M. Van der Put

A problem on coefficient fields and equations
over local rings


<http://www.numdam.org/item?id=CM_1975__30_3_235_0>
A PROBLEM ON COEFFICIENT FIELDS AND EQUATIONS
OVER LOCAL RINGS

M. van der Put

Introduction

Let $R$ be a noetherian local ring, $m$ its maximal ideal and $\pi: R \to K$ the natural map of $R$ onto its residue field $K$. Given a subfield $k$ of $R$ (hence $R$ has equal characteristic) does there exist a coefficient field of $R$ containing $k$?

Stated in a more general way: Given subfields $k \subseteq l$ of $K$ and a ring-homomorphism $\phi : k \to R$ such that $\pi\phi = \text{id}_k$, does $\phi$ extend to a ring-homomorphism $\Phi : l \to R$ with $\pi\Phi = \text{id}_l$?

As is well known, the answer is “yes” when $R$ is complete and $l/k$ is separable (See [3]).

In this paper we consider the case when $l/k$ is inseparable. A necessary condition for the existence of $\Phi$ is the existence for all $n \geq 1$ of a ring-homomorphism $\Phi_n : l \to R/m^n$ with $\pi\Phi_n = \text{id}_l$ and $\Phi_n|k = \phi$ (For convenience all the natural maps $R/m^a \to R/m^b$, $\infty \leq a \leq b \leq 1$, are denoted by $n$). Assume that this condition is satisfied and let $H_t$ denote the set of all $\Phi : l \to R/m^t$ with $\pi\Phi = \text{id}_l$ and $\Phi|k = \phi$. By assumption $H_t \neq \emptyset$ for all $t$ and clearly $\varprojlim H_t = \{\Phi : l \to R|\pi\Phi = \text{id}_l \text{ and } \Phi|k = \phi\}$. The problem splits in two parts:

(i) Is $\varprojlim H_t \neq \emptyset$?

(ii) If $\varprojlim H_t \neq \emptyset$ does there exist a $\Phi : l \to R$ with $\Phi|k = \phi$ and $\pi\Phi = \text{id}_l$?

Results

In Section 1 it is shown that (i) and (ii) have a positive answer for $l/k$ finitely generated and $R$ an $s$-ring, i.e. $R$ has the following property: For every ideal $F$ in $R[X_1, \ldots, X_N]$ there exists a function $s : \mathbb{N} \to \mathbb{N}$ such that for all $x = (x_1, \ldots, x_N) \in R^N$ with $F(x) \in m^{s(n)}$ there exists a $x' \in R^N$ with $x' \equiv x(m^n)$ and $F(x') = 0$. 

235
Further a list of s-rings is given. In Sections 2, 3 it is shown that
\[ \lim H_t \neq \emptyset \text{ if } \dim_{l/k} \mathcal{O}_{l/k} < \infty. \] In Sections 4, 5, 6 a proof is given of the statement: A complete local ring of equal characteristic is an s-ring. In Section 7 it is shown that some complete local rings of unequal characteristic are s-rings.

1. \( l/k \) finitely generated

**Definition:** A local ring \( R \) is called an s-ring if for any set \( F = (F_1, \ldots, F_k) \) of elements in \( R[X] = R[X_1, \ldots, X_N] \) there exists a function \( s : \mathbb{N} \to \mathbb{N}, s(n) = n \) for all \( n \), such that: For every \( x \in R^N \) with \( F(x) = 0(\text{ms}(n)) \) there exists \( x' \in R^N \) with \( x' \equiv x(m^n) \) and \( F(x') = 0 \).

**Example:**

1. Any Henselian discrete valuation ring \( R \), such that the quotient field of \( R \) is separable over the quotient field of \( R \) (equivalently \( R \) is Henselian and excellent) is an s-ring (see M. Greenberg [4]).

2. Any complete local ring of equal characteristic is an s-ring. This statement is close to an approximation theorem of M. Artin (see [2], Theorem (6.1)). Since there seems to be no proof available we will give a proof in Sections 4, 5 and 6.

3. If \( R \) is the Henselization of a local ring \( R_0 \) which is of essentially finite type over \( R \) and \( R_1 \) is a field or an excellent discrete valuation ring of equal characteristic, then \( R \) is an s-ring. This follows from (2) and M. Artin's approximation theorem ([2], Theorem 1.10).

4. Any analytic local ring over a complete valued field \( k \) ([\( k : k^p \] < \( \infty \) if char \( k = p \neq 0 \)) is an s-ring. We will discuss this in Section 8.

1.1 **Theorem:** Let \( R \) be an s-ring with residue field \( K \), let \( k \subset l \subset K \) be subfields such that \( l/k \) is finitely generated and \( \phi : k \to R \) a ringhomomorphism with \( \pi \phi = \text{id}_k \). There exists a positive integer \( v \) such that \( H_v \neq \emptyset \) implies \( \lim H_t \neq \emptyset \) and \( \phi \) extends to \( \Phi : l \to R \).

**Proof:** The field \( l \) can be considered as the quotient field of \( A = k[X_1, \ldots, X_N]/(F_1, \ldots, F_k) \), where the images of \( X_1, \ldots, X_i \) in \( l \) form a transcendence base of \( l/k \). The map \( \phi : k \to R \) extends to

\[ \phi^* : k[X_1, \ldots, X_N] \to R[X_1, \ldots, X_N] \]

in the obvious way and we obtain a set of polynomials \( \phi^*(F) \) in \( R[X_1, \ldots, X_N] \). Let \( s \) be its \( s \)-function and put \( v = s(1) \). The condition
$H_v \neq \emptyset$ is equivalent to the existence of $x \in R^N$ with $\phi^*(F)(x) \equiv 0(m^{n})$ and $\pi(x_i) = X_i$ where $X_i$ is the image of $x_i$ in $l$.

There exists $x' \in R^N$ with $x' \equiv x(m)$, $\phi^*(F)(x') = 0$. Consequently we have a map $\Phi : A = k[X_1, \ldots, X_N]/(F) \to R$ such that $\pi \Phi = \text{id}_A$. This map extends to $l$, the quotient field of $A$.

**Remark:** (1.1) solves both problems (i) and (ii) for finitely generated field extension $l/k$ and $s$-rings $R$.

## 2. Complete regular local rings

In this section we assume that $R$ is a complete regular local ring with residue field $K$ and $\text{ch} R = \text{ch} K = p > 0$. We assume $d = \text{dim} R$ and denote by $t_1, \ldots, t_d \in R$ a base for the maximal ideal. Further we always take $l = K$.

(2.1) **Theorem:** Let $k \subset K$ and $\phi : k \to R$ be given such that $\pi \phi = \text{id}_k$. Assume that $H_t \neq \emptyset$ for all $t$. If $\text{dim}_K \Omega_{k/k} < \infty$ then $\lim H_t \neq \emptyset$ and $\phi$ extends to $\Phi : K \to R$.

**Proof:** This is divided in some lemmata.

**Definition:** Let $G^t$ be the group of all $k$-automorphisms $\gamma$ of $K[\![T]\!]/(T)^t$ satisfying: $\gamma \equiv 1(m)$; $\gamma(T_i) = T_i$ ($i = 1, \ldots, d$). Let $G_n^t$ ($n \leq t$) denote the subgroup of $G^t$ consisting of the $\gamma$'s with $\gamma \equiv 1(m^n)$.

(2.2) **Lemma:**

(1) Let $\psi_0 \in H_t$ be given then $H_t = \psi_0 G^t$.
(2) $\psi_0 G_n^t = \{\psi \in H_t | \psi \equiv \psi_0(m^n)\}$.

**Proof (1):** For $\psi \in H_t$ we make the extension $\psi^e : K[\![T]\!]/(T)^t \to R/m^t$ given by $\psi^e(T_i) = t_i$ ($i = 1, \ldots, d$). This is an isomorphism. Then $\psi_0^{-1}\psi^e \in G^t$. Conversely, for $\gamma \in G^t$ we have $\psi = \psi_0 \gamma \in H_t$.

(2) If $\psi = \psi_0 \gamma$ then $\psi \equiv \psi_0(m^n)$ if and only if $\gamma \equiv 1(m^n)$.

**Definition:** $\chi : G_n^t \to \text{Der}_k(K, (T)^n/(T)^{n+1})$ is the map given by $\chi(\gamma)(\lambda) = \gamma(\lambda) - \lambda$ (where $\lambda \in K$; $\gamma \in G_n^t$).

(2.3) **Lemma:** The image $V$ of $\chi$ satisfies:

(1) $V + V \subset V$
(2) $a^n V \subset V$ for all $a \in K$
(3) \(V\) is a constructible subset of the finite-dimensional vectorspace \(\text{Der}_k(K, (T)^n/(T)^{n+1})\).

**Proof:** \(\gamma \in G_n^t\) can explicitly be described by \(\gamma(\lambda) = \sum_{|x| < n} \gamma_x(\lambda)T^x\), where: each \(\gamma_x\) is a \(k\)-linear map of \(K \rightarrow K\), \(\gamma_0 = id_k\), \(\gamma_x = 0\) if \(0 < |x| < n\), and for all \(a, b \in K\) and

\[\alpha : \gamma_x(ab) = \sum_{a_1 + a_2 = x} \gamma_{a_1}(a)\gamma_{a_2}(b)\]

Further

\[\chi(\gamma)(\lambda) = \sum_{|x| = n} \gamma_x(\lambda)T^x \mod (T)^{n+1} \].

