Annali della
Scuola Normale Superiore di Pisa
Classe di Scienze

Paolo Valabrega

On two-dimensional regular local rings and a lifting problem

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3e série, tome 27, nº 4 (1973), p. 787-807

<http://www.numdam.org/item?id=ASNSP_1973_3_27_4_787_0>

ON TWO-DIMENSIONAL REGULAR LOCAL RINGS AND A LIFTING PROBLEM ([1])

by Paolo Valabrega ([2])

Introduction.

In [10] and [11], in order to prove the existence of nonexcellent regular local rings of characteristic O, we showed that two classes of nonexcellent one-dimensional regular local rings of positive characteristic p can be lifted to characteristic O, i.e. these *DVR's* are isomorphic with a quotient ring R/pR, where R is a two-dimensional regular local ring of characteristic O.

In the present paper we want to investigate the lifting problem for *DVR's* in characteristic $p > 0$ from a general point of view.

Precisely we consider a one-dimensional regular local ring B of positive characteristic p and prove that, if B contains a coefficient field K and its fraction field is separably generated over $K(X)$ (where X is a suitable parameter), then there is an isomorphism: $B = R/pR$, where R is a two-dimensional regular local ring of characteristic O. Moreover R can be chosen faithfully flat as an algebra over Z_{pZ} (ring of integers localized at the prime p).

The translation of our lifting result into the language of Spectra shows that it is strictly related with a lifting theorem for smooth schemes (see [7], proposition 18.1.1.).

We remark also that our result gives a partial answer to a lifting problem modulo p^n for formally smooth algebras, extending to the non-complete situation results which are well known when the rings are supposed

---

Pervenuto alla Redazione il 26 Gennaio 1973.

([1]) The present paper was written while the author was supported by the CNR as a member of the GNSAGA.

([2]) Author's permanent address: Istituto matematico dell'Università — via Carlo Alberto, 10 — I0123 TORINO (Italy).

to be noetherian complete local rings (see [5], theorem 19.7.2 and remark 19.7.3).

To deal with our main preblem we need a few general results on formal power series rings. In particular we have to consider the following problem: let C be a discrete valutation ring, $\widehat{C}$ its completion and Y an indeterminate; if t is an arbitrary formal power series in $\widehat{C}[[Y]]$, does t belong to some non complete regular local ring R, with completion $\widehat{C}[[Y]]$ and containing $C[Y]$?

Our positive answer, with an explicit construction of the ring R, has applications both when $C = K[X]_{(X)}$ (where $K =$ field and $X =$ indeterminate) and when $C =$ complete discrete valutation ring with parameter the prime number p. It must be observed that this last case is really a key-point for our lifting.

The lifting result given in the present paper generalizes the main result of [11]. Also the main theorem of [10] can be slightly improved by means of properties that we prove here.

We are also able to produce a class of regular local rings of characteristic 0 and equal characteristic, which are not pseudogeometric, generalizing an example of Nagata (see [8], Appendix, example 7).

We wish to thank Michael Artin for some useful conversations on the subject of this paper.

n. 1.

All the rings considered are commutative with 1.

A *local ring* A, through the present paper, is a ring with a unique maximal ideal, but *not necessarily noetherian.*

We start with a few general properties of local domains and *DVR's.*

LEMMA 1: *Let A be any local domain with fraction field L, M any subfield of L and $B = A \cap M$.*

Then the following properties are true:

a) B is a local domain dominated by A;

b) if $\mathfrak{p} = aB$ is a principal ideal of B then $\mathfrak{p}A \cap B = \mathfrak{p}$.

PROOF: *a)* Let $\mathfrak{m}$ be the maximal ideal of A. We want to see that $\mathfrak{m} \cap B$ is the unique maximal ideal of B. In fact, if x is in $B - \mathfrak{m} \cap B)$, then x is invertible both in A and in M, hence in B.

q) Let $x = ay$, with $y \in A$, be in $\mathfrak{p}A \cap B$. Then $y \in A \cap M = B$, i.e. $x \in aB = \mathfrak{p}$.

LEMMA 2: *Let C be any DVR with fraction field M and parameter a. If L is a subfield of M containing a, then $R = L \cap C$ is a DVR with parameter a.*

PROOF: By lemma 1, a), R is a local domain dominated by C.

By lemma 1, b), we have: $aR = aC \cap R$. Therefore the maximal ideal of R is principal. Moreover $\bigcap_1^\infty a^n R \subseteq \bigcap_1^\infty a^n C = (O)$, since C is a Zariski ring ([2], chap. III, § 3, n. 3). This implies that R is a DVR with parameter a ([3], chap. VI, § 3, n. 6, proposition 9).

REMARK: Lemma 2 can be applied in the following situation: $C = K[[X]] =$ formal power series ring in the indeterminate X over the field K. Therefore, if F is any set of formal power series, then $K(X)(F) \cap K[[X]]$ is a DVR with parameter X and, of course, with completion $K[[X]]$.

We now give a few useful properties of two-dimensional regular local rings.

PROPOSITION 3: *Let C be any DVR and Y an indeterminate. If L is a subfield of the fraction field of $C[[Y]]$, such that $C[Y] \subseteq L$, then $R = L \cap C[[Y]]$ is a regular local ring with completion $\widehat{C}[[Y]]$.*

PROOF: By lemma 1, a), R is a local domain dominated by $C[[Y]]$.

Let now a be a parameter of C. We want to show that the maximal ideal of R is generated by a and Y. Let x be an element in R but not in $(a, Y)R$ and suppose that $x = \sum_0^\infty b_n Y^n$. If $b_0 = ac_0$, for a suitable $c_0 \in C$, then $x - ac_0 = Y\left(\sum_1^\infty b_n Y^{n-1}\right) \in R$. Hence $\sum_1^\infty b_n Y^{n-1} \in L \cap C[[Y]] = R$. This says that $x \in (a, Y)R$. Therefore b_0 must be invertible in C and x is invertible in R.

