Groups whose subgroups have distinct cardinalities

Greg Oman[*]

February 15, 2014

Abstract

A standard undergraduate algebra exercise is to prove that distinct subgroups of a finite cyclic group G have distinct cardinalities. In this note, we study this property for groups in general (and we do not limit our focus to finite groups). In particular, we determine all groups G for which distinct subgroups of G have distinct cardinalities.

1 Introduction

Let G be a finite cyclic group. A popular exercise which appears in many algebra textbooks (see for example Hungerford [5], exercise 6 of section 1.3) is to prove that for any positive integer d which divides $|G|$, G has a unique subgroup of order d. Since (by Lagrange's Theorem) the order of every subgroup of a finite group divides the order of the group, it follows that distinct subgroups of G have distinct cardinalities.

Generalizing the above exercise, the purpose of this note is to investigate the following question: Which (possibly infinite) groups G have the following property (D)?

(D) Distinct subgroups of G have distinct cardinalities.

We begin the paper by supplying a solution to exercise 6 of section 1.3 of [5], that is, we prove that every finite cyclic group has property (D). Conversely, we invoke The Sylow Theorems to prove that if G is any finite group with property (D), then G is cyclic. We then shift our attention to infinite groups. We start by establishing that for any prime p, the quasi-cyclic group $\mathbb{Z}(p^\infty)$ has property (D) (this follows easily from well-known properties of $\mathbb{Z}(p^\infty)$). Subsequently, we show that every *abelian* group with property (D) is isomorphic to either $\mathbb{Z}/\langle n\rangle$ for some positive integer n or to $\mathbb{Z}(p^\infty)$ for some prime p. Finally, we invoke an old result of Baer to prove that every group G with property (D) is abelian, completing the classification of such groups.

[*]University of Colorado, Colorado Springs

In the final section, we examine some properties related to property (D), and show that there is a sense in which our work is very difficult to generalize. Specifically, let G be a group. Say that G has property (L) if the subgroups of G are linearly ordered under set-theoretic inclusion, property (C) if every subgroup of G is characteristic[1] in G, and property (N) if every subgroup of G is normal in G. Now consider the following conditions:

(1) G has property (L).
(2) G has property (D).
(3) G has property (C).
(4) G has property (N).

We show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) but that none of the implications can be reversed. We supply plausibility arguments showing that the problems of classifying the groups in (3) or (4) seem to be quite difficult. We then conclude the paper by rederiving the classical characterization of the groups which satisfy (1).

2 Finite cyclic groups have property (D)

As mentioned in the introduction, it is well-known that if G is a finite cyclic group, then distinct subgroups of G have distinct cardinalities (cf. [5], exercise 6 of section 1.3 and Lang [6], p. 24), that is, G has property (D). We begin the body of the paper by sketching a short proof of this fact.

Proposition 1. *Let G be a finite cyclic group. Then distinct subgroups of G have distinct cardinalities.*

Proof. Let $G := \langle g \rangle$ be a finite cyclic group of order m, and 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 $g^d = (g^k)^\alpha$, and hence $\langle g^d \rangle \subseteq \langle g^k \rangle$.

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

3 All finite groups with property (D) are cyclic

Let G be a finite group. In the previous section, we prove that if G is cyclic, then G has property (D). We now establish the converse (which is a deeper result)

[1] Recall that a subgroup H of G is a *characteristic* subgroup of G if and only if $\varphi[H] = H$ for every automorphism φ of G.

via the Sylow Theorems. We begin by recalling that if p is a prime which divides the order of G, then a subgroup H of G is said to be a *Sylow p-subgroup of G* provided $|H| = p^m$ for some non-negative integer m and p^{m+1} does not divide $|G|$. We now recall Sylow's famous results (for a proof, see Theorem 6.4, pp. 34-35 of [6]. We will not have occasion to make use of (3) below, but we list it for the sake of completeness.):

