RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

PAOLO VALABREGA

On a lifting problem for principal Dedekind domains

Rendiconti del Seminario Matematico della Università di Padova, tome 51 (1974), p. 197-219

<http://www.numdam.org/item?id=RSMUP_1974__51__197_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 51 (1974)

On a Lifting Problem for Principal Dedekind Domains.

PAOLO VALABREGA (*)

SUMMARY - We prove that a principal Dedekind domain D of characteristic $p > 0$ containing a coefficient field and satisfying a slight condition on the fraction field is liftable to characteristic 0, i.e. there exists a two-dimensional regular domain R of characteristic 0 such that $R/pR = D$.

SUNTO - Dimostriamo che un dominio di Dedekind principale D con caratteristica $p > 0$, munito di corpo dei coefficienti e soddisfacente a una ulteriore condizione sul corpo delle frazioni è sollevab le a caratteristica 0, cioè esiste un dominio regolare R di dimensione 2 e caratteristica 0 tale che $R/pR = D$.

Introduction.

In our paper [9] we proved a lifting result for discrete valuation rings of characteristic $p > 0$ containing a coefficient field.

In the present paper we delocalize the preceding result, giving a lifting theorem for principal Dedekind domains containing a « coefficient field », i.e. a field K isomorphic with every residue ring modulo a non zero prime ideal. Precisely we show that such a domain in characteristic $p > 0$ is isomorphic with R/pR, (where R is a two-dimensional regular domain of characteristic 0), provided that a slight assumption on the fraction field of our Dedekind domain is fulfilled.

(*) Author's address: Istituto matematico dell'Università, via Carlo Alberto 10, Torino.

The present paper was written while the author was supported by the CNR as a member of the GNSAGA.

We remark that, when D is an algebra of finite type over a ground field K, i.e. D is the affine ring of a smooth curve, then lifting results are well known (see for instance [7], Proposition 18.1.1). But in the results given here we don't need any finiteness conditions of D over the ground field and they are valid both when D is finite and when D is not finite over K.

The paper contains also a few general results on Dedekind domains and regular domains in dimension 2, as well as examples of liftable rings both finitely and not finitely generated as algebras over the coefficient field.

1. All the rings are supposed to be commutative, with 1, but not necessary noetherian.

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

(i) *D is Dedekind*;

(ii) *K is contained in D*;

(iii) *for every maximal ideal $\mathfrak{P}$ of D, the canonical map: $K \to D/\mathfrak{P}$ is an isomorphism*;

(iv) *unique factorization holds in D, i.e. every maximal ideal is principal.*

EXAMPLE 1. Let K be an algebraically closed field of characteristic $p > 0$ and let D be the affine ring of a regular curve over K: $D = K[X_1, \ldots, X_n]/\mathfrak{I}$, where $\mathfrak{I}$ is a prime ideal. For every prime $\mathfrak{P}$ of D, $D/\mathfrak{P}$ is finite over K, hence the map $K \to D/\mathfrak{P}$ is an isomophism.

To satisfy property (iv) we can consider the affine line $K[X]$ or the parabola $K[X, Y]/(Y - f(X))$ or the hyperbola $K[X, Y]/(XY - 1)$ or the circle $K[X, Y]/(X^2 + Y^2 - 1)$.

DEFINITION 2. *Let K be a field of positive characteristic p. A lifting of K to characteristic 0 is a discrete complete valuation ring C with maximal ideal generated by the prime number p such that C/pC is isomorphic with K.*

REMARK. Given an arbitrary field of positive characteristic p, a lifting C always exists, as a consequence of [4], chap. 0, proposition 10.3.1.

DEFINITION 3. *Let C be a complete discrete valuation ring of characteristic 0 and maximal ideal generated by the prime number p. A C-domain S is a domain satisfying the following conditions*:

(i) *S is regular*;

(ii) *C is contained in S*;

(iii) *pS is a prime ideal contained in the radical of S*;

(iv) *S/pS is a (C/pC)-domain.*

DEFINITION 4. *Let K be a field of characteristic $p > 0$, C a lifting of K, D a K-domain. A C-lifting of D is a C-domain S such that S/pS and D are isomorphic as K-algebras.*

Whenever R is a C-domain or a K-domain, completion of R will always mean completion with respect to the topology of all maximal ideals, unless explicitly stated otherwise.

Now we give a few lemmas on K-domains and C-domains.

LEMMA 1. *Let D be a K-domain and $(\mathfrak{P}_i)_{i\in I}$ the set of all maximal ideals of D. Then there is an isomorphism of topological rings*:

$$\hat{D} = \prod_i (D_{\mathfrak{P}_i})\hat{} = \prod_i K[\![X_i]\!] ,$$

where X_i is a generator of $\mathfrak{P}_i$ in D.

PROOF. The first equality follows from [2], chap. III, § 2, n. 13, proposition 17, since the $\mathfrak{P}_i$'s are comaximal in D. Furthermore every $D_{\mathfrak{P}_i}$ is a discrete valuation ring with parameter X_i ([10], vol. I, chap. V, § 7, theorem 15) and coefficient field K. Therefore $D_{\mathfrak{P}_i}$ has completion isomorphic with $K[\![X_i]\!]$, as a corollary of Cohen's structure theorem ([8], chap. V, theorem 31.12).

REMARK. The canonical map: $D \to \hat{D} = \prod_i K[\![X_i]\!]$ is the diagonal, i.e. $a \to (a, a, \ldots, a, \ldots)$ ([2], chap. III, § 2, n. 13, proposition 17).

Observe that every X_i is an element of $K[\![X_j]\!]$, for every j. Moreover, if $i \neq j$, X_i and X_j are coprime, so that X_i is invertible in $D_{(X_j)}$, hence also in $K[\![X_j]\!]$. Therefore X_i generates in $\hat{D}$ an ideal whose general element $(x_j)_{j\in}$ has the following form: x_j is arbitrary for $j \neq 1$, $x_i \in X_i K[\![X_i]\!]$. In particular we see that $X_i\hat{D}$ is *always a prime ideal.*

LEMMA 2. *Let A be a noetherian domain and $M = (\mathfrak{m}_i)_{i\in I}$ the set of all maximal ideals of A. Then $A = \hat{A} \cap L$, where $\hat{A}$ is the completion of A with respect to the topology of all maximal ideals and L is the fraction field of A.*

PROOF. Following [2], chap. III, § 2, n. 13, proposition 17, we identify as usual $\hat{A}$ with the direct product $\prod_i (A_{\mathfrak{m}_i})\hat{}$.

We recall also that the canonical map $A \to \hat{A}$ is the diagonal: $x \to (x, x, \ldots, x, \ldots)$.

Now let $y = (y_i)_{i\in I}$ belong to $\hat{A} \cap L$, so that $y_i = a/b$, where a and b belong to A, for each i. Therefore y_i belongs to $(A_{\mathfrak{m}_i})\hat{} \cap L = A_{\mathfrak{m}_i}$, for every i. This implies that $(y_i)_{i\in I}$ is a constant sequence whose unique term belongs to $\bigcap_i A_{\mathfrak{m}_i} = A$, since the localizations are taken running all over the set of maximal ideals of A.