Now we want to show that R is a noetherian local ring. For this purpose, let's first consider the quotient field $K = C/aC$ and the ring $C[[Y]]/aC[[Y]] = K[[Y]]$. We want to see that R/aR is a DVR. But we have: $aR = aC[[Y]] \cap R$, by definition of R. Therefore R/aR is a subring of $K[[Y]]$, with maximal ideal generated by Y and separated in its Y-topology. This says that R/aR is a DVR ([3], chap. VI, § 3, n. 6, proposition 9).

Let's now go back to R. To see noetherian property it is enough to show that every prime ideal is finitely generated ([8], chap. I, theorem 3.4).

Of course every prime ideal containing a is finitely generated; therefore we can assume that $\mathfrak{P}$ is a prime ideal such that $a \notin \mathfrak{P}$.

The image of $\mathfrak{P}$ modulo aR is a principal ideal $Y^r(R/aR)$, where r is a suitable integer ≥ 1; se we can select b in $\mathfrak{P}$ such that its image modulo aR is Y^r. Then we obtain the following inclusions:

$$bR \subseteq \mathfrak{P} \subseteq (b, a)\, R.$$

If $x \in \mathfrak{P}$ then $x = bc_1 + ad_1$, where c_1 and d_1 are suitable elements in R. Since $x - bc_1 \in \mathfrak{P}$, d_1 is in $\mathfrak{P}$, i.e.: $d_1 = bc_2 + ad_2$, which implies: $x = b\,(c_1 + ac_2) + a^2\, d_2 = be_2 + a^2\, d_2$.

It is now clear that, for each n, we can choose e_n and d_n such that $x = be_n + a^n\, d_n$.

Therefore we deduce the following inclusions:

$$bR \subseteq P \subseteq \bigcap_1^\infty \,(b, a^n)\, R.$$

Extending the ideals to $C[[Y]]$ we obtain:

$$bC[[Y]] \subseteq \mathfrak{P}\, C[[Y]] \subseteq \bigcap_1^\infty \,(b, a^n)\; C[[Y]] = bC[[Y]],$$

the last equality depending on the fact that $C[[Y]]$ is a Zariski ring for the $aC[[Y]]$-topology ([2], chap. III, § 3, n. 3).

Hence we have:

$$bC[[Y]] = \mathfrak{P}\, C[[Y]].$$

Therefore lemma 1, b) says that $\mathfrak{P} = bR$.

So R is a local ring satisfying the following properties:

(i) R is noetherian;

(ii) the maximal ideal of R is generated by a and Y;

(iii) $C[Y]_{(a,Y)} \subseteq R \subseteq \widehat{C}[[Y]] = (C[Y]_{(a,Y)})^{\wedge}$.

Therefore we deduce that R has completion $\widehat{C}[[Y]]$ ([2], chap. III, § 3, n. 5, proposition 11). Hence R itself is regular ([9], vol. II, chap. VIII, §. 11).

A useful application of proposition 3 is the following key-result to deal with our lifting problem:

THEOREM 4: *Let C be any DVR, Y an indeterminate over its completion $\widehat{C}$ and $t = \sum_0^\infty a_n\, Y^n$ an arbitrary formal power series in $\widehat{C}[[Y]]$.*

Then there is a local ring R satisfying the following conditions:

(i) $C[Y, t, a_0, \dots, a_n, \dots] \subseteq R \subseteq \widehat{C}[[Y]]$;

(ii) *R is regular with completion* $\widehat{C}[[Y]]$;

(iii) *R is the smallest ring satisfying* (i) *and* (ii) (i.e. *if S satisfies* (i) *and* (ii), *then* $R \subseteq S$).

Furthermore such a ring R is not complete and its fraction field is generated over the fraction field of $C[Y]$ by $t, a_0, \dots, a_n, \dots$.

PROOF: Let's put: $L =$ fraction field of $C[a_0, \dots, a_n, \dots]$, $B = L \cap \widehat{C}$. By lemma 2, B is a DVR with completion $\widehat{C}$.

Now we consider the fraction field of $B[Y, t]$, say K, and put: $R = K \cap \widehat{C}[[Y]]$.

By proposition 3, R is regular local with completion $\widehat{C}[[Y]]$; hence it satisfies requirements (i) and (ii).

Property (iii) depends on the fact that a regular local ring R with fraction field K and completion $\widehat{R}$ satisfies always the following equality: $R = K \cap \widehat{R}$ ([8], chap. II, 18.4).

We want to show that R is not complete. But we know that $K =$ fraction field of R is contained in the fraction field of $\widehat{C}[Y, t]$, which is a simple extension of the fraction field of $\widehat{C}[Y]$, while $\widehat{C}[[Y]]$ has infinite transcendence degree over polynomials. Therefore $R \neq \widehat{C}[[Y]]$.

COROLLARY: *With notations of theorem* 5, *if $t \in C[[Y]]$, then there is the smallest local ring R such that:*

(i) *$t \in R$ and* $C[Y] \subseteq R \subseteq C[[Y]]$;

(ii) *R is regular with completion* $\widehat{C}[[Y]]$.

Moreover R is not the whole $C[[Y]]$.

PROOF: In the present situation the ring R of theorem 4 has fraction field generated by the unique element t over the fraction field of $C[Y]$.

R is different from $C[[Y]]$, since $C[[Y]]$ has infinite transcendence degree over $C[Y]$.

We give now a slightly more general result than the preceding corollary, exactly in the form we'll need for the lifting:

THEOREM 5: *Let C be a DVR, Y an indeterminate, t a formal power series in $C[[Y]]$ and S any regular local ring such that:*

1) $C[Y] \subseteq S \subseteq C[[Y]]$;

2) $\widehat{S} = \widehat{C}[[Y]]$.

Then there is the smallest local ring R such that:

(i) *$t \in R$ and $S \subseteq R \subseteq C[[Y]]$;*

(ii) *R is regular with completion $\widehat{C}[[Y]]$.*

Moreover the fraction field of R is generated by t over the fraction field of S.

PROOF: Put: $M =$ fraction field of S. Then $R = C[[Y]] \cap M(t)$ is a regular local ring with completion $\widehat{C}[[Y]]$, by proposition 3.

