of all groups. That is, we prove that an arbitrary group G is cyclic if and only if distinct subgroups of G have distinct indexes in G.

The finite case

Let G be a finite group. We begin with an easy lemma showing that distinct subgroups of G have distinct indexes in G if and only if distinct subgroups of G have distinct cardinalities.

Lemma 1. Let G be a finite group, and let H and K be subgroups of G. Then $(G : H) \neq (G : K)$ if and only if $|H| \neq |K|$.

Proof. Assume that G is a finite group and that H and K are subgroups of G. Then simply note that $(G : H) = (G : K)$ if and only if $|G|/|H| = |G|/|K|$ if and only if $1/|H| = 1/|K|$ if and only if $|H| = |K|$. The result follows. ■

Remark 1. The previous lemma can fail badly if G is infinite. To see this, let m and n be distinct positive integers. Then $(\mathbb{Z} : \langle m \rangle) \neq (\mathbb{Z} : \langle n \rangle)$, yet $|\langle m \rangle| = |\langle n \rangle| = \aleph_0$.

It is well-known that if G is a finite cyclic group, then distinct subgroups of G have distinct cardinalities (cf. [**7**], Exercise 6 of Section 1.3 or Lang [**10**], p. 24). We sketch a short proof of this fact below.

Proposition 1. Let G be a finite cyclic group. Then distinct subgroups of G have distinct indexes in G.

Proof. Let $G := \langle g \rangle$ be a finite cyclic group of order m. By Lemma 1, it suffices to show that distinct subgroups of G have distinct cardinalities. Let H be a subgroup of G. Then H is cyclic, whence $H = \langle g^k \rangle$ for some k with $1 \leq k \leq m$. Now let $d :=\gcd(k, m)$. We claim that $\langle g^k \rangle = \langle g^d \rangle$. Since $d|k$, the inclusion $\langle g^k \rangle \subseteq \langle g^d \rangle$ is clear. To prove the reverse implication, recall that $\alpha k + \beta m = d$ for some integers α and β. Hence $m|(d - \alpha k)$. We conclude that $g^d = g^{\alpha k} = (g^k)^\alpha$, and hence $\langle g^d \rangle \subseteq \langle g^k \rangle$.

To finish the proof, we suppose that H_1 and H_2 are subgroups of G of the same cardinality. We will show that $H_1 = H_2$. By our work above, it follows that $H_1 = \langle g^{d_1} \rangle$ and $H_2 = \langle g^{d_2} \rangle$ for some positive integers d_1 and d_2 which divide m. Thus $|H_1| = |\langle g^{d_1} \rangle| = \frac{m}{d_1} = |H_2| = \frac{m}{d_2}$. We deduce that $d_1 = d_2$, and therefore $H_1 = H_2$. ■

Remark 2. There are infinite groups G with the property that distinct subgroups of G have distinct cardinalities, yet such groups are not even close to being cyclic (they are not finitely generated). We remind the reader that the *quasi-cyclic group* $\mathbb{Z}(p^\infty)$, p a prime, is the subgroup of $\mathbb{Q}/\mathbb{Z}$ consisting of all fractions whose denominator is a power of p (modulo $\mathbb{Z}$). It turns out that an infinite group G has the property that distinct subgroups of G have distinct cardinalities if and only if G is a quasi-cyclic group. This was shown by W.R. Scott in Scott [**17**].

We now turn our attention to proving the converse of Proposition 1 within the class of finite groups. Our next proposition is known (see Corollary 7.14 of Isaacs [**8**] and Theorem 2.17 of Rotman [**16**]). We give two proofs: the first utilizes only undergraduate group theory while the second invokes a less well-known result due to Baer. We first state and prove a lemma.

Lemma 2. Let G be a group (not assumed to be finite) for which distinct subgroups of G have distinct cardinalities. Then every subgroup of G is normal.

Proof. Let G be a group with the above property, and let H be an arbitrary subgroup of G. Further, let $g \in G$ be arbitrary. Then the map $h \mapsto ghg^{-1}$ is a bijection between H and gHg^{-1}, whence $H = gHg^{-1}$. Since g was arbitrary, we deduce that H is normal in G. ■

Proposition 2. Let G be a finite group with the property that distinct subgroups of G have distinct indexes in G. Then G is cyclic.