PROPOSITION 3. *Let D be a K-domain and L a subfield of the fraction field od D, satisfying the following conditions*:

(i) *K is contained in L;*

(ii) *for every maximal ideal $\mathfrak{P}_i$ of D, L contains a parameter X_i of $D_{\mathfrak{P}_i}$, such that $X_i \in D$.*

Then $B = D \cap L$ is a K-domain with completion $\hat{D}$.

PROOF. First of all, every ideal X_iB is maximal in B, since we have:

$$X_iB = X_iD \cap B \quad \text{and} \quad K \subseteq B/X_iB \subseteq D/X_iD = K\,.$$

Let now $\mathfrak{P}$ be a prime ideal in B. We want to show that $\mathfrak{P}$ is either or X_iB, for some i.

So let x belong to $\mathfrak{P}$; x cannot be invertible in D, because it is invertible in L but not in B. Hence x belongs to some maximal ideal in D, say X_jD; this implies that $x \in X_jD \cap B = X_jB$. Therefore the whole ideal $\mathfrak{P}$ is contained in the set $E = \bigcup_i X_iB$.

Let's now assume that $X_j \notin \mathfrak{P}$, for every j. Choose x in $\mathfrak{P}$ arbitrarily.

Then $x = X_{i_1}x_1$, for a suitable index i_1 and a suitable element x_1 in B.

But $x_1 \in P$, so that: $x = X_{i_1}X_{i_2}x_2$, for suitable i_2 and x_2. Finally we see that $x = X_{i_1}X_{i_2}\ldots X_{i_n}x_n$, for every n, where $i_1, \ldots, i_n, \ldots$ is a sequence of indexes and x_n is a suitable element in B.

Therefore x belongs to the set $\bigcap_n (X_{i_1} \dots X_{i_n})D$, which is the 0 idea since every non zero element in a noetherian ring belongs only to finitely many primes of heigt 1.

Therefore, if we assume that no X_j belongs to $\mathfrak{P}$, our prime ideal must be (0).

If $\mathfrak{P} \neq (0)$, then there is an i such that $X_i B \subseteq \mathfrak{P}$, so that $\mathfrak{P} = X_i B$.

Therefore B is a principal Dedekind domain and for every prime $P = X_i B$ we have: $K \cong B/\mathfrak{P}$. Hence B is a K-domain.

As to completion of B, it is enough to observe that $\hat{B}$ is isomorphic, as a topological ring, with $\prod_i K[\![X_i]\!]$, hence with $\hat{D}$.

PROPOSITION 4. *Let S be a C-domain. Then the following properties are true*:

(i) *unique factorization holds in S;*

(ii) *for every maximal ideal m of S, there is an element $Y \in S$ that m is generated by p and Y;*

(iii) *there is a canonical isomorphism of topological rings*:

$$\hat{S} = \prod_i (S_{(p,Y_i)})\hat{} = \prod_i C[\![Y_i]\!] ,$$

where $((p, Y_i)S)_{i \in I}$ is the set of all maximal ideals of S.

PROOF. Put: $S/pS = D = K$-domain and let $(\mathfrak{P}_i)_{i \in I} = (X_i D)_{i \in I}$ be the set of all maximal ideals of D. Then choose an element in S, say Y_i, such that $Y_i = X_i$ modulo pS. Then $(p, Y_i)S$ is maximal, thanks to the following equality:

$$S/(p, Y_i)S = (S/pS)/(p, Y_i)(S/pS) = D/X_i D = K .$$

Let now $\mathfrak{P}$ be a prime ideal of S and assume that $p \in \mathfrak{P}$. Then P modulo pS is an ideal of the form $X_i D$, for some i, unless it is (0). In this last case we have simply: $P = pS$. Otherwise, $\mathfrak{P}$ is generated by p and Y_i, since $\mathfrak{P}$ contains every inverse image of elements in $X_i D$

Let's now consider a prime ideal $\mathfrak{P}$ such that $p \notin \mathfrak{P}$. Then $\mathfrak{P}$ modulo pS is generated by a suitable element $\bar{a}$, where a belongs to $\mathfrak{P}$.

Therefore we obtain the following inclusions:

$$aS \subseteq \mathfrak{P} \subseteq (a, p)S .$$

Let x be in $\mathfrak{P}$; then $x = ab_1 + pc_1$, so that c_i is in $\mathfrak{P}$, since $x - ab_1$ is and p is not. Hence we have:

$$x = ab_1 + p(ab_2 + pc_2) = ad_2 + p^2 e_2\,, \qquad \text{for } d_2 \text{ and } e_2 \text{ suitable in } S.$$

Finally: $x = ad_n + p^n e_n$, for every n.
So the following inclusions are true:

$$aS \subseteq P \subseteq \bigcap_n (a, p^n) S = aS\,,$$

the equality depending on the fact that S is a Zariski ring with respect to p-topology.

In conclusion: if $p \in \mathfrak{P}$ then either $\mathfrak{P} = pS$ or $\mathfrak{P} = (p, Y_i) S$ and is maximal; if $p \notin \mathfrak{P}$, then P is principal.

Therefore statement (ii) is proved and (i) follows from the fact that unique factorization holds if and only if every prime of height 1 is principal ([8], chap. I, theorem 13.1).

As to (iii), the first equality depends on [2], chap. III, § 2, n. 13, proposition 17. For the second part of (iii), let's consider the local ring $S_{(p,Y_i)}$: it is regular, has unequal characteristic and is unramified, since p belongs to a regular system of parameters ([8], chap. IV, n. 28). Hence its completion is isomorphic with $C[\![Y_i]\!]$ ([8], chap. V, Theorem 31.12).

PROPOSITION 5. *Let S be a C-domain and L a subfield of the total quotient ring of $\hat{S}$, satisfying the following conditions*:

(i) *S is contained in L;*

(ii) *there is a K-domain D such that*:

$$S/pS \subseteq R/pR \subseteq D \subseteq (S/pS)\hat{} = \hat{D}\,,$$

where $R = \hat{S} \cap L$.

Then R is a C-domain with completion $\hat{S}$.

PROOF. First of all, p belongs to $\mathrm{Rad}(R)$; in fact, let $x = (x_i)_{i \in I}$ be in R (assuming as usual that $\hat{S} = \prod_i C[\![Y_i]\!]$) and consider the element $1 - px = (1 - px_i)_{i \in I}$, which is invertible both in $\hat{S}$ and in L, since every component is invertible. This says that $1 - px$ is invertible in R, i.e. $p \in \mathrm{Rad}(R)$.

Let's now consider a prime ideal $\mathfrak{P}$ of R such that $p \in \mathfrak{P}$. If $\mathfrak{P} = (p, Y_i)R$ for some i (where Y_i generates with p a maximal ideal of S), then $\mathfrak{P}$ is maximal in R.