Clearly \(\chi(\gamma\gamma^*) = \chi(\gamma) + \chi(\gamma^*)\), hence (1). Further for \(a \in K\), \(\gamma \in G_n^t\) we define \(\gamma^a \in G_n^t\) by \(\gamma^a(\lambda) = \sum_{|x| < t} a^{|x|}\gamma_x(\lambda)T^x\). So we proved (2).

(3) Let \(\gamma : K \rightarrow K[[T]]/(T)^t\) be a homomorphism such that \(\gamma = 1(m)\) and \(\gamma\) is \(k\)-linear. Then for any \(\beta\) with \(p^\beta \geq t\) we find that \(\gamma|K^{p^\beta}(k)\) is the ordinary inclusion map, or what amounts to the same \(\gamma\) is \(K^{p^\beta}(k)\)-linear.

Let \(a_1, \ldots, a_d\) be a \(p\)-base of \(K/k\) (i.e. \(Q_{K/k}\) has base \(da_1, \ldots, da_d\)) then

\(K = K^{p^\beta}(k)[a_1, \ldots, a_d] = K^{p^\beta}(k)[X_1, \ldots, X_d]/(F)\) where \(F\) is some set of polynomials.

Consider \(F\) as a set of polynomials with coefficients in \(K[[T]]/(T)^t\) then there exists a natural bijection between \(G_n^t\) and

\(A\) is the set of elements \((x_1, \ldots, x_d) \in (K[[T]]/(T))^d\) such

that \(F(x_1, \ldots, x_d) = 0\) and \((x_1, \ldots, x_d) \equiv (a_1, \ldots, a_d)(m^n)\)

Consider the map

\[\chi^* : G_n^t \rightarrow \text{Der}_k(K, (T)^n/(T)^{n+1}) \simeq \text{Hom}_K(\Omega_{K/k}, (T)^n/(T)^{n+1}) \simeq \text{Hom}_K(Kda_1 + \ldots + Kda_d, (T)^n/(T)^{n+1}) \simeq ((T)^n/(T)^{n+1})^d\].

The image of \(\chi^*\) is the same as the image of \(A - (a_1, \ldots, a_d)\) in \(((T)^n/(T)^{n+1})^d\).

Since \(A\) is an algebraic set /\(K\) this image is constructible. Hence also \(W\) is constructible.

(2.4) **Lemma:** Let \((n, p) = 1\) and let \(W \neq \{0\}\) be a subset of \(K\) satisfying \(W + W \subseteq W\) and \(a^nW \subseteq W\) for all \(a \in K\). Then \(W = K\). (provided that \(K\) is infinite).
PROOF: We may suppose that $1 \in W$. Let $W_0$ be the smallest subset of $K$ which satisfies $1 \in W_0$, $W_0 + W_0 \subseteq W_0$, $a^n W_0 \subseteq W_0$ for all $n$. Then any element of $W_0$ has the form $\sum a_i^n$. Hence $W_0$ is a subring of $K$. For $f, g \in W_0$, $g \neq 0$ we have $f/g = g^{-n} f \cdot g^{n-1} \in W_0$. So $W_0$ is a subfield.

Since $K$ is infinite also $W_0$ is infinite. Take $x \in K$ and let $T$ be an indeterminate. Consider the polynomial

$$p(T) = \frac{(x + T)^n - x^n - T^n}{nT} = x^{n-1} + \ldots + xT^{n-2}.$$ 

For every $\lambda \in W_0^*$, $p(\lambda) \in W_0$. Take distinct elements $\lambda_1, \ldots, \lambda_{n-2} \in W_0^*$ and let $p(\lambda_i) = a_i \in W_0$. Then

$$p(T) = \sum_{i=1}^{n-2} a_i \prod_{j \neq i} \frac{T - \lambda_j}{\lambda_i - \lambda_j},$$

and belongs to $W_0[T]$. Hence the coefficient $x$ in $p(T)$ belongs to $W_0$. So $W = W_0 = K$.

(2.5) Lemma: The image of $\chi: G_n^* \to \text{Der}_K(K, (T)^n/(T)^{n+1})$ is a $K$-linear subspace.

PROOF: If $(n, p) = 1$ this follows from (2.3) part (1) and (2) and (2.4). If $p|n$ we have to use that the image $W$ is a constructible subset. Take $z \neq 0$, $z \in \text{Der}_K(K, (T)^n/(T)^{n+1})$ then $W \cap Kz$ is a constructible set, hence is finite or cofinite in $Kz$. Property (2) of (2.3) implies that either $Kz \subseteq W$ or $Kz \cap W = \{0\}$. So $W$ is a $K$-linear subspace.

Conclusion of the proof (2.1).

Let $H_n^* = \bigcap_{m \geq n} \text{im} (H_m \to H_n)$. It suffices to show that $H_{n+1}^* \to H_n^*$ is surjective since it follows that $\emptyset \neq \lim H_n^* \subseteq \lim H_n$. Choose $\phi_0 \in H_n^*$ and for $t > n$ let $\bar{H}_t$ be the preimage of $\phi_0$ in $H_t$. If we can show that $\bigcap_{t > n} \text{im} (\bar{H}_t \to \bar{H}_{n+1}) \neq \emptyset$ then any $\phi_1 \in \bigcap_{t > n} \text{im} (\bar{H}_t \to \bar{H}_{n+1})$ satisfies $\phi_1 \in H_{n+1}^*$ and $\phi_1$ is mapped onto $\phi_0 \in H_n^*$.

Take some $\alpha \in \bar{H}_t$ and consider the map $[\alpha]: \bar{H}_{n+1} \to G_n^{n+1}$ given by $[\alpha](\gamma) = \gamma$ for all $\gamma \in G_{n+1}$. Then we have an induced map

$$\bar{H}_t \to \bar{H}_{n+1} \xrightarrow{[\alpha]} G_n^{n+1} \xrightarrow{\gamma} \text{Der}_K(K, (T)^n/(T)^{n+1})$$

which depends on the choice of $\alpha \in \bar{H}_t$ but for which the image is independent of $\alpha \in \bar{H}_t$. According to (2.5) the image is a finite dimensional
vectorspace over $K$. Hence $\text{im}(\tilde{H}_t \to \tilde{H}_{n+1})$ is constant for $t \geq n$ and \( \bigcap \text{im}(\tilde{H}_t \to \tilde{H}_{n+1}) \neq \emptyset \).

3. Complete local rings

In this section we extend (2.1) to a more general case:

(3.1) **Theorem:** Let $R$ be a complete local ring with residue field $K$ and let subfields $k \subset l \subset K$ and a homomorphism $\tau : k \to R$ with $\tau \circ \pi = \text{id}_k$ be given. Suppose that $H_t \neq \emptyset$ for all $t$. Then if $\dim_l \Omega_{l/k} < \infty$ then $\lim H_t \neq \emptyset$ and $\tau$ extends to a $\phi : l \to R$ with $\pi \phi = \text{id}_l$.

**Proof:** First we introduce some notation. For any local ring $R$ of characteristic $p > 0$ we define $m^{[n]} = \text{the ideal generated by } \{x^{pn} | x \in m\}$. If $m$ is generated by $e$ elements then $m^{p^n e} \subseteq m^{[n]} \subseteq m^{p^n}$.

Instead of working with the powers of $m$ (as in Sections 1, 2) we can also work with the sequence of ideals $m^{[n]}$. Let $H_{[n]}$ denote the set of ring homomorphisms $\sim : l \to R/m^{[n]}$ such that $\tau |_{l} = \text{id}_l$ and $\tau |_k = T$. By assumption $H_{[n]} \neq \emptyset$. For each $\phi \in H_{[n]}$ we form $\phi |_{l^{p^n}(k)} : R/m^{[n]}$. This map is independent of the choice of $\phi$ and we will denote it by $\tau_{n}$. Further $l^{p^n}(k)$ will be abbreviated with $l_n$.

Indeed, $x \in l_n$ has the form $\sum a_i x^{p^n} (a_i \in k, x_i \in l)$ and for $\phi, \phi^* \in H_{[n]}$ we have

$$\phi(x) - \phi^*(x) = \sum \tau(a_i)(\phi(x_i) - \phi^*(x_i))^{p^n}.$$  

This is 0 since $\phi(x_i) - \phi^*(x_i) \in m$.

We define $A_n = R/m^{[n]} \otimes_l l$. In the next lemma we enumerate some properties of $A_n$.

