Eisenstein criterion

Canonical name	EisensteinCriterion
Date of creation	2013-03-22 12:16:32
Last modified on	2013-03-22 12:16:32
Owner	Daume (40)
Last modified by	Daume (40)
Numerical id	13
Author	Daume (40)
Entry type	Theorem
Classification	msc 13A05
Synonym	Eisenstein irreducibility criterion
Related topic	GausssLemmaII
Related topic	IrreduciblePolynomial2
Related topic	Monic2
Related topic	AlternativeProofThatSqrt2IsIrrational

Theorem (Eisenstein criterion)**.** *Let f be a primitive polynomial over a commutative unique factorization domain R, say*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \ .$$

If R has an irreducible element p such that

$$p \mid a_m \qquad 0 \leq m \leq n-1$$

$$p^2 \nmid a_0$$

$$p \nmid a_n$$

then f is irreducible.

Proof. Suppose

$$f = (b_0 + \ldots + b_s x^s)(c_0 + \ldots + c_t x^t)$$

where $s > 0$ and $t > 0$. Since $a_0 = b_0 c_0$, we know that p divides one but not both of b_0 and c_0; suppose $p \mid c_0$. By hypothesis, not all the c_m are divisible by p; let k be the smallest index such that $p \nmid c_k$. We have $a_k = b_0 c_k + b_1 c_{k-1} + \ldots + b_k c_0$. We also have $p \mid a_k$, and p divides every summand except one on the right side, which yields a contradiction. QED $\square$