The information on the ring R introduced in theorem 5 can be improved by the following

PROPOSIZIONE 6: *With notations of theorem 5, let a be a parameter for C and $\bar{t}$ the image of t modulo $aC[[Y]]$. Let's assume that t satisfies one of the following conditions:*

(i) *t is transcendental over S and $\bar{t}$ is transcendental over S/aS;*

(ii) *t is integral over S and $\bar{t}$ is integral over S/aS, both having the same degree over S and S/aS respectively.*

Then we have: $R/aR =$ the smallest DVR such that $(S/aS)[t] \subseteq R \subseteq (C/aC)[[Y]]$ and $\widehat{R} = (C/aC)[[Y]]$.

PROOF: It is enough to prove that $R/aR = (C/aC)[[Y[| \cap$ (fraction field of $(S/aS)[t]$).

Let now f/g be in R, with f and g in $S[t]$. If g is not in $aC[[Y]] \cap R = aR$, then the image of f/g is simply the quotient of the images, hence an element of $(C/aC)[[Y]]$ (fraction field of $(S/aS)[t]$).

Therefore we have to examine the case when $g \in aC[[Y]]$. Since f/g is a formal power series and $f = (f/g)g$, also f belongs to $aC[[Y]]$ and, if $g = a^r g'$, with $g' \notin aC[[Y]]$, then $f = a^r f'$, where f' could belong again to $aC[[Y]]$. Moreover, if f' really belongs to $aC[[Y]]$, there's nothing to prove, since the image of f/g is exactly 0. So we can assume that $f = a^r f'$, $g = a^r g'$, where r is a suitable integer ≥ 1 and both f' and g' are not in $aC[[Y]]$.

It is easy to see that the image of f/g is the same as the image of f'/g', since both the fractions are the same element in $C[[Y]]$.

Therefore we are done if we prove that f' and g' are elements of $S[t]$, i.e. if we prove that all the coefficients of f and g, as polynomials in t over S, are in $a^r S$.

We use induction on r. The step from r to $r+1$ being obvious, let's investigate the case $r = 1$.

I) t satisfies condition (i). The canonical images of f and g modulo $aC[[Y]]$ are 0, hence identically 0. This says that all the coefficients of f and g are in $aS = aC[[Y]] \cap S$.

II) t satisfies condition (ii). Let s be the degree of t over S. So every element of $S[t]$ can be written as a polynomial of degree less than s. Now, if f and g are in $aC][Y]]$, their images are identically 0, as above, in case I); but this says that all coefficients of f and g are in aS.

REMARK 1: Theorem 4 can be applied in the following situation: take any field K and two indeterminates X and Y. If $t = \sum_0^\infty a_n(X)\, Y^n$ is a formal power series in $K[[X, Y]]$, then theorem 4 says that t belongs to the regular local ring $R = K[[X, Y]] \cap K(t, X, Y, a_0(X), \dots)$.

If the $a_n(X)$'s are polynomials, then $R = K[[X, Y]] \cap K(t, X, Y)$.

REMARK 2: In [8] (Appendix, example 7) Nagata produces a ring which turns out to be an example of an equicharacteristic regular local ring of characteristic 0 and dimension 2 not excellent, not even pseudo-geometric (Nagata wanted to investigate analytic normality only, but really it can be seen that his ring satisfies also the properties now listed: for excellent property see [10], final remark; for pseudogeometric property see below). We recall shortly how to define this ring.

Take an arbitrary field K of characteristic 0 and two indeterminates X and Y. Then select a formal power series $w = \sum_1^\infty a_n X^n \in K[[X]]$, transcendental over polynomials. Now put:

$$z_1 = z = (Y + w)^2, \dots, z_{i+1} = [z - (Y + \sum_{j<i} a_j X^j)^2]/X^i, \dots,$$

$R = K[X, Y, z_1, \dots, z_n, \dots]_{m'}$, where m' = maximal ideal generated by $X, Y, z_1, \dots, z_n, \dots$.

Nagata proves the following properties:

(i) R is regular local with completion $K[[X; Y]]$;

(ii) zR is a prime ideal of R.

Therefore, if R is pseudogeometric, then R/zR is a pseudogeometric local domain ([8], chap. VI, 36.1), hence it is analytically unramified ([8], chap. VI, theorem 36.4). But it is easy to see that

$$(R/zR)^{\wedge} = K[[X, Y]]/(Y + w)^2 K[[X, Y]]$$

is not a reduced ring, since $Y + w$ is nilpotent. So R cannot be pseudo. geometric.

We observe that every z_n belongs to $K(X, Y, z) \cap K[[X, Y]]$; hence R is simply the smallest regular local ring containing polynomials and z, i.e. $R = K(X, Y, z) \cap K[[X, Y]]$.

Theorem 4 is useful to generalize Nagata's example, i.e. to produce *a* wide class of non pseudogeometric regular local rings of characteristic 0 and equal characteristic, according to the construction of the following

PROPOSITION 7: *Let K be a field of characteristic* 0, *X and Y two indeterminates and $t = \sum_{0}^{\infty} a_n(X) Y^n$ a non invertible formal power series in $K[[X, Y]]$ satisfying the following conditions:*

1) *t is transcendental over $K(X, Y, a_0(X), \dots, a_n(X), \dots)$;*

2) *$t = z^r$, where z is a suitable element in $K[[X, Y]]$ and r an integer not less than* 2.

Then the ring $R = K[[X, Y]] \cap K(X, Y, t, a_0(X), \dots, a_n(X), \dots)$ satisfies the following conditions:

(i) *R is regular local of characteristic* 0 *and dimension* 2;

(ii) *R is not excellent, not even pseudogeometric.*

PROOF: (i) is a consequence of theorem 4, with $C = K[X]_{(X)}$.

