ON UNIQUE FACTORIZATION DOMAINS

BY
PIERRE SAMUEL

A unique factorization domain (or UFD) is an integral domain in which every element $\neq 0$ is, in an essentially unique way (i.e., up to units), a product of irreducible ones. In spite of the simplicity of this notion, many problems concerning it have remained open for many years. For example the fact that every regular local ring is a UFD has been conjectured in the early 40's, many partial results in this direction have been proved, but the general case has been settled only in 1959 by M. Auslander and D. Buchsbaum [1]. Another open question was as to whether a power series ring over a UFD is a UFD; W. Krull studied it in a paper of 1938, and termed the answer "doubtful" ("zweifelhaft") [3]; we prove here that the answer to this question is negative. However, using the result of Auslander-Buchsbaum, we prove that a power series ring in any number of variables over a PID ("principal ideal domain") is a UFD. We also show, by counterexamples, that unique factorization is preserved neither by ground-field extension, nor by ground-field restriction.

I have received great help and stimulation from my friends M. Auslander, I. Kaplansky, and especially D. Buchsbaum. More particularly, Lemma 3.3 is essentially due to D. Buchsbaum, whereas the ideas leading to the proof of Theorem 2.1 came from discussions between him and me; after these discussions we arrived independently at a proof of this result.

1. Some preliminary results

In this paper all rings are assumed to be commutative and *noetherian* Let A be a noetherian domain; it is well known that the following conditions are equivalent:

(UF. 1) A is a UFD.
(UF. 2) Any two elements of A have a g.c.d.
(UF. 3) Any two elements of A have a l.c.m.
(UF. 4) The intersection of any two principal ideals of A is principal.
(UF. 5) Any irreducible element of A generates a prime ideal.
(UF. 6) Any prime ideal of height 1 of A is principal.

Furthermore, if A is a *local or semilocal* ring, these conditions are equivalent to:

(UF. 7) For any two elements a, b of A, we have $\mathrm{dh}(Aa + Ab) \leqq 1$ (where dh denotes the homological dimension of a module).

We say that an element a of a ring A is *prime* if the ideal Aa is prime; any prime element is irreducible; the converse is true in a UFD (by (UF. 5)).

The following lemmas are known, but we state and prove them for the reader's convenience:

Received April 26, 1960.

LEMMA 1.1. *Let A be a UFD, and S a multiplicative system in A; then the quotient ring A_S is a UFD.*

One can use the formula $A_S\, a \cap A_S\, b = A_S(Aa \cap Ab)$ $(a, b \in A)$ and (UF. 4). One can also take a family P of irreducible elements of A such that every irreducible element of A is an associate of one and only one element of P; then, if P' is the set of elements of P which divide some element of S, and if $P'' = P - P'$, then every element of A_S is, in one and only one way, the product of a unit (in A_S) and of elements of P'' (these elements being irreducible in A_S).

LEMMA 1.2 (Mori). *Let A be a noetherian ring, and $\mathfrak{m}$ an ideal contained in the Jacobson radical of A (so that A is a Zariski ring for the $\mathfrak{m}$-adic topology; see* ([10]), VIII, §4). *If the completion $\hat{A}$ is a UFD, so is A.*

We use (UF. 4). Let $a, b \in A$; set $\mathfrak{q} = Aa \cap Ab$. We have $\hat{A}\mathfrak{q} = \hat{A}a \cap \hat{A}b$ ([10], VIII, §4, Corollary 2 to Theorem 11), whence there exists $c' \in \hat{A}$ such that $\hat{A}\mathfrak{q} = \hat{A}c'$. Let c be an element of $\mathfrak{q}$ which is congruent to c' modulo $\hat{A}\mathfrak{m}\mathfrak{q}$; since c generates $\hat{A}\mathfrak{q}$ modulo $\hat{A}\mathfrak{m}\mathfrak{q}$, it generates $\hat{A}\mathfrak{q}$ by Nakayama's lemma (ibid., Theorem 9, (f)). Hence $\mathfrak{q} = \hat{A}\mathfrak{q} \cap A = \hat{A}c \cap A = Ac$ (ibid., Theorem 9, (a')), proving that $\mathfrak{q}$ is principal.

LEMMA 1.3. *Let A be a noetherian ring, $\mathfrak{m}$ an ideal contained in the Jacobson radical of A, and E a finitely generated A-module. For E to be a free A-module, it is necessary and sufficient that $E/\mathfrak{m}E$ be free over $A/\mathfrak{m}$ and that $\mathfrak{m} \otimes_A E \to E$ be a monomorphism* (*i.e.*, $\mathrm{Tor}_1(A/\mathfrak{m}, E) = 0$).

The necessity is clear. Conversely, let (x_i) $(i \in I)$ be a finite family of elements of E such that the $(\mathfrak{m}E)$-residues $\bar{x}_i$ form a basis of $E/\mathfrak{m}E$ over $A/\mathfrak{m}$. Let F be the free A-module A^I, $(e_i)_{i\in I}$ its canonical basis, and u the homomorphism of F into E defined by $u(e_i) = x_i$. By Nakayama's lemma, u is an epimorphism. Let R be its kernel: an element (a_i) of R is a system of elements of A such that $\sum_i a_i x_i = 0$. Since the $\bar{x}_i$ are linearly independent over $A/\mathfrak{m}$, we have $a_i \in \mathfrak{m}$ for every i, whence, by hypothesis, $\sum_i a_i \otimes x_i = 0$ in $\mathfrak{m} \otimes E$. Using the exact sequence

$$\mathfrak{m} \otimes R \to \mathfrak{m} \otimes F \to \mathfrak{m} \otimes E \to 0,$$

we see that $\sum_i a_i \otimes e_i$ is in $\mathrm{Im}(\mathfrak{m} \otimes R \to \mathfrak{m} \otimes F)$, whence

$$(a_i) = \sum_i a_i e_i \in \mathfrak{m}R,$$

and $R = \mathfrak{m}R$. From Nakayama's lemma, we conclude that $R = (0)$, i.e., that u is a monomorphism, and that E is free.

Remark 1.4. It follows from Lemma 1.3 that a finitely generated projective (or flat) module over a noetherian *local* ring is free. Thus, for a finitely generated module E over a noetherian ring A to be projective, it is necessary and sufficient that it be *locally free*, i.e., that $E_{\mathfrak{m}}$ be free over $A_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of A.

The following easy lemmas show that products of prime elements are "harmless" with respect to unique factorization. Notice that, if p is a prime element of a domain A, then A_{Ap} is the ring of a discrete valuation v_p (normed by $v_p(p) = 1$).

LEMMA 1.5. *Let A be a domain, a, b elements of A, x and y products of prime elements of A. For $Aa \cap Ab$ to be principal, it is necessary and sufficient that $Aax \cap Aby$ be principal.*

By induction on the number of prime factors in x and y, we are reduced to comparing $Aa \cap Ab$ and $Aa \cap Apb$ (p prime). Suppose $Aa \cap Ab = Ac$; then one sees easily that $Aa \cap Apb$ is equal to Apc if $v_p(a) \leqq v_p(b)$, and to Ac if $v_p(a) > v_p(b)$. Conversely, if $Aa \cap Apb = Ad$, $Aa \cap Ab$ is equal to Adp^{-1} if $v_p(a) \leqq v_p(b)$, and to Ad if $v_p(a) > v_p(b)$.

COROLLARY 1.6. *Let A be a domain, a an element of A, and y a product of prime elements of A. Then the ideal $Aa \cap Ay$ is principal.*

Take $x = b = 1$ in Lemma 1.5.

