Alabama Journal of Mathematics

Alabama Journal of Mathematics
Volume 48 (1) (2025), 23 – 25

Classroom Note

Warning: Polynomials Over Arbitrary Rings Can Surprise You

Peter Johnson

Auburn University, USA

Abstract

A couple of years ago I was, for the first time in 40 years, teaching a course in number theory, following Leveque's classic text [1]. In the course of a proof involving polynomials I stumbled to the realization that my smug confidence in my elementary knowledge of polynomials in one variable was not well founded. Here is one thing of several that shocked me: it can happen that a monic polynomial $p(x)$, with coefficients from commutative ring R with unit, can have distinct roots a, $b \in R$ such that there exist $f(x)$, $g(x) \in R[x]$ satisfying $p(x) = (x-a)f(x)$, and $p(x) = (x-b)g(x)$, yet there is no $h(x) \in R[x]$ satisfying $p(x) = (x-a)(x-b)h(x)$.

My purpose in this short paper is to alert my fellow algebraically naive peers to some of the surprises that might await them, and to look into why what we expect from our experiences with polynomials in one variable over fields may not hold over other rings. I hope some readers may be inspired, in appropriate circumstances, to devise exercises or propose questions on these matters for the purpose of exciting student curiosity. My attempts at curiosity-arousal in my number theory course aroused few, but I feel it was worth the effort.

Keywords: commutative ring with unit, monic polynomial, root of a polynomial, factor, zero divisor, nilpotent element.

MSC Classification: 13A05

1. Preliminaries

Throughout, let $(R, +, \cdot, 0, 1)$, or simply R, be a commutative ring with unit, meaning R contains a multiplicative identity, denoted by 1. A polynomial over R is a finite linear combination of the monomials $x^0 = 1, x, x^2, \ldots$, with coefficients in R. We assume the reader is familiar with addition and multiplication of polynomials. With these operations, $R[x]$, the set of polynomials over R, becomes a commutative ring with additive and multiplicative identities 0 and 1, shared with R. Two polynomials in $R[x]$ are the same if and only if the coefficients in their representations as linear combinations of the monomials x^n,

Email addresses: johnspd@auburn.edu
Received: April 1, 2024; Accepted: September 15, 2025

$n \geq 0$, are exactly the same. If $f(x) = a_n x^n + \cdots + a_0 \in R[x]$, with $a_n, \ldots, a_0 \in R$, and $a_n \neq 0$, then the degree of $f(x)$, denoted here by $\deg(f(x))$, is n. Thus each $a \in R\backslash\{0\}$, thought of as the polynomial $a \cdot x^0$, has degree 0 (the integer, not the 0 in R, unless $R = \mathbb{Z}$, the integers). Meanwhile, there are various conventions for the degree of $0 = 0 \cdot x^0$. The author prefers $\deg(0) = -\infty$, but this will not be an issue in what follows.

2. Division Theorem for Monic Polynomials

Math teachers are familiar with certain properties of $R[x]$ when R is a field. For instance, there is a division theorem: If $f(x), g(x) \in R[x]\backslash\{0\}$, you can divide $f(x)$ by $g(x)$: for some polynomials $q(x), r(x) \in R[x]$, $f(x) = q(x)g(x)+r(x)$ and $\deg(r(x)) < \deg(g(x))$. This theorem does not necessarily hold if R is not a field (does it ever hold when R is not a field?), but, as noted in [1], there is, for every R, a similar theorem for division by monic polynomials. A monic polynomial is one with leading coefficient 1: $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Thus, the only monic polynomial over R of degree 0 is 1, and the only monic polynomials over R of degree 1 are of the form $x - a$, $a \in R$. The division theorem for monic polynomial divisions in $R[x]$ is stated exactly as the division theorem for polynomials over a field, with the additional hypothesis that $g(x)$ is monic.

3. Root-Factor Theorem and Its Limitations

This theorem implies the Root-Factor Theorem in $R[x]$, for any commutative ring R with unit: if $f(x) \in R[x]\backslash\{0\}$, $a \in R$, and $f(a) = 0$, then, for some $q(x) \in R[x]$, $f(x) = (x - a)q(x)$. In the familiar environment of polynomials over a field, this leads to: if $f(x) \in R[x]\backslash\{0\}$, R is a field, and $a_1, \ldots, a_t \in R$ are distinct roots of $f(x)$, then for some $q(x) \in R[x]$, $f(x) = (x - a_1) \cdots (x - a_t)q(x)$. From this it follows that $f(x)$ can have no more than $\deg(f(x))$ distinct roots. But—and this may surprise some—for arbitrary commutative rings with unit, the intermediate theorem that if $a_1, \ldots, a_t \in R$ are distinct roots of $f(x) \in R[x]\backslash\{0\}$, then for some $q(x) \in R[x]$, $f(x) = (x-a_1) \cdots (x-a_t)q(x)$, fails. For instance, if $R = \mathbb{Z}_4$, the ring of integers modulo 4, the monic polynomial x^2 has 2 distinct roots, 0 and 2, and we have $x^2 = (x - 0)x$ and $x^2 = (x - 2)(x - 2)$ (note: in $\mathbb{Z}_4$, $2 = -2$), but $x^2 \neq (x - 0)(x - 2) = x^2 - 2x$.

