UNIVERSITATIS IAGELLONICAE ACTA MATHEMATICA, FASCICULUS XLVI
2008

REMARKS ON HENSELIAN RINGS

BY KRZYSZTOF JAN NOWAK

Abstract. The paper demonstrates how to derive Hensel's lemma from a theorem on regular roots of polynomial mappings over a Henselian ring. This is first done after P. M. Cohn's idea to apply linear algebra and matrices. Next, we provide another simple proof of a stronger version of Hensel's lemma due to M. Nagata.

The notion of a Henselian ring, introduced by G. Azumaya [**1**], was further developed by M. Nagata (cf. [**7**]). The theory of Henselian rings is closely related to that of étale algebras. We begin with some basic results concerning those notions. For a thorough treatment, we refer the reader to, e.g., [**9**].

Let A be an arbitrary commutative ring with unit. In view of Zariski's main theorem (cf. [**9, 8, 4**]), we may propose the following definition:

An A-algebra B is étale over A at a point $q \in \operatorname{Spec} B$ if it is unramified, flat and of finite presentation locally in the vicinity of q. More precisely, there are $b \in B \setminus q$ and $a \in A \setminus p$, with $p \in \operatorname{Spec} A$ lying under q, such that B_b is an unramified A_a-algebra and a flat A_a-module of finite presentation.

The assumption of finite presentation ensures, among others, that flatness and many other punctual properties propagate through a neighbourhood of a given point (cf. [**2, 5**]). One can dispose of it, provided that A is a noetherian ring. Consequently, for an algebra B of finite type over a noetherian ring A, to be étale at q depends on the local ring B_q only. Étale A-algebras can be characterized as follows.

With the above notation, B is étale over A at q iff it has a standard étale presentation in the vicinity of q. This means that there are $a \in A \setminus p$, $b \in B \setminus q$

1991 *Mathematics Subject Classification.* 13B40.
Key words and phrases. Étale algebras, Henselian rings, Hensel's lemma, Cohn's lemma.

and polynomials $f(T), g(T) \in A[T]$ in one variable such that the A-algebra

$$C := (A_a[T]/f(T))_{g(T)}$$

is A-isomorphic to B_b and the canonical image of $f'(T)$ in C is invertible. A ring C of the above form is called a standard étale A_a-algebra.

This characterization immediately implies that the set of those points $q \in \operatorname{Spec} B$ at which B is étale over A is open in the Zariski topology. One of the most important results about étale algebras is the following

Jacobian Criterion. *Consider a ring A and an ideal I in the ring of polynomials $A[T_1, \ldots, T_n]$. Let*

$$B := A[T_1, \ldots, T_n]/I, \quad q \in \operatorname{Spec} B \quad \textit{and} \quad r \in \operatorname{Spec} A[T_1, \ldots, T_n]$$

be the ideal lying under q. Then B is étale over A at q iff there exist $f_1, \ldots, f_n \in I$ and $g \in A[T_1, \ldots, T_n] \setminus r$ such that the canonical images of $f_1, \ldots, f_n$ in I_g generate I_g and

$$\textit{det}\,[\partial f_i/\partial T_j] \in A[T_1, \ldots, T_n] \setminus r.$$

Whenever the above conditions hold, then for any polynomials $g_1, \ldots, g_n \in I$, a necessary and sufficient condition for their images in I_r to generate I_r is that

$$\textit{det}\,[\partial g_i/\partial T_j] \in A[T_1, \ldots, T_n] \setminus r.$$

Given a local ring (A, m), we say that C is an étale local A-algebra if it is of the form $C = B_q$, where B is an étale A-algebra B at a point $q \in \operatorname{Spec} B$ that lies over m; obviously, q is a maximal ideal of B. Since C is faithfully flat over A, A is a subring of C. The Jacobian Criterion for étale local algebras can now be formulated as follows:

Given a local ring A, the local A algebra

$$(A[T_1, \ldots, T_n]/(f_1, \ldots, f_n))_q$$

is étale, whenever the jacobian det $[\partial f_i/\partial T_j]$ does not belong to the ideal q.

