Conference on Elliptic Curves and Modular Forms
Hong Kong, December 18-21, 1993

Complete intersections and Gorenstein rings

H.W. LENSTRA, JR.
DEPARTMENT OF MATHEMATICS # 3840
UNIVERSITY OF CALIFORNIA, BERKELEY, CA 94720–3840 USA
E-mail address: HWL@MATH.BERKELEY.EDU

This paper is devoted to the proof of the following fact from commutative algebra, which is a slight sharpening of a result of Wiles. Let $\mathcal{O}$ be a complete discrete valuation ring, R a complete noetherian local $\mathcal{O}$-algebra, B a finite flat local $\mathcal{O}$-algebra, and $\varphi: R \to B$, $\pi: B \to \mathcal{O}$ surjective $\mathcal{O}$-algebra homomorphisms. Suppose that the length of the $\mathcal{O}$-module $(\ker \pi\varphi)/(\ker \pi\varphi)^2$ is finite and bounded by the length of $\mathcal{O}/\pi(\mathrm{Ann}_B \ker \pi)$. Then φ is an isomorphism and B is a complete intersection.

We prove the following fact from commutative algebra, due to Wiles in the case that B is a Gorenstein ring.

Theorem. *Let $\mathcal{O}$ be a complete discrete valuation ring, R a complete noetherian local $\mathcal{O}$-algebra, B a finite flat local $\mathcal{O}$-algebra, and $\varphi: R \to B$, $\pi: B \to \mathcal{O}$ surjective $\mathcal{O}$-algebra homomorphisms. Then the following are equivalent.*

(i) *the length of the $\mathcal{O}$-module $(\ker \pi\varphi)/(\ker \pi\varphi)^2$ is finite and less than or equal to the length of $\mathcal{O}/\pi(\mathrm{Ann}_B \ker \pi)$;*

(ii) *the length of the $\mathcal{O}$-module $(\ker \pi\varphi)/(\ker \pi\varphi)^2$ is finite and equal to the length of $\mathcal{O}/\pi(\mathrm{Ann}_B \ker \pi)$,*

(iii) *B is a complete intersection, $\pi(\mathrm{Ann}_B \ker \pi) \neq 0$, and φ is an isomorphism.*

The terms are explained below

Rings are supposed to be commutative with 1. For the basic definitions from commutative algebra we refer to [**1**]. We write $\mathfrak{m}_R$ for the maximal ideal of a local ring R. By $\mathcal{O}$ we shall always denote a complete discrete valuation ring; the completeness assumption can be dropped, except where complete intersections are involved (this is mostly due to the naïve nature of our definition of a complete intersection below).

Finite flat. We shall call an $\mathcal{O}$-algebra *finite flat* if it is finitely generated and free as an $\mathcal{O}$-module. This is equivalent to it being finitely generated and *flat* as an $\mathcal{O}$-module, which is an easy fact that we shall not need (cf. [**1**], Exercise 7.16).

Key words one-dimensional local ring, complete intersection, congruence ideal
1991 Mathematics subject classification 13H10 The author thanks B. de Smit, B. Mazur, and R. Pink for their assistance and comments He was supported by NSF under grant No DMS 92-24205 Part of the work reported in this paper was done while the author was on appointment as a Miller Research Professor in the Miller Institute for Basic Research in Science

For a finitely generated free $\mathcal{O}$-module M we shall put $M^\dagger = \operatorname{Hom}_{\mathcal{O}}(M, \mathcal{O})$; this is an autoduality of the category of finitely generated free $\mathcal{O}$-modules.

Local $\mathcal{O}$-algebras. A *local* $\mathcal{O}$-algebra is an $\mathcal{O}$-algebra B that is local as a ring and for which the structure map $\mathcal{O} \to B$ maps $\mathfrak{m}_{\mathcal{O}}$ inside $\mathfrak{m}_B$.

Gorenstein rings. A finite flat local $\mathcal{O}$-algebra B is called *Gorenstein* if $B^\dagger$ is free of rank 1 as a B-module. This is *not* a relative notion: there is an absolute notion of "Gorenstein ring" that is equivalent to the given one for finite flat local algebras over a discrete valuation ring (see [**3**], Section 18), and which we will not need.

