As an immediate corollary we have that S_3, the symmetric group of degree 3, is isomorphic to D_3.

Acknowledgment. I wish to thank the referees for their comments.

REFERENCES

1. Joseph A. Gallian, *Contemporary Abstract Algebra, 4th ed.*, Houghton Mifflin, Boston, MA 1998.
2. W. Keith Nicholson, *Introduction to Abstract Algebra*, PWS-Kent, Boston, MA 1993.
3. Achilleas Sinefakopoulos, On groups of order p^2, this MAGAZINE **70** (1997), 212–213.

A Characterization of Infinite Cyclic Groups

CHARLES LANSKI
University of Southern California
Los Angeles, CA 90089-1113

Introduction We prove an interesting and nontrivial characterization of infinite cyclic groups, using only basic notions about groups: orders of elements, cyclic groups, cosets, commutators, and quotients.

THEOREM 1. *An infinite group is cyclic when each of its nonidentity subgroups has finite index.*

Why should we expect the number of cosets of subgroups to be crucial in determining the structure of infinite groups? An observation about cosets of subgroups of cyclic groups will motivate the theorem, but first we recall the definition of a cyclic group. For $\mathbb{Z} = (\mathbb{Z}, +)$ the group of integers under addition, G any group, and $g \in G$, let $\langle g \rangle = \{g^k \in G \mid k \in \mathbb{Z}\}$ denote the cyclic subgroup of G generated by g. A group G is called *cyclic* when $G = \langle g \rangle$ for some $g \in G$.

An important property of a cyclic group $G = \langle g \rangle$ is that each of its subgroups is cyclic and has the form $\langle g^m \rangle$ ([**2**, p. 59] or [**3**, p. 75]). The subgroups of $(\mathbb{Z}, +)$ are the $n\mathbb{Z} = \{nk \in \mathbb{Z} \mid k \in \mathbb{Z}\} = \langle n \rangle$ (the group operation is addition!) for all nonnegative integers n. When $n \geq 1$ the cosets of $n\mathbb{Z}$ in $\mathbb{Z}$, giving the integers modulo n, are $n\mathbb{Z}, n\mathbb{Z} + 1, n\mathbb{Z} + 2, \ldots,$ and $n\mathbb{Z} + (n-1)$, so $n\mathbb{Z}$ has exactly n distinct cosets in $\mathbb{Z}$. This simple but key observation is a special case of a result about cosets of subgroups in an arbitrary cyclic group which we state below.

A test to show groups are not cyclic When the collection $\{Hg \mid g \in G\}$ of all right cosets of a subgroup H in a group G is finite, we let $[G : H]$ denote the number of distinct cosets and call $[G : H]$ the *index* of H in G.

PROPOSITION. *Every nonidentity subgroup of a cyclic group has finite index.*

Proof. Let the cyclic group be $G = \langle g \rangle$ and let a nonidentity subgroup be $H = \langle g^m \rangle$ for some $m \geq 1$. We claim that $H = He, Hg, \ldots, Hg^{m-1}$ are all of the right cosets of H in G. Any right coset of H in G is Hg^t for some $t \in \mathbb{Z}$. Use the division algorithm in the integers to write $t = qm + r$ with $0 \leq r < m$. Since $(g^m)^z \in H$ for all $z \in \mathbb{Z}$, it follows that $Hg^t = H(g^m)^q g^r = Hg^r$. ∎

The fact that every nonidentity subgroup of a cyclic group has finite index is not very surprising, especially for finite groups! However, we can use the Proposition to show that certain groups are not cyclic. Our examples and some later arguments require this important fact: for any group G and subgroup H, $Hx = Hy$ exactly when $xy^{-1} \in H$ ([**2**, p. 81] or [**3**, p. 133]). An easy but useful application is that $Hx = H = He$ exactly when $x \in H$.

Example 1. $G = \mathbb{Z} \oplus \mathbb{Z}$ is not cyclic.

Consider the subgroup $H = \mathbb{Z} \oplus \langle 0 \rangle$ and the collection $\{H + (0, z) \mid z \in \mathbb{Z}\}$ of right cosets. If two of these cosets were equal, say $H + (0, z) = H + (0, z')$, for some $z, z' \in \mathbb{Z}$ then we would have $(0, z) - (0, z') = (0, z - z') \in H$ forcing $z = z'$. Therefore different elements of $\mathbb{Z}$ give rise to different cosets $H + (0, z)$ of H in G. Since there are infinitely many cosets and $H \neq \langle e_G \rangle$, we must conclude from the Proposition that G is not cyclic.

