Exploring Irreducible Elements: An Abstract Algebra Project

By Jim Coykendall, David E. Dobbs, and Bernadette Mullins

Abstract. This article describes a project for student investigation in abstract algebra. Through a process of experimentation, conjecture and proof, students determine the set of irreducible elements in the ring of integers modulo n. This provides students with an opportunity to discover, and prove for themselves, an interesting result that is not available in abstract algebra texts.

1. Introduction

The concept of an irreducible element is one of the fundamental ideas in abstract algebra. Informally, an element is irreducible if it cannot be factored properly (a formal definition is given in the following section). Introductory textbooks on the subject often give exercises such as "prove that $1 + 3\sqrt{-5}$ is irreducible in $\mathbf{Z}[\sqrt{-5}]$." In this note, we suggest a project in which students determine — through a process of experimentation; and making, testing, refining, and proving conjectures — the set of irreducible elements in the ring of integers modulo n. The pedagogical benefit of this project is that students explore the "irreducible" concept in a setting in which they will be able (with sufficient persistence) to draw their own conclusions about the irreducible elements of the ring. Since the answer to this question will not be found in their abstract algebra textbook, it is hoped that students will thereby gain a sense of discovery along with a deeper understanding of the "irreducible" concept.

2. Background Material

This section provides the pertinent definitions and may safely be skipped by those readers familiar with factorization concepts.

Definition: Let R be a commutative ring with identity, 1. An element $u \in R$ is called a *unit* of R if there exists some $v \in R$ such that $uv = 1$. The set of all units of R is denoted $U(R)$.

For example, the set of units of $\mathbf{C}[X]$, the polynomial ring over the complex numbers, is the set of nonzero constant polynomials, and the set of units of the ring of integers is $U(\mathbf{Z}) = \{1, -1\}$.

The definition of "irreducible element" found in abstract algebra textbooks is given in the context of integral domains. Therefore, we must generalize the definition to the context of commutative rings (possibly with nontrivial zero-divisors). The literature contains substantial research in the area of factorization in rings with zero-divisors (the references in [1] provide a useful overview). This work shows that the familiar concept of an irreducible element in an integral domain has three analogous but inequivalent extensions to the setting of commutative rings with zero-divisors. For this project, however, we restrict our attention to the following definition.

Definition: Let R be a commutative ring with identity, 1. A nonzero nonunit a of R is called an *irreducible element* of R if $a = bc$ with $b, c \in R$ implies that either b or c is a unit of R.

For example, the irreducible elements of $\mathbf{C}[X]$ are the linear polynomials $\{\alpha + \beta X : \alpha, \beta \in \mathbf{C} \text{ and } \beta \neq 0\}$ and the irreducible elements of $\mathbf{Z}$ are $\{\pm p : p \text{ is a prime integer}\}$.

Two elements that differ only by a unit factor are not considered to be significantly different for factorization purposes. To make this notion precise, we recall the following definition.

Definition: Let R be a commutative ring with identity and let $a, b \in R$. Then a and b are *associates* if $a = bu$ for some unit u of R.

"Being associates" is easily seen to impart an equivalence relation on the set of nonzero elements of a commutative ring R with identity. Moreover, if a and b are associates in R, then a is an irreducible element of R if and only if b is an irreducible element of R. Therefore, the equivalence relation induced by "being associates" restricts to an equivalence relation on the set of irreducible elements of R. Thus, for any R, it makes sense to ask for a set consisting of one element chosen from each of the corresponding equivalence classes; we refer to such a set as a "set of associate class representatives for the irreducible elements of R." For example, for the ring of integers, the most natural such set is the set of all positive prime integers. As another example, the most natural choice for the polynomial ring $\mathbf{C}[X]$ is the set of monic linear polynomials $\{\alpha + X : \alpha \in \mathbf{C}\}$.

A noteworthy consequence of this equivalence relation is the fact a ring element with a reducible (that is, not irreducible) factor must itself be reducible.

One final piece of terminology: for a nonzero nonunit $a \in R$, a factorization $a = bc$ in R is called a *proper* factorization if neither b nor c is a unit of R.

3. Project Description

This project asks students to determine a set of associate class representatives for the irreducible elements of $\mathbf{Z}_n \cong \mathbf{Z}/n\mathbf{Z}$, the ring of integers modulo n. Prior to embarking on this project, students have proved (either in class or in homework) that the group of units of this ring is $U(\mathbf{Z}_n) = \{u \in \mathbf{Z}_n : n$ and any coset representative of u are relatively prime integers$\}$.

In directing the project, our goal is to intrude as little as possible on the students' role as independent researchers. We suggest that students make multiplication tables for $\mathbf{Z}_n$, for $n = 2, \ldots, 36$ (most students use Microsoft Excel to do this), and then use these tables to explictly find the irreducible elements in each of these rings.

