Hensel's Lemma

Daniel Murfet

April 8, 2005

Let A be a ring which is complete for its $\mathfrak{a}$ topology, where $\mathfrak{a}$ is an ideal. We show how certain relations occurring in the ring $A/\mathfrak{a}$ (i.e., congruences mod $\mathfrak{a}$) may be "lifted" to analogous relations occurring in the ring A itself. The completeness of A is essential for this purpose. If $f \in A[x]$ then we denote by $\overline{f}$ the image of f in $(A/\mathfrak{m})[x]$ under the canonical map $A[x] \longrightarrow (A/\mathfrak{m})[x]$.

Important 1. In Zariski & Samuel *complete* means that every Cauchy sequence converges, and *local* means a Notherian ring with one maximal ideal. The only place where the Noetherian hypothesis is used in the following Theorem is to show that $\cap_s \mathfrak{m}^s = 0$, which is true for any Noetherian local ring (see Atiyah & Macdonald Corollary 10.19).

Alternatively, in Atiyah & Macdonald *complete* means that the morphism $A \longrightarrow \widehat{A}$ is an isomorphism, which is equivalent to every Cauchy sequence converging and $\cap_s \mathfrak{m}^s = 0$, and *local* means any ring with one maximal ideal.

The hypothesis necessary for the proof of the Theorem are: A must have one maximal ideal $\mathfrak{m}$, admit a limit for every Cauchy sequence in the $\mathfrak{m}$-adic topology, and have $\cap_s \mathfrak{m}^s = 0$. So in anybody's terminology, we require that A be a complete local ring.

Theorem 1 (Hensel's Lemma). *Let A be a complete local ring, $\mathfrak{m}$ its maximal ideal, and $f \in A[x]$ a monic polynomial of degree $n \geq 1$. Suppose there are coprime monic polynomials $G, H \in (A/\mathfrak{m})[x]$ of respective degrees $r, n-r$ $(r \geq 0)$ such that*

$$\overline{f} = GH$$

Then there exist monic polynomials $g, h \in A[x]$ of degrees $r, n-r$ with

$$\overline{g} = G, \quad \overline{h} = H, \quad f = gh$$

Proof. We recursively construct monic polynomials $g_i, h_i \in A[x]$ such that $f \equiv g_i h_i \pmod{\mathfrak{m}^i[x]}$ for all $i \geq 1$, where $\overline{g_i} = G$ and $\overline{h_i} = H$. Moreover we will show that the residues of g_i, h_i are unique in the sense that if $\overline{g'} = G, \overline{h'} = H$ and $f \equiv g'h' \pmod{\mathfrak{m}^i[x]}$ then $g_i \equiv g'$ and $h_i \equiv h'$ $\pmod{\mathfrak{m}^i[x]}$.

Given G, H choose representatives for the nonzero coefficients (making sure to choose 1 for $1 + \mathfrak{m}$). This defines two monic polynomials $g_1, h_1 \in A[x]$ of degrees $r, n-r$ with $\overline{g_1} = G$ and $\overline{h_1} = H$. Since

$$\overline{f} = GH = \overline{g_1 h_1}$$

We have $f \equiv g_1 h_1 \pmod{\mathfrak{m}[x]}$. Now assume that g_k and h_k have been constructed and shown unique for a certain $k \geq 1$. We must construct g_{k+1}, h_{k+1} and show they are unique. Our approach is to find $\delta, \epsilon \in \mathfrak{m}^k[x]$ of degrees $< r, n-r$ such that $g_{k+1} = g_k + \delta$, $h_{k+1} = h_k + \epsilon$ satisfy the necessary properties.

Since G, H are coprime they generate the unit ideal in $(A/\mathfrak{m})[x]$, so we can find polynomials $\alpha, \beta \in A[x]$ with

$$1 \equiv \alpha g_k + \beta h_k \qquad \text{mod } \mathfrak{m}[x] \tag{1}$$

We have $\Delta = f - g_k h_k \in \mathfrak{m}^k[x]$ by the inductive hypothesis. Multiplying by Δ we find that $\Delta \equiv \Delta\alpha g_k + \Delta\beta h_k \pmod{\mathfrak{m}^{k+1}[x]}$. We want to replace $\Delta\alpha, \Delta\beta$ by polynomials with degrees $< r, n-r$. Since h_k is monic we may apply the division algorithm to produce $\gamma, \epsilon \in A[x]$ with