LEMMA 1.7 (Nagata; see [5]). *Let A be a domain, and S the multiplicative system generated by any family $(x_i)_{i \in I}$ of prime elements. If A_S is a UFD, so is A.*

Let v_i be the normed valuation having A_{Ax_i} as valuation ring. Writing every element a' of A in the form $a' = a\prod_i x_i^{v_i(a')}$ (almost all exponents are 0 since A is noetherian), Lemma 1.5 shows that it is sufficient to prove that $Aa \cap Ab$ is principal whenever $v_i(a) = v_i(b) = 0$ for all i. We then have $A_S a \cap A = Aa$ and $A_S b \cap A = Ab$ (if $ad/s \in A$ with $s \in S$ and $d \in A$, then $v_i(d) \geqq v_i(s)$ for every i, and s divides d in A). On the other hand $A_S(Aa \cap Ab) = A_S a \cap A_S b$ is a principal ideal $A_S c$; we may assume that $c \in A$ and that $v_i(c) = 0$ for every i. Then

$$Aa \cap Ab = A \cap A_S a \cap A_S b = A \cap A_S c = Ac,$$

proving Lemma 1.7.

Remark 1.8. Lemma 1.7 may be used for proving the classical result that a polynomial ring $R[X]$ over a UFD is a UFD: the prime elements of R remain prime in $R[X]$; we take for S the set of nonzero elements of R; then $R[X]_S$ is $K[X]$ (K: quotient field of R) and is a UFD (since it is a PID); hence $R[X]$ is a UFD. This method does *not* work for power series.

2. Regular unique factorization domains

We say that a ring A is *regular* if, for every maximal ideal $\mathfrak{m}$, $A_{\mathfrak{m}}$ is a regular local ring.

THEOREM 2.1. *If A is a regular UFD, then $A[X]$ and $A[[X]]$ are regular UFD's.*

We first prove that $B = A[X]$ is regular. Let $\mathfrak{M}$ be a maximal ideal in B; set $\mathfrak{m} = A \cap \mathfrak{M}$. Then $B_{\mathfrak{M}}$ contains $B' = A_{\mathfrak{m}}[X]$, and is equal to $B'_{(\mathfrak{M} \cap B')}$. Since a quotient ring of a regular local ring is regular [9],[1] it is sufficient to prove that B' is regular; in other words, we may assume that A is a regular local ring, and that $\mathfrak{m}$ is its maximal ideal. Then $\mathfrak{M}/B\mathfrak{m}$ is a maximal ideal in $B/B\mathfrak{m} = (A/\mathfrak{m})[X]$, and is therefore principal; since $\mathfrak{m}$ is generated by $d = \dim(A)$ elements, $\mathfrak{M}$ is generated by $d + 1$ elements. On the other hand, we have in A a chain $\mathfrak{p}_0 < \mathfrak{p}_1 < \cdots < \mathfrak{p}_d = \mathfrak{m}$ of $d + 1$ prime ideals, whence, in B, the chain $B\mathfrak{p}_0 < B\mathfrak{p}_1 < \cdots < B\mathfrak{m} < \mathfrak{M}$; therefore the height $h(\mathfrak{M})$ is $\geqq d + 1$. It follows that $h(\mathfrak{M}) = \dim(B_{\mathfrak{M}}) = d + 1$, and that $B_{\mathfrak{M}}$ is a regular local ring.

We now prove that $C = A[[X]]$ is regular. Since the elements of $1 + CX$ are invertible, every maximal ideal $\mathfrak{M}$ of C contains X, and may therforee be written as $\mathfrak{M} = CX + C\mathfrak{m}$ where $\mathfrak{m}$ is a maximal ideal of A. Then $C_{\mathfrak{M}}$ is a dense local subring of $A_{\mathfrak{m}}[[X]]$. As above $A_{\mathfrak{m}}[[X]]$ is a regular local ring. Thus $C_{\mathfrak{M}}$ is also a regular local ring.

Let us now prove that $B = A[X]$ and $C = A[[X]]$ are UFD's. For B, it is well known since Gauss. Let a, b be two elements of C; we set $\mathfrak{q} = Ca \cap Cb$. Since $C_{\mathfrak{M}}$ is a UFD for every maximal $\mathfrak{M}$ [1], and since $C_{\mathfrak{M}}\,\mathfrak{q} = C_{\mathfrak{M}}\,a \cap C_{\mathfrak{M}}\,b$, $\mathfrak{q}$ is a "locally free" C-module, i.e., a projective C-module (Remark 1.4). To prove that $\mathfrak{q}$ is principal, we may, since X is prime in C, assume that X does not divide a or b (Lemma 1.5); then $\mathfrak{q}/X\mathfrak{q} = \mathfrak{q}/(CX \cap \mathfrak{q}) = (\mathfrak{q} + CX)/CX$, and $\mathfrak{q}/X\mathfrak{q}$ is a projective ideal in A. Since A is a UFD, $\mathfrak{q}/X\mathfrak{q}$ is principal, i.e., free (over A). Applying Lemma 1.3, we see that $\mathfrak{q}$ is free over C, i.e., principal, Q.E.D.

COROLLARY 2.2. *If A is a PID, then $A[[X_1, \cdots, X_n]]$ is a regular UFD.*

In fact A is obviously a regular UFD, and our assertion follows from Theorem 2.1 by induction on n.

Remark 2.3. If A is a regular UFD, so is every ring obtained from A by a finite number of polynomial and power series adjunctions of indeterminates (in any order.)

3. Power series over a UFD; reduction properties

Let A be a ring (noetherian, as usual) and let $R = A[[X]]$ be the power series ring in one variable over A. Given a series $u \in R$, we shall denote by u_j the coefficient of X^j in u, so that $u = \sum_{j=0}^{\infty} u_j X^j$. Let S be a multiplicative system in A; then R_S is a subring of $A_S[[X]]$ (which we shall denote by R^S), in general distinct from R_S ; in fact R^S is the (X)-adic completion of R_S , and is therefore a *flat* R-module.[2] The ring R_S is not a Zariski ring for

[1] See also M. AUSLANDER AND D. A. BUCHSBAUM, *Homological dimension in local rings*, Trans. Amer. Math. Soc., vol. 85 (1957), pp. 390–405.

[2] See J-P. SERRE, *Géométrie algébrique et géométrie analytique*, Ann. Inst. Fourier, Grenoble, vol. 6 (1955–1956), pp. 1–42.

its (X)-adic topology; but, if we denote by S' the set of all power series the constant term of which is in S, S' is a multiplicative system in R, $R_{S'}$ is a Zariski ring for its (X)-adic topology, and R^S is its (X)-adic completion. The proofs are straightforward, and may be left to the reader.

THEOREM 3.1. *Let A be a UFD such that $A_{\mathfrak{m}}[[X]]$ is a UFD for every maximal ideal $\mathfrak{m}$ of A. Then $A[[X]]$ is a UFD.*

Let u, v be any two elements of $R = A[[X]]$; we shall prove that $\mathfrak{q} = Ru \cap Rv$ is principal. As in Theorem 2.1, the maximal ideals $\mathfrak{M}$ of R are the ideals $\mathfrak{M} = R\mathfrak{m} + RX$, with $\mathfrak{m}$ maximal in A. For such a maximal ideal, we set $S = A - \mathfrak{m}$, and we use the previous notations. Since $R^S = A_{\mathfrak{m}}[[X]]$ is a UFD, and since it is the (X)-adic completion of the Zariski ring $R_{S'} = R_{\mathfrak{M}}$, $R_{\mathfrak{M}}$ is a UFD (Lemma 1.2); thus $\mathfrak{q}R_{\mathfrak{M}}$ is principal, i.e., free over $R_{\mathfrak{M}}$, whence $\mathfrak{q}$ is locally free, i.e., projective, over R. As at the end of the proof of Theorem 2.1, we conclude, using Lemma 1.3, that $\mathfrak{q}$ is principal, Q.E.D.

