Appeared in: Collect. Math. **48** 1–2 (1997), 85–96 (Proc. Journées Arithmétiques 1995)

A differential criterion for complete intersections

Bart de Smit

Econometrisch Instituut, Erasmus Universiteit Rotterdam,
Postbus 1738, 3000 DR Rotterdam, Netherlands
E-mail address: dsmit@wis.few.eur.nl

Abstract. Let A be a noetherian ring whose maximal spectrum has dimension at most 1. For instance, A can be a noetherian local ring or an order in a number field. Let B be a finite projective A-algebra that becomes étale over the total ring of quotients of A. In this note it is shown that B is of the form $A[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ if and only if the Fitting ideal $\mathrm{Fit}_B(\Omega_{B/A})$ of the module of differentials of B over A is free of rank 1 as a B-module. In particular, the ring of integers in a number field K is of the form $\mathbb{Z}[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ if and only if the different of K over $\mathbb{Q}$ is a principal ideal.

1. Introduction

In this note we explain a criterion to decide whether certain finite projective algebras are complete intersections. The criterion is formulated over an arbitrary noetherian base ring. Applied with base ring $\mathbb{Z}$ it tells us which orders in number fields are of the form $\mathbb{Z}[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$. Such orders are called complete intersection orders, and they share several ring-theoretic properties with the well-studied subclass of equation orders, i.e., orders of the form $\mathbb{Z}[\alpha]$. Applied with a complete discrete valuation ring as a base ring, the criterion gives results that have recently gotten attention in relation to Wiles' proof of Fermat's Last Theorem. We first state the theorem and then return to these two number-theoretic applications.

Rings and algebras in this note are supposed to be commutative with identity element. By a *complete intersection* over a ring A we mean an A-algebra of the from $A[X_1, \ldots, X_n]/(f_1, \ldots f_n)$ that is finitely generated as an A-module. Such an algebra is always projective as an A-module [3].

If A is a ring and $B = A[X_1, \ldots, X_n]/(g_1, \ldots, g_m)$ then the module of differentials $\Omega_{B/A}$ is the cokernel of the B-linear map $B^m \to B^n$ with matrix $(\partial g_i/\partial X_j)_{i,j}$. The Fitting ideal $\mathrm{Fit}_B(\Omega_{B/A})$ is the B-ideal generated by all $n \times n$ minors of this $m \times n$ matrix. Clearly, $\mathrm{Fit}_B(\Omega_{B/A})$ is a principal B-ideal if we can take $m = n$. The theorem below gives sufficient conditions for the converse to hold. We say that B is generically étale over A if $\Omega_{B/A}$ is annihilated by a non-zero divisor of A.

(1.1) Theorem. *Let A be a noetherian ring and let B be an A-algebra that is finitely generated and projective as an A-module. Then the following are equivalent:*

(1) *B is a generically étale complete intersection algebra over A;*

(2) *there exists a finite free B-module F and a short exact sequence*

$$0 \to F \to F \to \Omega_{B/A} \to 0.$$

If the maximal dimension of A is at most 1 then these are also equivalent to

(3) $\mathrm{Fit}_B(\Omega_{B/A})$ *is free of rank 1 as a B-module;*

(4) *B is generically étale over A and* $\mathrm{Fit}_B(\Omega_{B/A})$ *is a principal B-ideal.*

We explain the terminology in the next section and we give the proof in Section 3. The proof follows ideas of Mohan Kumar [7], Vasconcelos [14], and Lipman [10]. It uses a ring-theoretic result of Auslander-Buchsbaum [2] and a result of Serre [13] on projective modules. The equivalence of (1) and (2) in the case that B is reduced can also be deduced from Kunz [6, Th. 9.5].

Suppose that $\mathcal{O}$ is an order in a number field K. If $\mathcal{O}$ is the maximal order in K then $\mathrm{Fit}_{\mathcal{O}}(\Omega_{\mathcal{O}/\mathbb{Z}})$ is equal to the different of K over $\mathbb{Q}$; see [12, Ch. III, §7]. The theorem implies that $\mathcal{O}$ is a complete intersection over $\mathbb{Z}$ if and only if $\mathrm{Fit}_{\mathcal{O}}(\Omega_{\mathcal{O}/\mathbb{Z}})$ is a principal $\mathcal{O}$-ideal.

