1 More on Irreducible Polynomials

We will continue our discussion on irreducible polynomials.

1.1 Eisenstein's Criterion

Theorem 1.1

Let

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

If there is a prime p such that $p \nmid a_n$, $p \mid a_{n-1}, \ldots, p \mid a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Suppose, towards a contradiction, that $f(x)$ is reducible over $\mathbb{Q}$. This implies that $f(x)$ is reducible over $\mathbb{Z}$. We write

$$f(x) = g(x)h(x)$$

with $0 < \deg g(x), \deg h(x) < \deg f(x)$. We then write

$$g(x) = b_r x^r + \ldots + b_1 x + b_0$$

$$h(x) = c_s x^s + \ldots + c_1 x + c_0$$

It follows that

$$f(x) = g(x)h(x) = b_0c_0 + (b_1c_0 + b_0c_1)x + \ldots$$

If $p|a = b_0c_0$, then it follows that $p|b_0$ or $p|c_0$. We also know that $p \nmid a$, implying that $p^2 \nmid b_0$ *and* $p^2 \nmid c_0$. Suppose WLOG that $p|b_0$ and $p \nmid c_0$. Suppose this holds for the leading term, $p \nmid a_n = b_r c_s$; thus, $p \nmid b_r$ and $p \nmid c_s$. Let t be the minimal index such that $p \nmid b_t$ $(t < r < n = \deg f(x))$. Then, $p|a_t = b_t c_0 + b_{t-1}c_1 + \ldots b_0 c_t$. Because t is minimal, it follows that $p|b_{t-1} \ldots p|b_0$ all holds. This implies that

$$0 \equiv b_t c_0 + 0 \pmod{p}$$

but this is a contradiction since $b_0 \not\equiv 0 \pmod{p}$ and $c_0 \not\equiv 0 \pmod{p}$, a contradiction as $\mathbb{Z}/p\mathbb{Z}$ is an integral domain.

1.1.1 Cyclotomic Polynomial

Consider the pth Cyclotomic polynomial. That is, for any prime p, the pth Cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible over $\mathbb{Q}$.

1.1.2 Example: Polynomial

Is the polynomial

$$x^5 + 2x^2 + 2$$

irreducible?

Consider the prime $p = 2$. It's obvious that, for each coefficient, $2 \nmid 1$ is true, $2|2$ is true, and $2|2$ is true. Additionally, $4 \nmid 2$, so by Eisenstein's Criterion, it follows that this polynomial is irreducible.

1.2 Maximal Ideals

Theorem 1.2

Let $\mathbb{F}$ be a field and $p(x) \in F[x]$. Then, $\langle p(x) \rangle$ is maximal in $\mathbb{F}[x]$ if and only if $p(x)$ is irreducible over F.

Theorem 1.3

Let $\mathbb{F}$ be a field and $p(x)$ be an irreducible polynomial over $\mathbb{F}$. Then, $\mathbb{F}[x]/\langle p(x) \rangle$ is a field.

Corollary 1.1

Let $\mathbb{F}$ be a field and let $p(x), a(x), b(x) \in \mathbb{F}[x]$. If $p(x)$ is irreducible over $\mathbb{F}$ and $p(x)|a(x)b(x)$, then $p(x)|a(x)$ or $p(x)|b(x)$.