Chapter 1

2024-04-21 – Cyclotomic Polynomials

1.1 Explicit construction

For the cyclotomic polynomials there is always a coefficient which is exactly $1 \in \mathbb{Z}$ and maps to the relevant $1 \in R$ for any commutative unital zero-divisor-free factorial ring over which we consider the cyclotomic polynomial. Hence recall the famous Eisenstein's criterion to look up in your favourite algebra reference, with simplification to $\mathbb{Z}$ and $\mathbb{Q}$.

Proposition 1.1.1. *Let $f = \sum_i a_i X^i \in \mathbb{Z}[X]$ be a polynomial with coefficients in $\mathbb{Z}$ of degree N which is monic, i.e. a polynomial of degree N such that $a_N = 1$.*

Assume $a_0 = \pm p$ for $p \in \mathbb{N}$ a prime number, and assume in addition $p|a_i$ for each a_i with $i = 1, \ldots, N-1$. Then f is irreducible in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$.

Proof. Let $f = gh$ in $\mathbb{Q}[X]$. In fact the factors can be chosen as $g, h \in \mathbb{Z}[X]$ with both degrees strictly smaller than f's.

For $p \in \mathbb{Z}$ prime the ideal $(p) \subset \mathbb{Z}$ is a prime ideal, with quotient $\mathbb{Z}/(p) = \mathbb{F}_p$. On coefficients this induces a reduction ring homomorphism:

$$\pi \colon \mathbb{Z}[X] \to \mathbb{Z}/p[X].$$

By the assumptions on f get $\pi(f) = X^N$, but also $\pi(g)\pi(h) = X^N$ because $f = gh$ by the assumption before. Since $\mathbb{F}_p[X]$ is a euclidean domain it is also factorial, so $\pi(g) = a_i X^i$ and $\pi(h) = b_j X^j$ such that $i + j = N$ and $a_i b_j = 1 \in \mathbb{Z}/p$.

Hence we get for the integral g, h: $p|g_0$ and $p|h_0$, hence follows $p^2|a_0$, but we assumed $a_0 = p$ prime, which is a contradiction. So f was in fact irreducible in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$. $\square$