Theorem 3.1 shows that, in order to prove that a power series ring over a UFD A is a UFD, we may assume that A is local. We are now going to perform a partial reduction to the case in which A has dimension 2. We say that a noetherian ring A is a *Macaulay* ring if, for every maximal ideal $\mathfrak{m}$, $A_{\mathfrak{m}}$ is a local Macaulay ring ([10], Appendix 6). The reduction we have in mind is as follows:

THEOREM 3.2. *Let A be a Macaulay UFD such that $A_{\mathfrak{p}}[[X]]$ is a UFD for every prime ideal $\mathfrak{p}$ of height 2. Then $A[[X]]$ is a UFD.*

By Theorem 3.1, we may assume that A is local. We then proceed by induction on the dimension d of A. Our assertion is true for $d = 0, 1, 2$. Assume that our assertion has been proved for dimensions $0, 1, \cdots, d-1$, and let A be of dimension d. Let S be a multiplicative system in A, containing a nonunit. Then A_S is a UFD (Lemma 1.1). Every prime ideal $\mathfrak{P}$ of A_S is of the form $\mathfrak{P} = \mathfrak{p}A_S$, where $\mathfrak{p}$ is a prime ideal of A disjoint from S, and we have $(A_S)_{\mathfrak{P}} = A_{\mathfrak{p}}$. Since $\mathfrak{p}$ is not the maximal ideal of A, we have $h(\mathfrak{P}) \leqq d - 1$. Since every $A_{\mathfrak{p}}$ is a Macaulay ring ([10], Appendix 6, Theorem 2, Corollary 4), A_S is a Macaulay ring. On the other hand $(A_S)_{\mathfrak{P}}[[X]]$ is a UFD for every prime ideal $\mathfrak{P}$ of height 2. Thus it follows from Theorem 3.1 and from the induction hypotheses *that $A_S[[X]]$ is a UFD*; with the notations introduced in the beginning of the section, $R_{S'}$ is therefore a UFD (Lemma 1.2). From this we are going to deduce that $R = A[[X]]$ is a UFD. We may assume that $\dim(A) \geqq 3$. We shall prove that, for any $u, v \in R$, the ideal $Ru \cap Rv$ is principal; since RX is prime, we may assume (by Lemma 1.5) that the constant terms u_0, v_0 of u, v are $\neq 0$.

For every prime element p of A, we shall denote by n_p the normed valuation having A_{Ap} as valuation ring, and set

$$n(u, v) = \sum_p (n_p(u_0) + n_p(v_0)). \tag{1}$$

We shall prove that $Ru \cap Rv$ is principal by *induction* on the integer $n(u, v)$. The case $n(u, v) = 0$ is settled by the following lemma:

LEMMA 3.3. *Let A be any local UFD, and u, v two elements of $R = A[[X]]$ such that their constant terms u_0, v_0 are relatively prime in A. Then u, v are relatively prime, i.e., $Ru \cap Rv = Rw$.*

Since u and v have no common divisor, it is sufficient to prove that they have a l.c.m., i.e., that $\mathrm{dh}(Ru + Rv) \leqq 1$. We set $u = u_0 + Xu'$ and $v = v_0 + Xv'$. Since $Ru + Rv + RX = Ru_0 + Rv_0 + RX$, and since (u_0, v_0, X) is a prime sequence ([10], Appendix 6), we have

$$\mathrm{dh}(Ru + Rv + RX) = 2$$

([10], Chapter VII, §13, Lemma 6). If we prove that

$$(Ru + Rv) : RX = Ru + Rv,$$

then the same Lemma 6 will prove that $\mathrm{dh}(Ru + Rv) = 1$. Now if $Xw = au + bv$, with $a = a_0 + Xa'$ and $b = b_0 + Xb'$ in R, we have

$$X(w - a'u - b'v) = a_0 u_0 + b_0 v_0 + X(a_0 u' + b_0 v');$$

this implies $a_0 u_0 + b_0 v_0 = 0$, whence (since u_0 and v_0 are relatively prime) there exists c_0 in A such that $a_0 = c_0 v_0$ and $b_0 = -c_0 u_0$. We thus have

$$\begin{aligned} X(w - a'u - b'v) &= Xc_0(v_0 u' - u_0 v') \\ &= Xc_0((v - Xv')u' - (u - Xu')v') = Xc_0(vu' - uv'). \end{aligned}$$

Dividing by X we see that w belongs to $Ru + Rv$, and this proves Lemma 3.3.

We now come back to Theorem 3.2. For proving that $Ru \cap Rv$ is principal by induction on $n(u, v)$, we may assume that u and v have no common factor, and also (by Lemma 1.5) that neither u nor v has a nontrivial constant factor. Let s be a prime element of A, distinct from the prime divisors of u_0 and v_0; let S be the multiplicative system generated by s, and S' the set of all power series having their constant term in S. Since $R_{S'}$ is a UFD, u and v have a l.c.m. w^S in $R_{S'}$; we may assume that w^S is in R, and that it is not a multiple (in R) of any element of S'. We write $w^S = uw^S = vu^S$; then u^S and v^S are in R by the following lemma:

LEMMA 3.4. *Let A be a UFD, S a multiplicative system in A, and z an element of $R = A[[X]]$ such that z_0 is prime to every element of S. Then we have $zR^S \cap R = zR$.*

Suppose we have $(z_0 + z_1 X + \cdots)(b_0 s_0^{-1} + b_1 s_1^{-1} X + \cdots) \in R$, with $b_n \in R$, $s_n \in S$, b_n and s_n relatively prime. We have to prove that s_n is a unit for all n. This is true for $n = 0$ since $z_0 b_0 \in Rs_0$ and since z_0 and b_0 are prime to s_0. Suppose it is true for $0, 1, \cdots, n - 1$. Then, computing the coefficient of X^n, we see that $z_0 b_n s_n^{-1} \in R$; since $z_0 b_n$ is prime to s_n, this implies s_n is a unit. This proves Lemma 3.4.

This being so, we have $u_0^S = s^q u_0'$ and $v_0^S = s^q v_0'$, where u_0' divides u_0 and v_0' divides v_0. Since $u \in R_{S'} u^S$, there exist t in S' and a in R such that $tu = au^S$; we then have also $tv = av^S$. The constant terms verify

$$(2) \qquad a_0 = s^r a_0', \qquad t_0 = s^{q+r}, \qquad u_0 = a_0' u_0', \qquad v_0 = a_0' v_0'.$$

Let P be the set of common prime factors of u_0 and v_0; then a_0' is (up to a unit) a product of elements of P. *If* u_0' is a multiple of some $p \in P$, then $n_p(a_0') < n_p(u_0)$, whence $n(a, v) < n(u, v)$. By the induction hypothesis on $n(u, v)$, a and v have a l.c.m., whence also a g.c.d. d, and we can write $a = da''$ and $v = dv''$ with a'', v'' relatively prime. Since $tu = da''u^S$, and since d and t are relatively prime by Lemma 3.3, d divides u. Since it divides also v, and since we have assumed that u and v have no common factor, we have $d = 1$, whence a and v are relatively prime. Then the relation $tv = av^S$ shows that v divides v^S; hence v and v^S are associates in $R_{S'}$, whence $R_{S'} u \cap R_{S'} v = R_{S'} uv$, and $Ru \cap Rv = Ruw$ by Lemma 3.4.