Proof 1. Assume that G is a finite group such that distinct subgroups of G have distinct indexes in G. Then by Lemma 1, distinct subgroups of G have distinct cardinalities. If G is trivial, then of course G is cyclic and we are done. Thus suppose that G is nontrivial, and let $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ be the prime factorization of $|G|$. Fix i with $1 \leq i \leq k$, and let G_i be a Sylow p_i-subgroup of G. Since distinct subgroups of G have distinct cardinalities, we conclude that G_i is the unique (normal) Sylow p_i-subgroup of G. Thus G is the direct product of its Sylow subgroups (this is well-known; see [**7**], p. 96, for example):

$$G = G_1 \times G_2 \times \cdots \times G_k. \tag{1}$$

We now prove that G_i is cyclic. Without loss of generality, we may assume that $i = 1$. Recall from above that $|G_1| = p_1^{n_1}$; for simplicity, we set $p := p_1$ and $n := n_1$. Suppose by way of contradiction that G_1 is not cyclic. As stated in the introduction, every group is a union of its cyclic subgroups; let $\{H_1, H_2, \ldots, H_s\}$ be the collection of cyclic subgroups of G_1. Note that as G_1 is not cyclic, each H_i has cardinality strictly less than $|G_1| = p^n$. For each i satisfying $1 \leq i \leq s$, it follows from Lagrange's Theorem that $|H_i| = p^j$ for some integer j with $0 \leq j < n$. As distinct subgroups of G have distinct cardinalities, clearly G_1 inherits this property as well. We conclude that for each j with $0 \leq j < n$, at most one H_i has order p^j. Hence

$$|G_1| = |H_1 \cup H_2 \cup \cdots \cup H_s| \leq 1 + p + p^2 + \cdots + p^{n-1} = \frac{p^n - 1}{p - 1} < p^n = |G_1|,$$

and we have reached a contradiction. Thus G_1 is cyclic. We deduce that

$$G \cong \mathbb{Z}/\langle p_1^{n_1} \rangle \times \mathbb{Z}/\langle p_2^{n_2} \rangle \times \cdots \times \mathbb{Z}/\langle p_k^{n_k} \rangle \cong \mathbb{Z}/\langle p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \rangle, \tag{2}$$

whence G is cyclic. This completes the first proof. ■

Proof 2. We first show that G is abelian. Suppose not. Then by Lemma 2, G is a non-abelian group all of whose subgroups are normal, i.e., G is a Hamiltonian group. A result of Baer (see Baer [**2**]) implies that $G \cong Q_8 \times P$ for some abelian group P which has no elements of order 4 and for which all elements of P have finite order (recall that Q_8 is the quaternion group on 8 elements given by the presentation $Q_8 := \langle -1, i, j, k | (-1)^2 = 1,\ i^2 = j^2 = k^2 = ijk = -1 \rangle$). But then Q_8 inherits the property that distinct subgroups have distinct cardinalities, contradicting the fact that Q_8 has three subgroups of order 4. Thus G is abelian, and hence, by The Fundamental Theorem of Finitely Generated Abelian Groups, G is isomorphic to a finite direct product of cyclic groups each of prime power order. No two distinct summands can have orders that are powers of the same prime p, lest G have two distinct subgroups of order p. We deduce as in the conclusion of Proof 1 that G is cyclic. ■

Combining Proposition 1 and Proposition 2 yields

Theorem 1. *Let G be a finite group. Then G is cyclic if and only if distinct subgroups of G have distinct indexes in G.*

The infinite case

The goal of this section is to extend Theorem 1 to infinite groups. In particular, we will show that for any infinite group G, distinct subgroups of G have distinct indexes in G if and only if $G \cong \mathbb{Z}$. For brevity, let us say that an infinite group G with the property that distinct subgroups of G have distinct indexes in G has property (D). We begin by showing that all groups with property (D) are countable.

Lemma 3. Suppose G is a group with property (D). Then G is countable. Hence every nontrivial subgroup of G has finite index in G.

Proof. Suppose by way of contradiction that G is an uncountable group with property (D), and let $g \in G$ be arbitrary. Now set $H := \langle g \rangle$, and let $\{g_i : i \in I\}$ be complete set of right coset representatives for H in G. Finally, set $X := \{Hg_i : i \in I\}$. Define $\varphi : H \times X \to G$ by $\varphi((g^m, Hg_i)) := g^m g_i$. One checks easily that φ is a bijection between $H \times X$ and G. Thus $|G| = |\langle g \rangle| \cdot (G : \langle g \rangle)$. Since G is uncountable and $\langle g \rangle$ is countable, it follows from basic cardinal arithmetic that $|G| = (G : \langle g \rangle)$ (see Lang [**10**], Corollary 3.8, Appendix 2). Now choose any $x \in G - \{e\}$. Then $(G : \{e\}) = |G| = (G : \langle x \rangle)$. As G has property (D), we conclude that $\langle x \rangle = \{e\}$, a contradiction. Hence G is countable. If $H \neq \{e\}$ is any subgroup of G, then $(G : H) \leq |G| = (G : \{e\}) \neq (G : H)$. We deduce that $(G : H) < |G| = \aleph_0$, and thus H has finite index in G. ■

