Testing Irreducibility of polynomials over $\mathbb{Q}$

Jiang-Hua Lu

The University of Hong Kong

Algebra II, HKU

Thursday Feb 13, 2025

Outline

In this file:

1. §1.4: Testing Irreducibility of polynomials over $\mathbb{Q}$

§1.4: Testing Irreducibility of polynomials over $\mathbb{Q}$

Again, Why testing irreducibility of $f(x) \in \mathbb{Q}[x]$?

- Every irreducible $f \in \mathbb{Q}[x]$ gives a field extension of $\mathbb{Q}$ via

$$\mathbb{Q} \hookrightarrow \mathbb{Q}[x]/\langle f(x) \rangle.$$

Examples of irreducible $f(x) \in \mathbb{Q}[x]$?

Observation:

By clearing denominators, may assume that $f(x) \in \mathbb{Z}[x]$ but still want to test irreducibility of $f(x)$ over $\mathbb{Q}$.

Goal:

- Test whether or not a non-constant $f(x) \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$.

Example:

$$\frac{1}{3}x^7 + 5 \text{ is irreducible over } \mathbb{Q} \iff x^7 + 15 \in \mathbb{Z}[x] \text{ is irreducible over } \mathbb{Q}.$$

Theoretical basis for our tools: proper fac $\Leftarrow$ deg $\downarrow$

Recall Definition. For an integral domain R and non-constant $f(x) \in R[x]$,

irreducible

content

- a proper factorization of $f(x)$ in $R[x]$ is a product
$$f(x) = g(x)h(x),$$
where $g(x), h(x) \in R[x]$ are both non-constants.

Observations:

- For a general R, if $f(x) \in R[x]$ has a proper factorization in $R[x]$, then $f(x)$ reducible in $R[x]$;
- Converse is not true in general:
$$f(x) = 2x + 4 = 2(x + 2) \in \mathbb{Z}[x]$$
is reducible in $\mathbb{Z}[x]$ but has no proper factorization in $\mathbb{Z}[x]$.
- If R is a field, $f(x) \in R[x]$ is reducible iff $f(x)$ has a proper factorization in $R[x]$.

Lemma

(Gauss' Lemma on proper factorizations): For non-constant $f(x) \in \mathbb{Z}[x]$,

$\Leftrightarrow f(x) = h(x)g(x)$, $h, g \in \mathbb{Q}[x]$, $\deg h > 0$, $\deg g > 0$

$f(x)$ is reducible over $\mathbb{Q} \iff f(x)$ has a proper factorization in $\mathbb{Z}[x]$.

Proof. If f has a proper factorization in $\mathbb{Z}[x]$ then f is reducible over $\mathbb{Q}$.

- Assume that $f(x)$ is reducible over $\mathbb{Q}$.
- So $f(x) = g(x)h(x)$ for non-constant $g(x), h(x) \in \mathbb{Q}[x]$.
- Write $g(x) = \alpha g_1(x)$ and $h(x) = \beta h_1(x)$, where $\alpha, \beta \in \mathbb{Q}$ and $g_1(x), h_1(x) \in \mathbb{Z}[x]$ are both primitive. So $f(x) = \alpha\beta g_1(x)h_1(x)$.
- Write $\alpha\beta = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b > 0$, and $(a, b) = 1$. Then
$$bf(x) = ag_1(x)h_1(x) \in \mathbb{Z}[x].$$
- Since $(a, b) = 1$, $b | g_1(x)h_1(x)$.
- By Gauss' Lemma on products of Primitive Elements, $g_1(x)h_1(x)$ is primitive.
- Thus $b = 1$, so $f(x)$ has a proper factorization in $\mathbb{Z}[x]$.

Q.E.D.

Thus, for $f(x) \in \mathbb{Z}[x]$, non-constant,
$f(x)$ is irreducible over $\mathbb{Q}$
$\iff$ $f(x)$ has no proper factorization in $\mathbb{Z}[x]$.

Same statement when $\mathbb{Z}$ is replaced by any UFD R and $F = \mathrm{Frac}(R)$.

2nd proof using Gauss' Lemma relating irreducible elements in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$:

- Suppose that $f(x) \in \mathbb{Z}[x]$ is reducible over $\mathbb{Q}$.
- Write $f(x) = \gamma h(x)$, where $\gamma = \mathrm{cont}(f) \in \mathbb{Z}$, and $h(x) \in \mathbb{Z}[x]$ is primitive.
- By Gauss' Lemma relating irreducibile elements in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$, $h(x) \in \mathbb{Z}[x]$ is reducible.
- Being primitive, $h(x)$ has a proper factorization in $\mathbb{Z}[x]$.
- So $f(x)\gamma(x)$ has a proper factorization in $\mathbb{Z}[x]$.

Q.E.D.

Remark: Guass' Lemma on proper factorization holds when $\mathbb{Z}$ is replaced by any R which is a UFD and $\mathbb{Q}$ by $F = \mathrm{Frac}(R)$ (both proofs work).

Tool 1: Quadratic or cubic polynomials:

Easy observation: If a quadratic or cubic $f(x) \in \mathbb{Z}[x]$ has a proper factorization, it must have a linear factor and thus a rational root.

$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} r^{n-1} s + a_n r^n = 0$

Rational root test:

Lemma. If a polynomial

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Z}[x]$$

has a rational root $\frac{r}{s}$, where $r, s \in \mathbb{Z}$ are relatively prime, then

$$s | a_n \quad \text{and} \quad r | a_0.$$

If f is monic, i.e., if $a_n = 1$, then all of its rational roots are integers.

