Math 121. Eisenstein criterion and Gauss' Lemma

Let R be a UFD with fraction field K. The aim of this handout is to prove an irreducibility criterion in $K[X]$ due to Eisenstein: if $f = a_nX^n + \cdots + a_0 \in R[X]$ has positive degree n and π is a prime of R which does not divide a_n but does divide a_i for all $i < n$, yet $\pi^2 \nmid a_0$, then f is irreducible in $K[X]$. As we saw in class, this is immediately reduced to Gauss' Lemma (stated below), and we will focus on proving Gauss' Lemma. As an application of the method of proof, we will establish a UFD property for polynomial rings in several variables.

1. Gauss' Lemma

Before proving Gauss' Lemma, let's give one example of Eisenstein's criterion in action (the trick of "translation") and one non-example to show how the criterion can fail if we drop primality as a condition on π (recall that in the proof of Eisenstein's criterion, the role of π being prime was crucial for knowing that R/π is a domain, so $(R/\pi)[X]$ is a domain).

Example 1.1. Let p be a prime in $\mathbf{Z}$ and consider $\Phi_p = X^{p-1} + \cdots + X + 1 \in \mathbf{Z}[X]$. We claim that this is irreducible in $\mathbf{Q}[X]$ (this is easily verified by bare hands for $\Phi_2 = X+1$ and $\Phi_3 = X^2+X+1$, but for $p \geq 5$ it is clear that hands-on manipulation is pointless). To prove Φ_p is irreducible in $\mathbf{Q}[X]$, we make the change of variable $X \rightsquigarrow X+1$: it is equivalent to show $\Phi_p(X+1)$ is irreducible. But *this* is a polynomial to which Eisenstein applies in $\mathbf{Z}$ for the prime p.

Indeed, in $\mathbf{F}_p[X]$ we have by the magic of characteristic p that

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

so $\Phi_p(X) = (X-1)^{p-1}$ in $\mathbf{F}_p[X]$, so $\Phi_p(X+1) = X^{p-1}$ in $\mathbf{F}_p[X]$. This says that the monic polynomial $\Phi_p(X+1) \in \mathbf{Z}[X]$ of degree $p-1$ has all lower-degree coefficients divisible by p, so we just have to make sure the constant term of $\Phi_p(X+1)$ is not divisible by p^2. Ah, but the constant term is obtained by specializing the variable to zero, and $\Phi_p(1) = p$ by inspection.

Example 1.2. To show what goes wrong if we don't require primality, consider $\Phi_5 = X^4 + X^3 + X^2 + X + 1 \in \mathbf{Z}[X]$. Applying Eisenstein to $\Phi_5(X+1)$ with $p = 5$ shows irreducibility in $\mathbf{Q}[X]$, as we saw above. But consider the ring $R = \mathbf{Z}[\alpha]$ where $\alpha = (-1+\sqrt{5})/2$ satisfies $\alpha^2 + \alpha - 1 = 0$. Since α satisfies a monic quadratic with $\mathbf{Z}$ coefficients, $R = \mathbf{Z} \oplus \mathbf{Z}\alpha$ is finite free as a $\mathbf{Z}$-module. Using some elementary algebraic number theory (Math 154), it can be shown that R is a UFD. But the fraction field $K = \mathbf{Q}(\sqrt{5})$ of R has the property that in $K[X]$ we have the factorization

$$\Phi_5 = X^4 + X^3 + X^2 + X + 1 = (X^2 - \alpha X + 1)(X^2 - (-1-\alpha)X + 1),$$

as one checks by using the relation $\alpha^2 = -\alpha + 1$.

Thus, Φ_5 is reducible in $K[X]$ (the factorization even takes place in $R[X]$), but it is still true in R that $\Phi_5(X+1)$ has all lower degree coefficients divisible by 5 (as this is even true in $\mathbf{Z}$) and its constant term $\Phi_5(0) = 5$ is not divisible by 5^2 (one can check that $5/25 = 1/5$ does not lie in R). But Eisenstein's criterion does not apply to this situation over K with $\pi = 5 \in R$ since 5 is *not* prime in R! In fact, $\sqrt{5} = 2\alpha + 1 \in R$ has the property that it is a non-unit in R (check!) and its square is 5. Hence, $5 \in R$ admits a non-trivial factorization and thus is not prime.

Theorem 1.3. (*Gauss' Lemma*) *Let R be a UFD with fraction field K. If $f \in R[X]$ has positive degree and f is reducible in $K[X]$, then $f = gh$ with $g, h \in R[X]$ having positive degree.*

We should give a warning about how careful one has to be concerning factorization statements when the coefficient ring is not a field. For example, consider $2X$ in $\mathbf{Z}[X]$. Viewing $\mathbf{Z}[X]$ as an absract ring in its own right, clearly the element $2X$ is "reducible" in the sense that it is a product of two non-units (namely, 2 and X). In contrast, $2X \in \mathbf{Q}[X]$ is irreducible, since $2 \in \mathbf{Q}^{\times}$. The point is that whether or not an element is a unit may change if one passes to a bigger ring (and hence may get more units), so statements of "irreducibility" of an element in $R[X]$ when R is not a field (and hence not all nonzero elements of R are units) must be treated very carefully lest one make oversights.

