2.4 Lecture 9: Irreducibility in $\mathbb{Q}[X]$ and $\mathbb{Z}[X]$

Corollary 27. *Suppose* $f(X)$ *is a polynomial of degree* $\geqslant 2$ *in* $\mathbb{Z}[X]$. *Then* $f(X)$ *has a proper factorization in* $\mathbb{Q}[X]$ *if and only if it has a proper factorization in* $\mathbb{Z}[X]$, *with factors of the same degrees.*

This means : if $f(X)$ can be properly factorized in $\mathbb{Q}[X]$ it can also be properly factorized in $\mathbb{Z}[X]$; if it can be written as the product of two polynomials of degree $\geqslant 1$ with rational coefficients, it can be written as the product of two such polynomials with *integer* coefficients.
Proof: $\Longleftarrow$: This direction is obvious, since any factorization in $\mathbb{Z}[X]$ is a factorization in $\mathbb{Q}[X]$.
$\Longrightarrow$: First assume that $f(X)$ is primitive in $\mathbb{Z}[X]$.
Suppose that $f(X) = g_1(X)h_1(X)$ where $g_1(X)$ and $h_1(X)$ are polynomials of degree $k \geqslant 1$ and $m \geqslant 1$ in $\mathbb{Q}[X]$. Then there are integers a_1 and b_1 for which $a_1g_1(X)$ and $b_1h_1(X)$ are elements of $\mathbb{Z}[X]$, both of degree at least 1. Let d_1 and d_2 denote the greatest common divisors of the coefficients in $a_1g_1(X)$ and $b_1h_1(X)$ respectively. Then $(a_1/d_1)g_1(X)$ and $(b_1/d_2)h_1(X)$ are primitive polynomials in $\mathbb{Z}[X]$. Call these polynomials $g(X)$ and $h(X)$ respectively, and let a and b denote the rational numbers a_1/d_1 and b_1/d_2. Now

$$f(X) = g_1(X)h_1(X) \Longrightarrow abf(X) = ag_1(X)bh_1(X) = g(X)h(X).$$

Since $g(X)h(X) \in \mathbb{Z}[X]$ and $f(X)$ is primitive it follows that ab is an integer. Furthermore since $g(X)h(X)$ is primitive by Theorem 26, $abf(X)$ is primitive. This means $ab = 1$ or -1. Now either $ab = 1$ and $f(X) = g(X)h(X)$ or $ab = -1$ and $f(X) = (-g(X))h(X)$. Thus $f(X)$ factorizes in $\mathbb{Z}[X]$.

Finally, if $f(X)$ is not primitive we can write $f(X) = df_1(X)$ where d is the gcd of the coefficients in $f(X)$ and $f_1(X)$ is primitive. By Lemma 24 $f(X)$ is irreducible in $\mathbb{Q}[X]$ if and only if $f_1(X)$ is. By the above, $f_1(X)$ factorizes in $\mathbb{Q}[X]$ if and only if it factorizes in $\mathbb{Z}[X]$. Finally, $f(X)$ clearly factorizes in $\mathbb{Z}[X]$ if $f_1(X)$ does. □

Theorem 26 and Corollary 27 make the reducibility question in $\mathbb{Q}[X]$ much easier.

Theorem 28. *Let* $f(X) = a_nX^n + \cdots + a_1X + a_0$ *be a polynomial of degree* $n \geqslant 2$ *in* $\mathbb{Z}[X]$, *with* $a_0 \neq 0$. *If* $f(X)$ *has a root in* $\mathbb{Q}$ *this root has the form* b/a *where* a *and* b *are integers (positive or negative) for which* $b|a_0$ *and* $a|a_n$.

Proof: By Theorem 21, $f(X)$ has a root in $\mathbb{Q}$ only if $f(X)$ has a linear factor in $\mathbb{Q}[X]$. By Corollary 27 this happens only if

$$f(X) = (aX + b)(g(X))$$

where $a, b \in \mathbb{Z},\ a \neq 0$ and $g(X) \in \mathbb{Z}[X]$. Then if

$$g(X) = c_{n-1}X^{n-1} + \cdots + c_1X + c_0,$$

we have $ac_{n-1} = a_n$ and $b_0c_0 = a_0$. Thus $a|a_n,\ b|a_0$ and $-b/a$ is a root of $f(X)$ in $\mathbb{Q}$. □

Example: Let $f(X) = \frac{3}{5}X^3 + 2X - 1$ in $\mathbb{Q}[X]$. Determine if $f(X)$ is irreducible in $\mathbb{Q}[X]$.