For example, in $\mathbf{Z}_{12}$, the nonzero nonunits are $2, 3, 4, 6, 8, 9, 10$. It is easy to see from the multiplication table for $\mathbf{Z}_{12}$ that 2 is irreducible, since every possible factorization, $2 = (1)(2) = (2)(7) = (5)(10) = (10)(11)$, reveals a unit factor. Similarly, 10 is shown to be irreducible in $\mathbf{Z}_{12}$; but $3, 4, 6, 8, 9$ are reducible in $\mathbf{Z}_{12}$, since each has a proper factorization as a product of two nonunits: $3 = (3)(9)$, $4 = (2)(2)$, $6 = (2)(3)$, $8 = (2)(4)$, $9 = (3)(3)$.

Part of the discovery process involves seeing past the forest of data to the underlying concepts. For instance, we have noted that $\{2, 10\}$ is the set of irreducible elements of $\mathbf{Z}_{12}$. However, it is easy to see that 2 and 10 are associates in $\mathbf{Z}_{12}$, since $2 = (10)(5)$ and $5 = 5^{-1} \in U(\mathbf{Z}_{12})$. Based on the above work, we conclude that $\{2\}$ is a set of associate class representatives for the irreducible elements of $\mathbf{Z}_{12}$.

The following table lists associate class representatives for the irreducible elements of $\mathbf{Z}_n$ for small n. The rings $\mathbf{Z}_p$ (where p is prime) are not considered since they are fields and hence have no irreducible elements.

n	$4 = 2^2$	$6 = 2 \cdot 3$	$8 = 2^3$	$9 = 3^2$	$10 = 2 \cdot 5$
irreducibles	2	none	2	3	none

n	$12 = 2^2 \cdot 3$	$14 = 2 \cdot 7$	$15 = 3 \cdot 5$	$16 = 2^4$
irreducibles	2	none	none	2

n	$18 = 2 \cdot 3^2$	$20 = 2^2 \cdot 5$	$21 = 3 \cdot 7$	$22 = 2 \cdot 11$
irreducibles	3	2	none	none

n	$24 = 2^3 \cdot 3$	$25 = 5^2$
irreducibles	2	5

Consider again our example of $\mathbf{Z}_{12}$. Note that 2 is an irreducible element of $\mathbf{Z}_{12}$, but 3 is not. Also note that more than one factor of 2 appears in the prime factorization of $12 = 2^2 \cdot 3$, but only one factor of 3 appears. After further experimentation, students typically arrive at the following conjecture: if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is a prime-power factorization of n (with the p_i pairwise distinct prime integers), then the set $\{p_i : e_i \geq 2\}$ is a set of associate class representatives for the irreducible elements of $\mathbf{Z}_n$. For completeness, we include a proof of this result below.

Theorem: Let $n = p_1 \cdots p_s q_1^{e_1} \cdots q_t^{e_t}$ where the p_i, q_j are pairwise distinct prime integers and the exponents $e_i \geq 2$ for all i. Then $\{q_1, \ldots, q_t\}$ is a set of associate class representatives for the irreducible elements of $\mathbf{Z}_n$.

Proof: First, we show that each p_i is reducible in $\mathbf{Z}_n$. Without loss of generality, $i = 1$. Observe that p_1 is relatively prime to $p_2 \ldots p_s q_1^{e_1} \ldots q_t^{e_t} = \frac{n}{p_1}$. Thus, there exist $x, y \in \mathbf{Z}$ such that $1 = p_1 x + p_2 \ldots p_s q_1^{e_1} \ldots q_t^{e_t} y$. Multiplying both sides of this equation by p_1, we see that $p_1 = p_1^2 x + p_1 p_2 \ldots p_s q_1^{e_1} \ldots q_t^{e_t} y = p_1^2 x + ny$. Thus, $p_1 \equiv p_1^2 x \equiv (p_1)(p_1 x) \pmod{n}$, where neither p_1 nor $p_1 x$ is a unit of $\mathbf{Z}_n$ since neither p_1 nor $p_1 x$ is relatively prime to $n = p_1 \ldots p_s q_1^{e_1} \ldots q_t^{e_t}$. Thus, p_1 is indeed reducible in $\mathbf{Z}_n$.