In the context of Wiles' proof of Fermat's Last Theorem one takes a complete discrete valuation ring A as a base ring, and one considers only finite local A-algebras B with the same residue field as A. One can show that B is then a complete intersection over A if and only if B is of the form $A[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n)$; see [3]. The theorem above gives a criterion to decide whether B is a complete intersection in the case that B is generically étale over A. A slightly weaker criterion in this setting, which was suggested by Mazur, was shown recently by Lenstra with a method close to Wiles's arguments [9, pp. 106–108].

If B is a finite projective algebra over a ring A then we say that B is locally a complete intersection over A if for all primes $\mathfrak{p}$ of A the ring $B \otimes_A A_{\mathfrak{p}}$ is a complete intersection over the localization $A_{\mathfrak{p}}$. One can deduce from (1.1) that a finite projective algebra B over a noetherian ring A is both generically étale and locally a complete intersection if and only if $\mathrm{Fit}_B(\Omega_{B/A})$ is projective of rank 1 as a B-module. Some further ring-theoretic properties of (locally) complete intersections are mentioned in (2.4) below.

2. Terminology

In this section we give the definitions used in Theorem (1.1), and we mention some of the ingredients of the proof. The main statement of this section is the formulation in Proposition (2.6) of four equivalent criteria for a finite projective algebra over a noetherian ring to be generically étale.

(2.1) The maximal dimension and Serre's theorem. Let A be a ring, and let $X(A)$ be the set of prime ideals of A that can be written as an intersection of a collection of maximal ideals of A. We define the *maximal dimension* m-dim(A) of A to be the largest integer k for which there is a chain $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_k$ of prime ideals in $X(A)$ in which all inclusions are strict. In particular, m-dim(A) is at most the Krull-dimension dim(A) of A, and we have m-dim$(A) = 0$ if A is local. If B is a finite A-algebra then m-dim$(B) \leq$ m-dim(A), because pulling back prime ideals gives a map $X(B) \to X(A)$ that preserves strict inclusions [1, 5.8, 5.9]. It is not hard to show that m-dim(A) is the dimension of the topological subspace of $\mathrm{Spec}\, A$ consisting of the maximal ideals; cf. [5, Ch. I, §1].

A theorem of Serre [13, Th. 1] says that every finitely generated projective module of constant rank over a noetherian ring A is the direct sum of a free A-module and a projective A-module of rank at most m-dim(A). For Dedekind A and for local A this is well-known; see [8, Ch. III, Ex. 13] and [8, Ch. XVI, Th. 3.8].

(2.2) Fitting ideals. Let R be a ring and let M be a finitely generated R-module. Choose an R-linear surjection $R^n \xrightarrow{\varphi} M$ for some $n \geq 0$. The *Fitting ideal* $\mathrm{Fit}_R(M)$ is the R-ideal generated by the determinants $\det(v_1, \ldots, v_n)$ with $v_1, \ldots, v_n \in \mathrm{Ker}\, \varphi$. The ideal $\mathrm{Fit}_R(M)$ does not depend on the choice of φ. See [8, Ch. XIX, §2] for details. For each set X of R-module generators of $\mathrm{Ker}\, \varphi$, the Fitting ideal $\mathrm{Fit}_R(M)$ is already generated by those determinants for which the v_i are contained in X. If S is an R-algebra then $\mathrm{Fit}_S(M \otimes_R S) = \mathrm{Fit}_R(M) \cdot S$. If $M \cong R/\mathfrak{a}_1 \oplus \cdots \oplus R/\mathfrak{a}_n$ for R-ideals $\mathfrak{a}_i$, then $\mathrm{Fit}_R(M) = \mathfrak{a}_1 \cdots \mathfrak{a}_n$.

(2.3) The trace map. Let A be a ring and let B be a finite projective A-algebra, i.e., an algebra that is finitely generated and projective as an A-module. We denote by $B^\dagger$ the A-linear dual $\mathrm{Hom}_A(B, A)$ of B. It has a B-module structure given by $(b\varphi)(x) = \varphi(bx)$ with $b, x \in B$ and $\varphi \in B^\dagger$. Since B is projective as an A-module the canonical map $B \otimes_A B^\dagger \to \mathrm{End}_A(B)$ that sends $b \otimes \varphi$ to the endomorphism $x \mapsto b\varphi(x)$, is an isomorphism. The trace map $\mathrm{Tr}_{B/A}\colon B \to A$ is defined to be the composition of canonical maps $B \to \mathrm{End}_A(B) \cong B \otimes_A B^\dagger \to A$, where the first map sends b to the endomorphism $x \mapsto bx$ and the last map is the evaluation map $b \otimes \varphi \mapsto \varphi(b)$. This gives rise to a canonical B-linear map $\psi_{B/A}\colon B \to B^\dagger$ that sends x to the map $y \mapsto \mathrm{Tr}_{B/A}(xy)$.