Example 2. $(\mathbb{Q}, +)$ is not cyclic.

Consider the cosets $\{\mathbb{Z} + 1/p \mid p \text{ is a prime}\}$ of the subgroup $\mathbb{Z}$ of $\mathbb{Q}$. If $\mathbb{Z} + 1/p = \mathbb{Z} + 1/q$ for different primes p and q, then we must have $1/p - 1/q = (q - p)/pq \in \mathbb{Z}$. Thus $q - p = pqz$ for some $z \in \mathbb{Z}$. This is impossible, since then each prime would divide the other. Hence there are infinitely many cosets of $\mathbb{Z}$ in $(\mathbb{Q}, +)$, at least one for each prime, so as in Example 1 $(\mathbb{Q}, +)$ cannot be cyclic by the Proposition.

Exercise. Show that the group $(\mathbb{Q}^+, \cdot)$ of positive rationals under multiplication is not cyclic.

Exercise. Show that the subgroup $G = \{(a, b, c) \in \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \mid a + b + c = 0\}$ of $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$ is not cyclic.

About the theorem and its proof The converse of the Proposition for infinite groups is THEOREM 1. Of course the converse of a true statement need not be true, so why should we expect THEOREM 1 to be true? A counterexample does not seem easily found, and while this is not exactly convincing evidence for the truth of the assertion, it does make it more reasonable. In fact, Y. Fedorov [**1**] proved THEOREM 1 in 1951, but his result is not widely known. Although the statement of THEOREM 1 is quite elementary, its proof is not obvious, at least by elementary methods. The utility of the result itself is questionable since it is hard to see how we would know that each subgroup of a given infinite group has finite index. However, the result is appealing because of its simplicity and the definitive nature of the characterization it gives. Aside from this, it provides a nice example of how basic notions about groups, which are covered in a first abstract algebra course, can be combined to prove a nonstandard and pretty result about infinite groups.

Fedorov's theorem is not commonly found in textbooks, but a proof appears in W. R. Scott's Group Theory [**5**, p. 446], using rather sophisticated results, including the fundamental theorem of abelian groups, the transfer map, and results on FC-groups. Our goal is to present a proof using only basic facts and ideas about groups.

We will recall the relevant definitions as they are needed, but start with a description of our approach. There are two main steps. First we show that THEOREM 1 holds when G is abelian, and then observe that G must be "almost abelian": its center has finite index. Using this, the second step proves and applies an interesting result of I. Schur,

which shows that the commutator subgroup of G must be finite. This will result in a contradiction when G is not abelian. Let us begin the argument.

Throughout the proof, we will assume that G is an infinite group and if H is any nonidentity subgroup of G then $[G : H]$ is finite. We write $H \leq G$ when H is a subgroup of G, and when the order of $g \in G$ is finite we denote it by $o(g)$.

The proof for abelian groups Our first lemma concerns orders of elements and intersections of cyclic subgroups in G.

LEMMA 1.

(i) If $H \leq G$, then either $H = \langle e \rangle$ or H is infinite.

(ii) If $g \in G \setminus \{e\}$, then g has infinite order.

(iii) If $x, y \in G \setminus \{e\}$, then $\langle x \rangle \cap \langle y \rangle = \langle x^a \rangle = \langle y^b \rangle$ for some $a, b \in \mathbb{Z} \setminus \{0\}$.

Proof. For (i), if $H \neq \langle e \rangle$ then by our basic assumption $[G : H]$ is finite. Thus G is the union of finitely many right cosets of H, say $G = Hg_1 \cup \cdots \cup Hg_k$. If H is finite then each of these Hg_i has the same number of elements as H, as in the proof of Lagrange's theorem (see [**2**], [**3**], or [**4**]), and this forces G to be finite. Hence, H must be infinite. Now (i) implies (ii) since $H = \langle g \rangle \leq G$, and $\langle g \rangle$ is finite when $o(g)$ is finite ([**2**, p. 56] or [**3**, p. 72]). In (iii), the set $\{\langle x \rangle y^i \mid i \in \mathbb{Z}\}$ of cosets of $\langle x \rangle$ in G must be finite, so $\langle x \rangle y^i = \langle x \rangle y^j$ for some $i > j$. This forces $y^{i-j} = y^i (y^j)^{-1} \in \langle x \rangle$ and shows that $y^{i-j} \in \langle x \rangle \cap \langle y \rangle$. Now $y^{i-j} \neq e$ since by (ii) $y \in G \setminus \langle e \rangle$ has infinite order. Therefore $\langle x \rangle \cap \langle y \rangle$ is a nonidentity subgroup of both $\langle x \rangle$ and $\langle y \rangle$, so $\langle x^a \rangle = \langle x \rangle \cap \langle y \rangle = \langle y^b \rangle$ with both $a, b \in \mathbb{Z} \setminus \{0\}$ ([**2**, p. 59] or [**3**, p. 75]). ∎

