FACTORIZATION OF POLYNOMIALS

1. Polynomials in One Variable Over a Field

Theorem 1.1. *Let k be a field. Then the polynomial ring $k[X]$ is Euclidean, hence a PID, hence a UFD.*

Recall that the polynomial norm is

$$\mathrm{N} : k[X] - \{0\} \longrightarrow \mathbb{Z}_{\geq 0}, \quad \mathrm{N}f = \deg(f).$$

Note that nonzero constant polynomials have norm 0. Sometimes we define

$$\mathrm{N}0 = -\infty$$

as well.

The verification that the $k[X]$-norm makes $k[X]$ Euclidean is a matter of polynomial long division from high school. Specifically, given $f, g \in k[X]$ with $g \neq 0$, proceed as follows.

- (*Initialize*)
  Set $q = 0$ and $r = f$. Let $g = b_m x^m + \cdots$. (So $f = qg + r$.)
- (*Iterate*)
  While $\deg r \geq \deg g$,
  let $r = r_n x^n + \cdots$ and set $\delta = (r_n/b_m)x^{n-m}$
  replace q by $q + \delta$
  replace r by $r - \delta g$. (Still $f = qg + r$, and $\deg r$ has decreased.)
- (*Terminate*)
  Return q and r. (Now $f = qg + r$, and $\deg r < \deg g$.)

2. Primitive Polynomials and the Gauss Lemma

Definition 2.1. *Let A be a UFD. The* **content** *of a nonzero polynomial $f \in A[X]$ is any greatest common divisor of its coefficients. Thus the content is defined up to multiplication by units. A polynomial is* **primitive** *if its content is* 1*.*

Lemma 2.2 (Gauss)**.** *Let A be a UFD, and let $f, g \in A[X]$ be primitive. Then their product fg is again primitive.*

Proof. For any prime π of A, a lowest-index coefficient a_i of f not divisible by π exists because f is primitive, and similarly for a lowest-index coefficient b_j of g not divisible by π. The $(i+j)$-index coefficient of fg is an $i+j+1$-fold sum,

$$a_0 b_{i+j} + \cdots + a_{i-1}b_{j+1} + a_i b_j + a_{i+1}b_{j-1} + a_{i+j}b_0.$$

The first i terms are divisible by π by definition of i, and the similarly for the last j terms. But the middle term $a_i b_j$ is not, and hence the sum is not. ☐

Any nonzero polynomial $f \in A[X]$ takes the form

$$f = c_f \tilde{f} \quad \text{where } c_f \text{ is the content of } f \text{ and } \tilde{f} \text{ is primitive.}$$

And so the short calculation

$$fg = c_f\tilde{f}\,c_g\tilde{g} = c_f c_g \tilde{f}\tilde{g}$$

combines with the Gauss lemma to show that:

The content of the product is the product of the contents.

Naturally, the Gauss *Lemma* has an important consequence. On the face of things, a polynomial $f \in A[X]$ could be irreducible and yet have a nontrivial factorization in $k[X]$ where k is the quotient field of A. However, only slightly more generally than above, any nonzero polynomial $g \in k[X]$ takes the form

$$g = c_g\tilde{g}, \quad c_g \in k^\times,\ \tilde{g} \in A[X] \text{ primitive.}$$

Indeed, let

$$g = \sum_{i=0}^{d} (a_i/b_i)X^i,$$

and set $b_g = \mathrm{lcm}\{b_0, \cdots, b_d\}$. Then $b_g g$ has integral coefficients $a_i b_g/b_i$. Next set $a_g = \gcd\{a_0 b_g/b_0, \cdots, a_d b_g/b_d\}$, so that the suitably-scaled polynomial

$$\tilde{g} = (b_g/a_g)g$$

is primitive. Thus $g = c_g\tilde{g}$ as desired.