We are thus reduced to the case in which u_0' has no factor in P, and similarly for v_0'. Then, using (2), we see that we may assume that a_0', u_0', and v_0' are *pairwise relatively prime.* This implies that they are uniquely determined by u_0 and v_0, and therefore independent of s. This being so, we are going to use the hypothesis that A is a local Macaulay ring.

Let A be a ring, s an element of A, and $c = c_0 + c_1 X + \cdots$ a power series over A. We say that c is an *s-series* if $c_n \in As^n$ for every n. The s-series are the elements of $A[[sX]]$, and therefore sums and products of s-series are s-series. We need the following two lemmas:

LEMMA 3.5. *Let A be a local ring, s an element of A, $a = a_0 + a_1 X + \cdots$ and $b = b_0 + b_1 X + \cdots$ two power series over A such that ab is an s-series and that (a_0, b_0, s) is a prime sequence in A. Then there exists an invertible power series $y = 1 + y_1 X + \cdots$ over A such that yb is an s-series.*

We set $a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 = c_n s^n$ $(c_n \in A)$, and we suppose that the elements $y_1, \cdots, y_{n-1}$ have already been found; we then have $b_j + b_{j-1} y_1 + \cdots + b_0 y_j = z_j s^j$ with $z_j \in A$ for $j = 1, \cdots, n-1$. We have to prove the existence of y_n in A such that $b_n + b_{n-1} y_1 + \cdots + b_0 y_n \in As^n$, i.e., that $b_n + b_{n-1} y_1 + \cdots + b_1 y_{n-1} \in As^n + Ab_0$. Since (a_0, b_0, s) is a prime sequence, (a_0, b_0, s^n) is also a prime sequence ([10], Appendix 6), so that a_0 is prime to $As^n + Ab_0$. It then suffices to show that

$$a_0(b_n + b_{n-1} y_1 + \cdots + b_1 y_{n-1}) \in As^n + Ab_0.$$

Since $a_0 b_n \equiv -(a_1 b_{n-1} + \cdots + a_{n-1} b_1) \pmod{As^n + Ab_0}$, we are reduced to proving that

$$v_n = b_{n-1}(a_0 y_1 - a_1) + \cdots + b_1(a_0 y_{n-1} - a_{n-1}) \in As^n + Ab_0.$$

Let y' be the polynomial $1 + y_1 X + \cdots + y_{n-1} X^{n-1}$, and y'' the power series such that $y'y'' = 1$. The element v_n is the coefficient of X^n in the series $(b - b_0)(a_0 y' - a)$. For $n \geqq 1$, we thus have $v_n \equiv (a_0 by' - ba)_n \bmod Ab_0$.

Consider the polynomial $z = b_0 + z_1 sX + \cdots + z_{n-1} s^{n-1}X^{n-1}$; it is an s-series. Moreover we have $y'b \equiv z \bmod. X^n$, whence $b \equiv y''z \bmod. X^n$. Now, since the series $a_0 y' - a$ has no constant term, the series $v = b(a_0 y' - a)$ verifies $v \equiv y''z(a_0 y' - a) \bmod. X^{n+1}$, whence $v \equiv z(a_0 - ay'') \bmod. X^{n+1}$. Notice that $y''a = (ab)(y'b)^{-1}$; since $y'b$ is congruent to an s-series mod. X^n, and since its constant term b_0 is prime to S, $(y'b)^{-1}$ is congruent mod. X^n to an s-series over $A[b_0^{-1}]$, whence also over A. Therefore $y''a$ is congruent mod. X^n to an s-series, and so is $z(a_0 - ay'')$ (since z is an s-series). The coefficient of X^n in this series has been seen to be equal to v_n ; since it is $b_0(a_0 - ay'')_n + \sum_{j=1}^{n} z_j s^j (a_0 - ay'')_{n-j}$, we see that $v_n \in Ab_0 + As^n$. This concludes the proof of Lemma 3.5.

LEMMA 3.6. *Let A be a local UFD, s an element of A, S the multiplicative system generated by s, S' the multiplicative system in $R = A[[X]]$ formed by the series having their constant terms in S. Let u and u' be two elements of R such that*

(1) $u_0 = a_0 b_0$, $u_0' = a_0 s$, (a_0 , b_0 , s) *being a prime sequence in* A;

(2) $u \in R_{S'} u'$.

Then there exists $u'' = a_0 + u_1'' X + \cdots$ in R, associate of u' in R_S , and dividing u in R. We then have $u' \in Ru''$.

Let us write $u(X) = t(X)u'(X)$, where $t(X) = b_0 s^{-1} + t_1 X + \cdots$ is a series with coefficients t_n in A_S . Notice that $s^n t_{n-1} \in A$: in fact it is true for $n = 1$; supposing it is proved for $1, \cdots, n-1$, we see, by expressing that the coefficient of X^{n-1} in $t(X)u(X)$ is in A, that $t_{n-1} a_0 s \in As^{1-n}$; hence $t_{n-1} \in As^{-n}$ since a_0 is prime to s and since $t_{n-1} \in A_S$. We can thus write $t_{n-1} = b_{n-1} s^{-n}$ with $b_{n-1} \in A$. We set $X = sY$. Then

$$u(sY) = s^{-1}(b_0 + b_1 Y + \cdots)u'(sY) = (b_0 + b_1 Y + \cdots)(a_0 + u_1' Y + \cdots).$$

Since $u(sY)$ is an s-series with respect to Y, the two series in the right-hand side verify the hypotheses of Lemma 3.5. Thus there exists an invertible element $y(Y) = 1 + y_1 Y + \cdots$ of $A[[Y]]$ such that

$$y(Y)(a_0 + u_1' Y + \cdots) = s^{-1}y(Y)u'(sY)$$

is an s-series with respect to Y. Now,

$$s^{-1}y(Y) = s^{-1}y(s^{-1}X)$$

is an invertible element of $R^S = A_S[[X]]$, and $s^{-1}y(s^{-1}X)u'(X)$ is an element u'' of R. Since u' and u'' are associates in the completion R^S of the Zariski ring $R_{S'}$, and since they belong to $R_{S'}$, they are associates in $R_{S'}$ ([10], VIII, §4, Theorem 9, (a')). It is clear that $u_0'' = a_0$; since $u \in R^S u''$, Lemma 3.4 shows that $u \in Ru''$. Similarly we have that $u' \in Ru''$. This proves Lemma 3.6.

We can now rapidly terminate the proof of Theorem 3.2. Just before Lemma 3.5, we were reduced to proving that two series u, v have a l.c.m. in

$R = A[[X]]$ under the following additional hypotheses: we have $u_0 = a_0 u_0'$ and $v_0 = a_0 v_0'$ with a_0, u_0', v_0' pairwise relatively prime; for any prime element s of R which does not divide u_0 or v_0, u and v have a l.c.m. w^S in $R_{S'}$ (S': set of series having a power of s as constant term); we have $w^S = uw^S = vu^S$ with u^S, v^S in R and $u_0^S = s^q u_0'$, $v_0^S = s^q v_0'$. Since A is a Macaulay ring of dimension $\geqq 3$, we may choose s prime to $Au_0' + Aa_0$, so that (u_0', a_0, s) is a prime sequence; then (u_0', a_0, s^q) is also a prime sequence. In Lemma 3.6, we replace u by u, u' by u^S, a_0 by u_0', b_0 by a_0 and s by s^q: we see that there exists u'' in R, associate of u^S in $R_{S'}$, such that $u \in Ru''$ and $u^S \in Ru''$. Then $w = vu''$ is a l.c.m. of u, v in $R_{S'}$, and its constant term $a_0 u_0' v_0'$ is prime to s. By Lemma 3.4, we have $w \in Ru \cap Rv$; if $z \in Ru \cap Rv$, we have

$$z \in R_{S'} u \cap R_{S'} v \cap R = R_{S'} w \cap R = Rw$$

(Lemma 3.4); therefore $Ru \cap Rv = Rw$, and this concludes the proof of Theorem 3.2.