We need another lemma about indices of subgroups in order to prove THEOREM 1 for abelian groups. The lemma is a consequence of the multiplicative property of indices which is easy to prove for finite groups by using Lagrange's theorem ([**2**, p. 91], [**3**, p. 143] or [**4**, p. 41]).

LEMMA 2. *In any group A, let $H \leq K \leq A$ with $[A : H]$ finite. If $H \neq K$ then $[A : K] < [A : H]$.*

Proof. Let $Ha_1, \ldots, Ha_m$ be the distinct right cosets of H in A, so $A = Ha_1 \cup \cdots \cup Ha_m$. We may assume that $a_1 = e$. Now $Ha_j \subseteq Ka_j$ for each j implies that $A = Ka_1 \cup \cdots \cup Ka_m$. It follows that for any $g \in G$, $g \in Ka_j$ for some j, and so $Kg = Ka_j$. Thus $\{Ka_i\}$ contains all the right cosets of K in G. We want to show that $Ka_i = Ka_j$ for $i \neq j$. There is some $k \in K \setminus H$, and since $k \in A$, $k \in Ha_s$ for some $s > 1$. Therefore $a_s \in Hk \subseteq K$, so $Ka_s = K = Ke = Ka_1$ and $[A : K] < m = [A : H]$. ∎

LEMMA 3. *If G as above is an abelian group then G is cyclic.*

Proof. Let G be an abelian group. If $h \in G \setminus \langle e \rangle$ then $[G : \langle h \rangle]$ is finite, so there must be $x \in G$ for which $[G : \langle x \rangle]$ is minimal. If $\langle x \rangle = G$ the proof is finished, so assume that $y \in G \setminus \langle x \rangle$. From Lemma 1 we have that $x^s = y^k$ for some $s, k \in \mathbb{Z} \setminus \{0\}$. Set $\gcd(s, k) = d$ and suppose that $d > 1$. Write $k = da$, $s = db$, and use $xy = yx$ to get $(y^a x^{-b})^d = y^{ad} x^{-bd} = y^k x^{-s} = e$. Any nonidentity element of G has infinite order by Lemma 1, forcing $y^a = x^b$. However, $gcd(a, b) = 1$, so we may assume from the start that $d = 1$, and therefore that $1 = uk + vs$ for some $u, v \in \mathbb{Z}$ (see [**2**], [**3**], or [**4**]). Now set $g = y^v x^u$. Using again the fact that $xy = yx$, we compute that $g^k = y^{vk} x^{uk} = (y^k)^v x^{uk} = x^{sv} x^{uk} = x^{vs+uk} = x$. Similarly $g^s = y^{vs} x^{us} = y^{vs} (x^s)^u = y^{vs} y^{ku} = y^{vs+uk} = y$. These computations show that $x, y \in \langle g \rangle$; thus $\langle x \rangle \leq \langle g \rangle$ but $\langle x \rangle \neq \langle g \rangle$. By Lemma 2 $[G : \langle g \rangle] < [G : \langle x \rangle]$, contradicting the minimality of $[G : \langle x \rangle]$. Therefore, $y \in G \setminus \langle x \rangle$ is impossible, so $G = \langle x \rangle$ is cyclic. ∎

To prepare for the final step in the proof of THEOREM 1 we need to see that G is not far from being abelian, in the sense that its center has finite index. Recall that the *center* of G is $Z(G) = \{x \in G \mid xg = gx \text{ for all } g \in G\}$. It is straightforward to prove that $\langle e \rangle \leq Z(G) \leq G$.

