Gauss's lemma I

Canonical name	GausssLemmaI
Date of creation	2013-03-22 13:07:49
Last modified on	2013-03-22 13:07:49
Owner	bshanks (153)
Last modified by	bshanks (153)
Numerical id	17
Author	bshanks (153)
Entry type	Theorem
Classification	msc 12E05
Related topic	GausssLemmaII

There are a few different things that are sometimes called "Gauss's Lemma". See also Gauss's Lemma II.

Gauss's Lemma I: If R is a UFD and $f(x)$ and $g(x)$ are both primitive polynomials in $R[x]$, so is $f(x)g(x)$.

Proof: Suppose $f(x)g(x)$ not primitive. We will show either $f(x)$ or $g(x)$ isn't as well. $f(x)g(x)$ not primitive means that there exists some non-unit d in R that divides all the coefficients of $f(x)g(x)$. Let p be an irreducible factor of d, which exists and is a prime element because R is a UFD. We consider the quotient ring of R by the principal ideal pR generated by p, which is a prime ideal since p is a prime element. The canonical projection $R \to R/pR$ induces a surjective ring homomorphism $\theta : R[X] \to (R/pR)[X]$, whose kernel consists of all polynomials all of whose coefficients are divisible by p; these polynomials are therefore not primitive.

Since pR is a prime ideal, R/pR is an integral domain, so $(R/pR)[x]$ is also an integral domain. By hypothesis θ sends the product $f(x)g(x)$ to $0 \in (R/pR)[X]$, which is therefore the product of $\theta(f(x))$ and $\theta(g(x))$, and one of these two factors in $(R/pR)[x]$ must be zero. But that means that $f(x)$ or $g(x)$ is in the kernel of θ, and therefore not primitive.