Theorem 3.2 admits the following interesting corollary:

COROLLARY 3.7. *Let A be a Macaulay UFD such that $A_\mathfrak{p}$ is a regular local ring for every prime ideal $\mathfrak{p}$ of height 2. Then $A[[X]]$ is a UFD.*

Remark 3.8. It would be interesting to know whether the property that A is a Macaulay ring such that $A_\mathfrak{p}$ is regular whenever $h(\mathfrak{p}) = 2$, is transmitted to $A[[X]]$. It is true for the partial property of being a Macaulay ring. On the other hand, if $\mathfrak{P}$ is a prime ideal of height 2 in $R = A[[X]]$, $\mathfrak{P} \cap A$ is a prime ideal of height 2, 1, or 0; if A is a complete local ring of equal characteristic 0, the fact that $R_\mathfrak{P}$ is regular follows from the classical jacobian criterion [4]; the general case could possibly be handled in a similar way, in spite of the difficulties caused by the inseparable derivations. On the other hand, if A has the above-said property, so has the *polynomial* ring $A[X]$: no trouble for being a Macaulay ring; if $\mathfrak{P}$ is a prime ideal of height 2 in $A[X]$, then $\mathfrak{p} = A \cap \mathfrak{P}$ has height 1 or 2, whence $A_\mathfrak{p}$ is regular; and also $(A[X])_\mathfrak{P}$ is regular, since it is a quotient ring of $A_\mathfrak{p}[X]$ (see proof of Theorem 2.1).

4. Power series over a UFD. The two-dimensional case

Theorem 3.2 almost reduces the question, as to whether a power series ring over a UFD A is a UFD, to the case in which A has dimension 2. At any rate this two-dimensional case is the crucial one for our problem. The answer is that there exists a two-dimensional UFD A (which may be assumed to be local) such that $A[[X]]$ is *not* a UFD.

THEOREM 4.1. *Let A be a domain, a, b, c three elements of A, and i, j, k three integers. We assume: b is prime, b and c are relatively prime,*

$$a^{i-1} \notin Ab + Ac, \qquad a^i \in Ab^k + Ac^j, \qquad ijk - ij - jk - ki \geqq 0.$$

Then $R = A[[X]]$ is not a UFD.

Let S be the multiplicative system generated by c in A, S' the set of all power series having their constant terms in S. We set $R^S = A_S[[X]]$; it is the (X)-adic completion of the Zariski ring $R_{S'}$. Consider the series

$$v = cb - a^{i-1}X \in R. \tag{1}$$

The proof is in three steps.

(a) *No power series* $b + a_1 X + a_2 X^2 + \cdots \in R$ *is an associate of* v *in* R^S (*nor, a fortiori, in* $R_{S'}$).

In fact, if $(cb - a^{i-1}X)(c^{-1} + d_1 c^{-q}X + \cdots) \in R$, the coefficient of X must be in A, i.e., $d_1 bc^{1-q} - a^{i-1}c^{-1} \in A$, whence c^{q-2} divides $d_1 b$. Since c is prime to b, c^{q-2} divides d_1, and there exists d in A such that $d_1 = c^{q-2}d$. We thus have $dbc^{-1} - a^{i-1}c^{-1} \in A$, whence $a^{i-1} \in Ab + Ac$, in contradiction with the hypothesis.

(b) *There exist an integer* t *and a series*

$$v' = b^t c^{-1} + \cdots + b_{n-1} c^{-n} X^{n-1} + \cdots$$

in R^S ($b_i \in A$) *such that* $vv' \in R$.

We have to find elements $b_1, \cdots, b_n, \cdots$ of A such that

$$bb_1 - a^{i-1}b^t \in Ac, \qquad bb_n - a^{i-1}b_{n-1} \in Ac^n \quad \text{for} \quad n \geqq 2. \tag{2}$$

We take $b_1 = a^{i-1}b^{t-1}$, $b_2 = a^{2(i-1)}b^{t-2}$, and so on until $b_{ij-1} = a^{(i-1)(ij-1)}b^{t-ij+1}$; this is possible, provided $t \geqq ij$. The next relation (2) is

$$bb_{ij} - a^{ij(i-1)}b^{t-ij+1} \in Ac^{ij+1}.$$

Let us write $a^i = db^k + ec^j$ with $e, d \in A$. We thus get the relation

$$bb_{ij} - (db^k + ec^j)^{j(i-1)}b^{t-ij+1} \in Ac^{ij+1}.$$

In the binomial expansion of $(db^k + ec^j)^{j(i-1)}$, the terms in which c appears with an exponent $\leqq ij$ may be written as $b^{k(j(i-1)-i)}F_1(b^k, c^j)$, where F_1 is a form of degree i with coefficients in A. Our relation is thus equivalent to $bb_{ij} - b^{ijk-jk-ki-ij+t+1}F_1(b^k, c^j) \in Ac^{ij+1}$. It may be solved by taking $b_{ij} = b^{ijk-jk-ki-ij+t}F_1(b^k, c^j)$; notice that the exponent of b is $\geqq t$ since we have assumed that $ijk - jk - ki - ij \geqq 0$.

In general suppose we have determined $b_1, \cdots, b_{(n-1)ij}$ in such a way that $b_{(n-1)ij} = b^{t(n-1)}F_{n-1}(b^k, c^j)$, where $t(n-1) \geqq t \geqq ij$ and where F_{n-1} is a form of degree $(n-1)i$ with coefficients in A. We may then take

$$b_{(n-1)ij+1} = a^{i-1}b^{t(n-1)-1}F_{n-1}(b^k, c^j)$$

and so on until $b_{nij-1} = a^{(i-1)(ij-1)}b^{t(n-1)-ij+1}F_{n-1}(b^k, c^j)$ (multiplying each time by $a^{i-1}b^{-1}$). The next relation to be fulfilled is then

$$bb_{nij} - (db^k + ec^j)^{j(i-1)}b^{t(n-1)-ij+1}F_{n-1}(b^k, c^j) \in Ac^{nij+1}.$$

In the form $(db^k + ec^j)^{j(i-1)}F_{n-1}(b^k, c^j)$, the sum of the terms in which c has an exponent $\leqq nij$ may be written as $b^{k((n-1)i+(i-1)j-ni)}F_n(b^k, c^j)$ where F_n is a form of degree ni. Thus our congruence may be solved by taking $b_{nij} = b^{t(n-1)-ij+ijk-ki-kj}F_n(b_j^k, c^j)$. Since $ijk - ij - jk - ki \geqq 0$, the exponent $t(n)$ of b is $\geqq t(n-1)$. Thus b_{nij} satisfies the same conditions as $b_{(n-1)ij}$, and the coefficients b_q may therefore be found by induction on q.