Proposition 2 (The Sylow Theorems)**.** *Let G be a finite group, and suppose that p is a prime which divides the order of G. Then:*

(1) *Every subgroup of G whose order is a power of p is contained in some Sylow p-subgroup of G.*

(2) *All Sylow p-subgroups of G are conjugate (that is, if H and K are Sylow p-subgroups of G, then there exists some $g \in G$ such that $K = gHg^{-1}$).*

(3) *Let n_p be the number of Sylow p-subgroups of G. Then $n_p \equiv 1 \bmod p$.*

It is easy to see that (2) implies that a Sylow p-subgroup H of G is normal if and only if it is unique.

We will soon be able to prove the assertion made in the title of this section. We first prove a lemma and then recall a fact from the literature.

Lemma 1. *Suppose that G is a group (which may be infinite) which satisfies property (D) (we remind the reader that this means that distinct subgroups of G have distinct cardinalities). Then every subgroup of G is normal.*

Proof. Assume that G is a group which has property (D), and let H be an arbitrary subgroup of G. We will prove that H is normal. Toward this end, let $g \in G$ be arbitrary. Now note that $gHg^{-1} := \{ghg^{-1} : g \in H\}$ is a subgroup of G and that $H \cong gHg^{-1}$ (this can be seen via that map $\varphi : H \to gHg^{-1}$ defined by $\varphi(h) := ghg^{-1}$). Thus $|H| = |gHg^{-1}|$. Since G has property (D), we conclude that $H = gHg^{-1}$, whence H is normal in G. □

Fact 1 (See [5], p. 96)**.** *Let G be a finite group, and assume that for every p dividing the order of G, every Sylow p-subgroup of G is normal (whence by the comment following Proposition 2, unique). Then G is the direct product of its Sylow p-subgroups.*

We now prove that every finite group with property (D) is cyclic. We would not be surprised if the following result is in the literature, but a quick check of the standard texts [4]–[6] did not reveal it.

Proposition 3. *Let G be a finite group with property (D). Then G is cyclic.*

Proof. Assume that G is a finite group and that G has property (D). 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 $|G|$. Lemma 1 yields that every Sylow p_i-subgroup of G is normal in G, whence is unique. For each i, $1 \leq i \leq k$, let G_i be the Sylow p_i-subgroup of G. Fact 1 gives us that

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

Now fix an i with $1 \le i \le k$. We will 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. Then clearly G_1 is the union of its *proper* subgroups. Let $\{H_1, H_2, \ldots, H_s\}$ be the collection of proper subgroups of G_1. For each i satisfying $1 \le i \le s$, it follows from Lagrange's Theorem that $|H_i| = p^j$ for some integer j satisfying $0 \le j < n$. As G has property (D), clearly so does G_1. We conclude that for each j with $0 \le j < n$, G_1 has *at most one* subgroup of order p^j (in fact, G_1 has a subgroup of order p^j for every j satisfying $0 \le j \le n$, but we do not need this fact). We deduce that

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

and we have reached a contradiction. Thus G_1 is cyclic, and we have

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

whence G is cyclic (the final isomorphism is a direct result of The Chinese Remainder Theorem; see also [6], p. 24). This completes the proof. $\square$

4 A class of infinite groups with property (D)

As the title of this section indicates, we will display an infinite collection of groups which have property (D). These groups are the so-called *quasi-cyclic groups*, and they are defined as follows.

Definition 1. *Let p be a prime. Then the quasi-cyclic group of type p^∞, denoted $\mathbb{Z}(p^\infty)$, is the subgroup of $\mathbb{Q}/\mathbb{Z}$ defined by:*

$$\mathbb{Z}(p^\infty) := \{\mathbb{Z} + \frac{a}{p^n} : a \in \mathbb{Z}, n \in \mathbb{Z}^+\}.$$

These groups play a fundamental and important role in abelian group theory, and we will have more to say about them later. For now, we are interested in establishing that every quasi-cyclic group $\mathbb{Z}(p^\infty)$ has property (D). We begin with a lemma (the following properties of the quasi-cyclic groups are well-known; see Fuchs [3], pp. 23-25. We present a proof for completeness.).