In fact; let x be an element of $(p, Y_i)\hat{S} \cap R$, so that we can write:

$$x = \left(\ldots, \sum a_{j,n} Y_j^n, \ldots\right) = (x_j)_{j \in I} .$$

All the constant terms $a_{j,0}$ are elements of pC; so, in particular, we have: $a_{i,0} = pc_{i,0}$.

This implies: $x - pc_{i,0} = Y_i(x_j/Y_i)$, since Y_i is invertible in the j-th component of $\hat{S}$, whenever $j \neq i$.

Therefore x belongs to $(p, Y_i)R$.

Furthermore we have:

$$K = S/(p, Y_i)S \subseteq R/(p, Y_i)R \subseteq \hat{S}/(p, Y_i)\hat{S} = K .$$

Now we want to show that every maximal ideal is an ideal $(p, Y_i)R$, for a suitable i.

Let $\mathfrak{P}$ be a maximal ideal of R and x an element of $\mathfrak{P}$. Put: $x = (x_i)_{i \in I}$; then at least an x_j must be not invertible, i.e. x_j belongs to $(p, Y_j)C[\![Y_j]\!]$. So x belongs to $(p, Y_j)\hat{S}$. Hence we have just proved that $\mathfrak{P}$ is contained in the set $E = \bigcup_i (p, Y_i)\hat{S}$. If some Y_i belongs to $\mathfrak{P}$, we are done, because, in this case, $\mathfrak{P} = (p, Y_i)R$. Hence we suppose that no Y_i belongs to $\mathfrak{P}$.

For every x in $\mathfrak{P}$, we have: $x = pa_1 + Y_{j_1} b_1$, where j_1 is a suitable index.

Since $p \in \mathfrak{P}$, also $b_1 \in \mathfrak{P}$ and x can be written in the following way: $x = pa_n + Y_{j_1} Y_{j_2} \ldots Y_{j_n} b_n$, for every n, where a_n and b_n are suitable elements and possibly the indexes $j_1, j_2, \ldots, j_n$ are repeated.

Let's now put: $X_1 = Y_i$ modulo $p\hat{S}$. Then the X_i's generate maximal ideals in S/pS and, since $S/pS \subseteq D \subseteq \hat{D} = (S/pS)\hat{}$, it is easy to see that the X_i's generate also maximal ideals in D. So we see that x modulo $p\hat{S}$ belongs to all the ideals $(X_{j_1} X_{j_2} \ldots X_{j_n})D$, whose intersection is (0).

Therefore $x = pa$, for a suitable element a in $\hat{S}$. This says that $\mathfrak{P} = pR$, contradicting maximality of $\mathfrak{P}$.

So we proved that there must be an index j such that $\mathfrak{P} = (p, Y_j)R$.

If $\mathfrak{P}$ contains p but is not maximal, then we have just shown that $\mathfrak{P} = pR$.

Let now $\mathfrak{P}$ be a prime ideal such that $p \notin \mathfrak{P}$. We want to show that it is principal. If we can prove that $\mathfrak{P}$ modulo p is principal, we are done, because we can choose an a in $\mathfrak{P}$ which generates $\mathfrak{P}$ modulo p and see that $aR \subseteq \mathfrak{P} \subseteq (a, p)R$. Moreover we observe that

$$aR \subseteq \mathfrak{P} \subseteq (a, p^n)R \Rightarrow aR \subseteq \mathfrak{P} \subseteq \bigcap_i^{\infty} (a, p^n)R \subseteq a\hat{S} \cap R = aR.$$

Therefore it is enough to show that R/pR is a K-domain.

Let $\mathfrak{Q}$ be a prime ideal in R/pR and let $\mathfrak{P}$ be its inverse image in R. So p belongs to $\mathfrak{P}$ and $\mathfrak{P}$ is either pR or $(p, Y_i)R$, for some i. This says that $\mathfrak{Q}$ is either (0) or principal generated by X_i (where $X_i = Y_i$ modulo p). Hence R/pR is noetherian with every prime ideal generated by one element, i.e. R/pR is a K-domain.

Now we give a criterion to identify and construct subfields L of the total quotient ring of $\hat{A}$, where A is either a K-domain or a C-domain. In particular we deal with the case $L =$ fraction field of $A[x]$, where x is an element of A; in other words we want to investigate which x's are good to avoid 0-divisors in $A[x]$.

Since there is no special simplification in dealing with K- or C-domains our result concerns an integral domain A, in which unique factorization holds.

First we need the following

LEMMA 6. *Let A be a unique factorization domain with fraction field K, B an overdomain of A and x an element of B algebraic over A.*

Then the ideal of polynomials in $A[T]$ which vanish at x is principal and generated by a polynomial $f(T)$ such that:

(i) *the coefficients of $f(T)$ have no common factor in A (i.e. $f(T)$ is primitive in $A[T]$);*

(ii) *$f(T)$ has degree as small as possible among polynomials which vanish at x.*

PROOF. The element x is algebraic over K and has a minimal polynomial $g(T)$. Now $g(T)$ can be written as $f(T)/a$, where $a \in A$ and $f(T)$ is primitive. So both $g(T)$ and $f(T)$ are irreducible over K, which implies that $f(T)$ is also irreducible over A ([10], vol. I, chap. II, § 13 lemma 1). Moreover, if $h(T) \in A[T]$ vanishes at x, then $h(T) = f(T)z(T)$ in $K[T]$; this implies that $z(T)$ belongs to $A[T]$, by [10], vol. I, chap. II, § 13 lemma 1.

PROPOSITION 7. *Let A be a domain, $M = (\mathfrak{m}_i)_{i\in I}$ the set of all maximal ideals of A and $\hat{A}$ the completion of A with respect to the topology of the maximal ideals, so that: $\hat{A} = \prod_i (A_{\mathfrak{m}_i})\hat{}$.*

Assume moreover that $A_{\mathfrak{m}_i}$ is analytically irreducible, for every i, i.e. $(A_{\mathfrak{m}_i})\hat{}$ is a domain.

Given an element $x = (x_i)_{i\in I}$ in $\hat{A}$, a necessary and sufficient condition in order that $A[x]$ be a domain with fraction field contained in the total quotient ring of $\hat{A}$, is that x satisfy either of the following conditions:

(i) *every x_i is transcendental over A;*

(ii) *all the x_i's are algebraic over A, with a common minimal polynomial $f(T)$ (in the sense of lemma 6).*

PROOF. I) The condition is sufficient. We recall that an element $y = (y_i)_{i\in I}$ in A is a 0-divisor if and only if there is an index j such that $y_j = 0$ and an index k such that $y_k \neq 0$.

If condition (i) is satisfied, then an element $g(x) \in A[x]$ cannot be a 0-divisor, since this means that $g(x_i) = 0$, for some i; but $g(x_i) = 0$ implies that $g(T) = 0$.

Let's now assume that condition (ii) is satisfied and that an element $g(x) = (g(x_i))_{i\in I}$ has some zero component, say $g(x_j) = 0$.

So lemma 6 says that $f(T)$ is a factor of $g(T)$, hence $g(T)$ vanishes at every x_i, i.e. $g(x)$ is 0.

II) The condition is necessary. Let's assume that $A[x]$ is a domain with fraction field contained in the total quotient ring of $\hat{A}$.