(3.2) **Lemma:** (1) Each $A_n$ is a local ring and noetherian if $\dim \Omega_{l/k} < \infty$.
(2) The natural map $A_{n+1} \to A_n$ is surjective and has kernel $m(A_{n+1})^{[n]}$.
(3) $A = \lim A_n$ is a complete local ring and noetherian if $\dim \Omega_{l/k} < \infty$.
(4) $A/m(A)^{[n]} = A_n$.
(5) There is a natural bijection $\chi_n : \text{Hom}_R(A, R/m^{[n]}) \to H_{[n]}$ and all diagrams

\[
\begin{CD}
\text{Hom}_R(A, R/m^{[n]}) @>\chi_n>> H_{[n]}
\end{CD}
\]

\[
\begin{CD}
\text{Hom}_R(A, R/m^{[n+1]}) @>\chi_{n+1}>> H_{[n+1]}
\end{CD}
\]

are commutative.
PROOF: (1) $A_n$ is clearly local. If dim $\Omega_{l/k} < \infty$ and $a_1, \ldots, a_s$ is a $p$-base of $l/k$ then for all $n, l = l_n[a_1, \ldots, a_s]$. Hence $A_n$ is a finite $R/m^n[l]$-module and thus noetherian.

(2) The map $\rho : A_{n+1} \to A_n$ decomposes as follows:

$$R/m^{[n+1]} \otimes l \xrightarrow{\alpha} R/m^n \otimes l \xrightarrow{\beta} R/m^n \otimes l,$$

where $\alpha$ and $\beta$ are the obvious maps. Clearly ker $\rho \subseteq m(A_{n+1})^n$. The kernel of $\beta$ is generated by $\{\tau(x^{p^n}) \otimes 1 - 1 \otimes x^{p^n} | x \in l\}$. Take $\phi \in H_{[n+1]}$ then ker $\rho$ is generated by $m^n/m^{n+1}[n]_l$ and

$$\{(\phi(x) \otimes 1 - 1 \otimes x)^{p^n} | x \in l\}.$$

Hence ker $\rho \subseteq m(A_{n+1})^n$.

(3) That $A$ is a complete local ring (possibly not noetherian) follows from its definition. Let dim $\Omega_{l/k} < \infty$ and let $a_1, \ldots, a_s$ be a $p$-base of $l/k$. Choose elements $b_1, \ldots, b_s \in R$ with $\pi(b_i) = a_i (i = 1, \ldots, s)$. Consider the sequence of maps $\phi_n : R[y_1, \ldots, y_s] \to A_n$ given by $y_i \mapsto b_i \otimes l - 1 \otimes a_i$. This sequence of $R$-homomorphisms is coherent and each $\phi_n$ is surjective. Hence $\phi = \lim \phi_n : R[y_1, \ldots, y_s] \to A$ is a surjective $R$-homomorphism and $A$ is noetherian.

(4) $A/m(A)^n = \lim A_k/m(A_k)^n = A_n$ according to (2).

(5) For every $n$ we have a map $l \to A_n = R/m^n \otimes l$ by $x \mapsto 1 \otimes x$. This induces a map $l^l \to A$. Define $\chi_l$ by $\chi_l(\phi) = \phi \circ i$. This makes the diagrams commutative. Further $\text{Hom}_R(A, R/m^n) = \text{Hom}_R(A_n, R/m^n) = \text{Hom}_R(R/m^n \otimes l, R/m^n) = \text{the set of } l_n$-linear homomorphisms $\phi : l \to R/m^n = H_{[n]}$.

Conclusion of the proof of (3.1)

According to the lemma $\lim H_t \simeq \text{Hom}_R(A, R)$ and $A$ has the form $R[y_1, \ldots, y_s]/G$ where $G$ is some ideal.

Given is $\text{Hom}_R(A, R/m^t) \neq \emptyset$ for all $t$. Then by a theorem on the existence of an $s$-function for ideals in $R[y_1, \ldots, y_s]$ (see Section 4, Theorem (4.1)) we can conclude $\text{Hom}_R(A, R) \neq \emptyset$.

4. Equations over complete local rings

Let $R$ be a ring and let $X = (X_1, \ldots, X_h; X_{h+1}, \ldots, X_N)$ denote a set of indeterminates. The ring $R[X_1, \ldots, X_h][X_{h+1}, \ldots, X_N]$ will be denoted by $R[X_1, \ldots, X_h; X_{h+1}, \ldots, X_N]$ or by $R[X]$. We consider a complete local ring $R$ and sets of elements $F = (F_1, \ldots, F_s)$ in $R[X]$. A solution $x$
modulo $m^t$ of $F$ is a set of elements $x = (x_1, \ldots, x_N)$ with $x_1, \ldots, x_h \in m$ and $x_{h+1}, \ldots, x_N \in R$ such that $F_i(x_1, \ldots, x_N) \in m^t$ for all $i$. We abbreviate this by $F(x) \equiv 0(m^t)$. The ideal in $R[[X]]$ generated by $\{F_1, \ldots, F_s\}$ is also denoted by $F$. Solutions of $F$ modulo $m^t$ are into one-one correspondence with $\text{Hom}_R(R[[X]]/F, R/m^t)$.

A local noetherian ring $R$ is called a strong $s$-ring if for every $F$ in $R[[X]]$ there exists a function $s : \mathbb{N} \to \mathbb{N}$, $s(n) \geq n$ for all $n$, such that:

If $F(x) \equiv 0(m^{tn})$ then there exists $x'$ with $x' = x(m^n)$ and $F(x') = 0$.

We note that a strong $s$-ring is necessarily complete. In trying to prove the converse we have encountered some difficulties in the mixed characteristic case and we cannot show much more than:

(4.1) **Theorem:** Every noetherian complete local ring of equal characteristic is a strong $s$-ring.

Our proof of (4.1) follows closely proofs of M. Greenberg [4] and M. Artin [2] where special cases of (4.1) are treated.

(4.2) **Proposition:** (Descent). Let $R_0$ and $R$ be complete local noetherian rings and let $R_0 \to R$ be a finite map. If $R_0$ is a strong $s$-ring then so is $R$.

**Proof:** Let $e_1, \ldots, e_a$ be a base of the $R_0$-module $R$ and let $r_1, \ldots, r_b \in R_0^a$ be a base of the relations between $e_1, \ldots, e_a$. Let $m_0$ denote the maximal ideal of $R_0$ and $e$ an integer satisfying $m^e \subseteq m_0 R \subseteq m$. Let the set of equations $F = (F_1, \ldots, F_s)$ in $R[[X_1, \ldots, X_h; X_{h+1}, \ldots, X_N]]$ be given.

We introduce new variables

$$
\tilde{X}_{ij} (i = 1, \ldots, h; j = 1, \ldots, a); \quad X_{ij} (i = 1, \ldots, N; j = 1, \ldots, a);
$$

$$
Y_{il} (i = 1, \ldots, s; l = 1, \ldots, b); \quad Z_{il} (i = 1, \ldots, h; l = 1, \ldots, b).
$$

$F_i$ can be written as $\tilde{F}_i(x_1^e, \ldots, x_h^e; x_1, \ldots, x_N)$ where $\tilde{F}_i$ is a formal power series in the first $h$ variables and a polynomial in the last $N$ variables. Substitute in $\tilde{F}_i : X_i^e = \sum_{j=1}^a \tilde{X}_{ij} e_j$, $X_i = \sum_{j=1}^a x_{ij} e_i$. Then $\tilde{F}_i$ becomes $\sum_{j=1}^a G_{ij}(\tilde{X}_{., .}, X_{.}) e_j$ where $G_{ij} \in R_0[[\tilde{X}_{., .}; X_{.}]]$. Further

$$
(\sum_{j=1}^a X_{ij} e_j)^e = \sum_{j=1}^a H_{ij}(X_{.}) e_j
$$

for some $H_{ij} \in R_0[X_{.}]$. We consider over $R_0$ the system of equations $F^*$ in $R_0[[\tilde{X}_{., .}; X_{.}, Y_{.}, Z_{.}]]$ given by $G_{ij}(\tilde{X}_{., .}, X_{.}) + \sum_{l=1}^b Y_{il} r_{ij}$ and $H_{ij}(X_{.}) - \tilde{X}_{ij} + \sum_{l=1}^b Z_{il} r_{ij}$ where $r_l = (r_{l1}, \ldots, r_{la}) \in R_0^a(l = 1, \ldots, b)$.

By assumption the system $F^*$ has a function $s^*$. Then $s = e \cdot s^*$ is an
s-function for $F$. Indeed let $F(x) \equiv 0(m^{ex^*(n)})$. Write $x_i = \sum_{j=1}^{h} x_{ij} e_j$ ($x_{ij} \in R_0; i = 1, \ldots, N$) and $x_i = \sum_{j=1}^{h} \tilde{x}_{ij} e_j$ ($\tilde{x}_{ij} \in R_0; i = 1, \ldots, h$).

