Polynomial Factoring in Different Domains

Name: Krish Arora Date: 7/14/25

1 Introduction

In our journey through algebra, we've learned to factor polynomials using various techniques. However, what many students don't realize is that *how far* we can factor a polynomial depends on which number system we're working in. A polynomial that appears "completely factored" in one number system might factor further in a larger number system.

Today we'll explore polynomial factoring across different **integral domains** and **fields**, and learn about the fundamental theorem that governs polynomial factorization.

2 Definitions and Number Systems

2.1 Integral Domains and Fields

Definition (Integral Domain): An integral domain is a commutative ring with no zero divisors. In simpler terms, it's a number system where we can add, subtract, and multiply (with the usual properties), and where if $a \cdot b = 0$, then either $a = 0$ or $b = 0$.

Definition (Field): A field is an integral domain where every non-zero element has a multiplicative inverse. In other words, we can also divide by any non-zero element.

2.2 Common Number Systems

- $\mathbb{Z}$ = the integers $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ (integral domain, but not a field)
- $\mathbb{Q}$ = the rational numbers $\left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$ (field)
- $\mathbb{R}$ = the real numbers (field)
- $\mathbb{C}$ = the complex numbers $\{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$ (field)

Inclusion Chain: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

2.3 Polynomial Rings

When we write $F[x]$, we mean the ring of polynomials with coefficients from the system F. For example:

- $\mathbb{Z}[x]$ = polynomials with integer coefficients
- $\mathbb{Q}[x]$ = polynomials with rational coefficients
- $\mathbb{R}[x]$ = polynomials with real coefficients
- $\mathbb{C}[x]$ = polynomials with complex coefficients

3 Irreducible vs. Reducible Polynomials

Definition: A polynomial $p(x)$ of degree ≥ 1 in $F[x]$ is called **irreducible over** F if it cannot be written as a product of two polynomials of positive degree with coefficients in F.

If $p(x)$ can be factored into polynomials of positive degree over F, then $p(x)$ is **reducible over** F.

Key Insight: A polynomial's irreducibility depends on which coefficient system we're using!

4 Examples of Factoring Across Different Domains

4.1 Example 1: $x^2 - 2$

- **Over** $\mathbb{Z}[x]$**:** $x^2 - 2$ is irreducible (cannot be factored with integer coefficients)
- **Over** $\mathbb{Q}[x]$**:** $x^2 - 2$ is still irreducible (cannot be factored with rational coefficients)
- **Over** $\mathbb{R}[x]$**:** $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ (now it factors!)
- **Over** $\mathbb{C}[x]$**:** Same as over $\mathbb{R}[x]$ since $\sqrt{2} \in \mathbb{R} \subset \mathbb{C}$

4.2 Example 2: $x^2 + 1$

- **Over** $\mathbb{Z}[x]$**:** $x^2 + 1$ is irreducible
- **Over** $\mathbb{Q}[x]$**:** $x^2 + 1$ is irreducible
- **Over** $\mathbb{R}[x]$**:** $x^2 + 1$ is irreducible (no real square roots of -1)
- **Over** $\mathbb{C}[x]$**:** $x^2 + 1 = (x - i)(x + i)$ (factors with complex numbers!)

4.3 Example 3: $x^4 - 4$

Let's trace this step by step:

Over $\mathbb{Z}[x]$ **and** $\mathbb{Q}[x]$**:**

$$x^4 - 4 = x^4 - 2^2 = (x^2)^2 - 2^2 = (x^2 - 2)(x^2 + 2)$$

Both factors are irreducible over $\mathbb{Q}$ (as we can verify), so this is the complete factorization.

Over $\mathbb{R}[x]$**:**

$$x^4 - 4 = (x^2 - 2)(x^2 + 2) = (x - \sqrt{2})(x + \sqrt{2})(x^2 + 2)$$

Now $x^2 - 2$ factors, but $x^2 + 2$ is still irreducible over $\mathbb{R}$.

Over $\mathbb{C}[x]$**:**

$$x^4 - 4 = (x - \sqrt{2})(x + \sqrt{2})(x - i\sqrt{2})(x + i\sqrt{2})$$

Now everything factors completely!

5 The Fundamental Theorem of Algebra and Prime Factorization

5.1 Fundamental Theorem of Algebra

Theorem: Every non-constant polynomial in $\mathbb{C}[x]$ has at least one root in $\mathbb{C}$.

Corollary: Every polynomial of degree $n \geq 1$ in $\mathbb{C}[x]$ factors completely into n linear factors:

$$p(x) = a(x - r_1)(x - r_2) \cdots (x - r_n)$$

where a is the leading coefficient and $r_1, r_2, \ldots, r_n$ are the roots (counting multiplicity).