(2.4) Remark. With this terminology in place we can state two properties of (locally) complete intersections. We will not need them in the sequel. Let A be a ring and let B be a finite projective A-algebra which is locally a complete intersection over A. Then B is Gorenstein over A, which means that $B^\dagger$ is projective of rank 1 over B; cf. [6, E.16]. Moreover, if B is a complete intersection over A then $B^\dagger$ is free of rank 1 over B. Secondly, we have $\mathrm{Fit}_B(\Omega_{B/A}) = \mathrm{Ann}_B(\mathrm{Coker}\,\psi_{B/A}) = \mathrm{Fit}_B(\mathrm{Coker}\,\psi_{B/A})$. One can show these properties with [3, Prop. 1.1].

(2.5) Étale algebras. We say that a finite projective A-algebra B is *étale* if the following equivalent conditions hold:

(1) the map $\psi_{B/A}\colon B \to B^\dagger$ is an isomorphism;
(2) $\Omega_{B/A} = 0$;
(3) for all maximal ideals $\mathfrak{m}$ of A we have a $C_\mathfrak{m}$-algebra isomorphism $C_\mathfrak{m} \otimes_A B \cong C_\mathfrak{m} \times C_\mathfrak{m} \times \cdots \times C_\mathfrak{m}$, where $C_\mathfrak{m}$ is the algebraic closure of $A/\mathfrak{m}$.

Let us briefly sketch the proof that these statements are equivalent. Using the fact that $\Omega_{B/A}$ and $\psi_{B/A}$ are well-behaved under base change (cf. the proof of (2.6) below), and Nakayama's lemma, one first reduces to the case that A is a field, and then to the case that A is an algebraically closed field. Now B is a product of local Artin rings with residue field A, and we reduce to the case that B is local. Write $\mathfrak{m}$ for the maximal ideal of B. Note that the map $B \to B/(A + \mathfrak{m}^2) = \mathfrak{m}/\mathfrak{m}^2$ is a derivation, and that $\mathrm{Tr}_{B/A}(\mathfrak{m}) = 0$. Then deduce that all three statements are equivalent to $\mathfrak{m} = 0$.

(2.6) Proposition. *Let A be a noetherian ring with total ring of quotients $Q(A)$. For a finite projective A-algebra B the following are equivalent:*

(1) *the map $\psi_{B/A}\colon B \to B^\dagger$ is injective;*

(2) *$B \otimes_A Q(A)$ is étale over $Q(A)$;*

(3) *$\Omega_{B/A}$ is annihilated by a non-zero divisor of A;*

(4) *$\Omega_{B/A}$ is annihilated by a non-zero divisor of B.*

Recall that the total ring of quotients of A is the localization of A at the multiplicative set of non-zero divisors of A. We say B is *generically étale* over A if (1)–(4) hold. If A is a domain of characteristic zero, then a finite projective A-algebra B is generically étale if and only if it is reduced. In the remainder of this section we give the proof of (2.6). We start with a lemma in linear algebra.

(2.7) Lemma. *Let R be a noetherian ring, and let $f : P \to Q$ be an injection of finitely generated projective R-modules of the same constant rank $r \in \mathbb{Z}_{\geq 0}$. Then the following three statements are equivalent:*

(1) *f is injective;*

(2) *the induced map $\det f \colon \bigwedge^r P \to \bigwedge^r Q$ is injective;*

(3) *the induced map $f \otimes 1 \colon P \otimes_R Q(R) \to Q \otimes_R Q(R)$ is an isomorphism.*

Proof. The *associated primes* $\mathrm{Ass}(M)$ of an R-module M are those prime ideals $\mathfrak{p}$ of R for which $\mathfrak{p} = \mathrm{Ann}_R(x)$ for some $x \in M$. We show first that (1) is equivalent to

(4) for $\mathfrak{p} \in \mathrm{Ass}(R)$ the map $f_\mathfrak{p} \colon P_\mathfrak{p} \to Q_\mathfrak{p}$ of localizations is an isomorphism.