Then $(\sum_j x_{ij} e_j)^\prime = \sum_j \tilde{x}_{ij} e_j$ and so for suitable $z_{ij} \in R_0$ we have $H_{ij}(x. \ldots) - \tilde{x}_{ij} + \sum_{j=1}^{h} z_{ij} r_{ij} = 0$. Further $\sum_{j=1}^{h} G_{ij}(\tilde{x}. \ldots) e_j = \sum \tau_{ij} e_j$ with $\tau_{ij} \in m_0^{ex^*(n)}$ since $m_0^{ex^*(n)} \subseteq m_0^{ex^*(n)} R$. Hence for suitable $y_{il} \in R_0$ we have $G_{ij}(\tilde{x}. \ldots) + \sum y_{il} r_{ij} \in m_0^{ex^*(n)}$. So we found a solution modulo $m_0^{ex^*(n)}$ of $F^*$ namely $(\tilde{x}. \ldots, x. \ldots, y. \ldots, z. \ldots)$. Let $(\tilde{x}. \ldots, x. \ldots, y. \ldots, z. \ldots)$ be a solution of $F^*$ which is equivalent modulo $m_0^k R$ with $(\tilde{x}. \ldots, x. \ldots, y. \ldots, z. \ldots)$. Put $x_i = \sum_{j=1}^{h} x_{ij} e_j$.

Then $(\sum_j x_{ij} e_j)^\prime = \sum_j \tilde{x}_{ij} e_j$ and it follows that $x \equiv x(m^k)$ and $F(x) = 0$.

(4.3) Lemma: Let $R$ be a regular complete local ring. If there exists an $s$-function for every prime ideal in $R[X]$ then there exists an $s$-function for every ideal in $R[X]$.

Proof: Let $F$ be an ideal in $R[X]$. The radical of $F$ is the intersection of prime ideals $p_1, \ldots, p_t$ which have $s$-functions $s_1, \ldots, s_t$. For some number $d$ we have $F \supseteq p_1^d \ldots p_t^d$. Define $s = dt \max \{s_1, \ldots, s_t\}$. If $F(x) \equiv 0(m^{ex^*(n)})$ then for some $i$, $p_i(x) \equiv 0(m^{ex^*(n)})$. Hence there exists $x' \equiv x(m^k)$ with $p_i(x') = 0$ and in particular $F(x') = 0$.

Remark: (4.2) and (4.3) reduce the general statement to proving the existence of an $s$-function for prime ideals $F$ in $R[X]$ where $R$ is a complete regular local ring and $F \cap R = 0$. In the rest of the proof of (4.1) we apply induction on $\dim R$ and on $\dim R[X]/F$. According to the next lemma we may further assume that the quotient field of $R[X]/F$ is separable over the quotient field of $R$.

(4.4) Lemma: Suppose that $F$ is a prime ideal of $R[X]$, $R$ a regular complete local ring with $F \cap R = 0$, such that the quotient field of $A = R[X]/F$ is inseparable (i.e. not separable) over that of $R$. Then there exists an ideal $G \supseteq F$ of $R[X]$ and a function $\tau : \mathbb{N} \rightarrow \mathbb{N}$ ($\tau(n) \geq n$ for all $n$) such that $F(x) \equiv 0(m^{\tau(n)})$ implies $G(x) \equiv 0(m^\tau)$.

Proof: Let $f_1, \ldots, f_s \in A$ be linearly independent over $R$ such that $f_1^p, \ldots, f_s^p$ are dependent ($p = \text{char of } R > 0$). Hence $\alpha_1 f_1^p + \ldots + \alpha_s f_s^p = 0$ for some $\alpha_1, \ldots, \alpha_s \in R$ not all zero. Let $\{\alpha_1, \ldots, \alpha_t\}$ be a maximal $p$-independent subset over $R^p$. After multiplying with $\beta^p$, $\beta \neq 0$, $\beta \in R$ we may suppose $\alpha_i \in R'[\alpha_1, \ldots, \alpha_t]$ for all $i > t$. The equation $\alpha_1 f_1^p + \ldots + \alpha_s f_s^p = 0$ becomes $\sum_{0 \leq \beta_i < \beta} g_\beta \alpha_1^{t^1} \ldots \alpha_t^{t^t} = 0$ and not all $g_\beta \in F$. (Otherwise the $f_1, \ldots, f_s$ are linearly dependent over $R$). Put
G = (F, g_0 \geq F). The local ring B = \mathbb{R}[x_1, \ldots, x_t] has the free base \{x_1^{\beta_1} \ldots x_t^{\beta_t} \mid 0 \leq \beta_i < p\} over \mathbb{R}. Hence for some e we have

\[ m(B)^e \subseteq m(\mathbb{R})B \subseteq m(B). \]

Further since B is complete there exists a function \( \tau : \mathbb{N} \to \mathbb{N}, \tau(n) \geq n \) for all n, such that \( m(\mathbb{R})^{\tau(n)} \cap B \subseteq m(\mathbb{R})^{\tau(n)}B \). (See Nagata [5] Theorem (30.1) on page 103.)

If now \( F(x) \equiv 0(\mathbb{m}^{\tau(n)}) \) then \( \sum g_\beta(x)x_1^{\beta_1} \ldots x_t^{\beta_t} \equiv 0(m(\mathbb{R})^{\tau(n)}) \) and all \( g_\beta(x) \equiv 0(\mathbb{m}^{\tau(n)}) \). Hence \( G(x) \equiv 0(\mathbb{m}^{\tau(n)}) \).

(4.5) REMARK: It suffices to prove (4.1) in the following situation:

R is a complete regular local ring, F is a prime ideal of \( \mathbb{R}[X] \) such that

(1) The quotient field of \( \mathbb{R}[X]/F \) is separable over the quotient field of \( \mathbb{R} \).

(2) For all \( n \geq 1 \) there exists a solution of \( F(x) \equiv 0(\mathbb{m}^n) \).

If the second condition were not satisfied then F has clearly an s-function, namely \( s(n) = n + \max \{k \mid \text{there exists } x \text{ with } F(x) \equiv 0(\mathbb{m}^k)\} \).

Our next step in proving (4.1) will be to show that the conditions above imply that the Jacobian ideal of \( (F_1, \ldots, F_s) \) with respect to the variables \( X_1, \ldots, X_N \) is not contained in F. This will be done in Section 5.

### 5. Modules of differentials

Let \( \mathbb{R} \) be a complete regular local ring and let \( A = \mathbb{R}[X]/F \) satisfy the condition (4.5). Let s denote the height of the ideal F. We want to show that the ideal generated by the \( s \times s \)-minors of the Jacobian matrix

\[
\begin{pmatrix}
\frac{\partial F_1}{\partial X_1} & \ldots & \frac{\partial F_1}{\partial X_N} \\
\vdots & \ddots & \vdots \\
\frac{\partial F_s}{\partial X_1} & \ldots & \frac{\partial F_s}{\partial X_N}
\end{pmatrix}
\]

is not contained in F. We consider separately the cases \( \text{char } \mathbb{R} = p > 0 \) and \( \text{char } \mathbb{R} = 0 \).

(5.1) THEOREM: Suppose that \( \text{char } \mathbb{R} = p > 0 \) and let \( A = \mathbb{R}[X]/F \) satisfy

(1) F is a prime ideal and the quotient field L of A is separable over the quotient field K of R.

(2) \( \text{Hom}_\mathbb{R}(A, \mathbb{R}/\mathbb{m}) \neq \emptyset \).
Then $\text{rank}_A \Omega_{A/R} = \dim A - \dim R$ and the ideal of the $s \times s$-minors of $\partial F / \partial X$ is not contained in $F$.

**Proof:** Let $k$ be a coefficient field of $R$ and consider the exact sequence

$$
\Omega_{R/p[k]} \otimes A \xrightarrow{\alpha} \Omega_{A/p[k]} \otimes A \rightarrow \Omega_{A/R} \rightarrow 0.
$$

We note that $R^p[k]$ is a noetherian local in between $R^p = k^p[T_1^p, \ldots, T_d^p]$ and $R = k[T_1, \ldots, T_d]$. It's completion $R_1 = k[[T_1^p, \ldots, T_d^p]]$. Hence $\Omega_{R_1/R_1} \otimes A$ is a free $A$-module of rank $= \dim R$. Likewise the other modules in the sequence are finitely generated. The map $\alpha$ is injective since $\alpha \otimes 1_L : \Omega_{K/l} \otimes L \rightarrow \Omega_{L/l}$ is injective ($l$ = the quotient field of $R_1$ and $L/K$ is separable).

Hence $\text{rank} \Omega_{A/R} = \text{rank} \Omega_{A/R_1} - \dim R$ and we have to show that $\text{rank} \Omega_{A/R_1} = \dim A$.

Let $\rho : A \rightarrow k$ be an $R$-homomorphism (exists, since (2)) and let $p$ be its kernel. Then $B = \hat{A}_p$ has the properties (see [3] EGA IV, Ch. 0, (7.8.2) and (7.8.3))

(a) $B$ has no nilpotents.

(b) every minimal prime $q$ of $B$ satisfies $\dim B/q = \dim B (= \dim A_p = \dim A)$.

(c) the quotient field of $B/q$ is separable over $L$ (and hence over $k$).

Further since $A \subset B$ have no zero divisors $\text{rank}_A \Omega_{A/R_1} = \text{rank}_B \Omega_{A/R_1} \otimes B$. It is easily seen that $\Omega_{B/R_1} = \Omega_{B/R_1} \simeq \Omega_{A/R_1} \otimes B$. Hence the statement $\text{rank}_A \Omega_{A/R} = \dim A - \dim R$ will follow from lemma (5.2).