It has been known for some time (though not well-known) that $\mathbb{Z}$ is the unique infinite group G with the property that every nontrivial subgroup of G has finite index in G. Fedorov established this result in Fedorov [**5**]. More recently, Charles Lanski gave a self-contained proof of this result using only undergraduate-level group theory. It is not our purpose to give such a detailed proof in this paper; we refer the interested reader instead to Lanski [**11**]. Assuming a theorem of Schur, we can still present an elementary proof of Fedorov's result. The details follow.

Let G be a group, and recall that an element $g \in G$ is a *commutator* if $g = xyx^{-1}y^{-1}$ for some $x, y \in G$. The *derived subgroup* G' of G is the subgroup of G generated by all commutators of G. It is easy to see that G is abelian if and only if $G' = \{e\}$. In some sense, if G is close to being abelian, we may expect G' to be small. We now remind the reader that the *center* $Z(G)$ of G is defined by $Z(G) := \{x \in G : xg = gx \text{ for all } g \in G\}$.

Suppose that $Z(G)$ has finite index in an infinite group G. Then there is a sense in which $Z(G)$ is large. Thus we may conjecture that G is "close to" being abelian. If this is correct, then (as noted above) we may expect the derived subgroup G' of G to be "small". This conjecture (formalized appropriately) is correct, and is known as Schur's Theorem. We refer the reader to Theorem 2 of [**11**] for a self-contained proof.

Fact 1 (Schur's Theorem). For any group G, if $(G : Z(G))$ is finite, then so is G'.

We now prove a final lemma, then present the main theorem of this section.

Lemma 4. Let G be a group with property (D). Then G is finitely generated.

Proof. We assume that G has property (D) and we let $g_0 \neq e$ be an arbitrary element of G. Now set $H := \langle g_0 \rangle$. By Lemma 3, $(G : H)$ is finite; let $\{g_i : 1 \leq i \leq n\}$ be a complete set of right coset representatives of H in G. We claim that $G = \langle g_0, g_1, \ldots, g_n \rangle$. To see this, let $g \in G$ be arbitrary. Then $Hg = Hg_i$ for some i, $1 \leq i \leq n$. But then $gg_i^{-1} \in H = \langle g_0 \rangle$. Thus there is an integer m such that $gg_i^{-1} = g_0^m$. We conclude that $g \in \langle g_0, g_i \rangle \subseteq \langle g_0, g_1, \ldots, g_n \rangle$, and the proof is complete. ■

Theorem 2. *Let G be an infinite group. Then G is cyclic if and only if G has property (D).*

Proof. As noted in the introduction, $\mathbb{Z}$ has property (D). Conversely, suppose that G has property (D). We first prove that G is abelian. By Lemmas 3 and 4, G is countable and finitely generated; say $G = \langle x_1, x_2, \ldots, x_n \rangle$. We may assume that each x_i is a non-identity element of G. For each i, $1 \leq i \leq n$, recall that the *centralizer* $C(x_i)$ of x_i is defined by $C(x_i) := \{g \in G : gx_i = x_i g\}$. Note that each $C(x_i)$ is a subgroup of G containing the non-identity element x_i. Further, it is easy to see that for all $g \in G$, $g \in Z(G)$ if and only if $g \in C(x_i)$ for all i, $1 \leq i \leq n$. We deduce from Lemma 3 that each $C(x_i)$ has finite index in G. But then $C(x_1) \cap C(x_2) \cap \cdots \cap C(x_n) = Z(G)$ is also of finite index in G (it is well-known that a finite intersection of finite index subgroups also has finite index; see for example Proposition 4.9 of [**7**]). We now invoke Schur's Theorem to conclude that G' is finite. But then observe that $(G : G') = (G : \{e\}) = \aleph_0$. Since G has property (D), we see that $G' = \{e\}$, and hence G is abelian. By The Fundamental Theorem of Finitely Generated Abelian Groups, it follows that $G \cong \mathbb{Z} \times H$ for some group H which is a finite direct sum of cyclic groups. It remains to show that H is trivial. To see this, note that both H and $\{e\}$ have index $\aleph_0$ in the group $\mathbb{Z} \times H$. Since $\mathbb{Z} \times H$ has property (D), we conclude that H is trivial, and hence $G \cong \mathbb{Z}$. ∎

Remark 3 Consider the following weaker property (D′): every nontrivial subgroup of G has index less than $|G|$. It is not hard to prove that an infinite group G has property (D′) if and only if G is cyclic (one first shows that G is countable and then invokes Fedorov's result). But note that this property is not strong enough to distinguish the finite cyclic groups as *every* finite group has property (D′).