$deg(\epsilon) < n-r$ and $\Delta\alpha = \gamma h_k + \epsilon$. Since $\Delta\alpha \in \mathfrak{m}^k[x]$ we have $0 \equiv \gamma h_k + \epsilon \pmod{\mathfrak{m}^k[x]}$. Since h_k is monic it has degree $n-r$ in $(A/\mathfrak{m}^k)[x]$ and so the uniqueness of the division algorithm in $(A/\mathfrak{m}^k)[x]$ implies that $\gamma, \epsilon \in \mathfrak{m}^k[x]$. Then

$$\Delta \equiv \epsilon g_k + \delta h_k \qquad \text{mod } \mathfrak{m}^{k+1}[x] \tag{2}$$

where $\delta = \gamma g_k + \Delta\beta \in \mathfrak{m}^k[x]$. Since Δ and ϵg_k both have degree $< n$, so does δh_k, which implies that the degree of δ is $< r$. Considering the degrees of δ, ϵ we see that the polynomials $g_{k+1} = g_k + \delta$ and $h_{k+1} = h_k + \epsilon$ are monic of degrees $r, n-r$. Further (calculating mod $\mathfrak{m}^{k+1}[x]$)

$$\begin{aligned} g_{k+1}h_{k+1} &\equiv g_k h_k + \epsilon g_k + \delta h_k + \delta\epsilon \\ &\equiv g_k h_k + \Delta \\ &\equiv f \end{aligned}$$

Since $\delta\epsilon \in \mathfrak{m}^{2k}[x]$ and $2k \geq k+1$. The fact that $\delta, \epsilon \in \mathfrak{m}^k[x]$ implies that $\overline{g_{k+1}} = G$ and $\overline{h_{k+1}} = H$. So it only remains to prove uniqueness.

Suppose g', h' are monic polynomials of degrees $r, n-r$ such that $\overline{g'} = G$, $\overline{h'} = H$ and $f \equiv g'h' \pmod{\mathfrak{m}^{k+1}[x]}$. Then $\epsilon' = h' - h_k$, $\delta' = g' - g_k$ have degrees $< n-r, r$. Then by the inductive hypothesis the residues of g_k, h_k are unique, so $\epsilon', \delta' \in \mathfrak{m}^k[x]$. Hence $\epsilon'\delta' \in \mathfrak{m}^{k+1}[x]$. Calculating mod $\mathfrak{m}^{k+1}[x]$

$$\begin{aligned} 0 &\equiv f - g'h' \equiv f - g_k h_k - \delta' h_k - \epsilon' g_k - \epsilon'\delta' \\ &\equiv \Delta - (\epsilon' g_k + \delta' h_k) \end{aligned}$$

Subtracting this from (**??**) we have

$$0 \equiv \mu g_k + \nu h_k \qquad \text{mod } \mathfrak{m}^{k+1}[x]$$

Where $\mu = \epsilon - \epsilon'$ and $\nu = \delta - \delta'$ have degrees $< n-r, r$. Multiplying through by α and using the fact that by (**??**), $\alpha g_k + \beta h_k - 1 = m \in \mathfrak{m}[x]$, we have

$$\mu \equiv (\mu\beta - \alpha\nu)h_k - \mu m \qquad \text{mod } \mathfrak{m}^{k+1}[x]$$

But $\mu \in \mathfrak{m}^k[x]$ and $m \in \mathfrak{m}[x]$, so it follows that μ is a multiple of h_k in $(A/\mathfrak{m}^{k+1})[x]$. But in $(A/\mathfrak{m}^{k+1})[x]$ the polynomial μ has degree $< n-r$ and h_k has degree $n-r$. Hence $\mu \equiv 0 \pmod{\mathfrak{m}^{k+1}[x]}$. Similarly $\nu \equiv 0$. Hence, calculating mod $\mathfrak{m}^{k+1}[x]$

$$h' \equiv h_k + \epsilon' \equiv h_k + \epsilon \equiv h_{k+1}$$

And similarly $g' \equiv g_{k+1}$, which completes the proof of uniqueness.

If $1 \leq i < j$ then $f - g_j h_j \in \mathfrak{m}^j[x] \subseteq \mathfrak{m}^i[x]$ so $f \equiv g_j h_j \pmod{\mathfrak{m}^i[x]}$. Hence by uniqueness $g_i \equiv g_j$ and $h_i \equiv h_j \pmod{\mathfrak{m}^i[x]}$. This implies that the sequences of coefficients are Cauchy in A and hence converge to coefficients $a_0, \ldots, a_{r-1}$ (for the g_i) and $b_0, \ldots, b_{n-r-1}$ (for the h_i). Set

$$\begin{aligned} g &= a_0 + a_1 x + \ldots + a_{r-1}x^{r-1} + x^r \\ h &= b_0 + b_1 x + \ldots + b_{n-r-1}x^{n-r-1} + x^{n-r} \end{aligned}$$

It is easy to see that $\overline{g} = G$ and $\overline{h} = H$ by using the convergence of the coefficients and the fact that $\overline{g_k} = G, \overline{h_k} = H$ for all $k \geq 1$. We complete the proof by showing that $f = gh$.