The last statement of (5.1) follows directly from the exact sequence:

$$
A^m \xrightarrow{\alpha} \Omega_{R[X]/R} \otimes A \rightarrow \Omega_{A/R} \rightarrow 0,
$$

in which $\Omega_{R[X]/R} \otimes A$ is the free $A$-module on generators $dX_1, \ldots, dX_N$ and $\alpha$ is the map given by

$$
\alpha(a_1, \ldots, a_m) = \sum_{i=1}^{m} a_i dF_i = \sum_{i,j} a_i \frac{\partial F_i}{\partial X_j} dX_j.
$$

Indeed

$$
\dim A - \dim R = \text{rank} \Omega_{A/R} = N - \text{rank} \left( \frac{\partial F}{\partial X} \right) \text{ modulo } F
$$

and $\dim A = \dim R + N - \text{height } F$. 


DEFINITION: Let $A \to B$ be a ring homomorphism. By $\Omega_{B/A}$ we denote the universal finite module of differentials i.e.
(i) $\Omega_{B/A}$ is a finite $B$-module and $d : B \to \Omega_{B/A}$ is an $A$-derivation.
(ii) The natural map $\text{Hom}_B(\Omega_{B/A}, M) \to \text{Der}_A(B, M)$ is an isomorphism for all finitely generated $B$-modules $M$.

REMARK: (a) If $B$ is of essentially finite type over $A$ then $\Omega_{B/A} = \Omega_{B/k}$.
(b) If $B$ is a complete local noetherian ring with coefficient ring or field $A$ then $\Omega_{B/A}$ exists.
(c) If the noetherian local ring has a coefficient field $k$ of characteristic $p \neq 0$ then $\Omega_{A/k} = \Omega_{B/k}$.
(d) If $A = k[[X]]$ where $k$ is a field of characteristic $0$, then $\Omega_{A/k} = \Omega_{B/k}$.
(e) If $A = k[[X]][Y]$ then $\Omega_{A/k}$ does not exist.

(5.2) LEMMA: Let $B$ be a complete local ring such that
(i) $A \subset B$ is a coefficient ring (or field) consisting of non-zero divisors.
(ii) $B$ has no nilpotents and for every minimal prime $q$ of $B$, $\dim B = \dim B/q$.
(iii) For every minimal prime $q$ of $B$, the quotient field of $B/q$ is separable over that of $A$.

Then $\text{rank}_B \Omega_{B/A} = \dim B - \dim A$.

PROOF: (a) $\dim A = 1$ (i.e. $A$ is a discrete valuation ring with maximal ideal $pA$). The ring $B$ has the form $A[[X, \ldots, X_N]]/F$. Since $p$ is a non-zero divisor on $B$ we find that $F \neq pA[[X_1, \ldots, X_N]]$. Take an element $f \in F$ with non-zero image $\overline{f}$ in $k[[X_1, \ldots, X_N]]$ where $k = A/pA$. After a change of coordinates, $\overline{f}$ is general in $X_N$ of say order $d$. The Weierstrasz theorem for $k[[X_1, \ldots, X_N]]$ implies that for every $g \in A[[X_1, \ldots, X_N]]$ one has $g = q_0 f + r_0 + p g_1$ where $r_0 \in A[[X_1, \ldots, X_N-1]]$ has degree $X_n(r_0) < d$. By induction we find $g_0 = q_1 f + r_1 + p g_2, \ldots, g_n = q_n f + r_n + p g_{n+1}, \ldots$. Hence $g = (q_0 + q_1 + \ldots) f + (r_0 + p r_1 + \ldots)$. So we proved that for any $g \in A[[X_1, \ldots, X_N]]$ we can write $g = q f + r$ where $r \in A[[X_1, \ldots, X_N-1]]$ has degree $X_n(r) < d$. In particular $f = (\text{unit}) (X_n^d + \cdots + a_0)$ with all $a_i \in A[[X_1, \ldots, X_N-1]]$. So $A[[X_1, \ldots, X_n]]/F$ is a finite extension of $A[[X_1, \ldots, X_N-1]]/G$ where $G = F \cap A[[X_1, \ldots, X_N-1]]$. Repeating this proces we find that $B$ is finite over $A[[X_1, \ldots, X_n]]$. Since all the minimal primes $q$ of $B$ satisfy $\dim B/q = \dim B$ we have $q \cap A[[X_1, \ldots, X_n]] = 0$. The total quotientring $\text{Qt}(B) = K_1 \times \cdots \times K_n$ of $B$ is a product of fields $K_i = B/q_i$, where $q_1, \ldots, q_n$ are the minimal primes of $B$. Each $K_i$ contains the quotient field $K$ of $A[[X_1, \ldots, X_n]]$.

The natural map $\alpha : \Omega_{A[[X_1, \ldots, X_n]]/A} \otimes B \to \Omega_{B/A}$ has the property that $\alpha \otimes 1_{\text{Qt}(B)} : \Omega_{A[[X_1, \ldots, X_n]]/A} \otimes \text{Qt}(B) \to \Omega_{B/A} \otimes \text{Qt}(B)$ is an isomorphism.
Indeed for any $A$-derivation $D : A[[X_1, \ldots, X_l]] \to M$, $M$ a finitely generated $B$-module, we have a unique extension $D_i : K_i \to M \otimes_B K_i$ since $K_i$ is an finite separable extension of $K$. So we have a unique extension

$$D_1 \times \ldots \times D_l : \text{Qf}(B) \to M \otimes \text{Qf}(B) = (M \otimes K_1) \oplus \ldots \oplus (M \otimes K_l).$$

Since $\Omega^f_{A[EX_1, \ldots, X_n]/A}$ is a free module of rank $= \dim B - \dim A$ also rank $\Omega^f_{B/A} = \dim B - \dim A$.

(b) $A = k$ is a field of characteristic zero. Same proof as in case (a).

(c) $A = k$ is a field of characteristic $p \neq 0$. A refined version of the Weierstrasz-theorems yields that $B$ is a finite extension of $k[[X_1, \ldots, X_d]]$ such that $q \cap k[[X_1, \ldots, X_d]] = 0$ for all minimal primes and such that the quotient field of $B/q$ is separable over $k((X_1, \ldots, X_d))$ for all minimal primes $q$ of $B$. After this we can finish the proof as in case (a).

The characteristic zero case of (5.1) is more complicated. Let $A = R[[X]]/F$ satisfy (4.5) and let $A_0$ be the image in $A$ of $R[[X_1, \ldots, X_h]]$, hence $A_0 = R[[X_1, \ldots, X_h]]/G$ with $G = F \cap R[[X_1, \ldots, X_h]]$. Further $A = A_0[[X_{h+1}, \ldots, X_N]]/H$ where $H = F/G$. Complete local rings satisfy the universal chain condition, so height $F = \text{height } H + \text{height } G$.

Let $K_0$ be the quotient field of $A_0$ then $A \otimes A_0 K_0 = K_0[[X_{h+1}, \ldots, X_N]]/L$ where $L$ is the ideal generated by the image of $F$.

The usual ‘Jacobian criterium for simple points’ yields some height $H \times \text{height } H - \text{minor } \delta$ of the matrix

$$\frac{\partial F}{\partial X_{h+1}, \ldots, \partial X_N}$$

is not contained in $L$ (and hence not in $F$).

If we can find a height $G \times \text{height } G - \text{minor of }$ $\frac{\partial G}{\partial X_1, \ldots, \partial X_h}$

which is not contained in $G$ then we can combine this with $\delta$ to produce a height $F \times \text{height } F - \text{minor of }$

$$\frac{\partial F}{\partial X_1 \ldots \partial X_n}$$

which is not contained in $F$. Hence we showed that it suffices to prove:
(5.3) **THEOREM:** If $A = R[X_1, \ldots, X_N]/F$ satisfies (4.5) then some height $F \times \text{height } F - \text{minor of}$

$$\frac{\partial F}{\partial X}$$

is not contained in $F$.

**PROOF:** Suppose that there exists a $\rho \in \text{Hom}_R(A, R)$; after changing the coordinates we may suppose that $\rho(X_i) = 0$ for all $i$. So $F \subset (X_1, \ldots, X_N) = p$. The ring $B = \hat{A}_p$ has the properties: (i) $B$ has no nilpotents and (ii) For every minimal prime $q$ of $B$, $\dim B/q = \dim B = \dim A_p = \text{height } p/F = N - \text{height } F$. Further clearly

$$B = K[X_1, \ldots, X_N]/FK[X_1, \ldots, X_N]$$

where $K = \text{Qt}(B)$. From (5.2) it follows that

$$\frac{\partial F}{\partial X}$$

has an height $F \times \text{height } F - \text{minor which is not contained in}$ $FK[X_1, \ldots, X_N]$ (and hence not contained in $F$).

(5.4) **PROPOSITION:** Let $A$ be a coefficient ring or field (according to $\text{char } R/m > 0$ or $= 0$) of $R$. The assumptions (4.5) and $\text{Hom}_R(A, R) \neq \emptyset$ for $A = R[X]/F$ imply that the sequence $0 \to \Omega^f_L/A \otimes A \xrightarrow{\cdot \Omega^f_L/A} \Omega^f_{A/R} \to 0$ is exact.