LEMMA 4. *$Z(G) \neq \langle e \rangle$, so $[G : Z(G)]$ is finite.*

Proof. Let $g \in G \backslash \langle e \rangle$. Our basic assumption shows that $G = \langle g \rangle x_1 \cup \cdots \cup \langle g \rangle x_k$ for some $x_1 = e, x_2, \ldots, x_k \in G$. By Lemma 1, for each $1 \leq i \leq k$ there is some positive power $m(i)$ of g with $g^{m(i)} \in \langle x_i \rangle$. Set $m = m(1) \ldots m(k)$ and write $m = m(i)c(i)$. Then $g^m = (g^{m(i)})^{c(i)} \in \langle x_i \rangle$ for all x_i, which forces $g^m x_i = x_i g^m$. But G is the union of the various $\langle g \rangle x_j$, so for any $h \in G$, $h \in \langle g \rangle x_i$ for some i. Thus $h = g^t x_i$ for some $t \in \mathbb{Z}$ and now $g^m h = h g^m$, so we must have $g^m \in Z(G)$. In view of Lemma 1, $g^m \neq e$. Therefore $Z(G) \neq \langle e \rangle$ and it follows that $[G : Z(G)]$ is finite. ∎

A theorem of Schur Suppose we could show that Lemma 4 forces G to have a finite nonidentity subgroup when G is not abelian. Since G cannot have a finite nonidentity subgroup by Lemma 1, it must be abelian, so applying Lemma 3 would finish the proof. The most direct way to use Lemma 4 to produce a finite subgroup of G is to cite a result of I. Schur [**5**, p. 443] involving the *commutator* G' of G, i.e., the subgroup of G generated by all $x^{-1}y^{-1}xy$ for $x, y \in G$. Thus G' is the collection of all finite products of the $x^{-1}y^{-1}xy$ and their inverses. Standard facts about G' are that it is normal in G and that the quotient group G/G' is abelian ([**2**, p. 171] or [**4**, p. 65]).

Schur's result states that G' is finite when $[G : Z(G)]$ is finite. This pretty theorem is fairly well known, but it is not found in the standard introductory algebra texts, or even in many group theory texts. Its proof in [**5**] uses results on FC-groups. We provide an elementary and standard computational proof.

THEOREM 2 (SCHUR). *In any group A, if $[A : Z(A)] = k$ is finite then the commutator A' is finite.*

Proof. The proof is in 3 steps.

Step 1. There are only finitely many simple commutators $g^{-1}h^{-1}gh$ with $g, h \in A$. Let the distinct cosets of $Z(A)$ in A be $\{Z(A)a_1, \ldots, Z(A)a_k\}$. Then any $g \in A$ may be written $g = za_j$ for some $z \in Z(A)$ and some a_j. It follows from this and the definition of $Z(A)$ that, for $g, h \in A$ and some i and j, the simple commutator $g^{-1}h^{-1}gh = z_1^{-1}a_i^{-1}z_2^{-1}a_j^{-1}z_1 a_i z_2 a_j = a_i^{-1}a_j^{-1}a_i a_j$, and so there are only finitely many such.

Observe that $y^{-1}a_i^{-1}a_j^{-1}a_i a_j y = (y^{-1}a_i y)^{-1}(y^{-1}a_j y)^{-1}(y^{-1}a_i y)(y^{-1}a_j y)$, so every conjugate of a simple commutator is a simple commutator. Also note that, since $Z(A)$ a normal subgroup of A of index k, the quotient $A/Z(A)$ is a group of order k, so $g^k \in Z(A)$ for each $g \in A$ ([**2**, p. 91], [**3**, p. 136], or [**4**, p. 43]).

Step 2. For $g, h \in A$ and $n \geq 1$, $(g^{-1}h^{-1}gh)^n = ((hg)^{-1})^n (gh)^n c_1 c_2 \ldots c_{n-1}$, where each c_j is a simple commutator. If $n = 1$ then $g^{-1}h^{-1}gh = (hg)^{-1}gh$ as required. Assume the claim holds for the exponent $n \geq 1$. Then

$$\begin{aligned}
(g^{-1}h^{-1}gh)^{n+1} &= (g^{-1}h^{-1}gh)^n (g^{-1}h^{-1}gh) \\
&= ((hg)^{-1})^n (gh)^n c_1 c_2 \cdots c_{n-1} (hg)^{-1}(gh) \\
&= ((hg)^{-1})^{n+1} (gh)^{n+1} (gh)^{-n-1} (hg)(gh)^n c_1 \cdots c_{n-1} (hg)^{-1}(gh) \\
&= ((hg)^{-1})^{n+1} (gh)^{n+1} ((gh)^{-1}((gh)^{-n}(hg)(gh)^n (hg)^{-1})(gh)) \cdot \\
&\quad y^{-1}c_1 y y^{-1} c_2 y \cdots y^{-1} c_{n-1} y,
\end{aligned}$$