Assume that (1) holds. Suppose that $\mathfrak{p} \in \mathrm{Ass}(R)$, so $\mathfrak{p} = \mathrm{Ann}_R(x)$ for some $x \in R$. Clearly f injects xP to xQ. Since multiplication by x identifies $P/\mathfrak{p}P$ with xP and $Q/\mathfrak{p}Q$ with xQ, and since f commutes with multiplication by x, we deduce that the map $P/\mathfrak{p}P \to Q/\mathfrak{p}Q$ that one gets by reducing f modulo $\mathfrak{p}$ is injective. By localizing at $\mathfrak{p}$ we get an injection $P_\mathfrak{p}/\mathfrak{p}P_\mathfrak{p} \to Q_\mathfrak{p}/\mathfrak{p}Q_\mathfrak{p}$. But this is an injection of vector spaces of the same dimension, so it is an isomorphism. With Nakayama's lemma (4) follows.

Now assume that (4) holds and suppose that $V = \mathrm{Ker}\, f$ is not zero. By [8, Ch. X, 2.7] there exists a prime $\mathfrak{p} \in \mathrm{Ass}(V)$, so $\mathfrak{p} = \mathrm{Ann}_R(x)$ for some $x \in V$. Since V can be embedded in a finitely generated free R-module F we have $\mathrm{Ass}(V) \subset \mathrm{Ass}(F) = \mathrm{Ass}(R)$; see [8, Ch. X, 2.12]. But by (4) we then have $V_\mathfrak{p} = 0$, and in particular $ax = 0$ for some $a \in R - \mathfrak{p}$, which contradicts $\mathfrak{p} = \mathrm{Ann}_R(x)$. Thus $V = 0$, so (4) implies (1).

Using the fact that a matrix over a commutative ring is invertible if and only if its determinant is a unit, one sees that (4) is equivalent to the statement that $\det f_\mathfrak{p} \colon \bigwedge^r_{R_\mathfrak{p}} P_\mathfrak{p} \to \bigwedge^r_{R_\mathfrak{p}} Q_\mathfrak{p}$ is an isomorphism for all $\mathfrak{p} \in \mathrm{Ass}(R)$. Since exterior products commute with base change, and since we already have equivalence of (1) and (4), we conclude that (1) $\iff$ (2).

Since P and Q inject to $P \otimes_R Q(R)$ and $Q \otimes_R Q(R)$ it is clear that (3) implies (1).

We now assume (4) and we will show (3). We may assume that Q is free because $Q \oplus Q'$ is free for some projective R-module Q', and if we know (3) for the map $P \oplus Q' \xrightarrow{f \oplus 1} Q \oplus Q'$, then (3) follows for f. It suffices to show that the induced map

$\bigwedge^r P \otimes_R Q(R) \to \bigwedge^r Q \otimes_R Q(R)$ is an isomorphism, so we reduce to the case that $r = 1$ and Q is free. This means that f can be taken to be the inclusion of a projective R-ideal I of rank 1 in R. We have to show that I contains a non-zero divisor of R. One can infer this from a result of Auslander-Buchsbaum that we will need later (see the proof of (3.4)), but we will sketch an easier argument here. For every $\mathfrak{p} \in \mathrm{Ass}(A)$, our assumption says that $I_\mathfrak{p} = R_\mathfrak{p}$ and in particular this means that $I \not\subset \mathfrak{p}$. Since R is noetherian, the set $\mathrm{Ass}(R)$ is finite, and the union of all primes in $\mathrm{Ass}(R)$ is the set of zero divisors of R; see [8, Ch. X, 2.9]. Our non-zero divisor in I can now be produced with the following general fact, known as "prime avoidance."