(c) *R cannot be a UFD.*

Suppose R is a UFD. Set $u = vv'$. Let $u = u_1 \cdots u_q$ be the decomposition of u in irreducible factors in R; since the constant term of u is a power of b, and since b is prime, the constant term of each u_s is a power of b. Since b is prime to c, each u_s remains irreducible in the UFD $R_{S'}$. On the other hand, we have $u = vv' \in vR^S \cap R_{S'} = vR_{S'}$ (since $R_{S'}$ is a Zariski ring, and R^S its completion), whence $v' \in R_{S'}$ since R^S is a domain. Since v is obviously irreducible in $R_{S'}$ (its constant term being irreducible in A_S), the relation $vv' = u_1 \cdots u_q$ and the unique factorization in $R_{S'}$ show that v must be an associate of some u_s in $R_{S'}$. This contradicts (a), Q.E.D.

Remark 4.2. The condition $ijk - ij - jk - ki \geqq 0$ is surprisingly symmetric in the exponents i, j, k. I have tried to find weaker conditions by replacing the series $v = bc - a^{i-1}X$ by a more complicated one; but, for $v = bc - b^sX - a^{i-1}X^2$ (s large; the analogue of (a) works), the analogue of (b) requires again the *same* inequality $ijk - ij - jk - ki \geqq 0$. It may thus be possible that, to every UFD A, is attached a numerical invariant I (generalizing $ijk - ij - jk - ki$) such that $A[[X]]$ is a UFD for $I < 0$ and is not for $I \geqq 0$. At any rate, in a regular UFD, there cannot exist elements a, b, c and exponents i, j, k verifying the assumptions of Theorem 4.1.

Now, in order to disprove the conjecture that a power series ring over a UFD is a UFD, it is sufficient to construct a UFD containing three elements verifying the assumptions of Theorem 4.1. This is done in the following theorem:

THEOREM 4.3. *Let k be a perfect field of characteristic 2. The ring $B = k[x, y, z]$, where $z^2 - x^3 - y^7 = 0$, is a UFD, and so is the local ring $B_{(x,y,z)}$.*

The proof is divided into two lemmas:

LEMMA 4.4. *Let k be a perfect field of characteristic 2, and A the polynomial ring $k[x, y]$. We set $p = x$, $q = y^3$, $f = xp^2 + yq^2 = x^3 + y^7$. Let a, b be two relatively prime elements of A. Then every divisor of $a^2 + fb^2$ is an element of the same form (i.e., $a'^2 + fb'^2$).*

(a) Since a product of elements of the form $a^2 + fb^2$ is of the same form, it suffices to prove the lemma for irreducible divisors. Let us write

$$a^2 + fb^2 = uw,$$

with u irreducible. In A the squares are the elements $\sum_{i,j} a_{ij}\, x^{2i} y^{2j}$; they form a subring A^2 of A; the ring A is a free module over A^2, with $(1, x, y, xy)$ as basis. Let us write

$$(3) \qquad u = u_1^2 + u_2^2\, x + u_3^2\, y + u_4^2\, xy, \qquad v = v_1^2 + v_2^2\, x + v_3^2\, y + v_4^2\, xy.$$

Since $uv = a^2 + (bp)^2 x + (bq)^2 y$, the fact that $(1, x, y, xy)$ is a basis of A over A^2 gives the four relations:

$$(4.1) \qquad a = u_1 v_1 + u_2 v_2\, x + u_3 v_3\, y + u_4 v_4\, xy,$$

$$(4.2) \qquad bp = u_1 v_2 + u_2 v_1 + y(u_3 v_4 + u_4 v_3),$$

$$(4.3) \qquad bq = u_1 v_3 + u_3 v_1 + x(u_2 v_4 + u_4 v_2),$$

$$(4.4) \qquad 0 = u_1 v_4 + u_4 v_1 + u_2 v_3 + u_3 v_2\,.$$

Multiplying (4.2) by v_3, (4.3) by v_2, adding, and using the relation

$$u_2 v_3 + u_3 v_2 = u_1 v_4 + u_4 v_1$$

(this is (4.4) since A has characteristic 2), we get

$$(v_3 p + v_2 q)b = v_1(u_1 v_4 + u_4 v_1) + v_4(u_3 v_3\, y + u_2 v_2\, x) + u_4(v_3^2\, y + v_2^2\, x)$$

$$= v_4(a - u_4 v_4\, xy) + u_4(v - v_4^2\, xy) = v_4\, a + u_4\, v;$$

setting $v' = v_3 p + v_2 q$ and $u' = u_3 p + u_2 q$, we thus get

$$(5.1) \qquad bv' = v_4\, a + u_4\, v,$$

and similarly

$$(5.2) \qquad bu' = u_4\, a + v_4\, u.$$

It follows from (5.1) and (5.2) that $a(v_4^2\, u + u_4^2\, v) = b(v' v_4\, u + u' u_4\, v)$; since a and b are relatively prime, there exists t' in A such that $v_4^2\, u + u_4^2\, v = t'b$. Hence $t'bu = v_4^2\, u^2 + u_4^2(a^2 + fb^2) = b^2(u'^2 + fu_4^2)$, and b divides $t'u$. Since u is irreducible, it is prime to b (otherwise it would divide b, whence also a^2 $(= uv - fb^2)$, contradicting the hypothesis that a and b are relatively prime). Thus b divides t', and we may write $t' = bt$ with t in A; hence $v_4^2\, u + u_4^2\, v = tb^2$. The above formula for $tub^2 = t'bu$, and the analogous one for $t'bv$, thus give

$$(6) \qquad tu = u'^2 + fu_4^2\,, \qquad tv = v'^2 + fv_4^2\,.$$

(b) The first formula (6) has the same form as $vu = a^2 + fb^2$; let us write $t = t_1^2 + t_2^2\, x + t_3^2\, y + t_4^2\, xy$. In formulae (3), (4), (5), we replace u by itself, u_i by itself, v by t, v_i by t_i, a by u', and b by u_4; then u' is unchanged, and the analogue of (5.2) is $u_4 u' = u_4 u' + t_4 u$; this implies $t_4 = 0$ since $u \neq 0$. The analogue of (5.1) is $u_4(t_3 p + t_2 q) = t_4 u' + u_4 t$, whence $u_4(t - t_3 p - t_2 q) = 0$. If $t \neq t_3 p + t_2 q$, we have $u_4 = 0$, and, similarly, $v_4 = 0$. We will see later that the relation $u_4 = v_4 = 0$ suffices for reaching our conclusion.

(c) We now prove that, if $t = t_3 p + t_2 q$, we also have $u_4 = v_4 = 0$. Here we use the fact that $p = x$ and $q = y^3$. We thus have

$$t = t_1^2 + t_2^2 x + t_3^2 y = t_3 x + t_2 y^3. \tag{7}$$

Let j be the maximum of the degrees of t_2 and t_3. Since the monomials with nonzero coefficients in t_1^2, $t_2^2 x$, and $t_3^2 y$ are all distinct, the degree of t is at least $2j + 1$. On the other hand, since $t = t_3 x + t_2 y^3$, the degree of t is at most $j + 3$. Hence $2j + 1 \leqq j + 3$, $j \leqq 2$, and we can write $t_2 = a_0 + a_1 + a_2$, $t_3 = b_0 + b_1 + b_2$, where a_i and b_i are forms of degree i. Comparing terms of degrees 1, 3, 5 in (7), we get

$$a_0^2 x + b_0^2 y = b_0 x, \qquad a_1^2 x + b_1^2 y = b_2 x + a_0 y^3, \qquad a_2^2 x + b_2^2 y = a_2 y^3. \tag{8}$$

The first relation implies $b_0 = 0$, whence $a_0 = 0$. The third shows that y divides a_2, say $a_2 = yc_1$ (c_1 : form of degree 1), whence $xyc_1^2 + b_2^2 = c_1 y^3$; this implies that y divides b_2, say $b_2 = d_1 y$, whence $xc_1^2 + yd_1^2 = c_1 y^2$; applying the same process, we get $c_1 = yc_0$, $d_1 = yd_0$, and $xc_0^2 + yd_0^2 = yc_0$; this shows that $c_0 = d_0 = 0$, whence $a_2 = b_2 = 0$. The second relation (8) is now $a_1^2 x + b_1^2 y = 0$; since x and y are linearly independent over A^2, this implies $a_1 = b_1 = 0$. Therefore we have $t_2 = t_3 = 0$, $t = 0$, and, by (6), $u'^2 + (p^2 x + q^2 y)u_4^2 = 0$; the linear independence of 1, x, y over A^2 shows that $u_4 = 0$; similarly $v_4 = 0$.

