Exercise 6 – Polynomials over integers and rationals

November 11, 2026

Problem 1. Determine all rational roots of the following polynomials in $\mathbb{Z}[x]$:

a) $3x^5 - 2x^2 + x + 1$,

b) $x^3 - 7x^2 + 11x + 3$,

c) $2x^3 - x^2 + 3$.

Problem 2. For each pair of polynomials f and g, determine their greatest common divisor, $\mathrm{GCD}(f, g)$, in the indicated ring.

a) $f = 6x^3 - 6$, $g = 8x^2 - 8$ in $\mathbb{Z}[x]$,

b) ◁ $f = 6x^3 + 3x - 3$, $g = 6x^2 + 6x$ in $\mathbb{Q}[x]$,

c) $f = 6x^2y$, $g = 15xy^2 + x^3y$ in $\mathbb{Z}[x, y]$.

Problem 3. Show that the following polynomials are irreducible in the indicated rings:

a) $x^3 + x^2 + x + 3$ in $\mathbb{Z}[x]$,

b) $4x^3 - 15x^2 + 60x + 180$ in $\mathbb{Z}[x]$,

c) ◁ $x^5 - 36x^4 + 6x^3 + 30x^2 + 24$ in $\mathbb{Q}[x]$,

d) $x^{p-1} + x^{p-2} + \cdots + x + 1$ in $\mathbb{Z}[x]$, where p is a prime number.

Hint: For part (d), use the substitution $x \mapsto x + 1$ and apply the result from a previous exercise.

Problem 4. Factor the polynomial $2x^2 + 2x - 1$ into irreducible factors in the ring $\mathbb{Z}[\sqrt{3}][x]$.

Problem 5. Factor the polynomial $x^{16} - 1$ into irreducible factors in $\mathbb{Z}[x]$.

Problem 6. Prove that for every prime number p and every integer $n \geq 2$, the number $\sqrt[n]{p}$ is irrational.

Problem 7. Let $f \in \mathbb{Z}[x]$ be a primitive polynomial, and let p be a prime number that does not divide the leading coefficient of f.

Show that if f is reducible in $\mathbb{Z}[x]$, then its reduction modulo p is reducible in $\mathbb{Z}_p[x]$.

State the contrapositive of this statement.

Problem 8. Show that the polynomial $3x^4 + 7x^3 + 3x^2 - x + 5$ is irreducible in $\mathbb{Z}[x]$.

Hint: Consider the reduction modulo 2*.*

Homework. Show that the polynomial $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$, but its reduction modulo p is reducible in $\mathbb{Z}_p[x]$ for $p \in \{2, 3, 5\}$.

Note: it is actually reducible for every p prime, you can try to prove it on yourself.

Criteria for irreducibility over integer of rational polynomials

Theorem 1 (Rational Root Theorem)**.** *Let*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x],$$

where $a_n \neq 0$ *and* $a_0 \neq 0$*. If* f *has a rational root* $r = \frac{p}{q}$*, where* $p, q \in \mathbb{Z}$*,* $q \neq 0$*, and* $GCD(p, q) = 1$*, then*

$$p \mid a_0 \qquad \textit{and} \qquad q \mid a_n.$$

In particular, if f *is monic, every rational root of* f *must be an integer dividing its constant term.*

Theorem 2 (Eisenstein's Criterion)**.** *Let*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

Suppose there exists a prime number p *such that:*

1. $p \nmid a_n$,
2. $p \mid a_i$ *for all* $i = 0, 1, \ldots, n-1$,
3. $p^2 \nmid a_0$.

Then f *is irreducible in* $\mathbb{Q}[x]$*.*

If, in addition, f *is primitive (the greatest common divisor of its coefficients is* 1*), then* f *is also irreducible in* $\mathbb{Z}[x]$*.*

Theorem 3 (Gauss's Lemma)**.** *For every nonconstant primitive polynomial* $f \in \mathbb{Z}[x]$*, the following equivalence holds:*

$$f \textit{ is irreducible in } \mathbb{Z}[x] \iff f \textit{ is irreducible in } \mathbb{Q}[x].$$

Theorem 4 (Substitution Criterion)**.** *Let* K *be a field and let* $f \in K[x]$*. For any* $a \in K$*,*

$$f(x) \textit{ is irreducible in } K[x] \iff f(x+a) \textit{ is irreducible in } K[x].$$

Theorem 5 (Prime Criterion)**.** *Let* $f \in \mathbb{Z}[x]$ *be a primitive polynomial, and let* p *be a prime number such that* p *does not divide the leading coefficient of* f*.*

Write the reduction of f *modulo* p *as* $\overline{f}(x) \in \mathbb{Z}_p[x]$*. If* f *is reducible in* $\mathbb{Z}[x]$*, then* $\overline{f}$ *is reducible in* $\mathbb{Z}_p[x]$*.*