where $y = (hg)^{-1}(gh)$. By our observation just above, each $y^{-1}c_j y = d_{j+1}$ is a simple commutator, $(gh)^{-n}(hg)(gh)^n(hg)^{-1}$ is a simple commutator by definition, and its conjugate by gh, namely $d_1 = (gh)^{-1}((gh)^{-n}(hg)(gh)^n(hg)^{-1})(gh)$, is a simple commutator. Therefore we can write $(g^{-1}h^{-1}gh)^{n+1} = ((hg)^{-1})^{n+1}(gh)^{n+1}d_1d_2\ldots d_n$ with each d_i a simple commutator, and the claim holds by induction.

Using Step 1, assume that there are exactly m simple commutators.

Step 3. Any product of simple commutators is equal to a product of at most $m(k-1)$ simple commutators. Consider any product of $s \geq m(k-1)+1$ simple commutators. Since there are only m different simple commutators, one of them, say c, must appear at least k times in the product. Write the product as $g_1cg_2c\cdots g_kcg_{k+1}$ where each g_j is a product of simple commutators or is the identity of A, and the number of simple commutators appearing in all the g_j is $s-k$, including multiplicity. Now write

$$g_1cg_2c\cdots g_kcg_{k+1} = c^k(c^{-k}g_1c^k)(c^{-(k-1)}g_2c^{k-1})\cdots(c^{-2}g_{k-1}c^2)(c^{-1}g_kc)g_{k+1},$$

and observe that if g_j is a product of t simple commutators, then so is $c^{-i}g_jc^i$, using $y^{-1}uv\cdots wy = y^{-1}uyy^{-1}vy\cdots y^{-1}wy$ and our observation that a conjugate of a simple commutator is a simple commutator. Thus, we have $g_1cg_2c\cdots g_kcg_{k+1} = c^kh_1h_2\cdots h_{s-k}$ with each h_j a simple commutator. If $c = b^{-1}a^{-1}ba$, use Step 2 to rewrite

$$g_1cg_2c\cdots g_kcg_{k+1} = ((ab)^{-1})^k(ba)^kd_1\cdots d_{k-1}h_1\cdots h_{s-k},$$

with all d_j and h_j simple commutators. Since $(ba)^k \in Z(A)$, as we saw above, it follows that $(ba)^k = b^{-1}(ba)^kb = (ab)^k$, so $((ab)^{-1})^k(ba)^k = e$. Consequently, $g_1cg_2c\cdots g_kcg_{k+1} = d_1\cdots d_{k-1}h_1\cdots h_{s-k}$ is a product of $s-1$ simple commutators. This argument may be repeated as long as we have more than $m(k-1)$ simple commutators, and so produces a product of at most $m(k-1)$ simple commutators which is equal to the product of the s simple commutators to start with.

Since $(g^{-1}h^{-1}gh)^{-1} = h^{-1}g^{-1}hg$, the inverse of a simple commutator is again a simple commutator. Therefore, the elements in A' are just all finite products of simple commutators. Using Step 3, there are only finitely many such products since all the products of at most $m(k-1)$ of the m simple commutators will give all possible finite products of simple commutators, completing the proof. ∎

The proof of Theorem 1 We put the preceding pieces together to complete the proof of THEOREM 1. Using Lemma 4 we see that $[G : Z(G)] = k$ is finite, and now Schur's theorem yields that G' is finite. But the only finite subgroup of G is $\langle e\rangle$ by Lemma 1, so $G' = \langle e\rangle$. Thus, for all $g, h \in G$, $g^{-1}h^{-1}gh = e$, or equivalently $gh = hg$, and G is abelian. We conclude that G is cyclic from Lemma 3.

REFERENCES

1. Y. Fedorov, On infinite groups of which all nontrivial subgroups have a finite index, *Uspekhi Mat. Nauk.* 6 (1951), 187–189.
2. D. S. Dummit and R.M. Foote, *Abstract Algebra,* 2nd edition, Prentice-Hall, Upper Saddle River, NJ, 1999.
3. J. Gallian, *Contemporary Abstract Algebra*, 4th edition, Houghton Mifflin, New York, NY, 1998.
4. I. N. Herstein, *Topics in Algebra*, 2nd edition, Xerox College Publishing, Toronto, Ontario, Canada, 1975.
5. W. R. Scott, *Group Theory*, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1964.