As far as (ii) is concerned, let's prove first that tR is a prime ideal (of course it is proper, because t is not invertible in $K[[X, Y]]$). Let's assume that $(a/a')(b/b') = t(c/c')$, where $a, b, c\ a', b', c'$ are in $K[X, Y, t, a_0(X), \dots$ $\dots, a_n(X), \dots]$ and all the fractions are in R. We deduce: $c'ab = tca'b'$. Since t is transcendental over $K[X, Y, a_0(X), \dots, a_n(X), \dots]$, either c' contains the factor t or ab contains the factor t. If ab contains the factor t, we are done, because either a or b contains t, i e. either a or $b \in tR$. Let's now suppose that c' contains the factor t. Since c/c' is in $K[[X, Y]]$, i. e. $c = c'h$, with $h \in K[[X, Y]]$, c must contain the factor t either, for the unique factorization in the regular local ring $K[[X, Y]]$. So we can assume that c and c' have no common t factor, which says that c' is not divisible by t.

So we have just proved that R/tR is a local domain. If R is pseudogeometric, then R/tR is pseudogeometric either ([8], chap. VI, 36.1), hence it is analytically unramified ([8], chap. VI, theorem 36.4).

But it is easy to see that $(R/tR)^{\wedge} = K[[X, Y]]/z^r K[[X, Y]] =$ ring with nilpotent elements.

Since R excellent $\Longrightarrow R$ pseudogeometric ([5], 7.8.3., (vi)), (ii) is proved.

n. 2.

The main result of the present section is a lifting theorem for one-dimensional regular local rings of characteristic $p > 0$.

It is well known that, if K is an arbitrary field of positive characteristic p, then there is a DVR C such that:

(i) C has characteristic 0;

(ii) the maximal ideal of C is generated by the prime number p;

(iii) $C/pC \cong K$.

We'll say that such a ring is a *lifting* of K.

Of course, if C is a lifting of K, also $\widehat{C}$ ($= p$-completion of C) is a lifting of K. Therefore we can always choose a *complete lifting* of K (for an effective construction of such a ring C, see [4], 10.3.1.).

We recall that, if A is a local ring with maximal ideal $\mathfrak{m}$, a *coefficient field* K for A is a field satisfying che following conditions:

(i) $K \subseteq A$;

(ii) K is isomorphic with $A/\mathfrak{m}$ under the canonical map.

Of course a local ring A having a coefficient field K has the same characteristic as its residue field.

Let now A be a local ring with maximal ideal $\mathfrak{m}$ and characteristic 0, while $A/\mathfrak{m}$ has positive characteristic p. We shall say that C is a *coefficient ring* for A if the following conditions are satisfied:

(i) C is a complete DVR with maximal ideal generated by the prime number p and $C \subseteq A$;

(ii) C/pC is isomorphic with $A/\mathfrak{m}$ under the canonical map.

DEFINITION 1: *Let K be a field of positive characteristic p. A K-ring V is a local ring satisfying the following conditions:*

(i) *K is a coefficient field for V;*

(ii) *V is regular of dimension* 1.

In other words, if X is a parameter for V, we have:

$K[X]_{(X)} \subseteq V \subseteq K[[X]]$ and $\widehat{V} = K[[X]]$ ([9], vol. II, chap. VIII, § 12, corollary to theorem 27).

DEFINITION 2.: *Let C be a complete DVR of characteristic 0 with maximal ideal generated by the prime nuuber p. We say that a local ring U is a C-ring if the following conditions are satisfied:*

(i) *C is a coefficient ring for U;*

(ii) *U is regular of dimension 2.*

(iii) *U/pU is a k-ring.*

In other words, there is an indeterminate X over C such that:

$C[X]_{(p,X)} \subseteq U \subseteq C[[X]]$ and $\widehat{U} = C[[X]]$ ([8], chap. V, corollary 31.6 to theorem 31).

DEFINITION 3: *Let K be a field of positive characteristic p and C a complete lifting of K. We say that a C ring U is a C-lifting of a K-ring V if there is an isomorphism of C-algebras: $V \cong U/pU$.*

We are now ready to prove our main theorem:

THEOREM 8: *Let K be a field of positive characteristic p and C a complete lifting of K. Let then V and B two K-rings satisfying the following conditions:*

(i) $V \subseteq B$;

(ii) *V and B have a common parameter X;*

(iii) *the fraction field of B is separably generated over the fraction field of V.*

Then, if V admits a C-lifting U, B admits a C-lifting R such that $U \subseteq R$.

PROOF: Condition (ii) says that V and B have the common completion $K[[X]]$ and the following inclusions are true:

$$K[X]_{(X)} \subseteq V \subseteq B \subseteq K[[X]].$$

We know that there's a natural isomorphism: $U/pU \cong V$. Let Y an element of U whose image modulo p is X. Then we have:

$$U/(p, Y)U \cong (U/pU)/((p, Y)\, U/pU) \cong V/XV \cong K.$$

Therefore p and Y form a system of parameter for U and we obtain the following inclusions:

$$C[Y]_{(p,Y)} \subseteq U \subseteq C[[Y]] = \widehat{U}.$$

Moreover we have the following commutative diagram (where the vertical arrows means reduction modulo p):

$$\begin{array}{ccccccccc}
C & \longrightarrow & C[Y]_{(p,Y)} & \longrightarrow & U & \longrightarrow & & \longrightarrow & C[[Y]] \\
\downarrow & & \downarrow & & \downarrow & & & & \downarrow \\
K & \longrightarrow & K[X]_{(X)} & \longrightarrow & V & \longrightarrow & B & \longrightarrow & K[[X]].
\end{array}$$

Put: $k(V) =$ fraction field of V, $k(B) =$ fraction field of B. Then $k(B)$ is separably generated over $k(V)$, i.e. there is a transcendence basis A of $k(B)$ over $k(V)$ such that $k(B)$ is separable algebraic over $k(V)(A)$.

Therefore it is enough to prove the theorem when $k(B)$ is either purely transcendental or separable algebraic over $k(V)$.

STEP I: $k(B)$ is purely transcendental over $k(V)$ and $A = (\bar{t}_i)_{i \in I}$ is a transcendence basis for $k(B)$ over $k(V)$ such that $k(B) = k(V)(A)$.