**PROOF:** The only thing to show is the injectively of $\alpha$. Now $\Omega^f_{A/R}$ is equal to the free $A$-module on generators $dX_1, \ldots, dX_N$ divided by the submodule $A dF$. Since some height $F \times \text{height } F - \text{minor is not contained in } F$ we have $\text{rank}_A \Omega^f_{A/R} \leq N - \text{height } F = \dim A - \dim R$. By (5.2) $\text{rank}_A \Omega^f_{A/R} = \dim A - \dim A$ and $\Omega^f_{A/R}$ is a free-module of rank $\dim R - \dim A$. Let $K$ denote the quotient field of $A$ then for dimension reasons

$$0 \to \Omega^f_{K/A} \otimes K \to \Omega^f_{A/A} \otimes K \to \Omega^f_{A/R} \otimes K \to 0$$

is exact. Since $\Omega^f_{K/A} \otimes A$ is a free $A$-module, also $\alpha$ must be injective.

(5.5) **LEMMA:** Let $R$ be a complete local ring with a residue field $k$
which is algebraically closed and uncountable. Let $A = \mathbb{R}[X]/F$ satisfy $\text{Hom}_R(A, R/m^n) \neq \emptyset$ for all $n$. Then $\text{Hom}_R(A, R) \neq \emptyset$.

**Proof:** Fix a coefficient field of $R$ or in the unequal characteristic case a map $W(k) \to R$ where $W(k)$ denotes the ring of Witt-vectors over $k$. Then each $R/m^n$ has the structure of a finite-dimensional vector space over $k$ in which addition and multiplication are morphisms. Then $\text{Hom}_R(A, R/m^n)$ is an algebraic subset of $(R/m^n)^N$ (we identify a map $\rho$ with $(\rho(X_1), \ldots, \rho(X_N)) \in (R/m^n)^N$).

The intersection of a descending sequence of non-empty constructible sets is non-empty (see F. Oort [6], Lemma 2 on page 221). Hence

$$\bigcap_{m \geq n} \text{im} \left( \text{Hom}_R(A, R/m^n) \to \text{Hom}_R(A, R/m^n) \right) \neq \emptyset$$

and with the usual compactness-argument it follows that

$$\text{Hom}_R(A, R) = \varprojlim \text{Hom}_R(A, R/m^n) \neq \emptyset.$$
$F_1, \ldots, F_s$ ($s = \text{height } F$). By flatness $\{F_1, \ldots, F_s\}$ is a regular sequence on $R'[X]_s$ and all the associated ideals of $(F_1, \ldots, F_s)$ in $R'[X]_s$ have height $s$. Take a minimal prime $q$ of $FR'[X]$ such that

$$\text{Hom}_{R'}(R'[X]/q, R') \neq \emptyset$$

(5.5) guarantees the existence of $q$. Put $A_1 = R'[X]/q$.

Then we have a commutative diagram

$$
\begin{array}{c}
\Omega^f_{R'/A} \otimes A \\
\downarrow \gamma \\
0 \\
\end{array} \quad \begin{array}{c}
\Omega^f_{A'/A} \\
\beta \\
\Omega^f_{A'/R'} \\
0
\end{array}
$$

in which the row is exact according to (5.4). Clearly also $\gamma$ is injective. Hence $\alpha$ is injective and we are done.

6. Induction steps

In this section we finally give a proof of (4.1). Let $F \subset R[X]$ satisfy (4.5). Let $A$ be the ideal generated by the $s \times s$-minors of

$$\frac{\partial F}{\partial X}$$

(where $s = \text{height } F$). According to Section 5, $F \cong (F, A)$. By induction on $\dim R[X]/F$ there exists an $s$-function for $(F, A)$. Hence it suffices to show (6.1) in the equal characteristic case. In the unequal characteristic case we also have to consider elements $x$ with $F(x) \equiv 0(m^\infty)$, $\Delta(x) \equiv 0(m^b)$ and $\Delta(x) \equiv 0 (p, m^\infty)$.

(6.1) Proposition: Suppose that $F$ satisfies (4.5). Let $p$ denote the characteristic of $R/m$ considered as an element of $R$.

For all $n$ and $b$ there exists an $a \in \mathbb{N}$ such that $F(x) \equiv 0(m^a)$ and $\Delta(x) \equiv 0(p, m^b)$ imply the existence of $x' \equiv x(m^n)$ with $F(x') = 0$.

The proof of (6.1) requires a string of lemmata.

(6.2) Lemma: Let $R$ be a complete regular local ring (unramified in the unequal characteristic case) with infinite residue field. There is a finite set of subrings $R_1, \ldots, R_s$ of $R$ and $T \in R$ such that
(i) each $R_i$ is regular and $R_i[T] = R$
(ii) for any $g \in R$, $g \neq 0(p, m^b)$ there exists an $i$ such that

$$g = \text{(unit)}(T^d + a_{d-1}T^{d-1} + \ldots + a_0)$$

with $d < b$ and $a_1, \ldots, a_{d-1} \in R_i$.

**Proof**: The image $\tilde{g}$ of $g$ in $R/pR$ has order $c$, $c < b$; let $h$ be its homogeneous part of order $c$ (with respect to a presentation $\Lambda[X_1, \ldots, X_n]$ of $R$). Let $\Lambda_0$ be a finite subset of $\Lambda$ such that the set of residues in $\Lambda/p\Lambda$ is of cardinal $> b$. There are $\lambda_1, \ldots, \lambda_n \in \Lambda_0$ such that $\lambda_n \not\equiv 0(p)$ and $h(\bar{\lambda}_1, \ldots, \bar{\lambda}_n) \neq 0$. Put $Y_i = X_i - \lambda_i^{-1}\lambda_n^{-1}X_n$ for $i = 1, \ldots, n-1$ and $Y_n = X_n$. Then $h(X_1, \ldots, X_n) = k(Y_1, \ldots, Y_n)$ for some homogeneous polynomial $k$. Then $k(0, \ldots, 0, Y_n) = \bar{\lambda}_n^{-1}Y_n h(\bar{\lambda}_1, \ldots, \bar{\lambda}_n) \neq 0$. Hence $\tilde{g}$ is general in $T = Y_n = X_n$. By the Weierstrass-preparation theorem

$$g = \text{unit} \left( T^c + a_{c-1}T^{c-1} + \ldots + a_0 \right)$$

with $a_i \in R' = R[A_1, \ldots, Y_{n-1}]$.

(6.3) **Proposition**: (Induction on dim $R$). Let $F = (F_1, \ldots, F_m) \in R[X]$ and $G \in R[X]$. For all $n$ and $b$ there exists $a \in \mathbb{N}$ such that

$$F(x) \equiv 0(m^a) \quad G(x) \not\equiv 0(p, m^b)$$

imply the existence of $x' = x(m^a)$

with $F(x') \equiv 0G(x')$.

**Proof**: If $x$ satisfies $G(x) \not\equiv 0(p, m^b)$ then according to (6.2) there is a presentation $R = R'[T]$ and an integer $d < b$ such that

$$G(x) = \text{a unit times} \left( T^d + a_{d-1}T^{d-1} + \ldots + a \right)$$

with all $a_i \in m(R')$. Since we have a finite choice for $R'$ and $d$ we can restrict ourselves to a fixed choice for $R'$ and $d$.

Introduce new variables $A_0, \ldots, A_{d-1}$; $Y_1, \ldots, Y_N$; $Y_{ij} (i = 1, \ldots, N; j = 0, \ldots, d-1)$; $Z_i (i = 1, \ldots, h)$; $Z_{ij} (i = 1, \ldots, h; j = 0, \ldots, d-1)$. Then $C = R'[A_0, \ldots, A_{d-1}] \subset R'[A_0, \ldots, A_{d-1}]/(T^d + A_{d-1}T^{d-1} + \ldots + A_0) = D$ is a finite extension and there is a number $e$ with $m(D)^e \subseteq m(C)D$.

Make the substitutions:

$$X_i = Y_i(T^d + A_{d-1}T^{d-1} + \ldots + A_0) + \sum_{j=0}^{d-1} Y_{ij} T^j$$
\[ X_i^e = Z_i(T^d + A_{d-1} T^{d-1} + \ldots + A_0) + \sum_{j=0}^{d-1} Z_{ij} T^j \]

and consider Weierstrasz-division by \( W = T^d + A_{d-1} T^{d-1} + \ldots + A_0 \). Then

\[ G = Q(Z, Z \ldots, A, Y, Y \ldots) W + \sum_{j=0}^{d-1} G_j(Z, Z \ldots, A, Y, Y \ldots) T^j \]

\[ F_i = Q_j(Z, Z \ldots, A, Y, Y \ldots) W + \sum_{j=0}^{d-1} F_{ij}(Z, Z \ldots, A, Y, Y \ldots) T^j \]

where \( G_j, F_{ij} \) belong to \( R[Z \ldots, A \ldots][Y \ldots] \). Consider also the equations:

\( (Y_i W + Y_{ij} T^j)^e = (Z_i W + Z_{ij} T^j) \)

which amounts to the equations:

\[ Z_{ij} - H_j(Y \ldots) \in R[Z, Z \ldots, A \ldots][Y \ldots]. \]

The system of equations \( F^* = \{G_j, F_{ij}, H_{ij} - Z_{ij}\} \) over \( R \) has an almost solution with \( A_i = a_i \) as given above. Further by Weierstrasz-division

\[ x_i = y_i(T^d + A_{d-1} T^{d-1} + \ldots + A_0) + \sum_{j=0}^{d-1} y_{ij} T^j, \quad \text{all } y_{ij} \in R' \]

\[ x_i^e = z_i(T^d + A_{d-1} T^{d-1} + \ldots + A_0) + \sum_{j=0}^{d-1} z_{ij} T^j, \quad \text{all } z_{ij} \in m(R') \]

These elements satisfy

\[ \begin{cases} z_{ij} - H_{ij}(y \ldots) = 0 \\ G_j(z, a, y \ldots) = 0 \\ F_{ij}(z, a, y \ldots) = 0(m_0^{a-d}) \end{cases} \]

where \( m_0 \) is the maximal ideal of \( R' \).