Solution: By Lemma 24 $f(X)$ is irreducible in $\mathbb{Q}[X]$ if and only if $5f(X) = 3X^3+10X-5$ is irreducible. By Theorem 23 this would mean having no root in $\mathbb{Q}$. By Theorem 28 possible roots of $5f(X)$ in $\mathbb{Q}$ are

$$1, -1, 5, -5, \frac{1}{3}, -\frac{1}{3}, \frac{5}{3}, -\frac{5}{3}.$$

It is easily checked that none of these is a root. Since $f(X)$ is cubic it follows that $f(X)$ is irreducible in $\mathbb{Q}[X]$.

Note: A polynomial is called *monic* if its leading coefficient is 1. If $f(X)$ is a monic polynomial in $\mathbb{Z}[X]$ then any rational roots of $f(X)$ are integer divisors of the constant term (provided that this is not zero).

Example: Decide if the polynomial $f(X) = X^5 + 3X^4 - 3X^3 - 8X^2 + 3X - 2$ is irreducible in $\mathbb{Q}[X]$.

Solution : Possible rational roots of $f(X)$ are integer divisors of the constant term -2 - i.e. $1, -1, 2, -2$. Inspection of these possibilities reveals that -2 is a root. Thus $f(X)$ is reducible in $\mathbb{Q}[X]$.

Note: Since $f(X)$ has degree 5, a discovery that $f(X)$ had no rational roots would not have told us anything about the irreducibility or not of $f(X)$ over $\mathbb{Q}$.

There is one known criterion for irreducibility over $\mathbb{Q}$ that applies to polynomials of high degree, but it only applies to polynomials with a special property.

Theorem 29. *(The Eisenstein irreducibility Criterion) Let* $f(X) = a_n X^n + \cdots + a_1 X + a_0$ *be a polynomial in* $\mathbb{Z}[X]$ *where* $a_n \neq 0$*, and* $n \geqslant 2$*. Suppose that there exists a prime number* p *for which*

- p *divides all of* $a_0, a_1, \ldots, a_{n-1}$
- p *does not divide* a_n
- p^2 *does not divide* a_0.

Then $f(X)$ *is irreducible in* $\mathbb{Q}[X]$.

For example the Eisenstein test says that $2X^4 - 3X^3 + 6X^2 - 12X + 3$ is irreducible in $\mathbb{Q}[X]$ since the prime 3 divides all the coefficients except the leading one, and 9 does not divide the constant term.

Proof of Theorem 29: Assume (in the hope of contradiction) that $f(X)$ is reducible and write

$$f(X) = (\underbrace{b_s X^s + \cdots + b_1 X + b_0}_{g(X)})(\underbrace{c_t X^t + \cdots + c_1 X + c_0}_{h(X)})$$

where $g(X), h(X) \in \mathbb{Z}[X]$, $b_s \neq 0$, $c_t \neq 0$, $s \geqslant 1$, $t \geqslant 1$ and $s + t = n$.

Now $b_0 c_0 = a_0$ which means p divides exactly one of b_0 and c_0, as p^2 does not divide a_0. Suppose $p|b_0$ and $p \not| c_0$. Now $a_1 = b_1 c_0 + b_0 c_1$, which means $p|b_1$ since p divides a_1 and b_0 but not c_0. Similarly looking at a_2 shows that p must divide b_2. However p does not divide all the b_i - it does not divide b_s, otherwise it would divide $a_n = b_s c_t$.

Now let k be the least for which $p \not| b_k$. Then $k \leqslant s \Longrightarrow k < n$ and

$$a_k = b_k c_0 + \underbrace{b_{k-1} c_1 + \cdots + b_0 c_k}_{\text{all multiplesof } p}$$

Now $p \not| b_k c_0$ since $p \not| b_k$ and $p \not| c_0$. Since the remaining terms in the above description of a_k are all multiples of p, it follows that $p \not| a_k$, contrary to hypothesis.

We conclude that any polynomial in $\mathbb{Z}[X]$ satisfying the hypotheses of the theorem is irreducible in $\mathbb{Q}[X]$. $\square$

Note: Theorem 29 says nothing at all about polynomials in $\mathbb{Z}[X]$ for which no prime satisfies the requirements in the statement.