Now, if a nonzero polynomial $f \in A[X]$ has a nontrivial factorization $f = gh$ in $k[X]$ then in fact

$$f = c\tilde{g}\tilde{h}, \quad c \in k^\times,\ \tilde{g}, \tilde{h} \in A[X] \text{ primitive.}$$

By the Gauss Lemma, $\tilde{g}\tilde{h}$ is again primitive, and so $c \in R$. That is, the consequence of the Gauss Lemma is:

Theorem 2.3. *Let $f \in A[X]$ be nonzero. If f factors in $k[X]$ then it factors in $A[X]$.*

3. The Criteria of Schönemann and Eisenstein

Proposition 3.1 (Schönemann's Criterion)**.** *Let A be a UFD, and let $f(X) \in A[X]$ be monic of positive degree n. Suppose that for some element a of A and some prime ideal $\mathfrak{p}$ of A,*

$$f(X) = (X - a)^n \bmod \mathfrak{p}[X] \qquad \textit{and} \qquad f(a) \neq 0 \bmod \mathfrak{p}^2.$$

Then $f(X)$ is irreducible modulo $\mathfrak{p}^2[X]$ and hence $f(X)$ is irreducible in $A[X]$.

Especially the ideal $\mathfrak{p}$ could take the form $\mathfrak{p} = \pi A$ where $\pi \in A$ is prime.

Proof. We show the contrapositive statement, arguing that if $f(X)$ is reducible mod $\mathfrak{p}^2[X]$ then its reduction looks enough like $(X-a)^n$ to force $f(a) = 0 \bmod \mathfrak{p}^2$. Specifically, suppose that

$$f(X) = f_1(X)f_2(X) \bmod \mathfrak{p}^2[X].$$

The reduction modulo $\mathfrak{p}^2$ agrees modulo $\mathfrak{p}$ with the reduction modulo $\mathfrak{p}$,

$$f_1(X)f_2(X) = (X-a)^n \bmod \mathfrak{p}[X],$$

and so (since we may take $f_1(X)$ and $f_2(X)$ to be monic) we have for $i = 1, 2$,

$$f_i(X) = (X-a)^{n_i} \bmod \mathfrak{p}[X], \quad n_i \in \mathbb{Z}^+.$$

(Specifically, from $f_1(X)f_2(X) = (X-a)^n$ in $(A/\mathfrak{p})[X]$ where the polynomials now have their coefficients reduced modulo $\mathfrak{p}$, the same equality holds in $k[X]$ where k is the quotient field of the integral domain $A/\mathfrak{p}$. Because $k[X]$ is a UFD, $f_i(X) = (X-a)^{n_i}$ in $k[X]$ for $i = 1, 2$, but these equalities stand between elements of $(A/\mathfrak{p})[X]$, giving the previous display.) Consequently $f_i(a) = 0 \bmod \mathfrak{p}$ for $i = 1, 2$, and so the first display in the proof gives $f(a) = 0 \bmod \mathfrak{p}^2$ as desired. □

Corollary 3.2 (Prime Cyclotomic Polynomials are Irreducible)**.** *The pth cyclotomic polynomial*

$$\Phi_p(X) = X^{p-1} + \cdots + X + 1$$

is irreducible.

Proof. The relation $(X-1)\Phi_p(X) = X^p - 1$ gives

$$(X-1)\Phi_p(X) = (X-1)^p \bmod p\mathbb{Z}[X].$$

Since $\mathbb{Z}[X]/p\mathbb{Z}[X] \approx (\mathbb{Z}/p\mathbb{Z})[X]$ is an integral domain, we may cancel to get

$$\Phi_p(X) = (X-1)^{p-1} \bmod p\mathbb{Z}[X].$$

Also, $\Phi_p(1) = p \neq 0 \bmod p^2\mathbb{Z}$. So the proposition applies. □

The argument for prime-power cyclotomic polynomials is essentially the same since

$$\Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}) = \frac{X^{p^e} - 1}{X^{p^{e-1}} - 1}\,.$$

Corollary 3.3 (Eisenstein's Criterion)**.** *Let A be a UFD, and consider a polynomial*

$$f(X) = X^n + \cdots + a_1X + a_0 \in A[X].$$

Suppose that for some prime ideal $\mathfrak{p}$ of A,

$$\begin{aligned}&a_0 \in \mathfrak{p}, \quad a_1 \in \mathfrak{p}a_1, \quad \cdots, \quad a_{n-1} \in \mathfrak{p},\\ &a_0 \notin \mathfrak{p}^2.\end{aligned}$$

Then f is irreducible in $A[X]$.