If A and C have the same residue field, we call C an equiresidual étale local A-algebra. We say that a local ring (A, m, k) is Henselian if every monic polynomial $f(T) \in A[T]$ whose $(\mathrm{mod}\ m)$ reduction has a simple root $a \in k$ has a unique root $\alpha \in A$ lying over a. It can be easily checked through a standard étale presentation that a necessary and sufficient condition for a local ring A to be Henselian is that every equiresidual étale local A-algebra be isomorphic to A. This along with the Jacobian Criterion yields a theorem on regular roots of a polynomial mapping stated below.

Theorem on Regular Roots. *Let* (A, m, k) *be a Henselian ring,* $f_1, \dots, f_n \in A[T_1, \dots, T_n]$ *and* $\overline{f_1}, \dots, \overline{f_n} \in k[T_1, \dots, T_n]$ *be their reductions* $\mathrm{mod}\, m$. *If the polynomials* $\overline{f_1}, \dots, \overline{f_n}$ *possess a common regular root* $a \in k^n$ *(i.e.* $\det \left[\partial \overline{f_i}/\partial T_j(a)\right] \neq 0$*), then* $f_1, \dots, f_n$ *possess a unique common root* $\alpha \in A^n$ *lying over* a.

Now we can readily turn to our main purpose, and demonstrate how to derive Hensel's lemma from the above theorem. Our approach is based on Cohn's lemma ("Hensel's lemma for matrices" in his terminology), which was formulated by P. M. Cohn [**3**] for the complete valued field (with a principal valuation). He needed this lemma in order to prove Puiseux's theorem for the formal power series $k[[T]]$ over an algebraically closed field k of characteristic zero. His original idea was to prove an equivalent theorem to the effect that any $n \times n$ matrix over $k[[T]]$ has an eigenvalue that is a fractional power series over k. We shall first establish Cohn's lemma for arbitrary Henselian rings, and next, following his idea to apply linear algebra and matrices, show that it implies Hensel's lemma.

Cohn's Lemma. *Let* (A, m, k) *be a Henselian ring. Consider a partitioned matrix over* A

$$M = \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix}$$

such that the $(\mathrm{mod}\ m)$ *reduction* $\overline{M_2} = 0$ *of* M_2 *is zero matrix, and that the characteristic polynomials of the reductions* $\overline{M_1}$, $\overline{M_4}$ *over* k *are coprime. Then* M *is similar over* A *to a matrix of the form*

$$M \sim \begin{bmatrix} M_1' & 0 \\ M_3 & M_4' \end{bmatrix},$$

with common reduction $\mathrm{mod}\, m$.

For a proof, observe that

$$\begin{aligned} M &= \begin{bmatrix} I & -X \\ 0 & I \end{bmatrix} \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix} \begin{bmatrix} I & X \\ 0 & I \end{bmatrix} \\ &= \begin{bmatrix} M_1 - XM_3 & M_2 + M_1X - XM_4 - XM_3X \\ M_3 & M_4 + M_3X \end{bmatrix}. \end{aligned}$$

Therefore, it is sufficient to solve over A the matrix polynomial equation

$$XM_4 - M_1X + XM_3X - M_2 = 0.$$

The differential at zero of the left-hand side of this equation is

$$X \mapsto XM_4 - M_1X,$$

and its (mod m) reduction is

$$X \mapsto X\overline{M_4} - \overline{M_1}X.$$

It is a well-known fact from the theory of matrices that the latter k-linear mapping is an isomorphism, whenever the characteristic polynomials $f(T)$ and $g(T)$ of the matrices $\overline{M_1}$ and $\overline{M_4}$ are coprime. For the reader's convenience, we outline a proof below. If

$$1 \equiv f(T)q(T) + p(T)g(T) \quad \text{and} \quad h(T) := p(T)g(T) = c_n T^n + \ldots + c_0,$$

then $h(\overline{M_1}) = I$ and $h(\overline{M_4}) = 0$, because $f(\overline{M_1}) = 0$ and $g(\overline{M_4}) = 0$ by the Cayley–Hamilton theorem (see, e.g., [**6**], Chap. XV). Therefore, we get

$$X = \sum_{i=1}^{n} c_i (\overline{M_1}^i X - X\overline{M_4}^i).$$

But it is easy to express $\overline{M_1}^i X - X\overline{M_4}^i$ polynomially with respect to $\overline{M_1}$, $\overline{M_4}$ and $\overline{M_1}X - X\overline{M_4}$, say

$$\overline{M_1}^i X - X\overline{M_4}^i = P_i(\overline{M_1}, \overline{M_4}, \overline{M_1}X - X\overline{M_4}).$$