(2.8) Lemma. *Let R be ring, let I be an R-ideal, and let $\mathcal{S}$ be a finite collection of R-ideals, none of which contain I. If at most two ideals in $\mathcal{S}$ are not prime then I contains an element that does not lie in any ideal in $\mathcal{S}$.*

For a proof see [11, Ex. 1.6] or [4, §3.2]. This finishes the proof of (2.7). □

(2.9) Remark. For the equivalence of (1) and (2) the noetherian hypothesis is not needed. One can see this by reducing to the noetherian case, or by using a matrix argument [11, Ex. 2.4(b)]. The implication (3) ⇒ (1) also holds without the noetherian condition, but its converse does not. To see this, one may consider the following example, which was pointed out to the author by H. W. Lenstra, Jr. Let A be a Dedekind domain that has a maximal ideal $\mathfrak{m}$ that generates an infinite cyclic subgroup of the class group. Now let $R = A \oplus V$ where $V^2 = 0$ and V is the A-module $\bigoplus_\mathfrak{p} A/\mathfrak{p}$ with the direct sum taken over all maximal ideals of A that are distinct from $\mathfrak{m}$. One verifies that $\mathfrak{m}R = \mathfrak{m} \otimes_A R$, by checking each summand of R. Now $\mathfrak{m}$ is projective of rank 1 as an A-module, so $\mathfrak{m}R$ is a projective R-ideal of rank 1. Yet, it does not contain a non-zero divisor, and in fact $R = Q(R)$.

Proof of (2.6). We first note that $\psi_{B/A}$ is compatible with base change. More precisely, for any A-algebra A' one can put $B' = B \otimes_A A'$ and the composite map

$$B' \xrightarrow{\psi_{B'/A'}} \mathrm{Hom}_{A'}(B', A') \xrightarrow{\sim} \mathrm{Hom}_A(B, A) \otimes_A A'$$

is equal to the map $\psi_{B/A} \otimes 1$. Taking $A' = Q(A)$ we see with (2.7) that $B \otimes_A Q(A)$ is étale over $Q(A)$ if and only if $\psi_{B/A}$ is injective. This shows equivalence of (1) and (2).

To see that (2) and (3) are equivalent, note that $\Omega_{B \otimes Q(A)/Q(A)} = \Omega_{B/A} \otimes_A Q(A)$. Since $\Omega_{B/A}$ is finitely generated as an A-module it follows that $\Omega_{B \otimes Q(A)/Q(A)} = 0$ if and only if (3) holds.

Since B is flat over A, multiplication on B by a non-zero divisor of A is injective, so (3) implies (4). Now let us suppose that (4) holds and show (3). We may assume that B

is of constant rank $r \geq 1$ over A, so that $A \subset B$. We know that $\Omega_{B/A}$ is annihilated by some non-zero divisor $x \in B$. The *norm* $N(x)$ of x is the unique element of A such that multiplication by x on B induces multiplication by $N(x)$ on $\bigwedge_A^r B$. With Lemma (2.7) one sees that $N(x)$ is a non-zero divisor of A. We claim that $N(x) = xy$ for some $y \in B$, so that $N(x)$ also annihilates $\Omega_{B/A}$. To see this, write $B' = B \otimes_A B$, which we view as a B-algebra via the first factor, and let φ be the B-algebra homomorphism $B' \to B$ given by $a \otimes b \mapsto ab$. Multiplication by $1 \otimes x$ on B' now induces induces multiplication by $N(x)$ on $\bigwedge_B^r B'$. Using the isomorphism $\bigwedge_B^r B' \cong (\bigwedge_B^{r-1} \operatorname{Ker} \varphi) \otimes_B (\bigwedge_B^1 B)$, one then sees that $N(x) = yx$, where $y \in B$ is the element such that $1 \otimes x$ induces multiplication by y on $\bigwedge_B^{r-1} \operatorname{Ker} \varphi$. □

3. Proof of the theorem

For any B-module M that can be generated by m elements we have

$$\operatorname{Ann}_B(M)^m \subset \operatorname{Fit}_B(M) \subset \operatorname{Ann}_B(M). \tag{3.1}$$

See [8, Ch. XIX, Prop. 2.5] for a proof. Taking $M = \Omega_{B/A}$ one sees that $\operatorname{Fit}_B(\Omega_{B/A})$ contains a non-zero divisor of B if and only if $\operatorname{Ann}_B(\Omega_{B/A})$ does. With (2.6) it follows that (3) and (4) of Theorem (1.1) are equivalent.

By Lemma (2.7) one sees that (2) implies (3). In the case that m-dim$(A) \leq 1$ the converse follows from the observation that m-dim$(B) \leq$ m-dim(A) (see (2.1)) and the following proposition, which was given by Lipman [10] for local rings.