Multiplying each element of A by a suitable power of X, we can assume that $A \subseteq B$.

For each $i \in I$, choose $t_i \in C[[Y]]$ such that $t_i = \bar{t}_i$ modulo $pC[[Y]]$.

Then put: $E = (t_i)_{i \in I}$.

It is easy to see that the t_i's are algebraically independent over U. In fact, if $\sum_1^n a_i t_i = 0$ is a relation of algebraic dependence over U, we can clear any common factor p^r and assume that at least one a_i is not in pU. But this mean that, reducing modulo p, we obtain a non trivial relation of the $\bar{t}_i$'s over V.

Let's now put:

$L =$ fraction field of $U[E] = U[\dots, t_i, \dots]$, $S = L \cap C[[Y]]$.

By proposition 3 S is a regular local ring of dimension 2, with completion $C[[Y]]$.

We want to show that $S/pS = B$.

First of all, S/pS is a DVR with completion $K[[X]]$ containing both V and A. Hence it contains also $k(V)(A) \cap K[[X]] = k(B) \cap K[[X]] = B$.

So the only thing we have to prove is that $S/pS \subseteq B$.

Let's remark that, if $(t_1, \dots, t_n)$ is any finite subset of E, then $S_n = C[[Y]] \cap$ (fraction field of $U[t_1, \dots, t_n]$) is a regular local ring with completion $C[[Y]]$ and S is the union of all these regular subrings.

Therefore it is enough to show that $S_n/pS_n \subseteq B$, for every choice of the finite set $(t_1, \dots, t_n)$.

Since $S_n = C[[Y]] \cap$ (fraction field of $S_{n-1}[t_n]$), we can assume, without loss of generality, than $n = 1$, i.e. we consider the ring $S_1 = C[[Y]] \cap$ (fraction field of $U[t]$), where t is arbitrary in E.

But now the result is a consequence of proposition 7, since B contains the smallest DVR containing V and $\bar{t}$.

STEP II: $k(B)$ is separable algebraic over $k(V)$.

Let's introduce the following family $F = ((R_i, \mathfrak{m}_i))_{i \in I}$ of rings:

$(R_i, \mathfrak{m}_i) \in F$ if and only if R_i is a regular local ring with maximal ideal $\mathfrak{m}_i$ such that:

1) $U \subseteq R_i \subseteq C[[Y]]$;

2) $C[[Y]]$ is a completion of R_i;

3) $R_i / pR_i \subseteq B$.

F is not the empty family, since at least $U \in F$. Moreover it is inductive, i.e. the union of any chain in F is an element of F.

In fact, let $G = (\dots \subseteq R_i \subseteq R_j \subseteq \dots)$ be a chain in F.

Passing to the fraction fields, we obtain a chain of fields:

$$H = (\dots \subseteq L_i \subseteq L_j \subseteq \dots).$$

Put: $L = \cup H$. Then proposition 3 says that $L \cap C[[Y]] = R'$ is a regular local ring with completion $C[[Y]]$. But it is easy to see that $R' = \cup G$. In fact, if $R_i \in G$, then $R_i = L_i \cap C[[Y]] \subseteq L \cap C[[Y]]$. Moreover, if $z \in L \cap C[[Y]]$, then $z \in L_i \cap C[[Y]] = R_i$, for i suitable.

Furthermore, it is easy to check that $R' / pR' \subseteq B$.

By Zorn's lemma we can choose a maximal element in F, say $(R, \mathfrak{m})$.

Then B is an algebraic separable extension of R/pR. Let's suppose that $R/pR \neq B$ and select $\bar{t}$ in B but not in R/pR. Without loss of generality we can choose $\bar{t}$ integral over R/pR. In fact, if $\bar{t}$ is algebraic, there is always a suitable element $\bar{c} \in R/pR$ such that $\bar{c}\,\bar{t}$ is integral. Now, if $\bar{t} \in B - (R/pR)$ and $\bar{c} \in R/pR$, $\bar{c}\,\bar{t}$ can't belong to R/pR, since B is faithfully flat over R/pR, both rings being regular with completion $K[[X]]$ (see [2], chap. III, § 3, n. 5, proposition 9, and [1], chap. I, § 3, n. 4, remark 2).

Let $g[T] = T^r + \bar{c}_1 T^{r-1} + \dots + \bar{c}_r$ be the minimal polynomial of $\bar{t}$ over R/pR, i.e. $g(\bar{t}) = 0$ is a relation of integral dependence of degree as low as possible; $g(T)$ is irreducible over R/pR,

We want to show that it is possible to find an element $t \in C[[Y]]$ and and a polynomial $f(T) \in R[T]$ such that:

(i) $f(T)$ is monic and has image $g(T)$ modulo p;

(ii) t has image $\bar{t}$ modulo p;

(iii) $f(t) = 0$.

First of all, let's choose arbitrarily an inverse image x of $\bar{t}$ and inverse images c_i's of the $\bar{c}_i$'s $(i = 1, 2, \dots, r)$.

Let's now consider the following element:

$$a = rx^{r-1} + c_1 (r-1) x^{r-2} + \dots + c_{r-1}.$$

Since $\bar{t}$ is separable algebraic over R/pR, the element

$$\bar{a} = r \bar{t}^{r-1} + \bar{c}_1 \bar{t}^{r-2} + \dots + \bar{c}_{r-1}$$

is surely different from 0.

Therefore we have:

$$\bar{a} = X^s \bar{y},$$

where s is an integer ≥ 0 and $\bar{y}$ is an invertible element of B.

Let's select an inverse image y of y in $C[[Y]]$. We obtain:

$$a - Y^s y = pz = p \left(\sum_0^\infty z_n Y^n \right),$$

where the z_n's are suitable element in C.

Now we replace c_{r-1} by the following element:

$$c'_{r-1} = c_{r-1} - p \left(\sum_0^s z_n Y^n \right),$$

obtaining:

$$a' = a - p \left(\sum_0^s z_n Y^n \right) = Y^s y + pz - p \left(\sum_0^s z_n Y^n \right) =$$

$$= Y^s \left(y + p \left(\sum_{s+1}^\infty z_n Y^{n-s} \right) \right) = Y^s b,$$

where b is an invertible power series.

