When is Zn the only group of order n?

El. Math. *48* (1993)

0013-6018/93/030117-03$1.50 + 0.20/0

When is Z_n the only Group of Order n?

Joseph A. Gallian and David Moulton

Joseph Gallian received a Ph.D. degree from the University of Notre Dame in 1971 and has been at the University of Minnesota, Duluth since 1972. He is the author of over 50 papers and one book. He has received the Allendoerfer Award for exposition from the Mathematical Association of America and is an associate editor of the American Mathematical Monthly.

David Moulton received a B.A. degree from the University of California at Berkeley in 1989. He is currently a National Science Foundation Fellow at Berkeley working on a Ph.D. thesis under H.W. Lenstra. For the past four years he has assisted Professor Gallian with a summer undergraduate research program at Duluth.

It is an immediate corollary of Lagrange's Theorem that Z_n is the only group of order n when n is prime. In contrast, when $n = pq$, where p and q are primes, Z_n may or may not be the only group of order n. For example, Z_{15} is the only group of order 15 while there are two groups of order 21. So, how does one tell if Z_{pq} is the only group of order pq? The answer, as can be found in several undergraduate abstract algebra textbooks, is if and only if q does not divide $p - 1$ where $p > q$. (See, for instance, [7, p. 204].) Moving to three primes, both [3, p. 213] and [4, p. 335] show that $Z_{3\cdot5\cdot17}$ is the only

Eine der einfachsten Invarianten, welche einer Gruppe G zugeordnet werden können, ist deren Ordnung, also die Anzahl der in G enthaltenen Elemente. Tieferliegende Eigenschaften der Gruppe hängen oft auf nichttriviale Weise mit dieser natürlichen Zahl zusammen. Zum Beispiel lernt man als eines der ersten Resultate der Gruppentheorie, dass eine Gruppe von Primzahlordnung zyklisch ist und, da sie keine echten Normalteiler enthält, auch einfach. Ein um Grössenordnungen tiefer liegendes Resultat ist der Satz von W. Feit und J.G. Thompson (1963): Eine nichtabelsche Gruppe, deren Ordnung ungerade ist, besitzt einen echten Normalteiler, ist also insbesondere nicht einfach (sie ist sogar auflösbar). Im allgemeinen ist der Zusammenhang zwischen der Ordnung einer Gruppe und ihren Eigenschaften allerdings sehr unübersichtlich: Zur Ordnung 60 beispielsweise gibt es mehrere nichtisomorphe Gruppen; darunter befinden sich *zyklische*, nichtzyklische *abelsche*, ferner *nichtabelsche* und unter letzteren sogar eine *einfache* nichtabelsche. — In ihrer Arbeit beantworten Gallian und Moulton mit ganz einfachen Mitteln eine Fragestellung der erwähnten Art: Für welche Zahlen n ist jede Gruppe der Ordnung n zyklisch? *ust*

group of order $3 \cdot 5 \cdot 17$ as an application of the Sylow theorems and [3, p. 215] gives $n = 5 \cdot 7 \cdot 47$ as an exercise. In contrast, there are four groups of order $2 \cdot 3 \cdot 11$ (see [4, p. 337]).

In view of these examples it would be quite natural in an abstract algebra class to raise the following question: What is a necessary and sufficient condition on n so that Z_n is the unique group of order n? The answer is surprisingly simple and can be verified with no more theory than that which is contained in some undergraduate abstract algebra texts. As an added bonus for an instructor of an abstract algebra class, the proof illustrates one of the most important techniques in finite group theory: an induction/factor group argument.

Our result is not new. In fact, it was probably known in the 19th century! (See [2, p. 200], [6, pp. 56-57, 182], [5] and [8].) However, the only references we could find for it are in obscure sources in archaic English or German. Because of its potential for use in an undergraduate classroom, we felt that an accessible proof in a readily available source is desirable.

Before stating the condition we recall that if $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ is the prime decomposition of n, then $\phi(n)$, the Euler phi-function of n (which gives the number of positive integers less than or equal to n and relatively prime to n), is $p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\cdots p_t^{k_t-1}(p_t-1)$ (see [1, p. 80]).

Theorem. *For any positive integer n, Z_n is the unique group of order n if and only if* $\gcd(n, \phi(n)) = 1$.

We first prove a lemma.