Moreover, we suppose that there is an element x_j which is algebraic over A. Then x_j has a minimal polynomial $f(T)$ over A, by lemma 6. Hence we have: $f(x) = (f(x_i))_{i\in I} =$ *an* element in $\hat{A}$ with a 0 at the j-th place. But $A[x]$ is a domain, so no 0-divisor is allowed; this implies that $f(x)$ has 0 components everywhere: $f(x) = (f(x_i))_{i\in I} = (0_i)_{i\in}$.

Therefore $f(T)$ is a multiple of the minimal polynomial $f_i(T)$ of x_i, for every $i \neq j$. But, conversely, we see that each x_i, with $i \neq j$ is algebraic over A and its minimal polynomial $f_i(T)$ is a factor of $f(T)$. So $f(T) = f_i(T)$, for every $i \neq j$, and the x_i's have a common minimal polynomial.

REMARK. The problem is the characterization of domains A such that $A_{\mathfrak{m}}$ is analytically irreducible, for every maximal ideal $\mathfrak{m}$. If

A is a regular domain, in particular a Dedekind domain, the condition is satisfied, since $A_{\mathfrak{m}}$ is a regular local ring, whose completion is even regular. A wider class of rings satistying the condition contains any normal excellent domain, since an excellent normal local domain is analytically normal ([6], theorem 7.8.3.1, (v)).

PROPOSITION 8. *Let S be a C-domain and $x = (x_i)_{i \in I}$ an element of $\hat{S}$ satisfying the following conditions*:

(i) *$(S/pS)[\bar{x}]$ is contained in a K-domain D whose completion is $(S/pS)\hat{}$ ($\bar{x} = x$ modulo p)*;

(ii) *either* a) *every $\bar{x}_i = \bar{x}_i$ modulo p is transcendental over S/pS or* b) *all the x_i's are algebraic over S with a common minimal polynomial, which is irreducible modulo p.*

Then:

1) *$S[x]$ is a domain*;

2) *$R = \hat{S} \cap k(S[x])$, where $k(S[x]) =$ fraction field of $S[x]$ is a C-domain*;

3) *R/pR is the smallest K-domain containing both S/pS and $\bar{x}$, with completion $(S/pS)\hat{}$.*

PROOF. 1) is a consequence of proposition 7, when we remark that condition (ii), *a*) says that also the x_i's are transcendental over S, since an algebraic relation can be reduced modulo p.

2) Depends on proposition 5. In fact, is enough to show that R/pR is contained in the K-domain D, since other conditions in proposition 5 are trivial. Take $f(x)/g(x)$ in R and reduce modulo p, looking at $f(x)$ and $g(x)$ as elements in S. If $g(x)$ does not belong to $p\hat{S}$, the image of our fraction, by condition (i), is contained in the fraction field of D and also in $(S/pS)\hat{} = \hat{S}/p\hat{S}$, so it is in D, by lemma 2. If $g(x) \in p\hat{S}$, then also $f(x) \in p\hat{S}$, since the quotient is in $\hat{S}$.

This says that both $f(x)$ and $g(x)$ have image $= 0$ modulo p. If $\bar{x}$ is transcendental over S/pS, then these images are identically 0, so the coefficients of f and g have the common factor p, which can be cleared. When the x_i's and the $\bar{x}_i$'s are algebraic, x itself is algebraic, with the same minimal polynomial, say $h(T)$, which is irreducible modulo p, hence in particular irreducible over S.

By multiplication of both f and g by a common factor in S, we can assume that f and g are divisible by $h(T)$, with a rest of degree less than $h(T)$. So the equalities $f(x) = 0$, $g(x) = 0$ modulo p are now identical and the preceding argument is valid.

Finally, when $g(x) \in p^r \hat{S}$ we apply induction on r.

So proposition 5 can be applied.

3) First we inquire the problem of finding the smallest K-domain satisfying our conditions. It is easy to see that it is simply $B = (S/pS)\hat{} \cap \cap k((S/pS)[\bar{x}])$. In fact proposition 7 says that $(S/pS)[\bar{x}]$ is a domain; so the conclusion follows from lemma 2, provided that we prove that B is really a K-domain. We need proposition 3, whose unique non trivial condition to verify is that, for every maximal ideal $\mathfrak{P}_i$ of D, $k((S/pS)[\bar{x}])$ contains a parameter X_i of $D_{\mathfrak{P}_i}$, such that X_i belongs to D.

It is enough to show that S/pS contains such X_i's. So let's assume that S/pS has parameters $(Z_j)_{j \in I}$ and completion, written in the usual way: $(S/pS)\hat{} = \prod_j K[\![Z_j]\!]$. The parameter X_i in D generates a prime ideal also in $\hat{D} = (S/pS)\hat{}$, i.e. $X_i \prod_j K[\![Z_j]\!])$ is a prime ideal contained in the set $\bigcup Z_j (S/pS)\hat{}$. So $X_i (S/pS)\hat{} = Z{:}(S/pS)\hat{}$, for a suitable index w. Hence X_i and Z_w differ by an invertible element of $\hat{D}$, say z. But z belongs to D, since both X_i and Z_w are in D. Hence Z_w is a generator in D of the ideal $X_i D$, which is the property we had to prove.

Therefore $B = (S/pS)\hat{} \cap k((S/pS)[\bar{x}])$ is the smallest K-domain we are looking for.

But in the proof of 2) we checked that R/pR is a K-domain contained in $(S/pS)\hat{} \cap k((S/pS)[\bar{x}])$. So $R/pR\hat{} \cap k((S/pS)[\bar{x}])$ and 3) is proved.

PROPOSITION 9. *Let S be a C-domain and R its completion with respect to the p-topology. Then R is also a C-domain.*

PROOF. Since $\hat{S}$ is p-complete, we can look for the completion of S for the p-topology inside the ring $\hat{S}$, i.e. R is simply the p-closure of S in $\hat{S}$.

Now S is a Zariski ring for the p-topology, hence also R is.

Moreover we have: $R/pR = S/pS =$ domain. Therefore $\mathrm{Spec}(R)$ is connected, as $\mathrm{Spec}(R/pR)$ is ([3], § 10, corollary 10.7). This says that R is a regular domain, since it is the completion of the regular domain S ([3], § 10, corollary 10.11).

Since $C \subseteq R$, $p \in \mathrm{Rad}(R)$ and $R/pR = S/pS = K$-domain, we conclude that R is a C-domain.

2. In the present section we prove our main theorem, for which we need the following

LEMMA 10. *Let U be a C-domain with maximal ideals (p, Y_i)'s, z any element in $\hat{U}$ and $r_1, \ldots, r_s$ a finite set of positive integers.*

The there is a element z' in U such that:

$$z' - z \in (Y_{i_1}^{r_1} \ldots Y_{i_s}^{r_s})\hat{U} ,$$

where the Y_{i_1}'s are chosen arbitrarily among the Y_i's.

PROOF. Put: $z = (z_i)_{i \in I}$ (as usual we identify $\hat{U}$ with the ring $C[\![Y_i]\!]$).