Lemma 2. *Let p be a prime. Then the following hold:*

(1) *$\mathbb{Z}(p^\infty)$ is infinite.*
(2) *Every element of $\mathbb{Z}(p^\infty)$ has finite order.*
(3) *For any $x, y \in \mathbb{Z}(p^\infty)$, either $\langle x \rangle \subseteq \langle y \rangle$ or $\langle y \rangle \subseteq \langle x \rangle$ (hence the subgroups of $\mathbb{Z}(p^\infty)$ are linearly ordered by inclusion).*
(4) *Every proper subgroup of $\mathbb{Z}(p^\infty)$ is finite*[2].

[2] In fact, every proper subgroup of $\mathbb{Z}(p^\infty)$ is cyclic of cardinality a power of p.

Proof. Let p be a prime.

(1) It is readily checked that for distinct positive integers i and j, $\mathbb{Z} + \frac{1}{p^i} \neq \mathbb{Z} + \frac{1}{p^j}$.

(2) Consider an arbitrary element $x := \mathbb{Z} + \frac{a}{p^n} \in \mathbb{Z}(p^\infty)$. Then simply note that $p^n x = 0$, and (2) is proved.

(3) Let $x, y \in \mathbb{Z}(p^\infty)$ be arbitrary. We will prove that either $\langle x \rangle \subseteq \langle y \rangle$ or $\langle y \rangle \subseteq \langle x \rangle$. If either $x = 0$ or $y = 0$, the result is patent, so assume that x and y are nonzero. Write $x := \mathbb{Z} + \frac{a}{p^m}$ and $y := \mathbb{Z} + \frac{b}{p^n}$ where $a, b \in \mathbb{Z}$ are both prime to p and m, n are positive integers. By elementary number theory, there exist integers c, d, e, and f such that

$$ca + dp^m = 1, \text{ and} \tag{3}$$

$$eb + fp^n = 1. \tag{4}$$

Thus $cx = \mathbb{Z} + \frac{ca}{p^m} = \mathbb{Z} + \frac{1-dp^m}{p^m} = \mathbb{Z} + (\frac{1}{p^m} - d) = \mathbb{Z} + \frac{1}{p^m}$. Analogously, $ey = \mathbb{Z} + \frac{1}{p^n}$. We conclude that

$$\langle x \rangle = \langle \mathbb{Z} + \frac{1}{p^m} \rangle, \text{ and} \tag{5}$$

$$\langle y \rangle = \langle \mathbb{Z} + \frac{1}{p^n} \rangle. \tag{6}$$

Without loss of generality, assume that $m \leq n$. Then simply note that $\mathbb{Z} + \frac{1}{p^m} = \mathbb{Z} + \frac{p^{n-m}}{p^n} \in \langle y \rangle$ (by (6) above), and thus $\langle x \rangle \subseteq \langle y \rangle$. We conclude that the subgroups of $\mathbb{Z}(p^\infty)$ are linearly ordered by inclusion.

(4) Let H be a proper subgroup of $\mathbb{Z}(p^\infty)$. We will show that H is finite. Toward this end, let $x \in \mathbb{Z}(p^\infty) - H$. We conclude from (3) that $H \subseteq \langle x \rangle$. It now follows from (2) that H is finite. □

We conclude this section by showing that the quasi-cyclic groups possess property (D).