(d) We finally show how $u_4 = v_4 = 0$ implies the conclusion of our lemma. By (5.2) we have $u' = 0$, i.e., $u_3 p + u_2 q = 0$. Since p and q are relatively prime, there exists c in A such that $u_2 = cp$ and $u_3 = cq$. By (3) we conclude that $u = u_1^2 + c^2(p^2 x + q^2 y) = u_1^2 + c^2 f$, as asserted.

LEMMA 4.5. *Let A be a UFD, and f an irreducible element of A such that if a and b are relatively prime in A, then every divisor of $a^2 - fb^2$ is of the form $a'^2 - fb'^2$. Then $B = A[z]$, where $z^2 = f$, is a UFD.*

Since f is irreducible, it is not a square in the quotient field K of A, whence B is a domain. We give the proof in characteristic 2 (inseparable case); the separable case is analogous, and slightly simpler. We first prove that B is *integrally closed*. Let $c + dz$ ($c, d \in K$) be an element of $K(z)$ which is integral over B. Then its square is in K and is integral over A, whence belongs to A. The cases $c = 0$ and $d = 0$ are easy. We write $c = ua/v$, $d = ub/v$ with a, b, u, v in A, a, b relatively prime, and u, v relatively prime. We thus have $u^2(a^2 - fb^2) \in Av^2$. Since v is prime to u, it divides $a^2 - fb^2$, whence is of the form $v = w^2 - ft^2$; we also have $(a^2 - fb^2)/v^2 = w'^2 - ft'^2$ (w', t' in A), whence $a^2 - fb^2 = (vw')^2 - f(vt')^2$. Since f is irreducible, 1 and f are linearly independent over A^2, whence $a = vw'$, $b = vt'$. Since a and b are relatively prime, this implies $v = 1$, whence c, $d \in A$ and $c + dz \in B$. (In the separable case, the proof is easier and classical, since one can use the trace of $c + dz$, not only its norm.)

For proving that B is a UFD, we show that every prime ideal $\mathfrak{p}$ of height 1 of B is principal. The ideal $\mathfrak{p} \cap A$ is a prime ideal of height 1 of A, i.e., an

ideal Ac where c is irreducible. Since B is the integral closure of A in a purely inseparable extension, $\mathfrak{p}$ is the only prime ideal of B over Ac; hence Bc is a symbolic power $\mathfrak{p}^{(n)}$ of $\mathfrak{p}$. Let v be the normed valuation having $B_{\mathfrak{p}}$ as valuation ring, and let $a + bz$ $(a, b \in A)$ be a uniformizing element for v. We have $(a + bz)^2 = a^2 + fb^2 \in A \cap \mathfrak{P} = Ac$, whence $n = v(c) \leqq 2$. If $v(c) = 1$, we have $\mathfrak{p} = Bc$, and our assertion is proved. We thus suppose that $v(c) = 2$, so that $Bc = \mathfrak{p}^{(2)}$. We have $b \neq 0$, for, otherwise, $a + bz \in A$ and $v(c) = 1$. If $a = 0$, we easily see that $\mathfrak{p} = Bz$, since f is irreducible. We thus assume that a and b are $\neq 0$, and write $a = da'$, $b = db'$ with a', b' relatively prime. We have $2 = v(a^2 + b^2 f) = 2v(d) + v(a'^2 + b'^2 f)$; if $v(d) = 1$, we see that $v(c) = 1$, case already treated; thus $v(d) = 0$, $a' + b'z$ is a uniformizing element for v, and c divides $a'^2 + b'^2 f$ in A. Since a' and b' are relatively prime, the hypothesis shows that $c = v^2 + w^2 f$ with $v, w \in A$. Thus $c = (v + wz)^2$, $\mathfrak{p}$ is the only prime ideal of height 1 containing $v + wz$, and therefore $\mathfrak{p} = B(v + wz)$. This concludes the proofs of Lemma 4.5 and of Theorem 4.3.

Now we apply Theorem 4.1 to the ring $B = k[x, y, z]$ $(z^2 - x^3 - y^7 = 0)$ of Theorem 4.3 (or to the local ring $B_{(x,y,z)}$): we replace the elements a, b, c of Theorem 4.1 by x, y, z. The exponents i, j, k may then be taken to be 3, 7, 2. The decisive inequality $ijk - ij - jk - ki \geqq 0$ is verified since $42 - 21 - 14 - 6 = 1$. We have thus found a UFD A (which may be assumed to be local) such that $A[[X]]$ is not a UFD.

Remark 4.6. The completion of the local UFD $(k[x, y, z, X])_{(x,y,z,X)}$ (where $z^2 - x^3 - y^7 = 0$) is the ring $k[[x, y, z, X]]$. It is not a UFD by Lemma 1.2, since it is the completion of the local ring $A[[X]]$, where $A = (k[x, y, z])_{(x,y,z)}$.

Remark 4.7. Other equations than $z^2 - x^3 - y^7 = 0$ (over a perfect field of characteristic 2) give rise to UFD's: except in part (c) of Lemma 4.4 the only hypotheses which have been used are "$z^2 = f \in k[x, y]$, f irreducible, $f = p^2 x + q^2 y$ with p, q relatively prime". The computation made in part (c) of Lemma 4.4 may be extended to the following equations:

$$z^2 - x^3 - y^5 = 0, \qquad z^2 - x^3 - y^{11} = 0,$$

$$z^2 - x^3 - y^{13} = 0, \qquad z^2 - x^3 - y^{17} = 0,$$

$$z^2 - x^5 - y^7 = 0, \qquad z^2 - x^5 - y^9 = 0, \qquad z^2 - x^5 - y^{11} = 0.$$

All these systems of exponents, except the first one, verify the inequality $ijk - ij - jk - ki \geqq 0$. It seems likely that a great number of equations of the form $z^2 - x^{2r+1} - y^{2s+1} = 0$ give rise to UFD's, but, for the time being, I have not been able to find a general procedure. Notice also that everything in Theorem 4.3, except again part (c) of Lemma 4.4, works if the polynomial ring $k[x, y]$ is replaced by the power series ring $k[[x, y]]$; however I feel that the possibility of extending part (c) to power series is much less likely than the possibility of extending it to more general exponents; at any

rate it would be interesting to know whether the complete local ring $k[[x, y, z]]$ ($z^2 - x^3 - y^7 = 0$ or more general exponents, k perfect of characteristic 2) is a UFD. It would also be interesting to extend Theorem 4.3 to other characteristics $p \neq 0$ (the equation between x, y, z being a purely inseparable equation $z^p - f(x, y) = 0$): the computations in Lemmas 4.4 and 4.5 (especially 4.4) would be more complicated, but there is a fair chance that one should be able to handle them properly; on the other hand, very different methods would have to be used in characteristic 0. In this case, Mr. Mumford has proved recently that the complete local ring $k[[x, y, z]]$ (k: complex field) is a UFD if $z^2 - x^3 - y^5 = 0$, and is not a UFD if $z^2 - x^3 - y^7 = 0$.

