16. Eisenstein's criterion

1. *Eisenstein's irreducibility criterion*

Let R be a commutative ring with 1, and suppose that R is a *unique factorization domain.* Let k be the field of fractions of R, and consider R as imbedded in k.

[1.0.1] **Theorem:** Let

$$f(x) = x^N + a_{N-1}x^{N-1} + a_{N-2}x^{N-2} + \ldots + a_2x^2 + a_1x + a_0$$

be a polynomial in $R[x]$. If p is a prime in R such that p divides every coefficient a_i but p^2 does *not* divide a_0, then $f(x)$ is irreducible in $R[x]$, and is irreducible in $k[x]$.

Proof: Since f has coefficients in R, its *content* (in the sense of Gauss' lemma) is in R. Since it is monic, its content is 1. Thus, by Gauss' lemma, if $f(x) = g(x) \cdot h(x)$ in $k[x]$ we can adjust constants so that the content of both g and h is 1. In particular, we can suppose that both g and h have coefficients in R, and are monic.

Let

$$g(x) = x^m + b_{m-1}x^{m-1} + b_1x + b_0$$

$$h(x) = x^n + c_{m-1}x^{m-1} + c_1x + c_0$$

Not both b_0 and c_0 can be divisible by p, since a_0 is not divisible by p^2. Without loss of generality, suppose that $p|b_0$. Suppose that $p|b_i$ for i in the range $0 \le i \le i_1$, and p does *not* divide b_{i_1}. There *is* such an index i_1, since g is monic. Then

$$a_{i_1} = b_{i_1}c_0 + b_{i_1-1}c_1 + \ldots$$

On the right-hand side, since p divides $b_0, \ldots, b_{i_1-1}$, necessarily p divides all summands but possible the first. Since p divides *neither* b_{i_1} nor c_0, and since R is a UFD, p cannot divide $b_{i_1}c_0$, so cannot divide a_{i_1}, contradiction. Thus, after all, f does not factor. ///

2. *Examples*

[2.0.1] **Example:** For a rational prime p, and for any integer $n > 1$, not only does

$$x^n - p = 0$$

not have a *root* in $\mathbb{Q}$, but, in fact, the polynomial $x^n - p$ is *irreducible* in $\mathbb{Q}[x]$.

[2.0.2] **Example:** Let p be a prime number. Consider the p^{th} cyclotomic polynomial

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

We claim that $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$. Although $\Phi_p(x)$ itself does not directly admit application of Eisenstein's criterion, a minor variant of it does. That is, consider

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

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \ldots + \binom{p}{p-2}x + \binom{p}{p-1}$$

All the lower coefficients are divisible by p, and the constant coefficient is exactly p, so is not divisible by p^2. Thus, Eisenstein's criterion applies, and f is irreducible. Certainly if $\Phi_p(x) = g(x)h(x)$ then $f(x) = \Phi_p(x+1) = g(x+1)h(x+1)$ gives a factorization of f. Thus, Φ_p has no proper factorization.

[2.0.3] **Example:** Let $f(x) = x^2 + y^2 + z^2$ in $k[x, y, z]$ where k is *not* of characteristic 2. We make identifications like

$$k[x, y, z] = k[y, z][x]$$

via the natural isomorphisms. We want to show that $y^2 + z^2$ is divisible by some prime p in $k[y, z]$, and *not* by p^2. It suffices to show that $y^2 + z^2$ is divisible by some prime p in $k(z)[y]$, and *not* by p^2. Thus, it suffices to show that $y^2 + z^2$ is not a unit, and has no repeated factor, in $k(z)[y]$. Since it is of degree 2, it is certainly not a unit, so has *some* irreducible factor. To test for repeated factors, compute the *gcd* of this polynomial and its derivative, viewed as having coefficients in the field $k(z)$: [1]

$$(y^2 + z^2) - \frac{y}{2}(2y) = z^2 = \text{ non-zero constant}$$

Thus, $y^2 + z^2$ is a square-free non-unit in $k(z)[y]$, so is divisible by some irreducible p in $k[y, z]$ (Gauss' lemma), so Eisenstein's criterion applies to $x^2 + y^2 + z^2$ and p.

[2.0.4] **Example:** Let $f(x) = x^2 + y^3 + z^5$ in $k[x, y, z]$ where k is *not* of characteristic dividing 30. We want to show that $y^3 + z^5$ is divisible by some prime p in $k[y, z]$, and *not* by p^2. It suffices to show that $y^3 + z^5$ is divisible by some prime p in $k(z)[y]$, and *not* by p^2. Thus, it suffices to show that $y^2 + z^2$ is not a unit, and has no repeated factor, in $k(z)[y]$. Since it is of degree 2, it is certainly not a unit, so has *some* irreducible factor. To test for repeated factors, compute the *gcd* of this polynomial and its derivative, viewed as having coefficients in the field $k(z)$: [2]

$$(y^2 + z^2) - \frac{y}{2}(2y) = z^2 = \text{ non-zero constant}$$

[1] It is here that the requirement that the characteristic not be 2 is visible.

[2] It is here that the requirement that the characteristic not be 2 is visible.

Thus, $y^2 + z^2$ is a square-free non-unit in $k(z)[y]$, so is divisible by some irreducible p in $k[y, z]$ (Gauss' lemma), so Eisenstein's criterion applies to $x^2 + y^2 + z^2$ and p.

Exercises

16.[2.0.1] Prove that $x^7 + 48x - 24$ is irreducible in $\mathbb{Q}[x]$.

16.[2.0.2] Not only does Eisenstein's criterion (with Gauss' lemma) fail to prove that $x^4 + 4$ is irreducible in $\mathbb{Q}[x]$, but, also, this polynomial *does* factor into two irreducible quadratics in $\mathbb{Q}[x]$. Find them.

16.[2.0.3] Prove that $x^3 + y^3 + z^3$ is irreducible in $k[x, y, z]$ when k is a field not of characteristic 3.

16.[2.0.4] Prove that $x^2 + y^3 + z^5$ is irreducible in $k[x, y, z]$ even when the underlying field k is of characteristic $2, 3$, or 5.

16.[2.0.5] Prove that $x^3 + y + y^5$ is irreducible in $\mathbb{C}[x, y]$.

16.[2.0.6] Prove that $x^n + y^n + 1$ is irreducible in $k[x, y]$ when the characteristic of k does not divide n.

16.[2.0.7] Let k be a field with characteristic not dividing n. Show that any polynomial $x^n - P(y)$ where $P(y)$ has no repeated factors is irreducible in $k[x, y]$.