(3.2) Lemma (Lipman). *Let R be a noetherian ring with* m-dim$(R) \leq 1$ *and let M be a finitely generated R-module. Then $\operatorname{Fit}_R(M)$ is free of rank 1 as an R-module if and only if for every $n \geq 0$ and every R-module surjection $R^n \xrightarrow{\varphi} M$ the kernel of φ is free of rank n.*

Proof. "If" is clear, because by (2.7) the determinant of an injective endomorphism of R^n is a non-zero divisor. So let us assume that $\operatorname{Fit}_R(M)$ is free of rank 1, and let $R^n \xrightarrow{\varphi} M$ be a surjection of R-modules. Let V be the kernel of φ, and view elements of V as column vectors. We need to show that V is free of rank n over R.

Let us assume first that R is local. The Fitting ideal $\operatorname{Fit}_R(M)$ is generated by the $n \times n$ determinants over R whose columns lie in V. Since R is local, and $\operatorname{Fit}_R(M)$ is principal, we can pick $v_1, \ldots, v_n \in V$ so that $\Delta = \det(v_1, \ldots, v_n)$ is a generator of $\operatorname{Fit}_R(M)$. Now consider the map $R^n \xrightarrow{\alpha} R^n$ that sends $(a_i)_{i=1}^n$ to $a_1 v_1 + \cdots + a_n v_n$. This map is injective, because its determinant Δ is a non-zero divisor. By Cramer's rule, every $x \in R^n$ satisfies $\Delta x = \Delta_1 v_1 + \cdots + \Delta_n v_n$ where $\Delta_i = \det(v_1, \ldots, v_{i-1}, x, v_{i+1}, \ldots, v_n)$.

If $x \in V$ then $\Delta_i \in \mathrm{Fit}_R(M) = \Delta R$, and since Δ is a non-zero divisor it then follows that $x \in Rv_1 + \cdots + Rv_n$. Thus, α is an isomorphism $R^n \xrightarrow{\sim} V$.

Now let us drop the assumption that R is local. We know by the local case that V is locally free of rank n, and since R is noetherian this means that V is a projective R-module. Assume that $n \geq 1$. By Serre's theorem (2.1) we can write V as a direct sum of a free submodule F of rank $n-1$ and a projective submodule P of rank 1. If $w_1, \ldots, w_{n-1}$ is an R-basis of F, then the map $P \to \mathrm{Fit}_R(M)$, sending x to $\det(w_1, \ldots, w_{n-1}, x)$, is surjective. By Nakayama's lemma this map must be an isomorphism locally, so it is an isomorphism. Thus, P is free of rank 1, and V is free of rank n. □

Note that the noetherian condition was not used in the proof of the local case.

It remains to show that (1) and (2) in Theorem (1.1) are equivalent. For sufficiently large n we can write $B = R/I$ with $R = A[X_1, \ldots, X_n]$ and I an R-ideal. By the "second fundamental exact sequence" [11, Th. 25.2] we then have an exact sequence of B-modules

(3.3) $$I/I^2 \to \Omega_{R/A} \otimes_R B \to \Omega_{B/A} \to 0.$$

Since $\Omega_{R/A}$ is a free R-module of rank n, the B-module $\Omega_{R/A} \otimes_R B$ is free of rank n.

Suppose that statement (1) of (1.1) holds. Then we can choose our presentation of B as an A-algebra in such a way that I is an R-ideal generated by n elements. This means that we have a B-module surjection $B^n \to I/I^2$. Thus one gets an exact sequence

$$B^n \xrightarrow{\varphi} B^n \longrightarrow \Omega_{B/A} \longrightarrow 0$$

and we have $\mathrm{Fit}_B(\Omega_{B/A}) = (\det \varphi)B$. Since B is generically étale over A, the B-ideal $\mathrm{Ann}_B(\Omega_{B/A})$ contains a non-zero divisor of B, and by (3.1) it follows that $\det \varphi$ is a non-zero divisor of B. Therefore, φ is injective and (2) follows.

Let us now assume (2) and show (1). By tensoring the sequence in (2) with $Q(A)$ we see with (2.7) that $\Omega_{B/A} \otimes_A Q(A) = 0$, so that B is generically étale over A.

Let X be the image of I/I^2 in $B \otimes_R \Omega_{R/A} \cong B^n$ under the map in sequence (3.3) above. With the sequence in (2) Schanuel's lemma [8, Ch. XXI, Lemma 2.4] implies that $X \oplus F \cong F \oplus B^n$. Therefore X is projective over B of rank n.