We want to show that we can find a (unique) element z' in U such that the following congruences are simultaneously satisfied:

$$z' - z_{i_m} = Y_{i_1}^{r_1} \ldots Y_{i_s}^{i_s} q_{i_m} , \quad \text{for } m = 1, 2, \ldots, s \text{ and } q_{i_m}$$

suitable in $C[\![Y_i]\!]$.

First of all let us remark that Y_j is invertible in $C[\![Y_i]\!]$, whenever $j \neq i$; therefore it is enough to look for a z' such that:

$$z' - z_{i_m} = (Y_{i_m}^{r_m}) q_{i_m} , \quad \text{for every } m = 1, 2, \ldots, s .$$

To solve our simultaneous congruences, we can also subsitute z_{i_m} by a suitable polynomial of degree r_m, i.e. by an element:

$$z'_{i_m} = \sum_0^s z_{i_m, n} Y_{i_m}^n \quad \left(\text{if } z_{i_m} = \sum_0^\infty z_{i_m, n} Y_{i_m}^n\right), \quad \text{which belongs to } U.$$

Therefore we are done if the canonical map:

$$U \to \prod (U/(Y_i^{r_i}))$$

is onto whenever i runs through a finite set of indexes.

Finally it is enough to show that Y_i and Y_j are comaximal whenever $i \neq j$. But they are comaximal modulo pU and $p \in \mathrm{Rad}(U)$. Hence, they are really comaximal and the result follows from [1], chap. II, § 1, n. 2, proposition 5.

Since Y_i is invertible in $C[\![Y_j]\!]$ when $i \neq j$, we have also:

$$z' - z = Y_{i_1}^{r_1} \ldots Y_{i_s}^{r_s} u , \quad \text{where } u \in \hat{U} .$$

We are now ready for our main theorem:

THEOREM 11. *Let K be a field of positive characteristic p, C a lifting of K, V a K-domain and U a C-lifting of V. Let now B be a K-domain satisfying the following conditions*:

(i) $V \subseteq B$;

(ii) $\hat{V}$ *is a completion of* B;

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

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

PROOF. First of all we want to explain condition (ii). Let $(\mathfrak{P}_i)_{i \in I}$ be the set of maximalideals of V, where $\mathfrak{P}_i = X_i V$, for every i.

Then $\hat{V}$ is isomorphic with the ring $\prod_i K[\![X_i]\!]$ (lemma 1). We want to show that condition (ii) says that the ideals $X_i B$'s are the unique maximal ideals of B. Of course they are maximal, since $X_i \hat{V} = X_i \hat{B}$ is maximal in $\hat{B}$ and $X_i B = X_i \hat{B} \cap B$. Let now $\mathfrak{P}$ be a maximal ideal of B, say $\mathfrak{P} = bB$. Then the principal ideal $b\hat{B}$ is obviously maximal in $\hat{B}$, and it is contained in the set $\bigcup_i X_i B$. If $b \in X_j \hat{B}$, we see that $b\hat{B} = X_j \hat{B}$, so that b and X_j differ by an invertible element in $\hat{B}$.

Now both b and X_j belong to B, hence such an invertible element belongs to $\hat{B} \cap$ (fraction field of B) $= B$ (lemma 2).

Therefore P is generated by X_j and the parameters of V are enough to generate the maximal ideals of B.

Once for all the X_i's are the parameters for V and B; moreover the maximal ideals of U are generted by p and by elements Y_i's which are equal to the X_i's modulo p (see proposition 4). Hence, once for all we'll identify $\hat{U}$ with $\prod_i C[\![Y_i]\!]$ (see proposition 4).

So we get the following diagram (where vertical arrows mean reduction modulo p):

$$\begin{array}{ccccccc} C & \to & U & \longrightarrow & \hat{U} = \prod_i C[\![Y_i]\!] \\ \downarrow & & \downarrow & & \downarrow \\ K & \to & V & \to B \to & \hat{V} = \hat{B} = \prod_i K[\![X_i]\!] \,. \end{array}$$

We'll look for our lifting inside $\hat{U}$.

Put: $k(B)$ = fraction field of B, $k(V)$ = fraction field of V. 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 $T = (t_w)_{w \in W}$ is a transcendence basis such that $k(B) = k(V)(T)$. Without loss of generality, we can assume that $T \subseteq B$. In fact every t_i is a fraction a_i/b_i, with both a_i and b_i in B; so that the a_i's and the b_i's together form a system of generators for $k(B)$ over $k(V)$, belonging to B.

Then from this system we can choose a basis and we are done.

Let now $T' = (z_w)_{w \in W}$ be a set of elements of $U = \prod_i C[\![Y_i]\!]$ such that $z_w = t_w$ modulo $p\hat{U}$, for every w. It is easy to see that the z_w's are algebraically independent over U. Moreover the following fact is true: if $t_w = (t_{w,i})_{i \in I}$, then every $t_{w,i}$ is transcendental over V because t_w belongs to the integral domain B and $f(t_{w,i}) = 0$ implies $\big(f(t_{w,i})\big)_{i \in I} = (0$ (see also proposition 7).

Therefore every elements z_w has all components transcendental over U. Hence proposition 7 says that $U(T')$ is an integral domain with fraction field L contained in the total quotient ring of $\hat{U}$ (really proposition 7 deals with the adjonction of one element x, but the step to an arbitrary set T' is easy, for instance by transfinite induction).

Let's now introduce the new ring $R = L \cap \hat{U}$. By proposition 8, R is a C-domain and $R/pR \subseteq B$. Hence $k(R/pR)$ = fraction field of R/pR is contained in $k(B)$. On the other hand, let $f(t_1, \ldots, t_n)/g(t_1, \ldots, t_n)$ be a fraction in $k(B)$. Then we can lift the coefficient of both f and g to elements of U and $t_1, \ldots, t_n$ to $z_1, \ldots, z_n$ (elements of T'). So $f(t_1, \ldots, t_n)$ and $g(t_1, \ldots, t_n)$ can be lifted to elements in R, which says that $f(t_1, \ldots, t_n)/g(t_1, \ldots, t_n)$ belongs to the fraction field of R/pR. Therefore we get: $k(B) \subseteq k(R/pR)$; hence $k(R/pR) = k(B)$.

The last equality implies also: $R/pR = B$, by lemma 2.

So we are done in the present case.

STEP II). $k(B)$ is separable algebraic over $k(V)$. Consider the following family $F = (R_h)_{h \in H}$ of rings:

(i) every R_h is a C-domain;

(ii) $U \subseteq R_h \subseteq \hat{U}$, for every $h \in H$;

(iii) $\hat{U}$ is a completion of R_h, for every $h \in H$;

(iv) $R_h/pR_h \subseteq B$, for every $h \in H$.

Let $G = (\ldots \subseteq R_h \subseteq R_k \subseteq R_f \subseteq \ldots)$ be a chain in F. We want to show that G admits a least upper bound in F, precisely the ring $R' = \cup G = \ldots \cup R_h \cup R_k \cup R_f \ldots$.