Firstly, note that for $0 \leq i \leq n-1$

$$\begin{aligned} (gh)_i - (g_k h_k)_i &= \sum_{j=0}^{i} (g_j h_{i-j} - g_{k,j} h_{k,i-j}) \\ &= \sum_{j=0}^{i} (g_j - g_{k,j}) h_{i-j} + \sum_{j=0}^{i} g_{k,j}(h_{i-j} - h_{k,i-j}) \end{aligned}$$

Hence $(g_k h_k)_i \longrightarrow (gh)_i$ for all $0 \leq i \leq n-1$. But

$$f_i - (gh)_i = f_i - (g_k h_k)_i + (g_k h_k)_i - (gh)_i$$

And $f_i - (g_k h_k)_i \in \mathfrak{m}^k$ by construction. Hence $f_i - (gh)_i \in \cap_s \mathfrak{m}^s$. But $\cap_s \mathfrak{m}^s$ is zero in a Noetherian local ring (see Atiyah & Macdonald Corollary 10.19), and consequenty $f = gh$, as required. □

Recall that for a polynomial $f(x) \in A[x]$ over an arbitrary ring, an element $a \in A[x]$ is a *simple root* of f if $x - a$ divides $f(x)$ but $(x-a)^2$ does not divide $f(x)$.

Corollary 2. *Let A be a complete local ring, $\mathfrak{m}$ its maximal ideal, and $f(x)$ a monic polynomial over A. Suppose that $\overline{f}(x)$ admits a simple root $\alpha \in A/\mathfrak{m}$. Then there exists an element a of A, having α as $\mathfrak{m}$-residue, and such that $f(a) = 0$. Moreover, a is a simple root of $f(x)$.*

Proof. Write $\overline{f}(x) = (x-\alpha)G(x)$ where $G(x)$ is prime to $x - \alpha$. Then the Theorem shows the existence of monic polynomials $x - a, g(x)$ with $\overline{a} = \alpha$ and $\overline{g}(x) = G(x)$ such that $f(x) = (x-a)g(x)$. If a were a multiple root of $f(x)$ then we could write $f(x) = (x-a)^2 h(x)$ for some polynomial $h(x)$. But then $\overline{f}(x) = (x-\alpha)^2 \overline{h}(x)$ would imply that α is a multiple root of $\overline{f}(x)$, contradicting our assumption. □

Example 1. There are many applications of Hensel's Lemma. We highlight a few simple ones:

(1) Let $\mathfrak{m}$ be the maximal ideal (5) in $\mathbb{Z}$, and let A be the $\mathfrak{m}$-adic completion of $\mathbb{Z}$. Then A is a complete local ring whose maximal ideal $\widehat{\mathfrak{m}}$ consists of all Cauchy sequences $(a_i)_{i \geq 1}$ with each a_i a multiple of 5. The residue field of A is $GF(5)$ since

$$A/\widehat{\mathfrak{m}} \cong \mathbb{Z}/\mathfrak{m} = \mathbb{Z}_5$$

The polynomial $x^2 + 1$ has two simple roots in $GF(5)$, namely the classes of 2 and 3. Thus it has two simple roots in the 5-adic integers.

(2) Let A be the $\mathfrak{m}$-adic completion of $\mathbb{C}[z]$ where $\mathfrak{m} = (z)$. Then A is the complete local ring $\mathbb{C}[[z]]$ with maximal ideal (z). Consider the polynomial $f(x) = x^2 - (1+z) \in A[x]$. Note that

$$\mathbb{C}[[z]]/(z) \cong \mathbb{C}[z]/(z) \cong \mathbb{C}$$

Since $f(x) = (x-1)(x+1)$ in $(A/\mathfrak{m})[x]$, Hensel's Lemma implies that there are power series $\alpha(z), \beta(z) \in \mathbb{C}[[z]]$ with $x^2 - (1+z) = (x - \alpha(z))(x - \beta(z))$ and $\overline{\alpha(z)} = 1$, $\overline{\beta(z)} = -1$. Reducing coefficients modulo (z) amounts to looking at only the constant term, so that $\alpha(z) = 1 + \ldots$ and $\beta(z) = -1 + \ldots$. So Hensel's Lemma implies the existence of power series square roots for $1 + z$.