Complete intersections. Let B be a finite flat local $\mathcal{O}$-algebra that has the same residue class field as $\mathcal{O}$. The latter condition means that the natural map $\mathcal{O}/\mathfrak{m}_{\mathcal{O}} \to B/\mathfrak{m}_B$ is an isomorphism; it is satisfied if there is an $\mathcal{O}$-algebra homomorphism $B \to \mathcal{O}$, which is the case in the Theorem. We call B a *complete intersection* if, for some non-negative integer n, there are elements $f_1, \ldots, f_n \in \mathcal{O}[[X_1, \ldots, X_n]]$ (the two n's are the same!) such that $B \cong \mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n)$ as $\mathcal{O}$-algebras. Again, this is *not* a relative notion: there is an absolute notion of "complete intersection" that is equivalent to the given one for finite flat local algebras over a complete discrete valuation ring with the same residue class field (see [**3**], Section 21). We will not need this fact. What we do need about complete intersections is summarized in the following lemma.

Lemma 1. *Let n be a non-negative integer and $f_1, \ldots, f_n \in \mathcal{O}[[X_1, \ldots, X_n]]$. Suppose that $B = \mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n)$ is finitely generated and non-zero as an $\mathcal{O}$-module. Then B is a finite flat local $\mathcal{O}$-algebra with the same residue class field as $\mathcal{O}$, it is Gorenstein, and $B^\dagger$ has a B-generator λ with the property that the trace map $\operatorname{Tr}_{B/\mathcal{O}}: B \to \mathcal{O}$ is given by $\operatorname{Tr}_{B/\mathcal{O}} = d \cdot \lambda$, where d is the image of $\det\left(\frac{\partial f_i}{\partial X_j}\right)_{i,j}$ in B.*

Proof (sketch). Let $\pi_{\mathcal{O}}$ be a prime element of $\mathcal{O}$. For the first statement, it suffices to check that $f_1, \ldots, f_n, \pi_{\mathcal{O}}$ is a "regular" $\mathcal{O}[[X_1, \ldots, X_n]]$-sequence. One way to do this is by means of the "Koszul-complex" ([**3**], Theorem 16.8). Once one knows about regular sequences and the Koszul complex, one can prove the remaining statements by means of an argument due to Tate ([**4**], Appendix). □

A more general version of Lemma 1, in which $\mathcal{O}$ is allowed to be any noetherian ring, is proved in [**2**]. The main tool in the proof is again the Koszul complex.

The congruence ideal. Let B, C be rings and let $\pi: B \to C$ be a surjective ring homomorphism. Then the *congruence ideal* η_π of π is defined to be the C-ideal $\pi(\operatorname{Ann}_B \ker \pi)$, where $\operatorname{Ann}_B \ker \pi$ denotes the annihilator of $\ker \pi$ in B.

The terminology is explained by the following example. Let C, D be rings with ideals I, J, and suppose that an isomorphism $C/I \cong D/J$ is given. Put $B = C \times_{C/I} D = \{(x, y) \in C \times D : x \text{ and } y \text{ have the same image in } C/I\}$, and let $\pi: B \to C$ be the first projection. Then $\ker \pi = \{0\} \times J$, and if $\operatorname{Ann}_D J = 0$ then $\operatorname{Ann}_B \ker \pi = I \times \{0\}$ so that $\eta_\pi = I$. Since the elements of B are defined by means of a congruence mod I (more precisely, an equality in C/I), the ideal I may indeed be called a "congruence ideal".

The definition can be reformulated as follows. View C as a B-algebra via π. Then there is an isomorphism $\mathrm{Hom}_B(C,B) \cong \mathrm{Ann}_B \ker\pi$ sending f to $f(1)$, so η_π is just the image of the map $\mathrm{Hom}_B(C,B) \to \mathrm{Hom}_B(C,C) \cong C$ induced by π.

If $\eta_\pi = C$ then the sequence $0 \to \ker\pi \to B \to C \to 0$ of B-modules splits, so that B becomes a product of two rings. Hence if B and C are local, then one has $\eta_\pi = C$ if and only if π is an isomorphism. A "relative" version of this statement will, under additional hypotheses, be proved below (Lemma 3).

Suppose now that B is a flat $\mathcal{O}$-algebra and that $\pi\colon B \to \mathcal{O}$ is an $\mathcal{O}$-algebra homomorphism (necessarily surjective) with $\eta_\pi \neq 0$. We prove that

$$(\ker\pi) \cap (\,\mathrm{Ann}_B \ker\pi) = 0, \tag{2}$$

so that the surjective map $\mathrm{Ann}_B \ker\pi \to \eta_\pi$ given by π is actually an isomorphism. Let $x \in (\ker\pi)\cap(\,\mathrm{Ann}_B\ker\pi)$, choose $a \in \eta_\pi$, $a \neq 0$, and write $a = \pi(b)$ with $b \in \mathrm{Ann}_B \ker\pi$. Then we have $ax = (a-b)x = 0$, the first equality because $b \in \mathrm{Ann}_B\ker\pi$ and $x \in \ker\pi$, and the second because $a - b \in \ker\pi$ and $x \in \mathrm{Ann}_B\ker\pi$. Since B is flat, multiplication by a is injective, so $x = 0$, as required.

