

# Chapter 1

## 2024-04-21 – Cyclotomic Polynomials

### 1.1 Polynomials and power series with integer coefficients

**Definition 1.1.1.** Consider the set  $\mathbb{Z}[[X]] = \{ \sum_{i \geq 0} c_i X^i \mid c_i \in \mathbb{Z} \}$  of not necessarily finite sums in the monomials  $X^i$  with multiplication defined by  $(f(X)g(X))_i = \sum_k f_k g_{i-k}$  for each coefficient index  $i \geq 0$ . It is a commutative ring with unit  $1 \in \mathbb{Z} \subset \mathbb{Z}[[X]]$ .

It naturally includes the ring of integral polynomials  $\mathbb{Z}[X] \subset \mathbb{Z}[[X]]$ , which are integral power series with only finitely many non-zero coefficients and the multiplication as induced from power series. In particular  $1 \in \mathbb{Z} \subset \mathbb{Z}[X] \subset \mathbb{Z}[[X]]$  each have the same unit considered along the canonical subset inclusions.

It is confusing to assemble all the facts about units and primes  $\mathbb{Z} \subset \mathbb{Z}[X] \subset \mathbb{Z}[[X]]$  from the literature, so I summarise and prove them here as far as elementarily possible and conveniently enlightening.

**Proposition 1.1.2.** *The, multiplicative invertible elements, in short: units of  $\mathbb{Z}$  are plain the signs  $\mathbb{Z}^\times = \{\pm 1\}$ . The units in integral power series are given by  $\mathbb{Z}[[X]]^\times = \{ \sum_{i \geq 0} c_i X^i \mid c_i \in \mathbb{Z} \wedge c_0 \in \{\pm 1\} \}$ . Since each non-constant power series which is a unit in power series is either not a polynomial itself, or its inverse is a properly infinite power series, get  $\mathbb{Z}[X]^\times = \mathbb{Z}^\times = \{\pm 1\}$ .*

*Proof.* Clearly the units in  $\mathbb{Z}$  are exactly the non-zero elements  $n$ , which can be inverted in  $\mathbb{Z}$ , i.e. where  $\frac{1}{n} \in \mathbb{Q} \cap \mathbb{Z}$ . So  $|n| \geq 2$  is clearly not invertible in  $\mathbb{Z}$ , 0 is not invertible anywhere, but  $-1, 1$  clearly are each their own multiplicative inverse in any unital ring.

Let  $p = \sum c_i X^i$  be an integral power series which is a unit, i.e. for which there is a unique  $q = \sum d_i X^i$ , such that:

$$p \cdot q = \sum_{i,j} c_i \cdot d_j X^{i+j} = 1.$$

In degree 0 it follows:

$$c_0 d_0 = 1,$$

since the units of  $\mathbb{Z}$  are  $\{\pm 1\}$  without loss of generality we can assume  $c_0 = d_0 = 1$  by multiplying  $p, q$  each by  $-1$ . In particular the subset inclusion follows

$$\mathbb{Z}[[X]]^\times \subset \left\{ \sum_{i \geq 0} c_i X^i \mid c_i \in \mathbb{Z} \wedge c_0 \in \{\pm 1\} \right\}$$

For the  $\supset$ -inclusion consider without loss of generality a  $p = 1 + \sum_{i \geq 1} c_i X^i$  by multiplying with  $-1$  if necessary. As above we find necessarily an inverse power series has to start with the same constant term  $d_0 = 1$ . Hence we get in degree 1:

$$d_1 = -c_1.$$

It follows in degree 2:

$$c_0 d_2 + c_1 d_1 + c_2 d_0 = 0$$

giving

$$d_2 = c_1^2 - c_2.$$

Inductively assume  $d_i$  determined up to  $n - 1$  and consider degree  $n$ :

$$0 = \sum_{i=0, \dots, n} c_i d_{n-i} = d_n + \sum_{i=0, \dots, n-1} c_i d_{n-i}$$

which gives

$$d_n = - \sum_{i=0, \dots, n-1} c_i d_{n-i}.$$

Then  $q(X) = \sum_n d_n X^n$  satisfies  $pq = 1$  by the inductive construction of its coefficients, so  $p$  is a unit in integral power series.

Finally consider  $p \in \mathbb{Z}[X]^\times$ . On non-zero polynomials with integral coefficients we have a well-defined degree, i.e. a map  $\nu: \mathbb{Z}[X] \rightarrow \mathbb{N}$  which satisfies  $\nu(f \cdot g) = \nu(f) + \nu(g)$ , given by assigning to each polynomial the highest index such that its coefficient is non-zero.

