Eisenstein criterion in terms of divisor theory

Canonical name	EisensteinCriterionInTermsOfDivisorTheory
Date of creation	2013-03-22 18:00:45
Last modified on	2013-03-22 18:00:45
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	6
Author	pahio (2872)
Entry type	Theorem
Classification	msc 13A05
Related topic	DivisorTheory

The below theorem generalises Eisenstein criterion of irreducibility from UFD's to domains with divisor theory.

Theorem. Let $f(x) := a_0+a_1x+\ldots+a_nx^n$ be a primitive polynomial over an integral domain $\mathcal{O}$ with `http://planetmath.org/DivisorTheory`divisor theory $\mathcal{O}^* \to \mathfrak{D}$. If there is a prime divisor $\mathfrak{p} \in \mathfrak{D}$ such that

- $\mathfrak{p} \mid a_0,\, a_1,\, \ldots,\, a_{n-1}$,
- $\mathfrak{p} \nmid a_n$,
- $\mathfrak{p}^2 \nmid a_0$,

then the polynomial is irreducible.

Proof. Suppose that we have in $\mathcal{O}[x]$ the factorisation

$$f(x) = (b_0+b_1x+\ldots+b_sx^s)(c_0+c_1x+\ldots+c_tx^t)$$

with $s > 0$ and $t > 0$. Because the principal divisor (a_0), i.e. $(b_0)(c_0)$ is divisible by the prime divisor $\mathfrak{p}$ and there is a unique factorisation in the monoid $\mathfrak{D}$, $\mathfrak{p}$ must divide (b_0) or (c_0) but, by $\mathfrak{p}^2 \nmid (a_0)$, not both of (b_0) and (c_0); suppose e.g. that $\mathfrak{p} \mid c_0$. If $\mathfrak{p}$ would divide all the coefficients c_j, then it would divide also the product $b_sc_t = a_n$. So, there is a certain smallest index k such that $p \nmid c_k$. Accordingly, in the sum $b_0c_k+b_1c_{k-1}+\ldots+b_kc_0$, the prime divisor $\mathfrak{p}$ `http://planetmath.org/DivisibilityInRings`divides every summand except the first (see the definition of `http://planetmath.org/DivisorTheory`divisor theory); therefore it cannot divide the sum. But the value of the sum is a_k which by hypothesis is divisible by the prime divisor. This contradiction shows that the polynomial $f(x)$ is irreducible.