5.2 Prime Factorization for Polynomials

Just as integers have unique prime factorization, polynomials have unique factorization into irreducible polynomials.

Unique Factorization Theorem for Polynomials: If F is a field, then every non-constant polynomial in $F[x]$ can be written uniquely (up to order and units) as a product of irreducible polynomials in $F[x]$.

Irreducible Polynomials in Different Fields:

- Over $\mathbb{C}$: Only linear polynomials $(x - a)$ are irreducible
- Over $\mathbb{R}$: Linear polynomials and quadratics with negative discriminant
- Over $\mathbb{Q}$: More complex—requires tools like Eisenstein's criterion

6 Practice Problems

Part A: Basic Factoring Across Domains

1. For each polynomial, factor it as completely as possible over the given domain:

(a) $x^2 - 3$ over $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$

$\mathbb{Q}[x]$: Irreducible (The prime 3 satisfies Eisenstein's Criterion)

$\mathbb{R}[x] : (x + \sqrt{3})(x - \sqrt{3})$

$\mathbb{C}[x] : (x + \sqrt{3})(x - \sqrt{3})$

(b) $x^2 + 4$ over $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$

$\mathbb{Q}[x]$: Negative Discriminant

$\mathbb{R}[x]$: Negative Discriminant

$\mathbb{C}[x] : (x + 2i)(x - 2i)$

(c) $x^3 - 2$ over $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$

$\mathbb{Q}[x]$: Irreducible (The prime 2 satisfies Eisenstein's Criterion)

$\mathbb{R}[x]$: Not Irreducible (I don't know what it is though)

$\mathbb{C}[x]$: Same as Above

2. Consider the polynomial $p(x) = x^4 - 5x^2 + 6$.

(a) Factor $p(x)$ completely over $\mathbb{Q}[x]$.

let $y = x^2$

$y^2 - 5y + 6 = (y - 2)(y - 3)$

$(x^2 - 2)(x^2 - 3)$

(b) Factor $p(x)$ completely over $\mathbb{R}[x]$.

let $y = x^2$

$y^2 - 5y + 6 = (y - 2)(y - 3)$

$(x^2 - 2)(x^2 - 3) = (x + \sqrt{2})(x - \sqrt{2})(x + \sqrt{3})(x - \sqrt{3})$

(c) Factor $p(x)$ completely over $\mathbb{C}[x]$.

let $y = x^2$

$y^2 - 5y + 6 = (y-2)(y-3)$

$(x^2-2)(x^2-3) = (x+\sqrt{2})(x-\sqrt{2})(x+\sqrt{3})(x-\sqrt{3})$

Part B: Understanding Irreducibility

3. Determine whether each polynomial is irreducible over the given domain. Justify your answer.

(a) $x^2 + x + 1$ over $\mathbb{Q}[x]$

Irreducible since it is irreducible over $\mathbb{R}[x]$.

(b) $x^2 + x + 1$ over $\mathbb{R}[x]$

Irreducible because of negative discriminant.

(c) $x^3 + x + 1$ over $\mathbb{Q}[x]$ (Hint: Check for rational roots)

Irreducible because of no rational roots.

4. Show that $x^2 - 2$ is irreducible over $\mathbb{Q}[x]$ by proving that $\sqrt{2}$ is irrational.

Because of the Quadratic Formula, we know that $x^2 - 2$ only has roots $\sqrt{2}$ and $-\sqrt{2}$.

Assume $\sqrt{2} = \frac{a}{b}$ is in lowest term with the greatest common denominator being 1.

Then $a^2 = 2b^2$, so a is even.

Let $a = 2k$, then $4k^2 = 2b^2$ implies $b^2 = 2k^2$, so b is even, which means $\sqrt{2}$ is irrational.

Since it has no rational roots, it is irreducible over $\mathbb{Q}[x]$.

7 Challenge Problems

5. Consider the polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$.

(a) Show that $f(x) = \frac{x^5-1}{x-1}$ for $x \neq 1$.

(b) Use the fact that $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$ and the factorization of $x^5 - 1$ over $\mathbb{C}$ to factor $f(x)$ completely over $\mathbb{C}[x]$.

(c) What can you say about the irreducibility of $f(x)$ over $\mathbb{Q}[x]$? (This is the 5th cyclotomic polynomial)

6. Eisenstein's Criterion: A powerful tool for proving irreducibility over $\mathbb{Q}[x]$ is Eisenstein's criterion:

If $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with integer coefficients, and there exists a prime p such that:

- p does not divide a_n
- p divides a_i for all $i < n$
- p^2 does not divide a_0

then $p(x)$ is irreducible over $\mathbb{Q}[x]$.

Use Eisenstein's criterion to prove that $x^3 + 2x + 2$ is irreducible over $\mathbb{Q}[x]$.