Since \( F^* \) has an s-function, we find for sufficiently high \( a \in \mathbb{N} \) a solution \((z', a', y' \ldots) \equiv (z, a, y \ldots)(m_0^a)\) of \( F \). Define

\[ x_i = y_i(T^d + a_{d-1} T^{d-1} + \ldots + a_0) + \sum_{j=0}^{d-1} y_{ij} T^j. \]

Then \( x \equiv x'(m^a) \) and

\[ F_j(x') = 0(T^d + a_{d-1} T^{d-1} + \ldots + a_0) \]
for all $i$ and

$$G(x') = \text{unit } (T^d + a_{d-1} T^{d-1} + \ldots + a_0).$$

Hence $F(x') \equiv 0(G(x')).$

(6.4) **Lemma**: Let $F_1, \ldots, F_s \in R[X]$ and let $\delta$ be an $s \times s$-minor of

$$\frac{\partial F}{\partial X}$$

and let $a \neq 0$ be an element of $R$ and $x$ such that $F(x) \equiv 0(a\delta(x)^2)$. Then there exists $x' \equiv x(a\delta(x))$ with $F(x') = 0$.

**Proof**: We may suppose $x = 0$ and we may replace $R[X] by R[X]$. Then we are reduced to a well known case of this lemma. See [1] lemma (5.10) and (5.11).

**Conclusion of the proof of (4.1)**

Let $(i)$ resp. $(j)$ denote subsets of $s$ elements from $\{1, \ldots, m\}$ resp. $\{1, \ldots, N\}$ and let $\Delta_{(i), (j)}$ denote the corresponding $s \times s$-minor $(\partial F/\partial X)$.

For any $(i)$ let $F_{(i)}$ denote the ideal generated by $\{F_{a\delta(i)}\}$. The radical $\sqrt{F_{(i)}}$ of $F_{(i)}$ equals $p_{(i), 1} \cap \ldots \cap p_{(i), n} = \text{the intersection of prime ideals}$. Let $G_{(i)} = \bigcap \{p_{(i), a} | p_{(i), a} F\}$. By induction $(F, G_{(i)})$ has an $s$-function $s_{(i)}$ and $(F, \Delta)$ has an $s$-function $s$.

Let $F(x) \equiv 0(m^s)$ with $\tau$ sufficiently high, then:

(a) If $\Delta(x) \equiv 0(m^s(a))$ then there exists $x' \neq x(m^s)$ with $F(x') = \Delta(x') = 0$.

(b) If $\Delta(x) \not\equiv 0(m^s(a))$ then for some $(i)$ and $(j)$ we have

$$\Delta_{(i)\cup(j)}(x) \not\equiv 0(m^s(a)).$$

Choose $u \in R$, $u \neq 0$ of order $\tau'$, then by (6.3) there $x' \equiv x(m^{\tau'})$ with $F(x') \equiv 0(u\Delta_{(i)\cup(j)}(x)^2)$. By lemma (6.4) there exists $x'' \equiv x'(m^{\tau'})$ with $F_{(i)}(x'') = 0$ and $F(x'') \equiv 0(m^{\tau'})$ and $\Delta_{(i)\cup(j)}(x'') \equiv 0(m^s(a))$ where $\tau'$ is sufficiently high.

(c) For some minimal prime $p_{(i), a}$ of $F_{(i)}$ we have $p_{(i), a}(x'') = 0$. Since $\Delta_{(i)\cup(j)}(x'') \neq 0$ it follows that height $p_{(i), a}(x'') = s_{(i), a}$. If $p_{(i), a} = F$ we are finished.

If $p_{(i), a} \neq F$ then $p_{(i), a} \not\subseteq F$ and $G_{(i)}(x'') = 0$. So we find

$$(F(x''), G(x'')) \equiv 0(m^{\tau'}).$$
From the existence of $s_{(i)}$ we conclude that there is an element $x''' = x''(m^n)$ such that $F(x''') = G(x''') = 0$.

This concludes the proof of (4.1).

7. The mixed characteristic case

In this section we give the results that we could obtain in the mixed characteristic case.

(a) If the residue field $k$ of $R$ is finite then $R$ is clearly a strong s-ring since every $\text{Hom}_R(R[[X]]/F, R/m^n)$ is a finite set.

(b) If $\dim R = 1$ (i.e. $R$ is a discrete valuation ring of mixed characteristic) then $R$ is a strong s-ring. In this case we don’t need (6.3) and the hypothesis of (6.4) is automatically satisfied.

(c) For general $R$ we would have proved that $R$ is a strong s-ring if we could prove a more general version of (6.3), for instance: ‘For all $b$ and $n$ there exists $a \in \mathbb{N}$ such that $F(x) \equiv 0(m^a)$ and $G(x) \not\equiv 0(m^b)$ imply the existence of $x' \equiv x(m^n)$ with $F(x') \equiv 0(G(x'))$.

If $\dim R = 2$ and $[k : k^p] \lt \infty$ we will prove this more general version. But first another result.

(7.1) **Proposition:** Let $R$ be a complete local ring with residue characteristic $p \neq 0$. Suppose that $k = R/m$ is finite over $k^p$ and that for some $l$, $p^{l+1}R = 0$. Then $R$ is a strong s-ring.

(7.2) **Corollary:** Let $R$ be a complete local ring of residue characteristic $p \neq 0$. Let $k = R/m$ be finite over $k^p$. Given $F \subset R[[X]]$ there exists a function $\tau : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ such that for all $x$ with $F(x) \equiv 0(m^{\tau(a,b)})$ there exists $x' \equiv x(m^n)$ and $F(x') \equiv 0(p^aR)$.

**Proof:** Replace $R$ by $R/pR$ and apply (7.1).

**Proof of (7.1):** (a) Suppose that we have shown the existence of a local ring homomorphism $R_0 = W_{l+1}(k_0[[T_1, \ldots, T_d]]) \to R$ where $k_0$ is a subfield of $k$ which makes $R$ into a finite $R$-module. With (4.2) it suffices to show that $R_0$ is a strong s-ring. Let $F \subset R_0[[X]]$ be given. Replace each variable $X_i$ by a Witt-vector $(Y_i, 0, \ldots, Y_i, 1)$. Then the system $F$ is equivalent to a set of equations over $k_0[[T_1, \ldots, T_d]]$. From (4.1) the assertion (7.1) would follow.

(b) The structure theorem for complete local rings yields the existence of a finite map $R_1 = V/p^{l+1}V[[T_1, \ldots, T_d]] \to R$, where $V$ is a complete discrete valuation ring with $V/pV = k$. Let $K$ be a perfect field containing
k, then $V/p^{i+1}V \subset W_{i+1}(K)$ and $R_1 \subset W_{i+1}(K[S_1, \ldots, S_d])$ where $T_i \mapsto (S_i, 0, \ldots, 0)$ ($i = 1, \ldots, d$).

The image of $R_1$ contains $W_{i+1}(k[S_1, \ldots, S_d]p^i)$, since for any $f \in k[S_1, \ldots, S_d]$ there exists $f^* = (f, f_1, \ldots, f_i) \in R_1$ and hence

$$(f^*)^{p^i} = (f^{p^i}, 0, \ldots, 0)$$

belongs to $R_1$. Further

$p(f^*)^{p^i-1} = (0, f^{p^i}, 0, \ldots, 0), \ldots, p^j f^* = (0, \ldots, 0, f^{p^i})$

all belong to $R$.

So we found a finite map $W_{i+1}(k[S_1^p, \ldots, S_d^p]) \to R_1 \to R$ and the proof is completed.

(7.3) Theorem: Let $R$ be a complete regular local ring of mixed characteristic. Suppose that $k = R/m$ is finite over $k^p$. If $\dim R = 2$ then $R$ is a strong s-ring.

Proof: As remarked above we have to show that for

$G, F = (F_1, \ldots, F_m) \in R[[X]]$

and all $b$ and $n$ there exists $a \in \mathbb{N}$ such that $F(x) \equiv 0(m^a)$, $G(x) \equiv 0(m^b)$ implies that there exists $x' \equiv x(m^a)$ with $F(x') \equiv 0(G(x'))$.