Remark 4.8. The existence of a *complete* two-dimensional local UFD A such that $R = A[[X]]$ is *not* a UFD would have the following, rather strange, consequences. Every prime ideal $\mathfrak{P}$ of height 2 of R verifies $A \cap \mathfrak{P} \neq (0)$, for, otherwise, we would have a monomorphism of the two-dimensional *complete* local ring A into the one-dimensional local ring $R/\mathfrak{P}$, carrying maximal ideal into maximal ideal, and such that A and $R/\mathfrak{P}$ have the same residue field; this would contradict the existence of two analytically independent elements in A. Therefore, if we denote by S the set of nonzero elements of A, every prime ideal in R_S has height $\leqq 1$, whence R_S is a *Dedekind domain* (since it is obviously noetherian and integrally closed). However R_S is *not* a PID, for, otherwise, R would be a UFD by Lemma 1.7. Now, since R is a local ring, every finitely generated projective R-module is free (Remark 1.4), whereas this property is not shared by R_S.

5. Ground-field extensions

In this section we are going to show that unique factorization is preserved neither by ground-field extension, nor by ground-field restriction. Of course, our rings will remain integrally closed domains. The examples we give are taken from the theory of plane conics. We thus discuss first the conditions under which the affine coordinate ring of a conic is a UFD.

THEOREM 5.1. *Let C' be an irreducible conic in the affine plane, defined over a field k, let A be its affine coordinate ring (over k), and let C be the projective extension of C'.*

(a) *If C has no rational point over k, then A is a UFD;*

(b) *if C carries rational points over k, but if the points at infinity of C are not rational over k, then A is not a UFD;*

(c) *if the points at infinity of C are rational over k, then A is a UFD.*

Let X be a positive divisor on C, rational over k. This divisor is a "complete intersection" (i.e., there exists a positive divisor D in the projective plane, defined over k, such that $X = C \cdot D$) if and only if it has *even* degree: this comes from the facts that C has order 2, genus 0, and is normal. To every prime ideal $\mathfrak{p} \neq (0)$ in A corresponds a positive divisor $X'(\mathfrak{p})$ on C', which is prime-rational over k. For $\mathfrak{p}$ to be principal, it is necessary and

sufficient that there exist a positive linear combination I of the points at infinity of C, rational over k, such that $X'(\mathfrak{p}) + I$ is a complete intersection, i.e., has even degree.

In case (a), every rational divisor on C' has even degree (for, otherwise, C would carry a rational point; see [2], p. 33); we thus take $I = 0$, $\mathfrak{p}$ is principal, and A is a UFD. In case (b), let $\mathfrak{p}$ be the prime ideal in A corresponding to a rational point of C'; then $X'(\mathfrak{p})$ has degree one; on the other hand, if a rational divisor I has the points at infinity as components, its degree is even (if the two points at infinity are distinct, they must occur in I with the same coefficient since they are conjugate over k; if there is only one point P at infinity, $k(P)$ is a purely inseparable extension of degree 2 of k, and the coefficient of P in I must be a multiple of the order of inseparability, i.e., of 2). Thus no $X'(\mathfrak{p}) + I$ can have even degree, showing that $\mathfrak{p}$ is not principal, and that A is not a UFD. Finally, in case (c), any linear combination of the points at infinity is rational over k, showing that every prime ideal $\mathfrak{p} \neq (0)$ in A is principal, and that A is a UFD.

Now the examples are quite simple:

(1) Let C' be defined by $x^2 + 2y^2 + 1 = 0$ over Q. Then $Q[x, y]$ is a UFD by case (a), and $Q(i)[x, y]$ is not a UFD by case (b) ($i^2 = -1$).

(2) Let C' be defined by $x^2 + y^2 - 1 = 0$ over Q. Then $Q[x, y]$ is not a UFD by case (b), but $Q(i)[x, y]$ is a UFD by case (c).

6. Open problems

Some open questions, closely related with this paper, have been described in Remarks 3.8, 4.2, and 4.7. I will now describe another one.

The UFD's constructed in §4, as well as Mumford's $k[[x, y, z]]$ (k complex field, $z^2 - x^3 - y^5 = 0$), are not the first examples of nonregular UFD's. The first examples came from the following geometric origin: if V is an arithmetically normal projective variety such that every divisor on V is a complete intersection, then the homogeneous coordinate ring A of V is a UFD, and so is the local ring $A_{\mathfrak{m}}$ of the vertex of the projecting cone of V. The following are examples of such varieties:

(a) generic surface of order 4 in 3-space [6],

(b) Grassmann varieties [7],

(c) nonsingular hypersurfaces in a projective space of dimension $\geqq 4$ ([8]; algebraic proof in [5], in the case of hyperquadrics).

The last example seems to be the most interesting one, at least from an algebraic point of view. It leads to the following question:

"Let A be a local domain of dimension $\geqq 4$, which is a factor ring $R/(f)$ of a regular local ring by a principal ideal. Assume that $A_{\mathfrak{p}}$ is regular for every nonmaximal prime ideal $\mathfrak{p}$. Is A a UFD?"

One could try to weaken the hypothesis "A = regular/principal" to "A is a Macaulay ring". Under this weaker hypothesis the question could be more manageable by homological methods.

All the examples of UFD's I know are Macaulay rings. Is this true in general?

References

1. M. Auslander and D. A. Buchsbaum, *Unique factorization in regular local rings*, Proc. Nat. Acad. Sci. U. S. A., vol. 45 (1959), pp. 733–734.
2. C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Amer. Math. Soc. Surveys, no. 6, New York, 1951.
3. W. Krull, *Beiträge zur Arithmetik kommutativer Integritätsbereiche. V. Potenzreihenringe*, Math. Zeitschrift, vol. 43 (1938), pp. 768–782.
4. M. Nagata, *A Jacobian criterion of simple points*, Illinois J. Math., vol. 1 (1957), pp. 427–432.
5. ———, *A remark on the unique factorization theorem*, J. Math. Soc. Japan, vol. 9 (1957), pp. 143–145.
6. M. Noether, *Zur Grundlegung der Theorie der algebraischen Raumcurven*, Abh. Akad. Wiss. Berlin, 1882.
7. F. Severi, *Sulla varietà che rappresenta gli spazî subordinati di data dimensione, immersi in uno spazio lineare*, Ann. Mat. Pura Appl. (3), vol. 24 (1915), pp. 89–120.
8. ———, *Una proprietà delle forme algebriche prive di punti multipli*, Atti Accad. Lincei. Rend. Cl. Sci. Fis. Mat. Nat. (5), vol. 15 (1906), pp. 691–696.
9. J-P. Serre, *Sur la dimension homologique des anneaux et des modules noethériens*, Proceedings of the International Symposium on Algebraic Number Theory, Tokyo & Nikko, September, 1955, pp. 175–189.
10. O. Zariski and P. Samuel, *Commutative algebra, vol. II*, Princeton, Van Nostrand, 1960.

University of Illinois
Urbana, Illinois
Université de Clermont-Ferrand
Clermont-Ferrand, France