Over a GCD Domain – Part II

In this section we establish some important results about irreducibility and factorization for polynomials over a GCD domain.

Proposition 1 (Gauss' Lemma – Part II)**.** *Let R be a GCD domain with field of fractions F, and let $p(x) \in R[x]$ have positive degree. Then $p(x)$ is irreducible in $R[x]$ if and only if $p(x)$ is irreducible in $F[x]$ and primitive in $R[x]$.*

Proof. (type this) □

Combined with Eisenstein's criterion, Gauss's lemma provides an easy-to-apply irreducibility criterion.

Corollary 2. *If $p(x) \in R[x]$ (R a GCD domain) is Eisenstein and primitive, then $p(x)$ is irreducible in $R[x]$.*

Proof. Suppose $p(x) = a(x)b(x)$ with $a, b \in R[x]$. Since p is Eisenstein, WLOG $a(x)$ is a constant; say $a(x) = a_0$. Now $a_0 | p$ in $R[x]$, so that $a_0 | \mathsf{content}(p)$ in R. Since $p(x)$ is primitive, a is a unit in R, hence a unit in $R[x]$. So $p(x)$ is irreducible in $R[x]$. □

This criterion can be used to quickly verify that a given polynomial is irreducible – when it applies. Unfortunately there are plenty of irreducible polynomials to which this criterion does not apply. For example, $p(x) = x^2 + 1$ is primitive in $\mathbb{Z}[x]$, and in fact is irreducible. But it is not Eisenstein at any prime.

Proposition 3 (Rational Root Theorem)**.** *Let R be a GCD domain with fraction field F. Suppose $p(x) \in R[x]$. Let $\frac{u}{v} \in F$ be a fraction in lowest terms; that is, $\mathsf{gcd}\,(u, v) = 1$ in R. If $\frac{u}{v}$ is a root of $p(x)$, then u divides the constant coefficient of p, and v divides the leading coefficient of p.*

The Rational Root Theorem allows us to restrict the possible "rational roots" (that is, those in F, or equivalently factors over R of the form $ax - b$) to a finite list of possibilities. For example, applying this theorem to $p(x) = x^2 + 1$ we see that the only possible rational roots of $p(x)$ are ± 1, and it is easily seen that neither of these is a root. So by (???) this p is irreducible in $\mathbb{Z}[x]$.

Exercises

1. Let R be a GCD domain with $p(x), q(x) \in R[x]$ so that q is irreducible (hence prime), and let k be a natural number. Show that q^{k+1} divides p in $R[x]$ iff $q | p$ and $q^k | p'$ in $R[x]$. In particular, show that p is squarefree iff $\mathsf{gcd}\,(p, p') = 1$.