(1) If $G(x)$ has order $c(c < b)$ and $G(x) \equiv 0(p^c)$ then $G(x) = \text{unit } p^c$ and we can apply (7.2).

(2) If $G(x) \equiv 0(p^c, m^a)$ then applying (7.2) we are reduced to case (1), etc.

We see that we have only to do the case $G(x) = p^2a$ with $a \in R$ satisfying $a \not\equiv 0(p, m^d)$ where $d$ is some fixed number. Using (6.2) it is enough to consider the case

$G(x) = \text{unit } p^2(T^d + a_{d-1} T^{d-1} + \ldots + a_0)$

where $R = V[[T]], V$ a valuation-ring, and all $a_i \in V$ and moreover all $a_i \in m(V)$.

Let $I$ be the ideal generated by $p^2$ and $T^d + a_{d-1} T^{d-1} + \ldots + a_0$ with all $a_i \in m(V)$. Then $m(R)^{2d} \subset I$. Further there is a number $\varepsilon \geq 1$, independent of the choice of $a_0, \ldots, a_{d-1} \in m(V)$, such that

$ap^2 + b(T^d + a_{d-1} T^{d-1} + \ldots + a_0) \equiv 0(m(R)^{\varepsilon})$
implies \( ap^a \equiv 0(m^n) \).

Choose \( n \) such that \( n > 2da \). Now we proceed as in the proof of (6.3).

Choose new variables \( A_0, \ldots, A_{d-1}; Y; Y_{ij}; Z_i; Z_{ij} \) and substitute

\[
X_i = Y_i(T^d + A_{d-1} T^{d-1} + \ldots + A_0) + \sum Y_{ij} T^j
\]

\[
X_i^e = Z_i(T^d + A_{d-1} T^{d-1} + \ldots + A_0) + \sum Z_{ij} T^j
\]

Then

\[
G = Q(Z, Z, A, A, Y, Y)(T^d + A_{d-1} T^{d-1} + \ldots + A_0) + \sum G_j(Z, A, Y) T^j
\]

\[
F = Q_j(Z, Z, A, A, Y, Y)(T^d + A_{d-1} T^{d-1} + \ldots + A_0) + \sum F_{ij}(Z, A, Y) T^i Z_{ij} - H_{ij}(Y)
\]

We find a system of equations \( F^* \) over \( V \) namely \( \{ Z_{ij} - H_{ij}, G_j, F_{ij} \} \) and we are given an almost solution of \( F^* \).

So there is (for \( a \gg 0 \)) an \( x' \equiv x(m^n) \) with \( F(x'), G(x') \equiv 0 \) modulo \( (T^d + a_{d-1} T^{d-1} + \ldots + a_0) \).

According to (7.2) there is also an \( x'' \equiv x(m^n) \) with \( F(x''), G(x'') \equiv 0(p^a) \).

Hence \( x'' - x' \equiv 0(m^n) \). Since \( n > 2da \) we find \( a \) and \( b \) with

\[
x'' - x' = ap^a + b(T^d + a_{d-1} T^{d-1} + \ldots + a_0)
\]

and \( ap^a \equiv 0(m^n) \).

Put \( z = x'' - ap^a = x' + b(T^d + a_{d-1} T^{d-1} + \ldots + a_0) \) then \( z \equiv x(m^n) \) and \( F(z), G(z) \) are divisible by \( p^a \) and \( (T^d + a_{d-1} T^{d-1} + \ldots + a_0) \). So \( F(z) \) and \( G(z) \) are divisible by \( p^a(T^d + a_{d-1} T^{d-1} + \ldots + a_0) \). Since order \( G(z) = \) order \( G(x) \) we must have \( G(z) = \) unit \( p^a(T^d + a_{d-1} T^{d-1} + \ldots + a_0) \). It follows that \( F(z) \equiv 0(G(z)) \). End of the proof.

**REMARKS:** (1) F. Oort’s theorem 1: ‘Every complete local domain \( R \) is an \( f \)-ring’ will follow from the statement: ‘\( R \) is an \( s \)-ring’.

**PROOF:** Consider the polynomial \( F = XY \in R[X, Y] \); by assumption it has an \( s \)-function. Define \( f(i, j) = s(\max(i, j)) \) for all \( i, j \in \mathbb{N} \). Then \( x \in R^{m^i} \) and \( y \in R^{m^j} \) implies \( xy \in m^{f(i, j)} \). Indeed, \( F(x, y) \equiv 0(m^{s(\max(i, j))}) \) implies the existence of \( (x', y') \equiv (x, y)(m^{\max(i, j)}) \) and \( x'y' = 0 \). Since \( R \) has no zero divisors \( x' = 0 \) or \( y' = 0 \) and one finds a contradiction.

(2) Using Oort’s theorem 1 one can conversely prove that an \( s \)-function exists in some cases e.g.: If \( R \) is a complete local domain with quotient field \( K \). Then an \( s \)-function exists for every ideal \( F \subset R[X_1, \ldots, X_n] \) such that \( K[X_1, \ldots, X_n]/FK[X_1, \ldots, X_n] \) has Krull-dimension zero.
PROOF: As in (4.3), using the $f$-function of $R$ one reduces to the case where $F$ is a prime ideal and $F$ has a zero in every $R/m^a$. Let $P_i = P_i(X_i)$ be a minimal polynomial for $X_i \mod FK[X_1, \ldots, X_n]$ over $K$. The polynomials $P_i$ are irreducible over $K$ and are normed such that all coefficients belong to $R$.

Since $P_i$ has a zero in every $R/m^a$, it has a zero in $R$ according to [6] Theorem 2. Hence $F = (x_1 - a_1, \ldots, x_n - a_n)$ for suitable $a_1, \ldots, a_n \in R$. Clearly an $s$-function exists for $F$.

(3) It might be possible to extend the reasoning of (2) to more general cases.

8. Analytic local rings

In this section we want to show that analytic local rings $R$ over a complete valued field $k$ (with $[k:k^p] < \infty$ if char $k = p \neq 0$) are $s$-rings. Let $F \subset R[X_1, \ldots, X_n]$ be some ideal. According to (4.1) it suffices to show that every formal solution of $F$ can be approximated by solutions in $R$. This is again a theorem of M. Artin [1] theorem (1.2) in the case char $k = 0$. The only instance in Artin’s proof where char $k = 0$ is used is lemma (2.2) [1] page 283. It suffices to show the following:

(8.1) PROPOSITION: Let $k$ be a (pseudo-)complete valued field of char $p \neq 0$ with $[k:k^p] < \infty$, let $X = (X_1, \ldots, X_n)$, $Y = (Y_1, \ldots, Y_N)$; $k\{X, Y\}$ the ring of convergent power series over $k$ and $F \subset k\{X, Y\}$ a prime ideal such that (i) $F \cap k\{X\} = 0$ and (ii) $F$ has a solution in $k[[X]]$.

Then the ideal $A$ in $k\{X, Y\}$ generated by the height $F \times$ height $F$-minors of

$$\frac{\partial F}{\partial Y_1, \ldots, \partial Y_n}$$

is not contained in $F$.

PROOF: (Analogous to (5.1)). We are given $k\{X\} \subset k\{X, Y\}/F = A \subset k[[X]]$. Hence the quotient field $L$ of $A$ is separable over the quotient field $K$ of $k\{X\}$. So $\Omega_{K/k} \otimes L \xrightarrow{\beta} \Omega_{L/k}$ is injective. Consider the exact sequence

$$\Omega_{k\{X\}/k} \otimes A \xrightarrow{\alpha} \Omega_{A/k} \rightarrow \Omega_{A/k\{X\}} \rightarrow 0$$

with $\beta = \alpha \otimes_A 1_L$. Since $\Omega_{k\{X\}/k} \otimes A$ is a free $A$-module this implies that
α is injective and hence rank $\Omega_{A/k(X)} = \text{rank } \Omega_{A/k} = n$.

Weierstrasz-preparation theorem yields $k\{T_1, \ldots, T_a\} \subset A$ such that $A$ is finite and separable over $k\{T_1, \ldots, T_a\}$ and $a = \dim A$. The map $\gamma : \Omega_{k\{T_1, \ldots, T_a\}} \otimes A \to \Omega_{A/k}$ has the property $\gamma \otimes 1_L$ is bijective. So rank $\Omega_{A/k} = a = \dim A$.

Further we have an exact sequence:

$$A^m \xrightarrow{\delta} \Omega_{k(X), y/k(X)} \otimes A \to \Omega_{A/k(X)} \to 0$$

where $\delta$ is given by

$$\delta(a_1, \ldots, a_m) = \sum_i a_i dF_i = \sum_{i,j} a_i \frac{\partial F_i}{\partial Y_j} dY_j,$$

and $F = (F_1, \ldots, F_m)$. The middle term is a free module of rank $N$, and the term on the right has rank $a - n$. Hence some $(N + n - a) \times (N + n - a)$-minor of

$$\frac{\partial F_1 \ldots F_m}{\partial Y_1 \ldots Y_N}$$

is non-zero modulo $F$. Note further that $N + n - a = \text{height } F$.

REFERENCES

[3] J. Dieudonné and A. Grothendieck: Eléments de géométrie algébrique. IHES no. 20, 24,