Proof. Since r/s is a root, one has

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} r^{n-1} s + a_n r^n = 0.$$

The statement follows.

Q.E.D.

Example: If an integer D, $f(x) = x^2 - D$ is irreducible over $\mathbb{Q}$ iff D is not the square of any integer.

Pf: $f(x)$ has no integer root.

In general, if $f(x) \in \mathbb{Z}[x]$ is monic w/ deg 2 or 3, then f is irreducible over $\mathbb{Q}$ iff f has no integer roots

Example. $f(x) = x^3 + 5x + 2 \in \mathbb{Z}[x]$:

Only possible integer roots are ± 1, ± 2.

Check neither is a root.

Thus f is irred. over $\mathbb{Q}$.

Tool 2: Reduction modulo p

Let p be a prime number and

$$\pi_p : \ \mathbb{Z} \longrightarrow \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \quad , \ n \longmapsto \bar{n}$$

the projection. Have induced ring homomorphism

$$\pi_p : \ \mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x].$$

Lemma. Suppose that $f \in \mathbb{Z}[x]$ is non-constant and leading coefficient not divisible by p. Then

$$\pi_p(f) \in \mathbb{F}_p[x] \text{ is irreducible} \implies f(x) \in \mathbb{Q}[x] \text{ is irreducible.}$$

Proof of Lemma. We show that $f(x)$ has no proper factorization in $\mathbb{Z}[x]$.

- Suppose yes. Then $f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Z}[x]$ and

$$\deg(g) > 0 \quad \text{and} \quad \deg(h) > 0.$$

- Then $\pi_p(f) = \pi_p(g)\pi_p(h) \in \mathbb{F}_p[x]$.

  ie leadg coeff of f is not divisible by p
- The assumption on f implies that $\deg(\pi_p(f)) = \deg(f)$ and

$$\deg(\pi_p(g)) > 0 \quad \text{and} \quad \deg(\pi_p(h)) > 0,$$

  contradicting irreducibility of $\pi_p(f)$ in $\mathbb{F}_p[x]$.
- So $f(x)$ has no proper factorization in $\mathbb{Z}[x]$.
- Thus f is irreducible in $\mathbb{Q}[x]$.

Q.E.D.

Example. Let $f(x) = 35x^3 + 3x^2 + 4x - 7$ and let $p = 2$.

$\pi_2 : \mathbb{Z}[x] \longrightarrow \mathbb{Z}/2\mathbb{Z}[x]$ $\qquad \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$

$(\pi_2 f) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$

Claim: $f(x) = x^4 - 10x^2 + 1 \in \mathbb{Z}[x]$ is irreducible over $\mathbb{Q}$ but reducible mod p for every prime p.

To continue on Thursday.

Tool 3: Eisenstein's criteria.

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

1. If there exists prime number p such that

$$p|a_0, \quad p|a_1, \quad \cdots, \quad p|a_{n-1}, \quad p \nmid a_n, \quad p^2 \nmid a_0,$$

then f is irreducible over $\mathbb{Q}$;

2. If there exists a prime number p such that

$$p|a_1, \quad p|a_2, \quad \cdots, \quad p|a_n, \quad p \nmid a_0, \quad p^2 \nmid a_n,$$

then f is irreducible over $\mathbb{Q}$.

Example: $f(x) = x^n + p$ is irreducible over $\mathbb{Q}$ for any prime number p and any integer $n \geq 1$.

Example. For any integer $n \geq 1$,

$$f(x) = 2 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n$$

where $a_1, a_2, \cdots, a_{n-1}$ are even and a_n is odd, is irreducible in $\mathbb{Q}[x]$.

Proof of Eisenstein's criteria: Only need to prove 1), 2) being similar.

- Assume f has a proper factorization $f(x) = g(x)h(x)$, where $g(x), h(x) \in \mathbb{Z}[x]$ with $\deg(h) > 0$ and $\deg(g) > 0$.
- Then $\pi_p(f) = \pi_p(a_n)x^n = \pi_p(g)\pi_p(h)$.
- Then $\pi_p(g) = bx^k$ and $\pi_p(h) = cx^l$ for some non-zero $b, c \in \mathbb{F}_p$ and $k + l = n$.
- Thus p divides all but one coefficients of g, and similarly for h.
- Since $\pi_p(g)\pi_p(h) = \pi_p(a_n)x^n \neq 0$, p does not divide the leading coefficients of g and of h.
- Since both g and h have positive degrees, p divides the constant terms of both g and h, contradicting the assumption that $p^2 \nmid a_0$.

Q.E.D.

Tool 4: Change of variables:

Observation:

If $f(x) \in \mathbb{Q}[x]$, by setting $x = ay + b$, where $a, b \in \mathbb{Q}$ and $a \neq 0$, one get

$$g(y) = f(ay + b) \in \mathbb{Q}[y],$$

and $f(x) \in \mathbb{Q}[x]$ is irreducible if and only if $g(y) \in \mathbb{Q}[y]$ is irreducible.

Example: Let p be a prime, and consider the polynomial

$$f(x) = 1 + x + x^2 + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}.$$

Setting $y = x - 1$, one has

$$f(x) = f(y+1) = \frac{(y+1)^p - 1}{y} = y^{p-1} + C_1^p y^{p-2} + \cdots + p$$

which is irreducible in $\mathbb{Q}[x]$ by Eisenstein's Criterion. Since f is primitive, it is also irreducible over $\mathbb{Z}$.