Gorenstein rings and the congruence ideal. Suppose that B and C are finite flat local $\mathcal{O}$-algebras that are Gorenstein, and let $\pi\colon B \to C$ be a surjective $\mathcal{O}$-algebra homomorphism. Choosing isomorphisms $B \cong B^\dagger$, $C \cong C^\dagger$ of B-modules we find that $\mathrm{Hom}_B(C,B) \cong_B \mathrm{Hom}_B(C^\dagger, B^\dagger)$. The latter module is, by duality, isomorphic to $\mathrm{Hom}_B(B,C)$, which is easily seen to be generated by the map π. Thus η_π is a principal C-ideal, generated by the image of π under the map $\mathrm{Hom}_B(B,C) \cong \mathrm{Hom}_B(C,B) \to C$. This can be used as an alternative definition of the congruence ideal in the Gorenstein situation.

Lemma 3. *Let A and B be finite flat local $\mathcal{O}$-algebras, and let $\varphi\colon A \to B$, $\pi\colon B \to \mathcal{O}$ be surjective $\mathcal{O}$-algebra homomorphisms. Suppose that A is Gorenstein and that $\eta_{\pi\varphi} = \eta_\pi \neq 0$. Then φ is an isomorphism.*

Proof. One easily checks that φ induces a map $\mathrm{Ann}_A \ker\pi\varphi \to \mathrm{Ann}_B\ker\pi$. Applying (2) to π and to $\pi\varphi$ we find that π and $\pi\varphi$ induce isomorphisms $\mathrm{Ann}_B\ker\pi \to \eta_\pi$ and $\mathrm{Ann}_A\ker\pi\varphi \to \eta_{\pi\varphi}$. Thus from $\eta_{\pi\varphi} = \eta_\pi$ it follows that $\mathrm{Ann}_A\ker\pi\varphi \to \mathrm{Ann}_B\ker\pi$ is an isomorphism as well, and that $\varphi\,\mathrm{Ann}_A\ker\pi\varphi = \mathrm{Ann}_B\ker\pi$. Therefore we have

$$A/(\ker\varphi + \mathrm{Ann}_A\ker\pi\varphi) \cong \varphi A/\varphi\,\mathrm{Ann}_A\ker\pi\varphi = B/\,\mathrm{Ann}_B\ker\pi,$$

which is free as an $\mathcal{O}$-module since $B/\,\mathrm{Ann}_B\ker\pi$ can be viewed as a submodule of $\mathrm{End}_{\mathcal{O}}\ker\pi$. Also, applying (2) to $\pi\varphi$ we obtain

$$\ker\varphi \cap \mathrm{Ann}_A\ker\pi\varphi \subset \ker\pi\varphi \cap \mathrm{Ann}_A\ker\pi\varphi = 0.$$

We conclude that there is an exact sequence of A-modules

$$0 \to \ker\varphi \oplus \mathrm{Ann}_A\ker\pi\varphi \to A \to B/\,\mathrm{Ann}_B\ker\pi \to 0$$

consisting of finitely generated free $\mathcal{O}$-modules. Dualizing, we obtain an exact sequence of A-modules

$$0 \to (B/\operatorname{Ann}_B \ker\pi)^\dagger \to A^\dagger \to (\ker\varphi)^\dagger \oplus (\operatorname{Ann}_A \ker\pi\varphi)^\dagger \to 0.$$

Since A is supposed to be Gorenstein, we have $A^\dagger \cong_A A$. Tensoring with the residue class field k of A we find that $\dim_k(A^\dagger \otimes_A k) = 1$. By the exact sequence, this implies that one of $\dim_k((\ker\varphi)^\dagger \otimes_A k)$ and $\dim_k((\operatorname{Ann}_A \ker\pi\varphi)^\dagger \otimes_A k)$ is 0. Hence by Nakayama's lemma and duality one of $\ker\varphi$ and $\operatorname{Ann}_A \ker\pi\varphi$ is 0. But $\operatorname{Ann}_A \ker\pi\varphi \cong \eta_{\pi\varphi} \neq 0$, so $\ker\varphi = 0$ and φ is an isomorphism. □

The condition that A be Gorenstein cannot be omitted in Lemma 3. This is shown by the example $A = \{(x,y,z) \in \mathcal{O} \times \mathcal{O} \times \mathcal{O} : x \equiv y \equiv z \bmod \mathfrak{m}_{\mathcal{O}}\}$, $B = \{(x,y) \in \mathcal{O} \times \mathcal{O} : x \equiv y \bmod \mathfrak{m}_{\mathcal{O}}\}$, $\varphi((x,y,z)) = (x,y)$, $\pi((x,y)) = x$, in which $\eta_{\pi\varphi} = \eta_\pi = \mathfrak{m}_{\mathcal{O}}$. The ring B in this example is Gorenstein (even a complete intersection).