Proof. (of Theorem 1.3) If $f = c \cdot \widetilde{f}$ for some nonzero $c \in R$ and some $\widetilde{f} \in R[X]$, it suffices to treat $\widetilde{f}$ instead of f. Thus, by factoring out the greatest common divisor of the coefficients of f (which makes sense since the coefficient ring R is a UFD), we may assume that the coefficients of f have gcd equal to 1. We call such polynomials *primitive* (e.g., for $R = \mathbf{Z}$, we have that $7X^2 - 14X + 2$ is primitive in $\mathbf{Z}[X]$ whereas $6X^2 - 15$ is not).

The key fact we need is that a product of primitives is primitive. To prove it, let $g, h \in R[X]$ be such that $gh \in R[X]$ is not primitive. We wish to prove that one of g or h is not primitive. The non-primitivity of gh implies that some nonzero non-unit $c \in R$ divides all coefficients of gh. If π is an irreducible factor of c then π divides all coefficients of gh.

Let $\overline{R} = R/(\pi)$, a *domain* since π is irreducible and R is a UFD. Working in $\overline{R}[X]$, we have $\overline{g}\overline{h} = \overline{gh} = 0$. But a polynomial ring over a domain is again a domain (why?), so one of $\overline{g}$ or $\overline{h}$ vanishes. This says that π divides all coefficients of g or h, so one of these is non-primitive, as desired.

Say our given non-trivial factorization is $f = gh$ with $g, h \in K[X]$ having positive degree. If we write the coefficients of g as reduced form fractions with a "least common denominator" (possible since R is a UFD) and then consider the gcd of the numerators, we can write $g = qg_0$ where $q \in K^{\times}$ and $g_0 \in R[X]$ is primitive. Likewise, $h = q'h_0$ where $q' \in K^{\times}$ and $h_0 \in R[X]$ is primitive. Hence, $f = (qq')g_0h_0$ with f and g_0h_0 both primitive. Writing $qq' = a/b$ as a reduced-form fraction with a, b in the UFD R, $bf = ag_0h_0$ in $R[X]$. Comparing gcd's of coefficients on both sides, it follows that $a = bu$ with $u \in R^{\times}$ (!), so $qq' = u \in R^{\times}$. Hence, $f = (ug_0)(h_0)$ is a factorization of f in $R[X]$ with ug_0, h_0 having positive degree. ■

2. Refinements

The technique of studying primitive polynomials has some interesting further applications. We begin with a determination of the irreducibles in $\mathbf{Z}[X]$ using factorizations in $\mathbf{Z}$ and $\mathbf{Q}[X]$. More generally with any UFD:

Theorem 2.1. *If R is a UFD with fraction field K, then $R[X]$ is a UFD. An element $f \in R[X]$ is irreducible if and only if $f \in R$ is irreducible* (*degree* 0 *case*) *or f is primitive in $R[X]$ and irreducible in $K[X]$* (*positive degree case*).

For example, since $\mathbf{Z}^{\times} = \{\pm 1\}$, the irreducibles in $\mathbf{Z}[X]$ are the ordinary (positive) primes, primitive monic polynomials of positive degree which are irreducible over $\mathbf{Q}$, and negatives of these. The basic principle of the proof is to peel off the UFD property from $K[X]$, using the UFD property of R to control nonzero constant scaling factors which are absorbed as units when working over K. In particular, it must be stressed that the general UFD proof in this corollary *uses* the known special case when the coefficient ring is a field. That is, to use this corollary with $R = k$ a field (trivially a UFD) to deduce the UFD property of $k[X]$ would be circular reasoning.

Proof. As a warm-up, we begin by verifying the classification of irreducibles in $R[X]$. Since degrees add when multiplying, it is clear that an irreducible in R is irreducible in $R[X]$ (and a reducible in R is reducible in $R[X]$; a non-unit of R cannot become a unit in $R[X]$). Meanwhile, if $f \in R[X]$ has positive degree then it is reducible if it is not primitive (e.g., $6X + 15 \in \mathbf{Z}[X]$). If f is primitive, a non-trivial factorization $f = ab$ in $R[X]$ must have a and b of positive degree, so in $K[X]$ we get a non-trivial factorization. Note that conversely if $f \in R[X]$ is primitive of positive degree and f is reducible in $K[X]$ then f is also reducible in $R[X]$; this follows from Gauss' Lemma! Hence, we conclude that the irreducibles in $R[X]$ are exactly as advertised.