Therefore we can assume that $c_1, \dots, c_{r-1}$ are chosen in such a way that $a = Y^s b$, where s is a suitable integer ≥ 0 and b is an invertible element of $C[[Y]]$.

Let now $h(T)$ be an arbitrary inverse image modulo p of $g(T)$ (i.e. the coefficients of $h(T)$ are inverse images of the coefficients of $g(T)$). Since $g(\bar{t}) = 0$, we have: $h(x) = -pg_1$, where g_1 is a suitable power series. This is true in particular if $h(T)$ is the polynomial $T^r + c_1 T^{r-1} + \dots + c_{r-1} T + c_r$, where c_{r-1} is selected in the preceding way.

Now we try to solve the following equation (in the variable T):

$$T^r + c_1 T^{r-1} + \dots + c_{r-1} T + c_r = pb_1 + p^2 b_2 + \dots + p^n b_n + \dots,$$

where the b_i's are unknown elements of $C[[Y]]$ to be selected in a suitable way, submitted to the following condition: for every i, b_i is a polynomial in $C[Y]$, whose degree is not larger than s.

If the preceding property is satisfied, $\sum_1^\infty p^n b_n$ is of course an element of $C[[Y]]$, since $C[[Y]]$ is p-adically complete, and also an element of $C[Y]$, because of the restriction on degrees. This says that $\sum_1^\infty p^n b_n$ belongs to R. Hence, if we are able to satisfy the condition on degrees of the b_i's, our equation will have all coefficients in R.

In order to solve the equation, we look for a root of the following kind:

$$t = x + pa_1 + p^2 a_2 + \dots + p^n a_n + \dots,$$

where the a_i's must be determined, under the unique condition that $a_i \in C[[Y]]$, for each i.

Of course $\sum_1^\infty p^n a_n$ belongs to $C[[Y]]$, because $C[[Y]]$ is p-complete.

Moreover any element of $C[[Y]]$ can be written in the preceding way, if we allow the a_n's to be arbitrary power series.

Substitution of t for T in our equation gives the following equality in $C[[Y]]$:

$$paa_1 + p^2 (e_1(a_1, x) + aa_2) + \dots + p^n (e_{n-1}(a_1, \dots, a_{n-1}, x) + aa_n) + \dots =$$

$$= p(g_1 + b_1) + p^2 b_2 + \dots + p^n b_n + \dots,$$

where the e_i's are polynomials in the elements $a_1, \dots, a_i, x$ with coefficients in R.

Let's put:

$$g_1 = \sum_0^\infty g_{1,n} Y^n,$$

and choose:

$$b_1 = -\sum_0^s g_{1,n} Y^n ,$$

$$a_1 = (g_1 + b_1)/a = (g_1 + b_1)/(Y^s b) = (1/b)\left(\sum_{s+1}^{\infty} g_{1,n} Y^{n-s}\right).$$

Let's now suppose we have determined the a_i's and the b_i's, for every $i < n$. Then put:

$$e_{n-1}(a_1, \dots, a_{n-1}, x) = -\sum_0^{\infty} e_{n-1,j} Y^j ,$$

and choose:

$$b_n = -\sum_0^s e_{n-1,j} Y^j ,$$

$$a_n = (1/b)\left(\sum_{s+1}^{\infty} e_{n-1,j} Y^{j-s}\right).$$

The inductive construction allows us to obtain a root $t = x + pd$ of the polynomial $f(T) = T^r + c_1 T^{r-1} + \dots + c_r$, where c_{r-1} is chosen as we said above and c_r is obtained incorporating in the old c_r the term $\sum_1^{\infty} p^n b_n$.

Let's now consider the following ring:

$W =$ smallest regular local ring with completion $C[[Y]]$, containing both R and t.

Such a ring exists by theorem 5 and contradicts maximality of R by proposition 6. In fact W/pW is the smallest DVR with completion $K[[X]]$ coutaining both R/pR and $\bar{t}$; hence $W/pW \subseteq B$.

Therefore we conclude that $R/pR = B$.

BEMARK 1: In our proof we use strongly completeness of C. But the proof can be carried over with an arbitrary DVR C in the special case that $k(B)$ is purely transcendental over $k(V)$.

REMARK 2: The proof of theorem 8 contains also the following useful result on lifting of roots for separable polynomials:

Let K be a field of positive characteristic p and C a complete lifting of K. Let then V be a K-ring and U a C-lifting of V. If $\bar{t}$ is an element of $\widehat{V}$ root of the monic separable irreducible polynomial $g(T) \in V[T]$, then there are an element $t \in \widehat{U}$ and a polynomial $f(T) \in U[T]$ such that:

(i) *$f(T)$ is monic and has image $g(T)$ modulo p :*

(ii) *t has image $\bar{t}$ modulo p ;*

(iii) $f(t) = 0$.

Moreover, from the proof of theorem 7, it follows that all the coefficients of $f(T)$ can be chosen arbitrarily, except c_{r-1} and c_r, which are submitted to conditions.

REMARK 3 : If we take $V = K[X]_{(X)}$, then theorem 8 gives rise to the following special cases :

(i) $B =$ any DVR which is algebraic over $K[X]_{(X)}$, i.e. $B =$ any DVR between $K[X]_{(X)}$ and its henselization ${}^hK[X]_{(X)}$ (= algebraic closure of $K[X]_{(X)}$ in its completion $K[[X]]$: see [8], chap. VII, theorem 44.1).

In fact it is well known that $K((X))$ is a separable extension of $K(X)$, because $K[X]_{(X)}$ is a pseudogeometric local domain ([6], theorem 7.6.4). Therefore the algebraic closure of $K(X)$ in $K((X))$ is separable algebraic over $K(X)$, as a subextension of a separable extension ([9], vol. I, chap. II, § 15); and the same is true for each field M such that $K(X) \subseteq M$ and M is algebraic over $K(X)$.