Intermezzo on the Fitting ideal. Let B be a ring and let M be a finitely generated B-module, with generators $m_1, \ldots, m_r$. Let $f\colon B^r \to M$ map $(b_i)_{i=1}^r$ to $\sum_i b_i m_i$. Then the *Fitting ideal* $F_B M$ is the B-ideal generated by all elements of B of the form $\det(v_1, \ldots, v_r)$, with $v_1 \in \ker f, \ldots, v_r \in \ker f$ (viewed as column vectors); evidently, it suffices to let the v_i range over a set of *generators* for $\ker f$. The Fitting ideal is independent of the choice of the generators m_i. To see this, let $m_{r+1} = \sum_{i=1}^r c_i m_i$, with $c_i \in B$. One obtains generators for the kernel of $f'\colon B^{r+1} \to M$, $f'((b_i)_{i=1}^{r+1}) = \sum_{i=1}^{r+1} b_i m_i$, by taking generators for $\ker f$ (with a zero coordinate appended) together with the element $(-c_1, \ldots, -c_r, 1)$. The latter element will have to occur in any non-zero determinant built up from these generators of $\ker f'$. It follows that the Fitting ideal does not change if the system of generators $m_1, \ldots, m_r$ is changed into $m_1, \ldots, m_r, m_{r+1}$. Inductively, this implies that any two systems $m_1, \ldots, m_r$ and $m_1', \ldots, m_s'$ of generators give rise to the same Fitting ideal as their union $m_1, \ldots, m_r, m_1', \ldots, m_s'$.

We need three properties of the Fitting ideal. The first is

$$F_B M \subset \operatorname{Ann}_B M. \tag{4}$$

Namely, if $\sum_{j=1}^r v_{ij} m_j = 0$ for $1 \le i \le r$, then "multiplying by the adjoint" we see that $\det(v_{ij})$ annihilates each m_j and therefore M. Secondly, we have

$$F_C(M \otimes_B C) = \pi(F_B M) \tag{5}$$

when $\pi\colon B \to C$ is a surjective ring homomorphism. This is because $M \otimes_B C$ is, as a C-module, defined by the 'same' relations as those that define M as a B-module.

Thirdly, for $B = \mathcal{O}$ the Fitting ideal just measures the length: if M is a finitely generated $\mathcal{O}$-module, then $F_{\mathcal{O}} M = \mathfrak{m}_{\mathcal{O}}^{\text{length } M}$ (if M does not have finite length, interpret the right side to be 0). To prove this, one writes M as a direct sum of cyclic modules $\mathcal{O}/I_i$ and checks that $F_{\mathcal{O}} M$ is the product of the ideals I_i.

The congruence ideal and $(\ker\pi)/(\ker\pi)^2$. Let B and C be rings and let $\pi\colon B \to C$ be a surjective ring homomorphism for which $\ker\pi$ is finitely generated. Then $(\ker\pi)/(\ker\pi)^2$ is a C-module, and one has

$$F_C((\ker\pi)/(\ker\pi)^2) \subset \eta_\pi \subset \operatorname{Ann}_C((\ker\pi)/(\ker\pi)^2). \tag{6}$$

Namely, we have $F_B(\ker\pi) \subset \mathrm{Ann}_B \ker\pi \subset \mathrm{Ann}_B((\ker\pi)/(\ker\pi)^2)$, the first inclusion by (4) and the second one trivially. Now apply π. By (5) and $\mathrm{Ann}_B((\ker\pi)/(\ker\pi)^2) = \pi^{-1}\,\mathrm{Ann}_{\mathcal{O}}((\ker\pi)/(\ker\pi)^2)$ this gives (6).

In the case that is of interest to us, the first inclusion of (6) can be found in [**5**], Proposition 6.2, with a rather more complicated proof.