If α_i denotes the image of X_i in B then the Koszul complex of the regular sequence $X_1 - \alpha_1, \ldots, X_n - \alpha_n$ in $B[X_1, \ldots, X_n]$ is a finite resolution of B with projective R-modules; see [8, Ch. XXI, Th. 4.6]. An R-module M that has such a resolution is said to be *of finite projective dimension*. We will need two basic properties of this notion: a direct summand of a module of finite projective dimension is again of finite projective dimension, and secondly, if two out of three modules in a short exact sequence are of finite projective dimension, then so is the third. One can see this from the fact that a module M over a ring R is of finite projective dimension if and only if there is an integer d such that for all $k > d$ and all R-modules N we have $\mathrm{Ext}^k_R(M, N) = 0$; see [11, Appendix B]. By considering the exact sequence $0 \to I \to R \to B \to 0$ of R-modules, we conclude that I is an R-ideal of finite projective dimension.

In order to show that the map $I/I^2 \to X$ is an isomorphism we will use a result of Vasconcelos [14], which we now state in the form that is most convenient for our application.

(3.4) Proposition (Vasconcelos). *Let R be a noetherian local ring and let I be an R-ideal of finite projective dimension over R. Put $S = R/I$, and suppose that we have an S-linear surjection $I/I^2 \xrightarrow{\varphi} V$ for some free S-module V of rank $n = \dim R - \dim S$. Then φ is an isomorphism.*

Proof. We will use two basic facts: first, if x is neither a zero divisor nor a unit in a noetherian local ring R then $\dim R/xR = \dim R - 1$; see [1, 11.18]. Secondly, such an element x can often be shown to exist with a proposition of Auslander and Buchsbaum [2, Prop. 3.9]: in a noetherian ring every non-zero ideal of finite projective dimension contains a non-zero divisor. A short proof of this fact can also be found in Matsumura [11, Th. 19.8].

It is clear that (3.4) holds if $I = 0$, so assume that $I \neq 0$. We may also assume that $I \neq R$. By Auslander-Buchsbaum, I contains a non-zero divisor x of R. Putting $R' = R/xR$ and $I' = I/xR \subset R'$, we then have $S = R'/I'$ and $\dim R' - \dim S = n - 1$. If $n = 0$ then we get a contradiction, so (3.4) holds for $n = 0$.

For $n \geq 1$ we proceed with induction to n. Write $V \cong S \oplus V'$ and let π be projection on the first factor. Let f be the composition of surjections $I \longrightarrow I/I^2 \xrightarrow{\varphi} V \xrightarrow{\pi} S$. Consider the collection $\mathcal{S} = \mathrm{Ass}(R) \cup \{f^{-1}(\mathfrak{m}_S)\}$ of R-ideals, where $\mathfrak{m}_S$ is the maximal ideal of S. By (2.8) our non-zero divisor x in I can be chosen in such a way that $f(x) \notin \mathfrak{m}_S$. The restriction of f to xR then induces an isomorphism $xR/xI \xrightarrow{\sim} S$.

It follows that the short exact sequence $0 \to xR/xI \to I/xI \to I' \to 0$ splits, with the splitting map $I/xI \xrightarrow{f} S \xrightarrow{\sim} xR/xI$. This implies that I' is a direct summand of $I/xI = I \otimes_R R'$, so it has finite projective dimension over R'. Tensoring the split exact sequence over R with S we get an exact sequence $0 \to xR/xI \to I/I^2 \to I'/(I')^2 \to 0$. By the induction hypothesis the map $I'/(I')^2 = I/(xR + I^2) \to V/\varphi(xR) = V'$ is an isomorphism. It follows that φ is an isomorphism too. □

We continue the proof of the implication (2) ⇒ (1) of Theorem (1.1). Suppose that

$\mathfrak{m}$ is a maximal ideal of R containing I. Then the localization $I_\mathfrak{m}$ is an ideal of finite projective dimension in $R_\mathfrak{m}$. The pull-back $\mathfrak{m}_A$ of $\mathfrak{m}$ to A is a maximal ideal of A because B is integral over A; see [1, 5.8]. Since both R and B are flat over A one sees with [11, Th. 15.1] that

$$\dim R_\mathfrak{m} = \dim A_{\mathfrak{m}_A} + \dim R_\mathfrak{m}/\mathfrak{m}_A R_\mathfrak{m};$$
$$\dim B_\mathfrak{m} = \dim A_{\mathfrak{m}_A} + \dim B_\mathfrak{m}/\mathfrak{m}_A B_\mathfrak{m}.$$

