1 More on Irreducible Polynomials

We will continue our discussion on irreducible polynomials.

1.1 Primitive Polynomials

Lemma 1.1: Gauss's Lemma

The product of two primitive polynomials is primitive.

Proof. Let $f(x), g(x) \in \mathbb{Z}[x]$ be primitive, and suppose $f(x)g(x)$ is not primitive. Choose a prime p which divides the content of $f(x)g(x)$. Then

$$f(x)g(x) \equiv 0 \pmod{p}$$

Then, $f(x)g(x) \equiv 0 \pmod{p}$. However, $f(x), g(x) \not\equiv 0 \pmod{p}$. Let $\overline{f}(x), \overline{g}(x) \in \mathbb{F}_p[x]$ be the polynomials with $f(x) \equiv \overline{f}(x) \pmod{p}$ and $g(x) \equiv \overline{g}(x) \pmod{p}$. Then

$$f(x)g(x) \equiv \overline{f}(x)\overline{g}(x) \pmod{p}$$

which implies that $\overline{f}(x), \overline{g}(x)$ are zero-divisors in $\mathbb{F}_p[x]$. But, this is a contradiction as $\mathbb{F}_p[x]$ is a field and thus an integral domain. □

1.2 Reducibility over Rational Numbers Implies Reducibility Over Integers

Recall, from earlier, the following theorem.

Theorem 1.1

Let $f(x) \in \mathbb{Z}[x]$. $f(x)$ is reducible over $\mathbb{Q} \implies f(x)$ is reducible over $\mathbb{Z}$.

Proof. Write $f(x) = g(x)h(x)$ for $g(x), h(x) \in \mathbb{Q}[x]$. Without loss of generality, suppose $f(x)$ is primitive; otherwise, let c be the content of $f(x)$ and then let $\frac{1}{c}f(x) = \left(\frac{1}{c}g(x)\right)h(x)$. Let a be the least common multiple of the denominator of coefficients of $g(x)$, and let b be the least common multiple of the denominator of coefficients of $h(x)$. We can now clear denominators like so

$$abf(x) = (ag(x))(bh(x))$$

with $ag(x), bh(x) \in \mathbb{Z}[x]$. Let c_1 be the content of $ag(x)$ and c_2 be the content of $bh(x)$ so that

$$ag(x) = c_1 g_1(x)$$

$$bh(x) = c_2 h_1(x)$$

for primitives g_1, h_1. Then, $abf(x) = c_1 c_2 g_1(x) h_1(x)$ (here, we replaced $ag(x)$ and $bg(x)$ and reorganized them). Since $f(x)$ is primitive, the content of $abf(x)$ is ab. Since $g_1(x)$ and $h_1(x)$ is primitive, by Gauss's Lemma, we know that $g_1(x)h_1(x)$ is primitive; this implies that the content of $c_1 c_2 g_1(x) h_1(x)$ is $c_1 c_2$. This means that

$$ab = c_1 c_2$$

and thus $ab = c_1 c_2$, $\mathbb{Z}[x]$ is an integral domain, and so by multiplicative cancellation, $f(x) = g_1(x)h_1(x)$. By construction, we know that $g_1(x), h_1(x) \in \mathbb{Z}[x]$. □

1.2.1 Example: Concrete Polynomial

Suppose we are given the polynomial

$$f(x) = 6x^2 + x - 2 = \left(3x - \frac{3}{2}\right)\left(2x + \frac{4}{3}\right)$$

and we want to find a factorization of said polynomial over the integers.

Since $f(x)$ is reducible over $\mathbb{Q}$, it must be reducible over $\mathbb{Z}$. We can use the proof above as a guide for finding a factorization. Note that the coefficients of $f(x)$, on the left-hand side, are 6, 1, and -2. Therefore, $\gcd(6, 1, -2) = 1$ so $f(x)$ is a primitive polynomial.