Complete intersections and the congruence ideal. Let B be a finite flat local $\mathcal{O}$-algebra, let $\pi\colon B \to \mathcal{O}$ be an $\mathcal{O}$-algebra map, and suppose that B is a complete intersection. Then we have

$$F_{\mathcal{O}}((\ker\pi)/(\ker\pi)^2) = \eta_\pi. \tag{7}$$

This is proved by an explicit computation. Let $B = \mathcal{O}[[X_1, \dots, X_n]]/(f_1, \dots, f_n)$. The images b_j of X_j in B belong to $\mathfrak{m}_B$, and replacing X_j by $X_j - \pi(b_j)$ we may assume that $b_j \in \ker\pi$ Then $f_i(0) = 0$ for all i. To describe the $\mathcal{O}$-module $(\ker\pi)/(\ker\pi)^2$, one considers the ideal $\mathfrak{p}$ of $\mathcal{O}[[X_1, \dots, X_n]]$ generated by $X_1, \dots, X_n$, then $\mathfrak{p}/\mathfrak{p}^2$ is $\mathcal{O}$-free of rank n, and $(\ker\pi)/(\ker\pi)^2$ is $\mathfrak{p}/\mathfrak{p}^2$ modulo the submodule spanned by the images of $f_1, \dots, f_n$. The definition of the Fitting ideal now gives

$$F_{\mathcal{O}}((\ker\pi)/(\ker\pi)^2) = \mathcal{O}\det\Bigl(\frac{\partial f_i}{\partial X_j}(0)\Bigr)_{i,j} = \mathcal{O}\pi(d),$$

with d as in Lemma 1. To prove (7), it suffices, by (6), to prove the inclusion $\supset$. Let $x \in \eta_\pi$, and write $x = \pi(y)$ with $y \in \mathrm{Ann}_B \ker\pi$. By Lemma 1, we can choose $\lambda \in B^\dagger$ with $\mathrm{Tr}_{B/\mathcal{O}} = d\lambda$. From $\pi(d) - d \in \ker\pi$ we see that $(\pi(d) - d)y = 0$, so $\pi(d)\lambda(y) = (d\lambda)(y) = \mathrm{Tr}_{B/\mathcal{O}}(y)$. The trace of y can be computed from the action of y on the exact sequence $0 \to \ker\pi \to B \to \mathcal{O} \to 0$, and one finds that $\mathrm{Tr}_{B/\mathcal{O}}(y) = \pi(y) = x$. Therefore $x = \pi(d)\lambda(y) \in \mathcal{O}\pi(d) = F_{\mathcal{O}}((\ker\pi)/(\ker\pi)^2)$, as required.

The following result shows that one can recognize isomorphisms to complete intersections by looking at $(\ker\pi)/(\ker\pi)^2$.

Lemma 8. *Let R be a complete noetherian local $\mathcal{O}$-algebra, let B be a finite flat local $\mathcal{O}$-algebra, and let $\varphi\colon R \to B$, $\pi\colon B \to \mathcal{O}$ be surjective $\mathcal{O}$-algebra homomorphisms. Suppose that B is a complete intersection, that the map $(\ker\pi\varphi)/(\ker\pi\varphi)^2 \to (\ker\pi)/(\ker\pi)^2$ induced by φ is an isomorphism, and that these modules are of finite length over $\mathcal{O}$ Then φ is an isomorphism.*

Proof. Let n, f_i and the elements $b_j \in \ker\pi$ be as above, so that $\sum_j a_{ij}b_j \in (\ker\pi)^2$, where $a_{ij} = \frac{\partial f_i}{\partial X_j}(0)$. Since $(\ker\pi)/(\ker\pi)^2$ is of finite length we have $\det(a_{ij}) \neq 0$. Choose $r_j \in R$ with $\varphi(r_j) = b_j$. The hypothesis of the lemma implies that $r_1, \dots, r_n$ generate $\ker\pi\varphi$ modulo $(\ker\pi\varphi)^2$, so by Nakayama's lemma they generate $\ker\pi\varphi$. Hence together with $\mathfrak{m}_{\mathcal{O}}$ they generate $\mathfrak{m}_R$, so that there is a surjective $\mathcal{O}$-algebra map $\psi\colon \mathcal{O}[[X_1, \dots, X_n]] \to R$ sending X_j to r_j. The hypothesis of the lemma implies that $\sum_j a_{ij}r_j \in (\ker\pi\varphi)^2$, so there are $g_i \in \ker\psi$ with $\frac{\partial g_i}{\partial X_j}(0) = a_{ij}$. We have $g_i \in \ker\varphi\psi = (f_1, \dots, f_n)$ and therefore $g_i = \sum_l h_{il}f_l$, with $h_{il} \in \mathcal{O}[[X_1, \dots, X_n]]$. From $a_{ij} = \frac{\partial g_i}{\partial X_j}(0) =$

$\sum_l h_{il}(0)\frac{\partial f_l}{\partial X_j}(0) = \sum_l h_{il}(0)a_{lj}$ and $\det(a_{ij}) \neq 0$ we see that $(h_{il}(0))$ is the identity matrix. This implies that the matrix (h_{il}) is invertible, so that $f_l \in \ker\psi$. Hence the map ψ factors through B and gives a map $B \to R$ that is inverse to φ. This proves the lemma. □

We need one more technical result before we can prove the Theorem.