A unique solution to the matrix equation

$$X\overline{M_4} - \overline{M_1}X = Y$$

is thus given by the formula

$$X := \sum_{i=1}^{n} c_i P_i(\overline{M_1}, \overline{M_4}, Y),$$

which means that the the k-linear mapping under study is an isomorphism, as asserted.

Consequently, zero is a regular solution of the matrix polynomial equation

$$X\overline{M_4} - \overline{M_1}X + X\overline{M_3}X = 0.$$

Hence and by the theorem on regular roots, the initial matrix polynomial equation has a regular solution over A lying over zero matrix, which is the result required.

Corollary. *Under the above assumptions, if $\overline{M_2} = 0$, $\overline{M_3} = 0$ and the characteristic polynomials of $\overline{M_1}$, $\overline{M_4}$ are coprime, then M is similar over A to a matrix of the form*

$$M \sim \begin{bmatrix} M_1' & 0 \\ 0 & M_4' \end{bmatrix},$$

with common reduction mod m.

One can apply the above corollary along with some results from linear algebra (namely, the theorem on decomposition of a vector space over an endomorphism) to establish Hensel's lemma.

Hensel's Lemma. *Let (A, m, k) be a Henselian ring and $f(T) \in A[T]$ be a monic polynomial. Suppose that for the* $(\mathrm{mod}\ m)$ *reduction* $\overline{f}(T) \in k[T]$ *of f, there is $\overline{f}(T) = g_0(T) \cdot h_0(T)$, where $g_0(T), h_0(T) \in k[T]$ are monic coprime polynomials. Then $g_0(T), h_0(T)$ can be lifted to monic polynomials $g(T), h(T) \in A[T]$ such that $f(T) = g(T) \cdot h(T)$.*

To prove this, denote by M the companion matrix of the polynomial $f(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_0$:

$$M = \begin{bmatrix} 0 & 0 & \ldots & \ldots & 0 & \ldots & \ldots & -a_0 \\ 1 & 0 & \ldots & \ldots & 0 & \ldots & \ldots & -a_1 \\ 0 & 1 & 0 & \ldots & 0 & \ldots & \ldots & -a_2 \\ \vdots & \ddots & \ddots & \ddots & & & & \vdots \\ 0 & \ldots & \ldots & 1 & 0 & \ldots & \ldots & -a_{n-2} \\ 0 & \ldots & \ldots & \ldots & 1 & 0 & \ldots & -a_{n-1} \end{bmatrix},$$

and by $\overline{M}$ its reduction $\mathrm{mod}\, m$. By virtue of the theorem on decomposition of a vector space over an endomorphism (see, e.g., [**6**], Chap. XV), the matrix M is similar over A to a partitioned matrix of the form

$$M \sim \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix}$$

whose $(\mathrm{mod}\ m)$ reduction is of the form

$$\overline{M} \sim \begin{bmatrix} \overline{M_1} & 0 \\ 0 & \overline{M_4} \end{bmatrix}$$

and such that the characteristic polynomials of $\overline{M_1}$, $\overline{M_4}$ are $g_0(T), h_0(T)$, respectively. The above corollary implies that M is similar over A to a matrix of the form

$$M \sim \begin{bmatrix} M_1' & 0 \\ 0 & M_4' \end{bmatrix},$$

with common reduction $\mathrm{mod}\, m$ and, therefore, the characteristic polynomials $g(T), h(T) \in A[T]$ of the matrices M_1', M_4' are the lifts of $g_0(T), h_0(T)$, respectively. Clearly, $f(T) = g(T) \cdot h(T)$, which completes the proof.