In particular it follows for  $k \in \mathbb{Z}$  and  $p \in \mathbb{Z}[X] \setminus \{0\}$  arbitrary,  $0 = \deg(k)$  and  $\deg(kf) = \deg(f) > 0$ . For a unit we hence get  $0 = \deg(1) = \deg(pq) = \deg(p) + \deg(q)$ , hence follows  $\deg(p) = \deg(q) = 0$  in natural numbers, so  $p \in \{\pm 1\}$  with no non-trivial higher terms. If  $p$  is an integral polynomial invertible considered as a power series, then follows " $\deg(q) = \infty$ ". I.e. if there were a highest non-trivial coefficient for  $q$ , then  $pq = 1$  forces  $p$  and  $q$  to be constant and in the units of  $\mathbb{Z}$ .  $\square$

**Remark 1.1.3.** Do note how that describes the units in the integral power series ring which are themselves polynomials. Since there is not a well-defined degree map like on polynomials anymore, a  $q$  inverting a polynomial  $p$  multiplicatively can escape to "infinite degree", i.e. the inductive process describing the  $d_n$  does not stop to produce non-trivial coefficients. Thus no non-constant polynomial can have a multiplicative inverse in integral polynomials.

**Proposition 1.1.4.** Let  $f = gh$  in integral polynomials with  $f = \sum_i f_i X^i, g = \sum_i g_i X^i, h = \sum_i h_i X^i$  each finite sums with integer coefficients. Assume  $f_0 = 1$  and without loss of generality  $g_0 = h_0 = 1$ . It follows  $f, g, h \in \mathbb{Z}[[X]]^\times$ , and  $f^{-1} = h^{-1}g^{-1}$  with each factor a properly infinite power series, each having constant term 1 as well.

**Corollary 1.1.5.** *The units of integral power series decompose as*

$$\mathbb{Z}[[X]]^\times \cong \{\pm 1\} \oplus X\mathbb{Z}[[X]].$$

*Proof.* Let  $p$  be a unit in integral power series, i.e.  $p = \pm 1 + \sum_{i \geq 1} c_i X^i = \pm 1 + X \sum_i c_i X^{i-1}$  by our proposition above. The decomposition as indicated defines a map into the product, which is evidently injective and surjective. It is also just regarding a formal sum as a sum in a polynomial ring for the inverse map, one could regard the isomorphism as formal nonsense.  $\square$

**Corollary 1.1.6.** *For a unit  $f \in \mathbb{Z}[[X]]^\times$  get its inverse  $g$ , then  $f(X^n)$  has the same constant term as  $f$  does, and  $g(X^n)$  is the inverse for  $f(X^n)$ .*

*Proof.* Consider  $fg = 1$  as  $f(X)g(X) = 1$ , then follows  $f(X^n)g(X^n) = 1$ , hence the claim.  $\square$

## 1.2 Explicit construction

**Definition 1.2.1.** Call a polynomial  $f = \sum_i a_i X^i \in \mathbb{Z}[X]$  with  $a_0 = 1$  irreducible, if  $f = gh$  for  $g, h \in \mathbb{Z}[X]$  and  $g \notin \{\pm 1\}$  implies  $h \in \{\pm 1\}$ .

**Proposition 1.2.2.** *A polynomial  $f = \sum_i a_i X^i \in \mathbb{Z}[X]$  is irreducible if and only if any and hence all of its translates  $f_z(X) := f(X - z)$   $z \in \mathbb{Z}$  are irreducible.*

*Proof.* If  $f_z(X)$  were decomposable non-trivially as  $f_z(X) = g(X)h(X)$ , then get  $f(X - z) = g(X)h(X)$ , hence  $f(X) = g(X + z)h(X + z)$  decomposes  $f$ .  $\square$

**Proposition 1.2.3.** *If  $f = \sum_i a_i X^i$  is irreducible with  $a_0 = 1$ , then so is each of the polynomials given by inserting a power of  $X$ :  $f_n(X) := f(X^n)$  with  $n \geq 2$ .*

*Proof.* Assume we had a decomposition in  $\mathbb{Z}[X]$  of  $f_n$ :  $\sum_i a_i X^{ni} = f(X^n) = f_n(X) = g(X)h(X)$ . Show that  $g, h$  each are also of the form  $\bar{g}(X^n)$  and  $\bar{h}(X^n)$ , hence  $Z = X^n$  gives a decomposition  $f(Z) = g(Z)h(Z)$ .

Assume to contradiction for  $g$  and then necessarily  $h$  a coefficient  $g_i$  and  $h_{kn-i}$  both not equal to zero and  $g_i$  the  $i$ -minimal coefficient in  $g$ , such that  $i$  is not a multiple of  $n$ .

By multiplying  $g, h$  each with a sign, we can assume  $1 = a_0 = 1 \cdot 1 = g_0 \cdot h_0$  with  $g_0 = h_0 = 1$ . It follows  $g = 1 + g_i X^i + \sum_{j > i} g_j X^j$  and  $h = 1 + \sum_{j \geq 1} h_j X^j$ .  $\square$

*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 1.2.4.** *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  $i = 1, \dots, N - 1$ . 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:

$$\pi: \mathbb{Z}[X] \rightarrow \mathbb{Z}/p[X].$$

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  $\mathbb{Q}[X]$ .  $\square$