Next, we show that each q_j is irreducible in $\mathbf{Z}_n$. Without loss of generality, $j = 1$. Suppose that $q_1 \equiv ab \pmod{n}$ for some $a, b \in \mathbf{Z}_n$. Then $a \neq 0$. Moreover, in the ring of integers, $q_1 = ab + nz$ for some $z \in \mathbf{Z}$. Now, in $\mathbf{Z}$, q_1 divides n, and hence q_1 must also divide ab. Since q_1 is a prime integer, we may assume, without loss of generality, that q_1 divides a. Thus, $a = q_1 a'$ for some $a' \in \mathbf{Z}$. Also, $n = q_1 n'$, where $n' := \frac{n}{q_1} = p_1 \ldots p_s q_1^{e_1 - 1} q_2^{e_2} \ldots q_t^{e_t}$. Since

$e_1 \geq 2$ by assumption, it follows that $e_1 - 1 \geq 1$ and hence q_1 is a factor of n'. Dividing both sides of $q_1 = ab + nz$ by q_1, we see that $1 = a'b + n'z$. This shows that b and n' are relatively prime integers. Since $n' = p_1 \dots p_s q_1^{e_1 - 1} q_2^{e_2} \dots q_t^{e_t}$, no p_i or q_j can divide b. Thus b is also relatively prime to n, showing that b is a unit of $\mathbf{Z}_n$. Therefore, q_1 is irreducible in $\mathbf{Z}_n$, as asserted.

Next, we show that no elements of $\mathbf{Z}_n$ other than the q_j and their associates are irreducible. Let r be an arbitrary nonzero nonunit of $\mathbf{Z}_n$. Since r is not a unit, r and n cannot be relatively prime integers. Thus, either some p_i or some q_j must divide r in $\mathbf{Z}$. If p_i divides r, then r is reducible (since p_i is reducible). Thus, without loss of generality, some q_j divides r. Then $r = q_j r'$ for some $r' \in \mathbf{Z}$, and hence $r \equiv q_j r' \pmod{n}$. If r' is a unit of $\mathbf{Z}_n$, then r is an associate of q_j in $\mathbf{Z}_n$. In the remaining case, r' is a nonunit of $\mathbf{Z}_n$, and r is reducible in $\mathbf{Z}_n$ since $r = q_j r'$ is a proper factorization of r into two nonunits of $\mathbf{Z}_n$.

It remains only to verify that if q_j and q_k are associates in $\mathbf{Z}_n$, then $j = k$. Suppose that $q_j = q_k u$ in $\mathbf{Z}_n$, with $u \in U(\mathbf{Z}_n)$. Hence, $q_j - q_k u = zn$ for some $z \in \mathbf{Z}$, with u and n relatively prime integers. As q_k divides both $q_k u$ and zn in $\mathbf{Z}$, q_k must also divide $q_k u + zn = q_j$. Then the Fundamental Theorem of Arithmetic yields that $q_j = q_k$, and so $j = k$, to complete the proof. □

4. Classroom Experience

We have used this project in an undergraduate course in abstract algebra. Students completed the assignment by working in groups outside of class over a two-week period. During this time, students were also responsible for keeping up with other material covered in class and in the textbook. At the end of the first week, each group submitted an informal progress report to the instructor describing the conjectures they had generated. At the end of the second week, students submitted a formal report proving their results. Some groups identified the following corollary: if $n \geq 2$ is a square-free integer, then $\mathbf{Z}_n$ is devoid of irreducible elements.

5. Extensions

Interested students may investigate the following questions:

(1) For which $n \geq 2$ is it true that each nonzero, nonunit element of $\mathbf{Z}_n$ can be factored as a finite product of irreducible elements?

(2) For which $n \geq 2$ can each nonzero, nonunit element of $\mathbf{Z}_n$ be factored as a finite product of irreducible elements in an essentially unique way?

The first question is answered in [3] and the second in [2].

Depending on the interests and abilities of the students, a variety of additional related projects could be offered. For example, students could determine the irreducible elements in other finite commutative rings. Suitable rings may be constructed by taking direct products of finitely many finite rings or considering $R[X]/(f)$ where R is a finite ring and $f \in R[X]$ with leading coefficient 1. Additionally, students could investigate the alternate versions of the "irreducible" concept given in the literature (see [1] for the relevant definitions).

References

[1] D.D. Anderson and S. Valdes-Leon, *Factorization in Commutative Rings With Zero Divisors,* Rocky Mountain J. Math., **26** (1996), 439-480.

[2] M. Billis, *Unique Factorization in the Integers Modulo n*, Amer. Math. Monthly **75** (1968), 527.

[3] J. Coykendall, D. E. Dobbs and B. Mullins, *Factorization in Antimatter Rings*, Lecture Notes in Pure and Applied Mathematics, vol. 205, Marcel Dekker, New York, 1999, 217-226.

Department of Mathematics
300 Minard Hall
North Dakota State University
Fargo, North Dakota 58105-5075

Department of Mathematics
The University of Tennessee
Knoxville, TN 37996

Birmingham Southern College
900 Arkadelphia Road
Box # 549032
Birmingham, AL 35254