Proposition 4. *Let p be a prime. Then the quasi-cyclic group $\mathbb{Z}(p^\infty)$ has property (D).*

Proof. Let H and K be subgroups of $\mathbb{Z}(p^\infty)$ of the same cardinality. We will show that $H = K$. By (3) of Lemma 2, we may assume that $H \subseteq K$. Suppose first that K is infinite. Since $|H| = |K|$ and (by (4) of Lemma 2) all proper subgroups of of $\mathbb{Z}(p^\infty)$ are finite, we deduce that $H = K = \mathbb{Z}(p^\infty)$. Suppose now that K is finite. As $H \subseteq K$ and $|H| = |K|$, we see that $H = K$, concluding the proof. □

5 A classification of all groups with property (D)

We have seen that every finite cyclic group as well as every quasi-cyclic group has property (D). In this section, we will prove that these constitute all groups with this property. We begin by settling the abelian case, and then we prove that every group with property (D) is abelian.

Let p be a prime and let G be an abelian group. Then G is *p-divisible* provided $pG = G$ (that is, $\{pg : g \in G\} = G$). Moreover, G is *divisible* if $nG = G$ for every positive integer n. It is easy to check that G is divisible if and only if G is p-divisible for every prime p. We will need the following lemma (this is exercise 2 on p. 67 of [3]).

Lemma 3. *Let G be an abelian group. Then G is either divisible or has a maximal subgroup.*

Proof. Suppose that G is an abelian group which is not divisible. We will prove that G has a maximal subgroup. Since G is not divisible, there is some prime p such that G is not p-divisible. Thus $pG \subsetneq G$. It follows that G/pG is a nonzero vector space over the field $\mathbb{Z}/\langle p\rangle$, and hence we obtain the following sequence of surjections:

$$G \to G/pG \to \mathbb{Z}/\langle p\rangle. \tag{7}$$

Composing, we get a surjective group homomorphism $\varphi : G \to \mathbb{Z}/\langle p\rangle$. If K is the kernel of this map, then $G/K \cong \mathbb{Z}/\langle p\rangle$. Since $\mathbb{Z}/\langle p\rangle$ has exactly two subgroups, it follows that there are exactly two subgroups of G containing K, whence K is a maximal subgroup of G. □

We will also make use of the following theorem, which describes the structure of divisible abelian groups. (see [3], Theorem 19.1 for a proof).

Proposition 5 (Structure Theorem for Divisible Abelian Groups)**.** *Let G be an abelian group. Then G is divisible if and only if there is a collection $\{G_i : i \in I\}$ of abelian groups such that*

(1) *For every i, either $G = \mathbb{Q}$ or $G = \mathbb{Z}(p^\infty)$ for some prime p.*

(2) $G \cong \bigoplus_{i\in I} G_i$.[3]

We now classify the abelian groups with property (D).

Proposition 6. *Let G be an abelian group. Then G has property (D) if and only if G is either a finite cyclic group or a quasi-cyclic group.*

Proof. We saw in Proposition 1 and Proposition 4 that finite cyclic groups and quasi-cyclic groups have property (D). Now let G be an arbitrary abelian group with property (D). If G is finite, then G is cyclic by Proposition 3. Now assume

[3]We remind the reader that the direct sum $\bigoplus_{i\in I} G_i$ is the group whose ground set is the set of all sequence $(g_i : i \in I)$ with the property that $g_i \in G_i$ for each i and all but finitely many of the g_i are equal to 0. Further, $(g_i : i \in I) + (h_i : i \in I) := (g_i + h_i : i \in I)$.

that G is infinite. We claim that G is divisible. If not, then Lemma 3 yields that G has a maximal subgroup M. But then G/M is simple, whence $G/M \cong \mathbb{Z}/\langle p \rangle$ for some prime p. But then M has finite index in G. It follows from basic cardinal arithmetic that $|M| = |G|$, contradicting that G has property (D). We conclude that G is divisible. By The Structure Theorem for Divisible Abelian Groups, $G \cong \bigoplus_{i \in I} G_i$, where for each i, $G_i = \mathbb{Q}$ or $G_i = \mathbb{Z}(p^\infty)$ for some prime number p. We claim that $|I| = 1$. Otherwise, simply delete a summand, and we obtain a proper subgroup H of G of the same cardinality as G, contradicting that G has property (D). Hence $|I| = 1$, and $G \cong \mathbb{Q}$ or $G \cong \mathbb{Z}(p^\infty)$ for some prime p. Clearly $\mathbb{Q}$ does not have property (D) (since $\mathbb{Z}$ is a proper infinite subgroup of $\mathbb{Q}$), whence $G \cong \mathbb{Z}(p^\infty)$ for some prime p. □