Lemma. *A finite non-cyclic group G all of whose proper subgroups are cyclic has a nontrivial proper normal subgroup.*

Proof of Lemma. Suppose G does not have a nontrivial proper normal subgroup. If H and K are any two distinct maximal subgroups of G then since H and K are cyclic, the normalizer $N(H \cap K)$ of $H \cap K$ contains both H and K and therefore is G. Thus, $H \cap K$ is a proper normal subgroup of G and so must be trivial. Hence, any two distinct maximal subgroups of G intersect in the identity. Now fix a maximal subgroup H of G. Since H is not normal, its normalizer is H and so $H \cap x^{-1}Hx = \{e\}$ for all $x \notin H$. Thus, the number of nonidentity elements of H and its conjugates is $(|H| - 1)$ $|G : N(H)| = (|H| - 1)\ |G : H| = |G| - |G : H| \geq |G|/2$. Since $|G : H| \geq 2$ and the number of elements in H and its conjugate is $|G| - |G : H| + 1$, there is at least one element y not in H or any of its conjugates. Letting K be a maximal subgroup of G containing y, we find at least $|G|/2$ nonidentity elements in K and its conjugates. Because we have shown that any two maximal subgroups of G have only the identity in common we have produced at least $|G|$ nonidentity elements in G. This absurdity completes the proof of the lemma.

Proof of Theorem. Suppose G is a noncyclic group of minimum order n such that $\gcd(n, \phi(n)) = 1$. Since every proper subgroup of G of order m satisfies $\gcd(m, \phi(m)) = 1$, every proper subgroup of G is cyclic. Thus, by the Lemma, G has a proper nontrivial

normal subgroup H, and by the minimality of $|G|$ we know that both H and G/H are cyclic. Since $G/C(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$ and $|\mathrm{Aut}(H)| = \phi(|H|)$ divides $\phi(n)$ (see [4, p. 165] and [4, p. 108]), we see that $|G/C(H)|$ divides both n and $\phi(n)$, so $|G/C(H)| = 1$ and therefore H is central in G. But this implies that G is abelian ([4, p. 152]). From the condition $(n, \phi(n)) = 1$, we know that n is square-free. Thus G is a direct product of cyclic groups of prime order for distinct primes. It follows that G is cyclic [4, p. 116]. This establishes sufficiency.

Conversely, suppose $\gcd(n, \phi(n)) \neq 1$. If there is a prime p for which p^2 divides n, then $Z_p \times Z_{\frac{n}{p}}$ is not cyclic ([4, p. 116]). Thus we may now assume that n is square-free and that there are prime divisors p and q of n such that $q < p$ and q divides $p-1$. Since $U(p) = \{1, 2, \cdots, p-1\}$ is a cyclic group under multiplication modulo p and has order $p-1$, there is an element s in $U(p)$ of order q (see [4, p. 123 and p. 70]). Then $H = \langle a, b | a^q = b^p = e, a^{-1}ba = b^s \rangle$ is a non-abelian group of order pq (see [7, p. 204]) and $H \times Z_{\frac{n}{pq}}$ is a noncyclic group of order n. This completes the proof.

A refinement of our argument (but still requiring no additional theory) provides an answer to the following natural generalization of the question we have just addressed: What is a necessary and sufficient condition on n so that every group of order n is abelian? The condition was given by Dickson [2, p. 200] 90 years ago: Every group of order n is abelian if and only if the prime factorization of n has the form $p_1 p_2 \cdots p_i q_1^2 q_2^2 \cdots q_j^2$ and n is relatively prime to $(p_1 - 1)(p_2 - 1) \cdots (p_i - 1)(q_1^2 - 1)(q_2^2 - 1) \cdots (q_j^2 - 1)$.

The first author was supported by the National Science Foundation (grant number DMS 9000742) and the National Security Agency (grant number MDA 904-91-H-0036).

References

[1] George Andrews, Number Theory, W.B. Saunders, Philadelphia, 1971.

[2] L.E. Dickson, Definitions of a group and a field by independent postulates, Trans. Amer. Math. Soc. **6** (1905) 198–204.

[3] John Fraleigh, A First Course in Abstract Algebra, 4th ed., Addison-Wesley, Reading, MA, 1989.

[4] Joseph Gallian, Contemporary Abstract Algebra, 2nd ed., D.C. Heath, Lexington, MA, 1990.

[5] Hartmut Göhner, Zu welchen natürlichen Zahlen n gibt es nur eine Gruppe der Ordnung n?, Mathematische-Physikalische Semesterberichte **25** (1978) 12–20.

[6] G.A. Miller, H.F. Blichfeldt and L.E. Dickson, Theory and Applications of Finite Groups, Dover, New York, 1961.

[7] Hiram Paley and Paul Weichsel, A First Course in Abstract Algebra, Holt, Rinehart and Winston, New York, 1966.

[8] T. Szele, Über die endlichen Ordnungszahlen zu denen nur eine Gruppe gehört, Comment. Math. Helv. **20** (1947) 265-267.

Joseph A. Gallian
Department of Mathematics and Statistics
University of Minnesota, Duluth
Duluth, Minnesota 55812, USA

David Moulton
Department of Mathematics
University of California, Berkeley
Berkeley, California 94720, USA