Put: $L_h =$ fraction field of R_h, for every $h \in H$. Then we have: $R' = \left(\bigcup_{h \in H} L_h\right) \cap \hat{U}$. Since $\bigcup_{h \in H} L_h = L'$ is a subfield of the total quotient ring of $\hat{U}$, we see that R' is a C-domain with completion $\hat{U}$, by proposition 5. Hence conditions (i)-(iv) are satisfied.

Therefore F is inductive and admits a maximal element R.

First of all, the C-domain R must be complete for the p-topology. In fact the p-completion of R is a C-domain, by proposition 9, and conditions (i)-(iv) are obviously satisfied. Hence maximality of R says that $R = (R, pR)\hat{}$.

Let's now assume that $R/pR \neq B$. Then there is an element $\bar{t}$ in B which doesn't belong to R/pR. Such an element is automatically separable agebraic over R/pR; and multiplication by a suitable element of R/pR makes it integral.

Let

$$f(T) = T^r + \bar{c}_1 T^{r-1} + \bar{c}_2 T^{r-2} + \ldots + \bar{c}_{r-1} T + \bar{c}_r ,$$

be its minimal polynomial over R/pR.

Then choose arbitrary inverse images, say $c_1, \ldots c_r$ of the $\bar{c}_i$'s in R and put:

$$g_1(T) = T^r + c_1 T^{r-1} + c_2 T^{r-2} + \ldots + c_{r-1} T + c_r .$$

We want to show that the coefficient c_i's can be chosen in such a way that $g_1(T)$ has a root t in $\hat{U}$ whose image modulo p is exactly $\bar{t}$.

Let x be an arbitrary inverse image of $\bar{t}$ in $\hat{U}$, so that we have: $g_1(x) = pw$, for a suitable w in $\hat{U}$.

Let's now consider the following element:

$$a = g_1'(x) = rx^{r-1} + c_1(r-1)x^{r-2} + \ldots + c_{r-1} .$$

Since $\bar{a} = f'(\bar{t})$ is different from 0 in the Dedekind domain B, we have:

$$\bar{a} = X_{i_1}^{r_1} \ldots X_{i_s}^{r_s} \bar{y} ,$$

where $\bar{y}$ is a suitable invertible element in B.

Choose $y =$ some inverse image of $\bar{y}$ in $\hat{U}$, obtaining:

$$a - X_{i_1}^{r_1} \dots X_{i_s}^{r_s} y = pz = p(z_i)_{i \in I} = p\Big(\dots, \sum_0^\infty z_{i,n} X_i^n, \dots\Big) .$$

By lemma 10 there is an element $z' \in R$ such that:

$$z' = z = X_{i_1}^{r_1} \dots X_{i_s}^{r_s} u ,$$

where u is a suitable element of $\hat{U} = \hat{R}$.

Let's now substitute in $g_1(T)$ the coefficient c_{r-1} by

$$c'_{r-1} = c_{r-1} - pz' ,$$

obtaining:

$$a' = a - pz' = X_{i_1}^{r_1} \dots X_{i_s}^{r_s} y + pz - pz' = X_{i_1}^{r_1} \dots X_{i_s}^{r_s} v ,$$

where v is a suitable element invertible in $\hat{R}$.

Therefore we can assume that the coefficient c_{r-1} of $g_1(T)$ is selected in such a way that

$$a = X_{i_1}^{r_1} \dots X_{i_s}^{r_s} y, \quad \text{for } y \text{ suitable invertible element of } \hat{R}.$$

Of course the new coefficient c_{r-1} is still an inverse image in R of $\bar{c}_{r-1}$.

Now we look for a root $t = x + pa_1 + p^2 a_2 + \dots + p^n a_n + \dots$ in $\hat{R}$ of the equation:

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

where the b_n's are supposed to be unknown elements of R, to be selected in a suitable way.

Of course p-completeness of R allows us to conclude that t will be a solution of an equation with coefficients in R, since $pb_1 + \dots + p^n b_n + \dots$ belongs to $(R, pR)\hat{} = R$.

Substitution of t for T in the equation gives the following equality:

$$paa_1 + p^2(e_1(a_1, x) + aa_2) + \dots + p^n(e_{n-1}(a_1, \dots, a_{n-1}, x) + aa_n) + \dots = \\ = p(b_1 - w) + p^2 b_2 + \dots + p^n b_n + \dots ,$$

where $pw = g_1(x)$.

Put: $w = (w_i)_{i \in I}$ and choose $b_1 = an$ element in R such that $b_1 - w = X_{i_1}^{r_1} \dots X_{i_s}^{r_s} w'$, where $w' \in \hat{R}$.

Then put: $a_1 = (b_1 - w)/a$, which belongs to $\hat{R}$, since $b_1 - w$ is divisible by $X_{i_1}^{r_1} \dots X_{i_s}^{r_s}$.

Let's assume that we have determined the elements $a_1, b_1, \dots, a_n, b_n$.

Then we select b_{n+1} such that:

$$b_{n+1} - e_n(a_1, \dots, a_n, x) = X_{i_1}^{r_1} \dots X_{i_s}^{r_s} e_n' ,$$

where e_n' is a suitable element in $\hat{R}$.

Now we put:

$$a_{n+1} = (b_{n+1} - e_n(a_1, \dots, a_n, x))/a ,$$

which is an element of $\hat{R}$.

Therefore $t = x + \sum_1^\infty p^n a_n$ is a root in $\hat{R}$ of the polynomial $g(T) = g_1(T) - \sum_1^\infty p^n b_n \in R[T]$.

Since $f(T)$ is irreducible, it is easy to see that also $g(T)$ is irreducible over R. Moreover we have:

$$0 = g(t) = (g(t_i))_{i \in I} \Rightarrow g(t_i) = 0 , \quad \text{for every } i \in I .$$

Hence $g(T)$ contains as a factor the minimal polynomial $h(T)$ of t_i, for every i. But $g(T)$ is irreducible; so $g(T)$ is the common minimal polynomial of the t_i's. Therefore proposition 7 says that $R[t]$ is an integral domain with fraction field contained in the total quotient ring of $\hat{R}$.

Now put: $L =$ fraction field of $R[t]$, $R' = L \cap \hat{R}$. Then the C-domain R' contradicts maximality of R.

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

REMARK 1. The first example of a liftable K-domain is the affine ring of a smooth factorial plane curve over an algebraically closed field K.

In fact, consider the K-domain $V = K[X, Y]/(\bar{f}(X, Y))$ (for conditions of $\bar{f}$ to get unique factorization in V, see example 1). Take then $f(X, Y) \in C[X, Y]$ such that $f = \bar{f}$ modulo $pC[X, Y]$.

We claim that the ring $U = \left(C[X, Y]/(f(X, Y))\right)_{1+(p)}$ is the required lifting.