Lemma 9. *Let B be a finite flat local $\mathcal{O}$-algebra, and let $\pi\colon B \to \mathcal{O}$ be an $\mathcal{O}$-algebra homomorphism. Then there is a finite flat local $\mathcal{O}$-algebra A, together with a surjective $\mathcal{O}$-algebra homomorphism $\varphi\colon A \to B$, such that A is a complete intersection and the map $(\ker\pi\varphi)/(\ker\pi\varphi)^2 \to (\ker\pi)/(\ker\pi)^2$ induced by φ is an isomorphism.*

Proof. Let $b_1, \dots, b_n$ generate $\ker\pi$. We first prove that $\mathcal{O}[b_1, \dots, b_n] = B$. Let $C = \mathcal{O}[b_1, \dots, b_n]$. Since B is finite over C the ring C is local, and its maximal ideal $\mathfrak{m}_C = \mathfrak{m}_B \cap C$ contains $b_1, \dots, b_n$. Clearly C is Noetherian. We have $B = \mathcal{O} + \ker\pi = \mathcal{O} + (\sum_j Bb_j) \subset C + \mathfrak{m}_C \cdot B$, so Nakayama's lemma implies that $C = B$.

The surjective B-linear map $B^n \to \ker\pi$ sending $(c_j)_{j=1}^n$ to $\sum_j c_j b_j$ gives upon tensoring with $\mathcal{O}$ a surjective map $\mathcal{O}^n \to (\ker\pi)/(\ker\pi)^2$. Choose generators $(a_{ij})_{j=1}^n$, $i = 1, \dots, n$, for the kernel of the latter map. This can be done, since every submodule of $\mathcal{O}^n$ is generated by n elements. For each i we have $\sum_j a_{ij}b_j \in (\ker\pi)^2$, so $g_i(b_1, \dots, b_n) = 0$ for some polynomial $g_i \in \mathcal{O}[X_1, \dots, X_n]$ of the form $g_i = (\sum_j a_{ij}X_j) +$ (terms of degree ≥ 2); here, and below, "degree" means "total degree".

Since B is finite over $\mathcal{O}$, there is a non-negative integer m with the property that the expressions $\prod_j b_j^{m_j}$ of degree $\sum_j m_j \leq m$ span B as an $\mathcal{O}$-module. Enlarging m, if necessary, we can achieve that each g_i has degree at most $m+2$. Write $b_i^{m+1} = h_i(b_1, \dots, b_n)$, where $h_i \in \mathcal{O}[X_1, \dots, X_n]$ has degree at most m. We define

$$f_i = X_i^{m+3} - X_i^2 h_i + g_i \in \mathcal{O}[X_1, \dots, X_n] \qquad (1 \leq i \leq n).$$

Evidently, we have

$$\begin{gathered} f_i(b_1, \dots, b_n) = 0, \\ f_i = X_i^{m+3} + (\text{terms of degree} \leq m+2), \\ f_i = \sum_j a_{ij}X_j + (\text{terms of degree} \geq 2) \end{gathered}$$

for $1 \leq i \leq n$.