Now we prove that every nonzero non-unit $f \in R[X]$ is a product of irreducibles, the factorization being unique up to ordering and unit multiples. For elements of degree 0, the only possible factorizations involve elements of degree 0. Thus, the UFD property of R settles both the existence and uniqueness aspects for degree 0 elements in $R[X]$ (the unit ambiguity is not a problem, since $R[X]^\times = R^\times$). Now consider $f \in R[X]$ with positive degree. We use the UFD property of R to write $f = cf_0$ with $c \in R$ and f_0 primitive. By Gauss' Lemma, if f_0 is not irreducible in $K[X]$ then it has a non-trivial factorization $f_0 = g_0h_0$ in $R[X]$ with g_0 and h_0 of positive degree, and clearly necessarily primitive (as f_0 is primitive). Inducting on degrees, we conclude that any positive degree primitive in $R[X]$ is a product of positive degree primitives which are irreducible in $K[X]$ (and hence irreducible in $R[X]$, by Gauss' Lemma). If we also apply the UFD property of R to the coefficient c, we can break up the factorization $f = cf_0$ into $f = \prod p_i \cdot \prod \pi_j$ where $p_i \in R$ are irreducibles (there are none of these if f is primitive) and $\pi_j \in R[X]$ are positive degree primitive irreducibles (necessarily also irreducible in $K[X]$, by Gauss' Lemma). This proves the existence of factorization into irreducibles.

For the uniqueness aspect, suppose $f \in R[X]$ of positive degree admits two factorizations

$$\prod p_i \cdot \prod \pi_j = f = \prod p'_r \cdot \prod \pi'_s,$$

where the p_i's and p'_r's are the degree 0 factors and the π_j's and π'_s's are the positive degree irreducible factors (necessarily irreducible in $K[X]$, from the classification of irreducibles in $R[X]$). In $K[X]$, the π_j's and π'_s's are irreducible and $\prod \pi_j = u \prod \pi'_s$ where $u = \prod p'_r \cdot \prod p_i^{-1} \in K^\times$ is a unit. Hence, by the UFD property of $K[X]$ we conclude that the two collections $\{\pi_j\}$ and $\{\pi'_s\}$ are the same up to ordering and $K^\times$-multiple. But these collections consist of *primitives*, and if $g, h \in R[X]$ are primitive then g, h are $K^\times$-multiples in $K[X]$ if and only if they are $R^\times$-multiples in $R[X]$. To see this, note that if $g = ch$ for some $c \in K^\times$ then we write $c = a/a'$ with $a, a' \in R - \{0\}$ having no non-trivial common factor (this can be done since R is a UFD), so then $a'g = ah$ in $R[X]$. The gcd's of the collection of R-coefficients on each of the two sides are a' and a respectively, since g and h are *primitive*, so since gcd's are only well-defined up to unit multiple we conclude that $a = a'u$ for $u \in R^\times$, whence $c = a/a' = u \in R^\times$ as desired.

We conclude that the two collections $\{\pi_j\}$ and $\{\pi'_s\}$ are the same up to ordering and $R^\times$-multiple. Cancelling, we see that $\prod p_i$ and $\prod p'_r$ in R are off by unit multiple, so by the UFD property of R we deduce that $\{p_i\}$ and $\{p'_r\}$ are the same up to ordering and $R^\times$-multiple. This proves the uniqueness of factorization into irreducibles in $R[X]$ (up to ordering and unit multiples). ■

Corollary 2.2. *If R is a UFD, so is $R[X_1, \dots, X_n]$ for all $n \geq 1$.*

Proof. The case $n = 1$ is the preceding corollary. Since $R[X_1, \dots, X_n] \simeq (R[X_1, \dots, X_{n-1}])[X_n]$ for $n > 1$, we may induct on n (note the need to have the previous corollary for *arbitrary* UFD's in order to carry out the induction!). ■

As one example, $\mathbf{Z}[X_1, \dots, X_n]$ is a UFD for all $n \geq 1$. It is actually *not* a PID for any $n \geq 1$. Likewise, $k[X_1, \dots, X_n]$ is a UFD for $n \geq 1$, but it is not a PID when $n > 1$. To give counterexamples to the PID property, one just has to check that if R is a UFD which is *not* a field and $\pi \in R$ is an irreducible (which exists by the UFD property applied to any non-zero non-unit, such elements existing in R precisely when R is not a field), then (π, X) is a non-principal ideal in $R[X]$. This is a pleasant exercise.

It is also instructive to chase through the proof of the UFD property in several variables to try to make it effective. For example, follow the method of proof used above to factor

$$-6X^3 + 6X^2Y^2 + 6X^3Y - 3XY + 3Y^3 + 3XY^2 \in \mathbf{Z}[X, Y]$$

into irreducibles.