(i) More generally the following situation is included in our result: choose any finite set $(a_1, \dots, a_n)$ of formal power series in $K[[X]]$ and put: $L = K(X, a_1, \dots, a_n)$, M any separable algebraic extension of L contained in $K((X))$ (for instance L itself).

Then the ring $B = M \cap K[[X]]$ is a DVR with completion $K[[X]]$ (see n. 1, lemma 2). Moreover the fraction field of B is separably generated over $K(X)$, since it is separable algebraic over a finitely generated extension of $K(X)$, which is separably generated because it is separable ([9], vol. I, chap. II, § 15).

Therefore theorem 8 says such a B can be lifted to characteristic 0.

It must be observed that ${}^hK[X]_{(X)}$ has a well known lifting, independently on theorem 8, i.e. the henselization of $C[Y]_{(p, Y)}$.

We dont't say anything new if, in theorem 8, we take $V =$ henselization of $K[X]_{(X)}$. In fact any separably generated extension of the algebraic closure of $K(X)$ in $K((X))$ is also separably generated over $K(X)$ itself.

REMARK 4 : Theorem 8 contains a generalization of the main result in [11], i.e. the existence of regular local rings of characteristic 0 and unequal characteristic, with arbitrary residue field, which are not excellent, not even pseudogeometric. In fact it is enough to consider any non excellent DVR with fraction field separably generated over $K(X)$: its lifting is our counterexample.

Such a ring can be obtained as $K[[X]] \cap L$, where L is a field satisfying the following conditions:

(i) $K(X) \subseteq L \subseteq K((X))$;

(ii) L is separably generated over $K(X)$;

(iii) $K((X))$ is not separable over L.

As far as condition (iii) is concerned, it is enough to observe that a one-dimensional regular local ring, is excellent if and only if the fraction field of the completion is separable over the fraction field of the ring itself ([6], 7.3.19., (iv)).

REMARK 5: In [10], giving a lifting to characteristic 0 for a basic example of non excellent DVR in characteristic $p > 0$, we showed also that there are liftable DVR's which are not finitely generated over polynomials, not even of finite transcendence degree (except, of course, $K[[X]]$ itself). To obtain a slightly larger class of liftable DVR's, we give now a generalization of the main result contained in [10]:

First we give a lemma on lifting of fields:

LEMMA 9: *Let E be a DVR of characteristic 0 and maximal ideal generated by the prime number $p > 0$. Put: $k = E/pE$. If K is an algebraic extension of k, then there is a DVR C with maximal ideal generated by p such that:*

(i) *C contains E and is an integral extension of E;*

(ii) *C/pC and K are k-isomorphic.*

PROOF: see [4], 10.3.1.4.: it is easy to see that the ring C constructed there as direct limit of a suitable family of extensions $(A_\lambda)_{\lambda \in \Lambda}$ of E is really integral over E, since every A_λ can be chosen integral over E.

PROPOSITION 10: *Let k be a field of characteristic $p > 0$, K an algebraic extension of k such that $[K:k] = +\infty$ and X an indeterminate.*

Let V be the following ring: $f = \sum_0^\infty a_n X^n \in K[[X]]$ is in V if and only if $[k(a_0, \dots, a_n, \dots) : k] < +\infty$.

Then there is a lifting C of K such that V is C-liftable to characteristic 0.

PROOF: Choose liftings E and C of k and K respectively, such that C is integral over E (lemma 9).

Let's now define the following subring S of $C[[X]]$: $f = \sum_0^\infty c_n X^n$ belongs to S if and only if $E[c_0, \dots, c_n, \dots]$ is finitely generated as an E-module.

Now put: $R = L \cap C[[X]]$, where $L =$ fraction field of S.

Since any element of C is integral over E, $C \subseteq R$. Therefore R is a regular local ring with completion $\widehat{C}[[X]]$ (n. 1, proposition 3).

We want to show that $R/pR = V$.

First we need to prove that, if $g = p\left(\sum_0^\infty c_n X^n\right)$ is in S, then also $g/p \in S$.

Since the pc_n's give a finite E-module, they contain a finite set of generators for the E-module $E[pc_0, \dots, pc_n, \dots]$:

$$1, pc_0, \dots, (pc_0)^{r_0}, \dots, pc_t, \dots, (pc_t)^{r_t}.$$

Hence we have, for each n:

$$pc_n = \text{polynomial in the } pc_i\text{'s } (0 \leq i \leq t).$$

This implies:

$$c_n = \text{polynomial in the } c_i\text{'s } (0 \leq i \leq t).$$

Therefore we obtain: $E[c_0, \dots, c_n, \dots] = E[c_0, \dots, c_t] =$ finite E-module, since C is integral over E.

By an inductive argument it can be seen that if $g = p^r g'$ is in S, then also g' is in S.

Now consider an element a/b in R, with a and b in S. The image of a/b modulo p is the quotient of the images, after we clear any possible common factor p^r both from a and from b. But, if $a = p^r a'$ and $b = p^r b'$, we know that a' and b' are in S. Hence the image of a/b is the same as the image of a'/b' which is in $K[[X]] \cap$ (fraction field of V) $= V$.

So we proved that $R/pR \subseteq V$.

Let now $f = \sum_0^\infty c_n X^n$ be in V, so that $k(c_0, \dots, c_n, \dots) =$ finite extension of $k = k(c_0, \dots, c_r)$, for a suitable r.

Therefore we have: $c_n = h_n(c_0, \dots, c_r)$, for every $n > r$, where h_n is a polynomial with coefficients in k, for every n.

Let $e_0, \dots, e_r$ be arbitrary inverse images of $c_0, \dots, c_r$ in C. Then $E[e_0, \dots, e_r]$ is a finite E-module which reduces to $k(c_0, \dots, c_r)$ modulo p.

Therefore there are elements $e_{r+1}, \dots, e_n, \dots \in E[e_0, \dots, e_r]$ whose images are $c_{r+1}, \dots, c_n, \dots$.

Hence $\sum_0^\infty e_n X^n$ is an inverse image of $f = \sum_0^\infty c_n X^n$.