Proof. Because $f(X) = X^n \bmod \mathfrak{p}[X]$ and $f(0) \neq 0 \bmod \mathfrak{p}^2$, the proposition applies with $a = 0$. □

In modern texts, Eisenstein's Criterion is proved directly with no reference to Schönemann's Criterion, as follows. The product of two polynomials

$$\begin{aligned}g(X) &= b_\ell X^\ell + \cdots + b_1X + b_0 \in A[X], \quad b_\ell \neq 0,\\ h(X) &= c_mX^m + \cdots + c_1X + c_0 \in A[X], \quad c_m \neq 0\end{aligned}$$

is

$$g(X)h(X) = \sum_{k=0}^{\ell+m} \sum_{i+j=k} b_ic_jX^k.$$

The constant term is b_0c_0, so if we are to have $f(X) = g(X)h(X)$ then since

$$a_0 = b_0c_0$$

and a_0 contains exactly one power of π, we may assume by symmetry that b_0 is divisible by one power of π and c_0 by none. Let b_k be the lowest-indexed coefficient of $g(X)$ not divisible by π. Then also

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_kc_0$$

is not divisible by π, and so $k = n$. Thus the only possible factorization of f is $f(X) = cg(X)$ where $c \in A$ is not a unit. But f is primitive, so such a factorization is impossible.

Also, modern texts prove that prime cyclotomic polynomials are irreducible by using Eisenstein's Criterion, as follows. Since

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X^2 + X^1 + 1,$$

the finite geometric sum formula gives

$$\Phi_p(X) = \frac{X^p - 1}{X - 1},$$

so that

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \frac{\sum_{i=1}^{p} \binom{p}{i} X^i}{X} = \sum_{i=0}^{p-1} \binom{p}{i+1} X^i.$$

Thus $\Phi_p(X+1)$ satisfies Eisenstein's Criterion at p by properties of the binomial coefficients, making it irreducible over $\mathbb{Z}$. Consequently, $\Phi_p(X)$ is irreducible: any factorization $\Phi_p(X) = g(X)h(X)$ would immediately yield a corresponding factorization $\Phi_p(X+1) = g(X+1)h(X+1)$ since the mapping property of polynomials says that replacing X by $X+1$ gives an $\mathbb{Z}$-linear endomorphism of $\mathbb{Z}[X]$, and in fact an automorphism since the inverse map is obvious. But no such corresponding factorization of $\Phi_p(X+1)$ exists, so no factorization of $\Phi_p(X)$ exists either.

Note how much tidier the Schönemann argument is. See David Cox's January 2011 *Monthly* article for the story of Schönemann's and Eisenstein's criteria.

4. Polynomials over a UFD

Theorem 4.1. *Let A be a UFD. Then the polynomial ring $A[X]$ is again a UFD.*

Proof. Let k be the quotient field of A. Since $k[X]$ is a UFD, the issue is only to show that the unique factorization restricts to the subring $A[X]$.

We have already shown that any nonzero polynomial $g \in k[X]$ takes the form

$$g = c_g \tilde{g}, \quad c_g \in k^\times, \ \tilde{g} \in A[X] \text{ primitive.}$$

Now let $f \in A[X]$ have degree at least 1. Then f factors uniquely into irreducibles in $k[X]$,

$$f = f_1 \cdots f_r.$$

The factorization rewrites as

$$f = c_1 \tilde{f}_1 \cdots c_r \tilde{f}_r, \quad \text{each } c_i \in k^\times, \ \text{each } \tilde{f}_i \in A[X] \text{ irreducible and primitive.}$$

Consolidate the constants to get

$$f = c\tilde{f}_1 \cdots \tilde{f}_r, \quad \text{c} \in k^\times, \ \text{each } \tilde{f}_i \in A[X] \text{ irreducible and primitive.}$$

The Gauss lemma says that $\tilde{f}_1 \cdots \tilde{f}_r$ is again primitive, and thus c is the content of f, an element of A,

$$f = c\tilde{f}_1 \cdots \tilde{f}_r, \quad c \in A, \ \text{each } \tilde{f}_i \in A[X] \text{ irreducible and primitive.}$$

