Gauss's lemma II

Canonical name	GausssLemmaII
Date of creation	2013-03-22 13:07:52
Last modified on	2013-03-22 13:07:52
Owner	bshanks (153)
Last modified by	bshanks (153)
Numerical id	18
Author	bshanks (153)
Entry type	Theorem
Classification	msc 12E05
Synonym	Gauss' lemma II
Related topic	GausssLemmaI
Related topic	EisensteinCriterion
Related topic	ProofOfEisensteinCriterion
Related topic	PrimeFactorsOfXn1
Related topic	AlternativeProofThatSqrt2IsIrrational
Defines	primitive polynomial

Definition. A polynomial $P = a_n x^n + \cdots + a_0$ over an integral domain D is said to be *primitive* if its coefficients are not all divisible by any element of D other than a unit.

Proposition (Gauss). Let D be a unique factorization domain and F its field of fractions. If a polynomial $P \in D[x]$ is reducible in $F[x]$, then it is reducible in $D[x]$.

Remark. The above statement is often used in its contrapositive form. For an example of this usage, see `http://planetmath.org/AlternativeProofThatSqrt2IsIrrati` entry.

Proof. A primitive polynomial in $D[x]$ is by definition divisible by a non invertible constant polynomial, and therefore reducible in $D[x]$ (unless it is itself constant). There is therefore nothing to prove unless P (which is not constant) is primitive. By assumption there exist non-constant $S, T \in F[x]$ such that $P = ST$. There are elements $a, b \in F$ such that aS and bT are in $D[x]$ and are primitive (first multiply by a nonzero element of D to chase any denominators, then divide by the gcd of the resulting coefficients in D). Then $aSbT = abP$ is primitive by Gauss's lemma I, but P is primitive as well, so ab is a unit of D and $P = (ab)^{-1}(aS)(bT)$ is a nontrivial decomposition of P in $D[X]$. This completes the proof.

Remark. Another result with the same name is Gauss' lemma on quadratic residues.

From the above proposition and its proof one may infer the

Theorem. If a primitive polynomial of $D[x]$ is divisible in $F[x]$, then it splits in $D[x]$ into primitive prime factors. These are uniquely determined up to unit factors of D.