M. Nagata established (cf. [**7**], Chap. VII, § 44) a much stronger version of Hensel's lemma, wherein the polynomial $f(T) \in A[T]$ does not have to be monic:

Nagata's Version of Hensel's Lemma. *Let* $f(T) \in A[T]$ *and* $\overline{f}(T) = g_0(T) \cdot h_0(T)$*, where* $g_0(T), h_0(T) \in k[T]$ *are coprime polynomials and one of them, say* $g_0(T)$*, is monic. Then* $g_0(T), h_0(T)$ *can be lifted to polynomials* $g(T), h(T) \in A[T]$ *such that* $g(T)$ *is monic and* $f(T) = g(T) \cdot h(T)$.

This strengthening, however, requires a different proof. Denote by $\mathcal{P}_l(R)$ the free module of polynomials of degree $< l$ over a ring R. Take $m := \deg g_0$ and any $n \geq \deg h_0$. We shall still need the following easy observation:

Claim. *The polynomials* $g_0(T), h_0(T)$ *are coprime iff the linear mapping*

$$\Phi : \mathcal{P}_m(k) \times \mathcal{P}_n(k) \ni (q, p) \longrightarrow g_0 p + q h_0 \in \mathcal{P}_{m+n}(k)$$

is surjective (and thus an isomorphism).

We shall apply this observation for $m := \deg g_0$ and

$$n := \deg f - \deg g_0 = \deg f - m \geq \deg h_0.$$

If $a \in A$ is the leading coefficient of the polynomial $f(T)$, consider the following polynomial mapping φ with components of degree 2:

$$\varphi : \mathcal{P}_m(A) \times \mathcal{P}_n(A) \ni (p, q) \longrightarrow (T^m + p) \cdot (aT^n + q)) - aT^{m+n} \in \mathcal{P}_{m+n}(A).$$

Let $\overline{a}$ and $\overline{\varphi}$ denote the $(\bmod\ m)$ reductions of a and φ, respectively. Then the differential of $\overline{\varphi}$ at the point

$$(g_0 - T^m, h_0 - \overline{a}T^n)$$

coincides obviously with the linear mapping Φ. But the above claim ensures that Φ is an isomorphism. Hence and by the theorem on regular roots, $g_0(T), h_0(T) \in k[T]$ can be lifted to unique polynomials $g(T), h(T) \in A[T]$ such that $f(T) = g(T) \cdot h(T)$, which is the required conclusion.

The foregoing stronger version of Hensel's lemma yields, as an immediate consequence, the Weierstrass preparation theorem for polynomials, stated below.

Preparation Theorem for Polynomials. *Let* (A, m, k) *be a Henselian ring and* $f(T) \in A[T]$ *be a polynomial of degree* n *and of a finite order* d*, i.e. its reduction* $\overline{f}(T) \in k[T]$ *has zero of multiplicity* n*. Then there exist unique polynomials* $g(T), h(T) \in A[T]$ *such that* $f(T) = g(T) \cdot h(T)$*, where* g *is a Weierstrass polynomial of degree* d *(i.e., it is monic and its* $(\bmod\ m)$ *reduction is* T^d*) and* $h(0)$ *is a unit of* A.

References

1. Azumaya G., *On maximally central algebras*, Nagoya Math. J., **2** (1950), 119–150.
2. Bourbaki N., *Eléments de Mathématique: Algèbre Commutative*, Hermann, Paris, 1961–1965.
3. Cohn P. M., *Puiseux's theorem revisited*, J. Pure Appl. Algebra, **31** (1984), 1–4.
4. Grothendieck A., *Eléments de Géométrie Algébrique*, Vol. **IV**, Publ. Math. I.H.E.S. 1964–1967.
5. Grothendieck A., Dieudonné J. A., *Eléments de Géométrie Algébrique*, Springer-Verlag, 1971.
6. Lang S., *Algebra*, Addison-Wesley Publ. Co., Reading, Mass., 1965.
7. Nagata M., *Local Rings*, Interscience Publ., New York, London, 1962.
8. Peskine C., *Une généralisation du «main theorem» de Zariski*, Bull. Sc. Math. (2), **90** (1966), 119–127.
9. Raynaud M., *Anneaux Locaux Henséliens*, Lect. Notes Math., **169**, Springer-Verlag, 1970.

Received December 5, 2008

Institute of Mathematics
Jagiellonian University
ul. Łojasiewicza 6
30-348 Kraków, Poland
e-mail: `nowak@im.uj.edu.pl`