REMARK 6: Proposition 10 contains, as a special case, the main result of [10]: it is enough to choose $k = K^p$, taking care of the condition that $[K : K^p] = +\infty$. In this situation it is easy to see that $K[[X]]$ is algebraic purely inseparable over V.

But proposition 10 contains also quite different situations: for instance, if we choose $k = F_p$ (integers modulo p), $K =$ algebraic closure of F_p, then it is easy to check that every formal power series $f \in K[[X]]$ which is purely inseparable over V is in V. In fact, let $f = \sum_0^\infty c_n X^n$ be such that $f^q \in V$, with $q = p^r$. Then $F_p(c_0^q, \dots, c_n^q, \dots)$ is finite over F_p; so there are elements $c_0, \dots, c_t$ such that: $c_n^q = f_n(c_0^q, \dots, c_t^q)/g_n(c_0^q, \dots, c_t^q)$, where the f_n's and the g_n's are polynomials with coefficients in F_p. Since $F_p = F_p^q$, there are polynomials f_n' and g_n' such that:

$$c_n = f_n'(c_0, \dots, c_t)/g_n'(c_0, \dots, c_t).$$

We conclude that $F_p(c_0, \dots, c_n, \dots) = F_p(c_0, \dots, c_t) =$ finite F_p-module.

Theorem 8 says that not only the preceding rings V are liftable, but also every B such that $k(B)$ is purely transcendental over $k(V)$. As far as separable algebraic extensions are concerned, theorem 8 can be applied only when the lifting C of K is a complete DVR (see remark 1).

REMARK 7: We should observe that, given a field K of positive characteristic p, there is a complete lifting of K, say C, which is faithfully flat as an algebra over the integers localized at p, Z_{pZ} (this fact follows from [4], proposition 10.3.1.).

Hence a C-liftable K-ring B admits really a C lifting R which is a faithfully flat Z_{pZ}-algebra. In fact $C[[X]]$ is faithfully flat over Z_{pZ} ([2], chap. III, § 3, corollary 3 to theorem 3); hence R is faithfully flat over Z_{pZ} ([1], chap. I, § 3, n. 4, remark 2^0).

The preceding fact allows us to relate our lifting with a problem of lifting for formally smooth algebras.

Grothendieck ([6], theorem 19.7.2.) proves the following result: let A be a noetherian local ring, I an ideal of A, $A_0 = A/I$, B_0 a noetherian complete local ring, $A_0 \to B_0$ a local homomorphism giving B_0 a structure of formally smooth A_0-algebra. Then there is a noetherian local ring B, which is complete and a flat A-algebra, such that $B \otimes_A A_0 = B_0$ (isomorphism of A_0-algebras).

If we suppose A_0 complete for its natural topology as a local ring, and if we want to eliminate the condition of completeness on B_0, we can see ([6], 19.7.3.) that the question is reducible to the following one: if B_0 is a regular local ring containing F_p (but not necessarily complete), is $B_0 \cong R_n/pR_n$, for each n, being R_n a flat $(Z/p^n Z)$-algebra?.

Theorem 8 gives a partial answer, in a special case, to the question of lifting modulo p^n. In fact, if B has a C-lifting R, then $R_n = R/p^n R = R \otimes_{Z_{pZ}} (Z/p^n Z)$ is a $(Z/p^n Z)$-flat algebra ([1], chap. I, § 3, n. 3, corollary to proposition 5). Moreover we have: $R_n/pR_n = R/pR = B$.

REMARK 8: In [7], proposition 18.1.1., Grothendieck gives the following lifting theorem for smooth schemes:

Let S be a prescheme, S_0 a closed subprescheme, X_0 a smooth S_0-prescheme, x_0 a point of X_0. Then there is an open neighbourhood of x_0, say $U_0 \subseteq X_0$, a smooth S-prescheme U and an S_0-isomorphism $U \times_S S_0 = U_0$.

Theorem 8 gives a slight generalization (formally smooth instead of smooth), but in a special case (a class of particularly simple preschemes) to the preceding result.

In fact, let's translate theorem 8 into the language of geometry:

Let K be a field of positive characteristic p and C a lifting of K, complete for its p-topology. Let then B be a K-ring (def. 1) and put: $S = Spec(C)$, $S_0 = Spec(K)$, $X_0 = Spec(B)$. Now S_0 is a closed subscheme of S and X_0 is formally smooth over S_0 ([5], theorem 19.6.4.). Then there is a formally smooth S scheme $U = Spec(R)$, such that X_0 is isomorphic with $U \times_S S_0$. Moreover R is a regular local ring.

The unique non trivial fact we have to prove is that the ring R we defined in theorem 8 is formally smooth as a C-algebra. But this depends on [5], theorem 19.7.1.

REFERENCES

[1] BOURBAKI, N., *Algèbre Commutative,* chap. I-II, Hermann, Paris, 1961.

[2] BOURBAKI, N., *Algèbre Commutative,* chap. III IV, Hermann, Paris, 1965.

[3] BOURBAKI, N., *Algèbre Commutative,* chap. V-VI, Hermann, Paris, 1964.

[4] GROTHENDIECK, A., *E. G. A.*, chap. II, Publ. I. H. E. S., Paris, 1964.

[5] GROTHENDIECK, A., *E. G. A.*, chap. IV, 1ere partie, Publ. I.H.E.S., Paris, 1964.

[6] GROTHENDIECK, A., *E. G. A.*, chap. IV, 2me partie, Publ. I.H.E.S., Paris, 1965.

[7] GROTHENDIECK, A., *E. G. A.*, chap. IV, 4me partie, Publ. I.H.E.S., Paris, 1967.

[8] NAGATA, M., *Local Rings,* Interscience, New York, 1962.

[9] SAMUEL-ZARISKI, *Commutative Algebra,* Van Nostrand, New York, 1960.

[10] VALABREGA, P., *Regular local rings and excellent rings,* Journal of Algebra, 26, 1973.

[11] VALABREGA, P., *Regular local rings and excellent rings II,* Journal of Algebra, 26, 1973.