A p-adic proof of Gauss's lemma

William Jones

The goal of this note is to provide a proof of a fundamental result in commutative algebra:

Theorem 1 (Gauss's Lemma). *If R is a UFD and $f \in R[x]$ is written as gh in $R_0[x]$, where g, h are both monic, then $g, h \in R[x]$.*

Equivalently, monic f is irreducible in $R[x]$ if and only if it is irreducible in $R_0[x]$.

Here R_0 denotes the localization of R at 0; i.e., R's quotient field. This will be proved using p-adic methods following the argument detailed by Bruno Joyal on Math.SE 696669. I think it's neat, which is why it's here!

Let p be a prime of R. Then every nonzero $z \in R_0$ can be written uniquely as $ab^{-1}p^k$, where a, b, p are all coprime. Denote by $|-|_p$ the **p-adic absolute value** on R_0, defined by the rule

$$|ab^{-1}p^k|_p = \mathbf{N}(p)^{-k}$$

and $|0|_p = 0$, where $\mathbf{N}(p) = |R/p|$. This defines a metric on R_0 which satisfies the **ultrametric inequality**: $|a+b|_p \leqslant \max\{|a|_p, |b|_p\}$.

Lemma 1. *Let $z \in R_0$. The inequality $|z|_p \leqslant 1$ holds for every prime p of R if and only if $z \in R$.*

Proof. Since $\mathbf{N}(p) > 1$, we have that $\mathbf{N}(p)^{-k} \leqslant 1$ if and only if $k \geqslant 0$. Thus $|z|_p \leqslant 1$ if and only if p does not appear in z's denominator in reduced form. But this is true for every prime if and only if z's denominator is a unit. □

It follows from the ultrametric inequality that when $|a|_p \neq |b|_p$, then $|a+b|_p = \max\{|a|_p, |b|_p\}$; i.e., equality holds in the ultrametric inequality. This suggests that the following definition is sensible: if $f = \sum a_i x^i \in R_0[x]$, then we define $|f|_p = \max |a_i|_p$. We may extend Lemma 1 easily.

Lemma 2. *Suppose $f \in R_0[x]$. Then $|f|_p \leqslant 1$ for every prime p of R if and only if $f \in R[x]$.*

Moreover, this extension of $|-|_p$ to $R[x]$ satisfies a multiplicativity property: $|ab|_p = |a|_p|b|_p$, which can be verified by a calculation.

We are now in a position to prove Theorem 1.

Proof of Theorem 1. Let f be a polynomial in $R[x]$ which splits into monic g, h in $R_0[x]$. Fix a prime $p \in R$. Then by Lemma 2, we have that $|f|_p \leqslant 1$, and as f is monic (as a product of monics), it follows that $|f|_p = 1$.

Then $|g|_p|h|_p = 1$, but as each of g and h are monic, it follows that $|g|_p$ and $|h|_p \geqslant 1$, so in fact each of $|g|_p$ and $|h|_p$ are 1. Thus $g, h \in R[x]$ by Lemma 2. $\square$