Putting $k = A/\mathfrak{m}_A$ one sees that $B \otimes_A k$ is artinian so its localization $B_\mathfrak{m}/\mathfrak{m}_A B_\mathfrak{m}$ has dimension zero. The ring $R_\mathfrak{m}/\mathfrak{m}_A R_\mathfrak{m} = k[X_1, \ldots, X_n]_\mathfrak{m}$ has dimension n; see [11, Ex. 5.1] or [4, §13]. We are now in the situation that $\dim R_\mathfrak{m} = n + \dim R_\mathfrak{m}/I_\mathfrak{m}$ and we know that $X_\mathfrak{m}$ is free of rank n over $R_\mathfrak{m}/I_\mathfrak{m}$. This means that we can apply (3.4) and conclude that the surjection $I_\mathfrak{m}/I_\mathfrak{m}^2 \to X_\mathfrak{m}$ is an isomorphism. Since this holds for all maximal ideals $\mathfrak{m}$ of R that contain I, it follows that the map $I/I^2 \to X$ is an isomorphism.

We now proceed as in Mohan Kumar [7]. Let m be the B-rank of F and consider the ring $R' = R[Y_1, \ldots, Y_m]$ with the ideal $I' = IR' + (Y_1, \ldots, Y_m)$ then $R'/I' = B$ and $I'/(I')^2 \cong X \oplus F \cong F \oplus B^n \cong B^{n+m}$. Take $n + m$ elements f_i in I' that generate I'/I'^2 as a B-module and let J be the R'-ideal generated by the f_i. Now I'/J is an ideal in R'/J that is equal to its own square. With the determinant trick [1, 2.5] it follows that it is generated by an idempotent $e \bmod J$ with $e \in R'$, so that we have a product-decomposition of rings $R'/J = R'/I' \times I'/J$. But then $B = R'/I' = R'[Z]/(J, (1-e)Z - 1)$, so we have now written B as an A-algebra with the same number of generators and relations. This finishes the proof of Theorem (1.1). □

(3.5) Remark. In the proof of the implication (2) $\Rightarrow$ (1) we needed $n + m + 1$ generators to write B as a complete intersection algebra over A, where n is the minimal number of algebra generators of B over A and m is the rank of the module F in (2). If m-dim$(A) \leq 1$ then m-dim$(B) \leq 1$, so by (2.1) the B-module I/I^2 in the proof is free, and we need only $n + 1$ generators.

References

1. M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass., 1969.
2. M. Auslander, D. A. Buchsbaum, *Homological dimension in local rings*, Trans. Amer. Math. Soc. **85** (1957), 390–405.
3. B. de Smit, H. W. Lenstra, Jr., *Finite complete intersection algebras and the completeness radical*, in preparation.
4. D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Math. **150**, Springer-Verlag, New York, 1994.
5. R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math. **52**, Springer-Verlag, New York, 1977.
6. E. Kunz, *Kähler differentials*, F. Vieweg, Braunschweig, 1986.
7. N. Mohan Kumar, *Complete intersections*, J. Math. Kyoto Univ. **17** (1977), 533–538.
8. S. Lang, *Algebra*, 3rd ed., Addison-Wesley, Reading, Mass., 1993.
9. H. W. Lenstra, Jr., *Complete intersections and Gorenstein rings*, pp. 99–109 in: J. Coates, S. T. Yau (eds), *Elliptic curves, modular forms, and Fermat's Last Theorem*, International Press, Boston, 1995.
10. J. Lipman, *On the Jacobian ideal of the module of differentials*, Proc. Amer. Math. Soc. **21** (1969), 422–426.
11. H. Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986.
12. J.-P. Serre, *Local fields*, Graduate Texts in Math. **67**, Springer-Verlag, New York, 1979.
13. J.-P. Serre, *Modules projectifs et espaces fibrés à fibre vectorielle*, Seminaire Dubreil-Pisot 1957/58 no. 23; pp. 531–543 in: *Collected Papers*, Vol. I, Springer-Verlag, Berlin, 1986.
14. W.V. Vasconcelos, *Ideals generated by R-sequences*, J. Algebra **6** (1967), 309–316.