Conclusion

Combining Theorem 1 and Theorem 2 yields the main result of the paper:

Theorem 3. *Let G be an arbitrary group. Then G is cyclic if and only if distinct subgroups of G have distinct indexes in G.*

Summary. In this note, we provide a new characterization of the cyclic groups. Recall that if G is a group and H is a subgroup of G, then the *index* of H in G is the cardinality of the set of right (left) cosets of H in G. We prove that an arbitrary group G is cyclic exactly when distinct subgroups of G have distinct indexes in G.

References

1. C. Ayoub, A note on a theorem of F. Szász, *Rev. Roumaine Math. Pures Appl.* **11** (1966) 269–270.
2. R. Baer, Situation der untergruppen und struktur der gruppe, *S.B. Heidelberg. Akad. Wiss.* **2** (1933) 12–17.
3. C. Bagiński and J. Krempa, On a characterization of infinite cyclic groups, *Publ. Math. Debrecen* (1-2) **63** (2003) 249–254.
4. M. Deaconescu and R. Khazal, A characterization of the finite cyclic groups, *An. Univ. Timisoara Ser. Math.-inform.* (1) **32** (1994) 37–40.
5. Y. Fedorov, On infinite groups of which all nontrivial subgroups have a finite index, *Uspekhi Mat. Nauk.* **6** (1951) 187–189.
6. L. Fuchs, *Abelian Groups*, Publishing House of the Hungarian Academy of Sciences, Budapest, 1958.
7. T. Hungerford, *Algebra. Reprint of the 1974 original.*, Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980.
8. M. Isaacs, *Algebra: a Graduate Course. Reprint of the 1994 original.* Graduate Studies in Mathematics, 100. American Mathematical Society, Providence, RI, 2009.
9. K. Kovács, On a characterization of cyclic groups by sums and differences, *Studia Sci. Math. Hungar.* (3-4) **36** (2000) 307–311.
10. S. Lang, *Algebra. Revised third edition.*, Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.
11. C. Lanski, A characterization of infinite cyclic groups, *Math. Mag.* (1) **74** (2001) 61–65.
12. J. Morales Rodríguez, Another characterization of finite cyclic groups, *Miscelánea Mat.* **53** (2011) 33–37.
13. J. Morales Rodriguez, A characterization of the finite cyclic groups, XXXI National Congress of the Mexican Mathematical Society (Spanish) (Hermosillo, 1998), 303–305, *Aportaciones Mat. Commun.* **25** Soc. Mat. Mexicana, México, 1999.

14. N. Ramakrishna, T. Eswarlal, and Saibaba, G.S.V.S., A characterization of cyclic groups in terms of L-fuzzy subgroups, *Southeast Asian Bull. Math.* (5) **33** (2009) 913–916.
15. N. Ramakrishna and T. Eswarlal, A characterization of cyclic groups in terms of L-fuzzy subgroups II, *Southeast Asian Bull. Math.* (6) **33** (2009) 1171–1174.
16. J. Rotman, *An Introduction to the Theory of Groups. Fourth edition.*, Graduate Texts in Mathematics, 148. Springer-Verlag, New York, 1995.
17. W.R. Scott, Groups and cardinal numbers, *Amer. J. Math.* **74** (1952) 187–197.
18. F. Szász, On groups every cyclic subgroup of which is a power of the group, *Acta Math. Acad. Sci. Hungar.* **6** (1955) 475–477.
19. F. Szász, On groups of which all non-trivial powers are cyclic groups, *Magyar Tud. Akad. Mat. Fiz. Oszt. Közl.* **5** (1955) 491–492.
20. J. Thévenaz, A characterization of the cyclic groups, *Arch. Math. (Basel)* (3) **52** (1989) 209–211.
21. G. Walls, A characterization of finite cyclic groups, *An. Univ. Timisoara Ser. Math.-Inform.* (2) **42** 141–149.