Put $D = \mathcal{O}[X_1, \dots, X_n]/(f_1, \dots, f_n)$. Then there is a surjective $\mathcal{O}$-algebra map $\psi\colon D \to B$ sending the image of X_j to b_j. Each monomial of degree greater than $n(m+2)$ in $X_1, \dots, X_n$ is divisible by X_i^{m+3} for some i, so is modulo f_i congruent to an $\mathcal{O}$-linear combination of monomials of smaller degrees. This implies that the monomials of degree at most $n(m+2)$ span D as an $\mathcal{O}$-module, so that D is finite over $\mathcal{O}$. Since $\mathcal{O}$ is complete, it follows that D is a product of complete local rings: $D = \prod_{\mathfrak{n}} D_{\mathfrak{n}}$, where $\mathfrak{n}$ ranges over the maximal ideals of D; to see this, write for each positive integer t the Artin ring $D/\mathfrak{m}_{\mathcal{O}}^t D$ as a product of local rings (see [**1**], Theorem 8.7), and take the projective limit over t. One of these maximal ideals is the image of the maximal ideal $\mathfrak{m} = (\mathfrak{m}_{\mathcal{O}}, X_1, \ldots, X_n)$ of $\mathcal{O}[X_1, \ldots, X_n]$ in D; so we have $D = D' \times D_{\mathfrak{m}}$, where $\mathfrak{m}D' = D'$ and $D_{\mathfrak{m}}$ is complete. Thus, if we complete at $\mathfrak{m}$ then the equality $D = \mathcal{O}[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ turns into $D_{\mathfrak{m}} = \mathcal{O}[[X_1, \ldots, X_n]]/(f_1, \ldots, f_n)$, and the surjection $\psi\colon D \to B$ turns into a surjection $\varphi\colon D_{\mathfrak{m}} \to B$. By Lemma 1 it follows that $D_{\mathfrak{m}}$ is a complete intersection. From $f_i = \sum_j a_{ij} X_j +$ (terms of degree ≥ 2) we see that the kernel of the surjective map $\mathcal{O}^n \to (\ker \pi\varphi)/(\ker \pi\varphi)^2$ that sends $(c_j)_{j=1}^n$ to the image of $\sum_j c_j X_j$ is generated by the elements $(a_{ij})_{j=1}^n$, $i = 1, \ldots, n$. This implies that the map $(\ker \pi\varphi)/(\ker \pi\varphi)^2 \to (\ker \pi)/(\ker \pi)^2$ induced by φ is an isomorphism. The lemma follows, with $A = D_{\mathfrak{m}}$. □

Corollary 10. *Let B be a finite flat local $\mathcal{O}$-algebra, and let $\pi\colon B \to \mathcal{O}$ be an $\mathcal{O}$-algebra homomorphism with $\eta_\pi \neq 0$. Then B is a complete intersection if and only if $F_{\mathcal{O}}((\ker \pi)/(\ker \pi)^2) = \eta_\pi$.*

Proof. "Only if" we know from (7). To prove "if", we choose $\varphi\colon A \to B$ as in Lemma 9. Then we have

$$\eta_{\pi\varphi} = F_{\mathcal{O}}((\ker \pi\varphi)/(\ker \pi\varphi)^2) = F_{\mathcal{O}}((\ker \pi)/(\ker \pi)^2) = \eta_\pi,$$

the first equality by (7), the second from Lemma 9, and the last by hypothesis. Lemma 1 asserts that A is Gorenstein. Now apply Lemma 3. □

We prove the Theorem. The implication (iii)⇒(ii) is immediate from (7) and the second inclusion of (6), and (ii)⇒(i) is clear. To prove (i)⇒(iii), we note that

$$\eta_\pi \subset F_{\mathcal{O}}((\ker \pi\varphi)/(\ker \pi\varphi)^2) \subset F_{\mathcal{O}}((\ker \pi)/(\ker \pi)^2) \subset \eta_\pi,$$

the first inclusion by the hypothesis in (i), the second because there is a surjective map $(\ker \pi\varphi)/(\ker \pi\varphi)^2 \to (\ker \pi)/(\ker \pi)^2$, and the third by (6). We conclude that we have equality everywhere. The finite length hypothesis in (i) now implies that $\eta_\pi \neq 0$, so Corollary 10 shows that B is a complete intersection. Lemma 8, finally shows that φ is an isomorphism. This completes the proof of the Theorem.

REMARK. R. Pink pointed out that Lemma 1, of which we only sketched the proof, can be bypassed entirely. To do this one verifies the conclusion of Lemma 1 and the equality (7) directly for the only ring to which it needs to be applied, namely the ring A constructed in the proof of Lemma 9. One proceeds as follows.

One starts by proving that the $\mathcal{O}$-algebra $D = \mathcal{O}[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ constructed in the proof of Lemma 9 has the two following properties: first, D is free of rank $(m+3)^n$ as an $\mathcal{O}$-module, the images of the monomials $\prod_{i=1}^n X_i^{k_i}$ with $0 \leq k_i \leq m+2$ forming a basis; and, second, the D-module

$D^\dagger = \mathrm{Hom}_{\mathcal{O}}(D, \mathcal{O})$ is free of rank 1, a basis being formed by the linear map $\lambda\colon D \to \mathcal{O}$ that sends the monomial $\prod_{i=1}^{n} X_i^{m+2}$ to 1 and the other basis elements to 0. The proof of these properties is a straightforward verification that exploits the shape of the relations f_i. It follows that D is Gorenstein. From $D = D' \times A$ it follows that A is Gorenstein as well.