We now need to clear the denominators of the two factors of $6x^2 + x - 2$. The left-hand factor $\left(3x - \frac{3}{2}\right)$ has common denominator 2 and the right-hand factor $\left(2x + \frac{4}{3}\right)$ has common denominator 3. So, we multiply both sides of the equation by $2 \cdot 3$, like so

$$\begin{aligned} 6x^2 + x - 2 &= \left(3x - \frac{3}{2}\right)\left(2x + \frac{4}{3}\right) \\ &\implies 2 \cdot 3(6x^2 + x - 2) = 2\left(3x - \frac{3}{2}\right)3\left(2x + \frac{4}{3}\right) \\ &\implies 2 \cdot 3(6x^2 + x - 2) = \boxed{(6x-3)(6x+4)} \end{aligned}$$

We now look for the content of the two integer factors (boxed above). The left factor $(6x - 3)$ has content 3, while the right factor $(6x + 4)$ has content 2. We can now factor these constants out, giving us

$$2 \cdot 3(6x^2 + x - 2) = 3(2x - 1) \cdot 2(3x + 2)$$

We see that the constants on both sides can be canceled out. Doing so, we have

$$6x^2 + x - 2 = (2x - 1)(3x + 2)$$

so we are done.

1.3 Mod p Irreducibility Test

Theorem 1.2

Let p be a prime and $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) \geq 1$. Let $\overline{f}(x) \in \mathbb{F}_p[x]$ be such that

$$f(x) \equiv \overline{f}(x) \pmod{p}$$

If $\overline{f}(x)$ is irreducible over $\mathbb{F}_p$ and $\deg \overline{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Proof. We prove the contrapositive. Suppose $f(x)$ is reducible over $\mathbb{Q}$. Then, if $\deg \overline{f}(x) \neq \deg f(x)$, then we are done. Otherwise, we have that $f(x) = g(x)h(x)$ over $\mathbb{Q}$, which implies that

$$0 < \deg g(x), \deg h(x) < \deg f(x)$$

This implies that $f(x) = g_1(x)h_1(x)$ over $\mathbb{Z}$ by the theorem we proved above and with

$$0 \leq \deg g_1(x), \deg h_1(x) < \deg f(x)$$

This implies that

$$\overline{f}(x) = \overline{g_1}(x)\overline{h_1}(x) \text{ over } \mathbb{F}_p$$

We know that $\deg f(x) = \deg \overline{f}(x)$ and $\deg g(x) \geq \deg \overline{g_1}(x)$ and $\deg h_1(x) \geq \deg \overline{h_1}(x)$. We then have

$$\begin{aligned} \deg \overline{f}(x) &= \deg \overline{g_1}(x) + \deg \overline{h_1}(x) \\ &\leq \deg g_1(x) + \deg h_1(x) \\ &= \deg f(x) = \deg \overline{f}(x) \end{aligned}$$

So, thus, $\deg g_1(x) = \deg \overline{g_1}(x)$ and $\deg h_1(x) = \deg \overline{h_1}(x)$ and so we have that

$$0 < \deg \overline{g}(x), \deg \overline{h}(x) < \deg f(x) = \deg \overline{f}(x)$$

and thus we are done. □

1.3.1 Example: Polynomial

Is the polynomial

$$f(x) = 21x^3 - 3x^2 + 2x + 9$$

irreducible?

We pick $p = 2$. This gives us

$$f(x) \equiv x^3 + x^2 + 1 = \overline{f}(x) \pmod{p}$$

Since $\deg f(x) = \deg \overline{f}(x) = 3$, this condition is satisfied. We now need to check if $\overline{f}(x)$ is irreducible over $\mathbb{F}_2$. To do so, we can just brute-force it:

$$\overline{f}(0) = 0 + 0 + 1 = 1$$

$$\overline{f}(1) = 1 + 1 + 1 = 3 \equiv 1$$

As this polynomial has no roots and $\deg \overline{f}(x) = 3$, the reducibility test for degrees 2 and 3 states that $\overline{f}(x)$ is irreducible. Therefore, $f(x)$ is irreducible over $\mathbb{Z}$.