To complete our classification, it suffices to show that every group with property (D) is abelian. Toward this end, we employ a classical result of Baer (whose proof is beyond the scope of this paper).

Proposition 7 (Baer [1])**.** *Suppose that G is nonabelian and that every subgroup of G is normal. Then there is a torsion abelian group P (that is, all elements of P have finite order) with no elements of order 4 such that $G \cong Q_8 \times P$, where Q_8 is the quaternion group with 8 elements*[4]*.*

We conclude this section with the following theorem which, along with Proposition 6, yields a complete description of the groups with property (D).

Theorem 1. *Every group with property (D) is abelian. Thus a group G has the property that distinct subgroups of G have distinct cardinalities if and only if G is finite cyclic or quasi-cyclic.*

Proof. Suppose by way of contradiction that G is a nonabelian group with property (D). Then Lemma 1 tells us that every subgroup of G is normal. By Baer's result above, $G \cong Q_8 \times P$ for some group P. Since subgroups of G clearly inherit property (D), we conclude that Q_8 has property (D). But Q_8 has three subgroups of order 4 (namely $\{1, -1, i, -i\}$, $\{1, -1, j, -j\}$, and $\{1, -1, k, -k\}$), and we have reached a contradiction. □

We conclude the section by remarking that Baer's result along with The Fundamental Theorem of Finitely Generated Abelian Groups yields a very short proof of Proposition 3. However, we find it interesting that an undergraduate-level proof exists, which is why we included it in this paper.

6 Remarks on possible generalizations

The primary objective of the remainder of this paper is to illustrate difficulties which arise if one attempts to generalize (in a natural way) the classification of groups with property (D). To wit, let G be a group. Then (as stated in the introduction) say that G has property (L) if the subgroups of G are linearly

[4] Q_8 is given by the presentation $Q_8 := \langle -1, i, j, k | (-1)^2 = 1,\ i^2 = j^2 = k^2 = ijk = -1 \rangle$.

ordered under set-theoretic inclusion, property (C) if every subgroup of G is characteristic in G, and property (N) if every subgroup of G is normal in G. Now consider the following conditions:

(1) G has property (L).
(2) G has property (D).
(3) G has property (C).
(4) G has property (N).

Then the following relationships hold:

Proposition 8. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4)*, but none of the implications can be reversed.*

Proof. Let G be a group.

(1) $\Rightarrow$ (2): It is readily checked (as in the proof of Lemma 2) that if G has property (L), then all proper subgroups of G are finite. It is now easy to see that G has property (D). To see that the implication cannot be reversed, simply note that $\mathbb{Z}/\langle 6\rangle$ has property (D) but not property (L) (since it has a subgroup H of order 2 and a subgroup K of order 3; by Lagrange's Theorem, K cannot contain H).

(2) $\Rightarrow$ (3): Suppose G has property (D). If $\varphi : G \to G$ is an automorphism and H is a subgroup of G, simply note that $|H| = |\varphi[H]|$, whence $H = \varphi[H]$ since G has property (D), and we see that H is a characteristic subgroup of G. The group $\mathbb{Z}(2^\infty) \oplus \mathbb{Z}(3^\infty)$ has property (C) but not property (D). That $\mathbb{Z}(2^\infty) \oplus \mathbb{Z}(3^\infty)$ has property (C) follows quickly from the fact that $\mathbb{Z}(2^\infty) \oplus \mathbb{Z}(3^\infty)$ is a subgroup of $\mathbb{Q}/\mathbb{Z}$, and distinct subgroups of $\mathbb{Q}/\mathbb{Z}$ are not isomorphic (whence this property is inherited by $\mathbb{Z}(2^\infty) \oplus \mathbb{Z}(3^\infty)$); see [3], pp. 23-25 and p. 68, exercise 25 for further details.

