Math 521A

4.5 – Irreducibility in $\mathbb{Q}[x]^*$

*This is an optional topic

Problem: Given $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$, decide whether $f(x)$ is irreducible.

Note: If we let $c = \mathrm{lcm}\{\text{denominators of } a_0, \ldots, a_n\}$, then the polynomial $cf(x) \in \mathbb{Z}[x]$. Moreover, $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $cf(x)$ is.

Theorem (Gauss' Lemma)

Let $f(x) \in \mathbb{Z}[x]$. Then $f(x)$ factors as a product of polynomials of degrees m and n in $\mathbb{Q}[x]$ if and only if $f(x)$ factors as a product of polynomials of degrees m and n in $\mathbb{Z}[x]$.

Gauss' Lemma simplifies the problem of deciding whether a polynomial $f(x) \in \mathbb{Q}[x]$ is irreducible to the problem of deciding whether an associate of $f(x)$ with coefficients in $\mathbb{Z}$ can be factored as a product of polynomials of smaller degrees in $\mathbb{Z}[x]$.

Example

Show that $x^4 + x + 1 \in \mathbb{Q}[x]$ cannot be factored as a product of two polynomials of degree 2 in $\mathbb{Q}[x]$.
Solution: If that were possible, then

$$x^4 + x + 1 = (x^2 + ax + b) \cdot (x^2 + cx + d) \text{ in } \mathbb{Z}[x],$$

whence

$$x^4 + x + 1 = x^4 + (a + c)x^3 + (ac + b + d)x^2 + (ad + bc)x + bd \text{ in } \mathbb{Z}[x].$$

In conclusion,

$$\begin{cases} a + c & = & 0 \\ ac + b + d & = & 0 \\ ad + bc & = & 1 \\ bd & = & 1 \end{cases}.$$

Try and solve the above equations in $\mathbb{Z}$, and you will reach a contradiction. This shows that $x^4 + x + 1$ cannot be factored as a product of two polynomials of degree 2 in $\mathbb{Z}[x]$, and hence neither in $\mathbb{Q}[x]$ by Gauss' Lemma.

Theorem (Rational Root Test)

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. *If* $\frac{r}{s}$ *with* $(r, s) = 1$ *is a root of* $f(x)$, *then* $r | a_0$ *and* $s | a_n$.

Example

Apply the rational root test to the polynomial $f(x) = x^4 + x + 1$ to show that it has no roots in $\mathbb{Z}$.

Solution: Any rational root of the polynomial would be of the form $\frac{r}{s}$ where $r|1$ and $s|1$. So, the candidate roots are -1 and 1. It is easy to see that neither integer is a root of $f(x)$. In conclusion, $f(x)$ has no roots in $\mathbb{Q}$.

Remark: Together, the last two examples show that $x^4 + x + 1$ is irreducible in $\mathbb{Q}[x]$.

Theorem (Eisenstein's Criterion)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ be a nonconstant polynomial. If there is a prime p such that

(a) $p \mid a_0, a_1, \ldots, a_{n-1}$;

(b) $p \nmid a_n$;

(c) $p^2 \nmid a_0$,

then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Example

Show that $g(x) = x^3 + 2x + 10$ is irreducible in $\mathbb{Q}[x]$.

Solution: Eisenstein's criterion with $p = 2$.

Another useful criterion is the following:

Theorem (Theorem 4.25)

Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, and suppose p is a positive prime that does not divide a_n. If

$$\overline{a_n}x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_1}x + \overline{a_0}$$

is irreducible in $\mathbb{Z}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$. Here, $\overline{a_i} = a_i \bmod p,\ i = 0, \ldots, n$.

Example

Show that $g(x) = x^4 + 10x^3 + 15x^2 + 5x + 2$ is irreducible in $\mathbb{Q}[x]$.

Solution: Apply Theorem 4.25 with $p = 5$. Basically, you need to check that $x^4 + 2$ has no roots in $\mathbb{Z}_5$ and it cannot be factored as a product of two polynomials of degree 2 in $\mathbb{Z}_5[x]$.