In fact we have the following properties:

(i) p generates a prime ideal in $C[X, Y]/(f(X, Y))$, since $(p)+(f)$ is prime in $C[X, Y]$ as inverse image of the prime ideal in $K[X, Y]$ generated the irreducible polynomial $\bar{f}(X, Y)$;

(ii) p belongs to $\mathrm{Rad}(U)$ by construction;

(iii) every ideal of U containing properly pU is generated by p and another element; in particular every maximal ideal, which contains p by (ii), has two generators; hence the noetherian domain U is regular at every maximal ideal, i.e. it is regular.

We conclude that U is a C-domain which lifts V.

REMARK 2. Starting with V as in remark 1, we want to apply our main theorem; hence we need separably generated extensions L of $k(V)$.

We want to show that, if we consider any finite set $(t_1, \ldots, t_r)$ of elements in $\hat{V}$, such that $V[t_1, \ldots, t_r]$ is a domain with fraction field contained in the total quotient ring of $\hat{V}$, then L is separable (hence separably generated) over $k(V)$.

In fact consider the i-th component of the t_j's: $t_{1i}, \ldots, t_{ri}$.

They are elements of $K[\![X_i]\!]$, which is the completion for the X_i-adic topology of the excellent ring $V_{(X_i)}$ ([6], 7.8.3., (ii) and (iii)).

Therefore $K[\![X_i]\!]$ is separable over $V_{(X_i)}$ and $t_{1i}, \ldots, t_{si}$ generate a separable, hence separably generated extension ([10], vol. I, chap. II, § 13, theorem 30).

Let $(t_{1i}, \ldots, t_{si})$ be a separating transcendence basis, whence $t_{s+1i}, \ldots, t_{ri}$ are separable algebraic over the field $k(V)(t_{1i}, \ldots, t_{si})$.

Since $V[t_1, \ldots, t_r]$ is a integral domain, all the components $t_{1j}, \ldots, t_{sj}$ are algebraically independent over V. Moreover we can assume, without loss of generality, that $t_{s+1i}, \ldots, t_{ri}$ are integral over $k(V)(t_{1i}, \ldots, t_{si}) \cap \cap \hat{V}$. Hence t_{hi} $(h = s+1, \ldots, r)$ has separable minimal polynomial f_{hi}. But also t_{hj}, for every j, must have the same minimal polynomial (proposition 7), so that the separable polynomial $f_h = f_{hi}$ $(i \in I)$ is the minimal polynomial of t_h over $k(V)(t_1, \ldots, t_s)$.

Therefore t_h is separable algebraic, for $h = s+1, \ldots, r$, and $k(V)(t_1, \ldots, t_r)$ is separably generated.

REMARK 3. If V is a liftable K-domain and t is an element of $\hat{V}$ which gives rise to an integral domain $B = k(V)(t) \cap \hat{V}$, then B is not automatically a K-domain, since there are troubles for noetherian property.

In fact, also in the simple case when $V = K(X) =$ affine line over an algebraically closed field K, we cannot adjoint $t \in \hat{V}$ arbitrarily.

As usual we identify $\hat{V}$ with the ring $\prod_i K[\![X - a_i]\!]$, where a_i runs over K (every maximal ideal of $K[X]$ has the form $(X - a_i)K[X]$).

Now take $t = (t_i)_{i \in I}$, where $t_i = (X - a_i) f_i \in (X - a_i) K[\![X - a_i]\!]$.

Then the ring $k(V)(t) \cap \hat{V}$ cannot be noetherian, since all the ideals $(X - a_i)(k(V)(t) \cap \hat{V})$ are principal primes, as it can be easily verified, and t belongs to all of then, while in a noetherian domain a non zero element belongs to a finite number of principal primes, since there height is 1.

Therefore we want to look for conditions sufficient to obtain that the ring $k(V)(t) \cap \hat{V}$ be a K-domain with completion $\hat{V}$, whenever V is a K-domain.

(i) First of all we have the following general result:

PROPOSITION 12. *Let V be a semilocal K-domain and L a field such that: $k(V) \subseteq L \subseteq$ (total quotient ring of $\hat{V}$).*

Then $B = L \cap \hat{V}$ is a semilocal K-domain with completion $\hat{V}$.

PROOF. Let $(\mathfrak{P}_i)_{i \in I} = (X_i V)_i$'- the set of all maximal ideals of V, so that we have the usual identification $\hat{V} = \prod_i K[\![X_i]\!]$.

Since $X_i B = X_i \hat{V} \cap B$, all the X_i's generate prime ideals in B.

Morevover we have: $K = V/(X_i V) \subseteq B/(X_i B) \subseteq V/(X_i V) = K$, so that the X_i's really generate maximal ideals of B.

Furthermore, it is easy to see that every prime ideal $\mathfrak{P}$ of B is contained in the set $\bigcup_i X_i B$; since I is finite, we obtain that $\mathfrak{P} = X_j B$, for some j.

Therefore B is noetherian, since every prime ideal is finitely generated. Moreover every maximal ideal ideal is principal; hence B is a Dedekind domain and obviously a K-domain with completion $\hat{V}$.

Proposition 12 says that, if V is the K-domain of remark 1, for instance, then every ring B separably generated over V_S is liftable, whenever S is the complement in V of a finite set of maximal ideals: in fact V_S is a semilocal Dedekind domain, hence every ideal in V_S is principal ([10], vol. I, chap. V, § 7, theorem 16), hence it is factorial.

(ii) Now we want to give examples of liftable rings with infinitely many primes, different from the affine ring of a smooth factorial curve.

First we need the following

PROPOSITION 13. *Let V be a K-domain and L a field such that: $k(V) \subseteq L \subseteq$ (total quotient ring of $\hat{V}$).*

Then $B = L \cap \hat{V}$ is a K-domain with completion $\hat{V}$ if the following condition is satisfied: for every $x \in B$, there are only finitely primes P belons to $P\hat{V}$, unless $x = 0$.

PROOF. The proof runs exactly as in proposition 3. Every prime ideal $\mathfrak{P}'$ of B is contained in the set $\bigcup_i X_i B$ (where the X_i's generate the maximal ideals of V). If $x \in \mathfrak{P}'$, then $x = X_{i_1} \dots X_{i_n} x_n$, for every n, i.e. $x = 0$; unless some X_i belongs to P', which means that $\mathfrak{P}' = X_i B$.

We are then ready for the first example:

EXAMPLE 2. Take $V = K[X] =$ affine ring of the line over an algebraically closed field K. Then consider the following polynomial in $V[T]$:

$$f(T) = T^2 - c(X) ,$$

where $c(X)$ is a polynomial in V without any square root in $V = K[X]$.

Put: $K = (a_i)_{i \in I}$, so that the maximal ideals of V are the ideals $(X - a_i)V$, for every $i \in I$.

Reducing $f(T)$ modulo $(X - a_i)V$, we obtain:

$$f_i(T) = T^2 - c(a_i) .$$

The polynomial $f_i(T)$, for every $i \in I$, has two roots in K, since K is algebraically closed: let k_i be either of these roots.

Observe that, if the characteristic is $p > 2$ (as we will assume from now on), all the $f_i(T)$'s are separable polynomials over V and K respectively; hence k_i is always a simple root of $f_i(T)$.