(3) $\Rightarrow$ (4): Suppose that G has property (C), and let H be a subgroup of G. For any $g \in G$, the map $\varphi : G \to G$ defined by $\varphi(x) := gxg^{-1}$ is an automorphism of G. Since G has property (C), we conclude that $\varphi(H) = gHg^{-1} = H$, whence H is normal in G. To see that the implication cannot be reversed, simply consider the group $G := \mathbb{Z}/\langle 2\rangle \times \mathbb{Z}/\langle 2\rangle$. As G is abelian, G has property (N), yet $\mathbb{Z}/\langle 2\rangle \times \{0\}$ is not characteristic since it is not mapped into itself via the automorphism $(x, y) \mapsto (y, x)$. $\square$

We now address the following (somewhat vague) question: Can our work be generalized by classifying the groups in (3) or (4) above? At present, it seems the answer is 'no'. More specifically, note that every abelian group has property (N), and the class of abelian groups is much too monstrous to yield to a classification theorem (even the subgroups of $\mathbb{Q} \times \mathbb{Q}$ are not completely understood). But can we dispose of (3)? It turns out that there are examples of abelian groups G with extremely complicated structure for which the inversion map is the only non-trivial automorphism of G (see p. 592 of Cutolo, Smith, and Wiegold [2], for example); any such group G clearly satisfies property (C).

So it seems that a classification of the groups in (3) is presently out of reach as well.

We conclude the paper with a corollary which characterizes the quasi-cyclic groups.

Corollary 1. *Let G be an infinite group. Then the following are equivalent*[5]*:*

(1) $G \cong \mathbb{Z}(p^\infty)$ *for some prime* p*.*

(2) *The subgroups of* G *are linearly ordered by inclusion.*

(3) *Distinct subgroups of* G *have distinct cardinalities.*

Proof. Let G be an infinite group.

(1) $\Rightarrow$ (2): See (3) of Lemma 2.

(2) $\Rightarrow$ (3): This is the implication "(1) $\Rightarrow$ (2)" of Proposition 8.

(3) $\Rightarrow$ (1): Immediate from Theorem 1. □

References

[1] R. Baer, *Situation der untergruppen und struktur der gruppe,* S. B. Heidelberg. Akad. Wiss., Vol. 2, pp 12–17, 1933.

[2] G. Cutolo, H. Smith, and J. Wiegold, *Finiteness conditions on characteristic closures and cores of subgroups,* J. Group Theory, Vol. 12, pp 591–610, 2009.

[3] Fuchs, L., "Abelian Groups", Publishing House of the Hungarian Academy of Sciences, Budapest, 1958.

[4] Herstein, I.N., "Topics in Algebra", Blaisdell, Waltham, 1964.

[5] Hungerford, T., "Algebra", Springer, New York, 1974.

[6] Lang, S., "Algebra. Revised third edition", Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[7] Lotto, B., *Stacked groups,* Amer. Math. Monthly, Vol. 114, No. 9, pp 811–812, 2007.

About the author:

Greg Oman

Greg is an assistant professor of mathematics at The University of Colorado, Colorado Springs. He works in a number of areas, but specializes in ring theory,

[5] The equivalence of (1) and (2) is well-known; we refer the reader to Lotto [7] for a self-contained proof.

semigroup theory, and universal algebra. Though he misses his family and friends (and The Sweet!) back in Ohio, he is loving the beautiful mountains, the 300 plus days of sunshine per year, and the lack of humidity.

University of Colorado, Colorado Springs, Colorado, 80918.
goman@uccs.edu