A second factorization,

$$f = d\tilde{g}_1 \cdots \tilde{g}_s, \quad d \in A, \ \text{each } \tilde{g}_i \in A[X] \text{ irreducible and primitive}$$

is the same as the first one in $k[X]$. Thus $s = r$ and $\tilde{g}_i = c_i \tilde{f}_i$ with $c_i \in k^\times$ for each i. It quickly follows that $dc_1 \cdots c_r = c$, and the factorization is unique. (But as always, *unique* means *unique up to units.*) □

Corollary 4.2. *Let A be a UFD, and let n be a positive integer. Then the polynomial ring $A[X_1, \cdots, X_n]$ is again a UFD.*

As an example of some ideas in the writeup thus far, let k be a field, let $n \geq 2$ be an integer, let $a_0, \cdots, a_{n-1}$ be indeterminates over k, and consider the UFD

$$A = k[a_0, \cdots, a_{n-1}].$$

Its quotient field is $K = k(a_0, \cdots, a_{n-1})$, the field generated over k by the indeterminates, the field of rational expressions in the indeterminates. We want to show that the general degree n polynomial over k,

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0,$$

is irreducible in $K[X]$. By Theorem 2.3 it suffices to show that $f(X)$ is irreducible in $A[X]$. But

$$A[X] = k[a_0, \cdots, a_{n-1}][X] = k[a_0, \cdots, a_{n-1}, X],$$

and so it suffices to show that $f(X)$ is does not factor in the UFD $k[a_0, \cdots, a_{n-1}, X]$. Any such factorization would reduce modulo X to a factorization in the quotient ring

$$B = k[a_0, \cdots, a_{n-1}, X]/\langle X \rangle \approx k[a_0, \cdots, a_{n-1}].$$

But the reduction of $f(X)$ in B is (after the isomorphism) simply a_0. Thus the reduction has no factorization, and we are done. (Alternatively, we could define $B' = k[a_0, \cdots, a_{n-1}, X]/\langle a_1, \cdots, a_{n-1} \rangle$ and apply the Eisenstein–Schönemann criterion to the reduction $X^n + a_0$ of $f(X)$ in B'.)

5. Kronecker's Factoring Algorithm

Factoring in the integer ring $\mathbb{Z}$ is a finite process. The most naive method, trial division, requires $\sqrt{n}$ steps to find a factor of n. The next proposition and its corollary show, for example, that factorization in $\mathbb{Z}[X_1, \cdots, X_n]$ is also a finite process.

Proposition 5.1. *Let A be a UFD with a factoring algorithm. Then $A[X]$ is again a UFD with a factoring algorithm.*

Proof. Let $f(X) \in A[X]$ have degree d. We may investigate only whether f has a factor g of degree at most $e = \lfloor d/2 \rfloor$.

Consider the values $f(a_0), \cdots, f(a_e)$ for $e+1$ distinct a-values. If f has a factor g as above then $g(a_i) \mid f(a_i)$ in A for $i = 0, \cdots, e$. Algorithmically, each $f(a_i)$ is a product of finitely many irreducible factors, giving finitely many possibilities for each $g(a_i)$. Each possibility for the values $g(a_0), \cdots, g(a_e)$ determines a unique polynomial $g(X) \in k[X]$ (where k is the field of quotients of A) having degree at most e. Specifically, g can be computed by Lagrange interpolation,

$$g(X) = \sum_{i=0}^{e} g(a_i) \prod_{\substack{j=0 \\ j \neq i}}^{e} \frac{X - a_j}{a_i - a_j}\,.$$

For each such g, the division algorithm in $k[X]$ (where k is the field of quotients of A) shows whether g is a factor of f in $k[X]$ and the Gauss Lemma says that in fact the division algorithm is showing us whether g is a factor of f in $A[X]$. $\square$

In practice the algorithm is hopelessly inefficient, and much better algorithms exist. The point here is only that an algorithm exists at all.

Corollary 5.2. *Let A be a UFD with a factoring algorithm, and let n be a positive integer. Then $A[X_1, \cdots, X_n]$ is again a UFD with a factoring algorithm.*