For every $i \in I$, $K[X]$ can be considered as a subring of $K[X]_{(X-a_i)}$ whose completion for the $(X - a_i)$–adic topology is the ring $K[\![X - a_i]\!]$.

Now $K[\![X - a_i]\!]$ is a henselian ring, being a complete local ring ([8], chap. V, theorem 30.3); so k_i can be lifted to a simple root of $f(T)$ in $K[\![X - a_i]\!]$, say t_i.

Now put: $t = (t_i)_{i \in I}$, $L =$ fraction field of $V[t]$.

We want to show that $B = L \cap \hat{V}$ is a K-domain with completion $\hat{V}$.

By proposition 12 we have only to prove that every $x \in B$, $x \neq 0$, doesn't belong to infinitely many primes $(X - a_i)B$.

Therefore it is enough to show that, if $g(T)$ is a polynomial in $V[T]$, then $g(t_i)$ belongs to $(X - a_i)Y$ only for finitely many a_i's.

In fact every element of B has the form $g(t)/h(t)$, where $g(T)$ and $h(T)$ belong to $V(T)$. Now $g(t)/h(t)$ belongs to $(X - a_i)$ if and only if $g(t)/h(t)$ has the i-th component in $(X - a_i)$. This means that the i-th component must be in $(X - a_i)$, i.e. $g(t_i)(X - a_i)$.

Let's divide $g(T)$ by $f(T)$:

$$g(T) = f(T)q(T) + r(T) ,$$

where $r(T)$ has degree 0 or 1.

Then we have: $g(t) = r(t)$, so that we can assume:

$$g(T) = a(X)\,T + b(X) .$$

Finally we want to avoid infinitely many equalities of the following kind:

$$a(a_i)\,k_i + b(a_i) = 0 .$$

Hence we would get:

$$\big(a(a_i)\big)^2\big(c(a_i)\big) = \big(b(a_i)\big)^2 , \quad \text{for infinitely many } a_i\text{'s.}$$

Since a polynomial has only finitely many roots, we obtain:

$$\big(a(X)\big)^2 c(X) = \big(b(X)\big)^2 ,$$

which is absurd, since $c(X)$ is not a square in $K[X]$.

EXAMPLE 3. Let K be any algebraically closed field of characteristic 3, X an indeterminate and put: $V = K[X]_S$, where S is the multiplicative system $(1 - X, (1 - X)^2 \ldots)$.

Let's then consider the following polynomial in $V[T]$:

$$Q(X, T) = T^3 + XT - 1/(1 - X) .$$

First of all we remark that $Q(X, T)$ has a root in $K[\![X]\!]$, as a poly-

nomial in $K[\![X]\!][T]$; precisely its unique root is the formal power series $h(X) = \sum_0^\infty c_n X^n$, where the c_n's are defined recursively as follows:

$$c_0 = 1\,, \quad c_1 = 1\,, \quad c_2 = 0\,, \ \ldots$$

$$c_{3n} = c_{3n+1} = 1\,, \quad c_{3n-1} + c_n^3 = 1\,.$$

So $h(X)$ is also the unique root of $(1-X)Q(X, T)$ whose coefficients belong to $K[X]$. Since $h(X)$ is not a polynomial in $K[X]$, $(1-X)Q(X, T)$ has no root in $K(X)$, which says that it is irreducible over $K[X]$, since the degree is 3 and a decomposition gives always a linear factor.

Therefore we deduce that $(1-X)Q(X, T)$ is irreducible over $K(X)$, $K[X]$ being a UFD ([10], vol. I, chap. II, § 13, lemma 1). So $Q(X, T)$ is irreducible over $K(X)$ and also over $K[X]_S = V$, $Q(X, T)$ being primitive over V ([10], loc. cit.).

Now, for every $a_i \in K$, $a_i \neq 1$, the equation $Q(a_i, T) = 0$ has at least a root k_i, K being algebraically closed. Moreover, if $a_i \neq 0$, $Q(a_i, T)$ is separable over $K =$ residue field of $V_{(X-a_i)}$; hence k_i is liftable to a root t_i of $Q(X, T)$ in $K[\![X-a_i]\!]$.

As to $a_i = 0$, we have just proved the existence of the root $h(X)$ in $K[\![X]\!]$.

Consider now the element $t = (t_i)_{i\in I}$, where t_i is the root of Q in $K[\![X-a_i]\!]$ now constructed and is $h(X)$ when $a_i = 0$.

We want to show that $B = k(V[t]) \cap \hat{V}$ is a K-domain using proposition 12.

So let's assume that a polynomial $f(X, T)$ of degree less or equal to 2 satisfies the following equalities:

$$f(a_i, k_i) = 0\,,$$

for infinitely many a_i's.

Let's put: $f(a_i, k_i) = p(a_i)k_i^2 + q(a_i)k_i + r(a_i) = 0$.

By combination of the two equations:

$$k_i^3 + a_i k_i - 1/(1-a_i) = 0 \tag{1}$$

$$p(a_i)k_i^2 + q(a_i)k_i + r(a_i) = 0\,, \tag{2}$$

we can find an equation of the first degree having k_i as a root:

$$k_i = G(a_i)/Z(a_i)\,, \tag{3}$$

with G and Z suitable polynomials.

Therefore, for infinitely many a_i's k_i is a root of the equation:

$$k_i = G(a_i)/Z(a_i)\,.$$

As an easy consequence we deduce that $Q(X, T)$ is divisible by the polynomial $T - G(X)/Z(X)$, so that $Q(X, T)$ is reducible over the fraction field of V, i.e. $Q(X, T)$ is reducible over V ([10], loc. cit.), which is an absurd.

REMARK 4. The C-lifting R of the K-domain B given in theorem 11 is a flat C-algebra. In fact C is a principal ideal domain and R is an integral domain, hence it has no torsion ([1], chap. I, § 2, n. 4, proposition 3, (ii)).

REFERENCES

[1] N. BOURBAKI, *Algèbre Commutative*, chap. I-II, Hermann, Paris, 1961.
[2] N. BOURBAKI, *Algèbre Commutative*, chap. III-IV, Hermann, Paris, 1967.
[3] GRECO - SALMON, *Topics in m-adic topologies*, Springer, Berlin, 1971.
[4] A. GROTHENDIECK, *E.G.A.*, chap. II, I.H.E.S., Paris, 1964.
[5] A. GROTHENDIECK, *E.G.A.*, chap. IV, 1ere partie, I.H.E.S., Paris, 1964.
[6] A. GROTHENDIECK, *E.G.A.*, chap. IV, 2me partie, I.H.E.S., Paris, 1965.
[7] A. GROTHENDIECK, *E.G.A.*, chap. IV, 4me partie, I.H.E.S., Paris, 1967.
[8] M. NAGATA, *Local Rings*, Interscience, New York, 1962.
[9] P. VALABREGA, *On two dimensional regular local rings and a lifting problem*, Annali della Scuola Normale Sup., Pisa 1973.
[10] ZARISKI - SAMUEL, *Commutative Algebra*, Van Nostrand, New York, 1958.

Manoscritto pervenuto in redazione il 12 settembre 1973.