4. Zero Divisors and Polynomial Roots

To see how this violation of the ordinary mathematician-on-the-street's casual-but-deep beliefs about polynomials can exist, let us consider the case $t = 2$. Suppose that $f(x) \in R[x]\backslash\{0\}$ is monic and $a, b \in R$ are distinct roots of $f(x)$. By the Root-Factor Theorem, for some $q(x) \in R[x]$, $f(x) = (x - a)q(x)$. Now, pay attention! We have $0 = f(b) = (b - a)q(b)$, and if we are not careful, we might conclude, from $b - a \neq 0$, that $q(b) = 0$, and then, from the Root-Factor Theorem again, that $q(x) = (x - b)q_1(x)$ for some $q_1(x) \in R[x]$. This chain of inference is valid if R is an integral domain, a ring with no zero divisors, so that $cd = 0$ and $c, d \in R$ implies that at least one of c and d is 0. Therefore, no monic polynomial over an integral domain can have more roots in the ring than its degree. (In fact, because every integral domain is a subring of a field, the same is true of all polynomials with coefficients in an integral domain.) We can ask: is the same true for some or all commutative rings with unit that contain zero divisors? Just because the proof doesn't work... But here is a trivial argument that shows that the answer is no for every commutative ring with unit containing zero divisors. Suppose $a, b \in R\backslash\{0\}$ and $ab = 0$. Then the polynomial ax, of degree 1, has at least two roots in R, 0 and b.

5. Nilpotent Elements and Infinitely Many Roots

To drive a truck through the question, let $\mathbb{Z}$ denote the ring of integers, and let $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = R$, with coordinate-wise addition and multiplication. Then R is a commutative ring with additive identity $(0,0)$ and multiplicative identity $(1,1)$. If $a = (1,0) \in R \backslash \{(0,0)\}$, then the polynomial ax has roots $(0,b)$, $b \in \mathbb{Z}$; infinitely many! But suppose we restrict our query to monic polynomials in $R[x]$? The only monic polynomial of degree 1 in $R[x]$, x, has a unique root in R, so those trivial examples disposing of the previous question are washed away. I foresee that algebraists reading this, if any, will now almost immediately think of nilpotents, which are non-zero ring elements r such that for some integer $n > 1$, $r^n = 0$. These are easy to come by: take a ring of upper triangular square matrices, with entries from some other ring, equipped with entry-wise addition and matrix multiplication. If the matrices are $k \times k$, $k > 1$, then for every matrix m in the ring with all zeros on its main diagonal, $m^k = 0$ and therefore $m^n = 0$ for all integers $n \geq k$. We can easily arrange for there to be infinitely many such m, but it is not easy to arrange for the matrix multiplication to be commutative. The following does the job, but it is the simplest of a countable infinity of such examples, for each R.

Example Let $(H, +, \cdot, 0, 1)$ be a commutative ring with unit, and let $R = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in H \right\}$, the set of 2×2 upper triangular matrices with constant diagonal, with entries from H. If R is equipped with entry-wise addition and matrix multiplication then R becomes a commutative ring, with additive and multiplicative identities $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, respectively. For every $b \in H$, $\begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Therefore, if H is infinite, for each $n \geq 2$, the monic polynomial $x^n \in R[x]$ has infinitely many roots in R.

6. Open Questions and a Theorem

That was disappointingly easy! But it does leave us with two unexpected byproducts, a question and a theorem.

Open Question: *Can there exist a commutative ring R with unit and with no nilpotent elements, and a monic polynomial $f(x) \in R[x]$ with more than* $\deg(f(x))$ *roots in R?*

The modifier "Open" above means that the author does not know the answer to the question.

Theorem 6.1. *If R is a commutative ring with unit, then R is an integral domain if and only if no $f(x) \in R[x] \backslash \{0\}$ has more than* $\deg(f(x))$ *roots in R.*

The theorem sounds nifty, but it is trivially implied by previous remarks, including the "only if" assertion, which follows from the fact that every integral domain is a subring of a field.

References

[1] William LeVeque, *Fundamentals of Number Theory*, Addison-Wesley, 1977.