Next one studies $\eta_{\pi\psi}$, where $\psi\colon D \to B$ is as in the proof of Lemma 9. Since D is Gorenstein, one has $\mathrm{Ann}_D(\ker \pi\psi) = \mathrm{Hom}_D(\mathcal{O}, D) \cong \mathrm{Hom}_D(D, \mathcal{O}) = \mathcal{O} \cdot \pi\psi$, which shows that $\mathrm{Ann}_D(\ker \pi\psi)$ is free of rank 1 over $\mathcal{O}$. To exhibit a generator, one writes $f_i = \sum_{j=1}^{n} f_{ij} X_j$, where the polynomials f_{ij} are such that $f_{ii} - X_i^{m+2}$ and f_{ij} (for $i \neq j$) have degree at most $m+1$. From (4), with $M = \ker \pi\psi$, one sees that $\det(f_{ij})$ belongs to $\mathrm{Ann}_D(\ker \pi\psi)$, and it is in fact a generator of $\mathrm{Ann}_D(\ker \pi\psi)$ since $\lambda(\det(f_{ij})) = 1$. Applying $\pi\psi$ one finds that $\eta_{\pi\psi}$ is generated by $\det(a_{ij})$. This is the same as saying that $F_{\mathcal{O}}((\ker \pi\psi)/(\ker \pi\psi)^2) = \eta_{\pi\psi}$. Passing to A one concludes that $F_{\mathcal{O}}((\ker \pi\varphi)/(\ker \pi\varphi)^2) = \eta_{\pi\varphi}$.

Now that one knows the Gorenstein property and equality (7) for the complete intersections constructed in Lemma 9 one can pass to the more general case of Corollary 10. That is, if B and π are as in Corollary 10, *then B is a complete intersection if and only if B is a complete intersection and Gorenstein, and if and only if $F_{\mathcal{O}}((\ker \pi)/(\ker \pi)^2) = \eta_\pi$*. To prove this, suppose that B has one of these properties, and let $\varphi\colon A \to B$ be as in Lemma 9. Since A is known to have all three properties, it suffices to show that φ is an isomorphism. In the case that $F_{\mathcal{O}}((\ker \pi)/(\ker \pi)^2) = \eta_\pi$ this is done as in the proof of Corollary 10 given above. In the other cases B is a complete intersection, so φ is an isomorphism by Lemma 8; note that $(\ker \pi)/(\ker \pi)^2$ has finite length by the second inclusion of (6).

In all our results we assumed that the finite flat local $\mathcal{O}$-algebra B is provided with an $\mathcal{O}$-algebra homomorphism $\pi\colon B \to \mathcal{O}$. Similar results can be proved for more general finite flat $\mathcal{O}$-algebras B. The role of π can then be played by the multiplication map $\mu\colon B \otimes_{\mathcal{O}} B \to B$, which is defined by $\mu(b_1 \otimes b_2) = b_1 b_2$, and the role of the base ring $\mathcal{O}$ is taken over by B. As an example, we prove the following proposition, which was suggested by B. Mazur. Recall that the module $\Omega_{B/\mathcal{O}}$ of Kähler differentials is defined to be the B-module $(\ker \mu)/(\ker \mu)^2$ (see [**3**], Section 25).

Proposition. *Let B be a finite flat local $\mathcal{O}$-algebra that has the same residue class field as $\mathcal{O}$, and denote by μ the multiplication map $B \otimes_{\mathcal{O}} B \to B$. Suppose that the B-module $\Omega_{B/\mathcal{O}}$ has finite length. Then B is a complete intersection if and only if the congruence ideal η_μ is principal and equal to $F_B(\Omega_{B/\mathcal{O}})$.*

We note that the finite length condition for $\Omega_{B/\mathcal{O}}$ is equivalent to the K-algebra $B \otimes_{\mathcal{O}} K$ being étale, where K is the field of fractions of $\mathcal{O}$; if K has characteristic 0, then it equivalent to the nil-radical of B being zero.

The proof of the Proposition is analogous to the proof of Corollary 10. We go through the changes that need to be made.

For the "only if" part, suppose that $B \cong \mathcal{O}[[X_1, \dots, X_n]]/(f_1, \dots, f_n)$ as $\mathcal{O}$-algebras. Since B is finite flat over $\mathcal{O}$, there is a B-algebra isomorphism $\mathcal{O}[[X_1, \dots, X_n]] \otimes_{\mathcal{O}} B \cong B[[X_1, \dots, X_n]]$. This implies that we have $B \otimes_{\mathcal{O}} B \cong$

$B[[X_1,\dots,X_n]]/(f_1,\dots,f_n)$ as B-algebras, where $B\otimes_{\mathcal{O}}B$ is viewed as a B-algebra via the second factor. As in the first half of the proof of (7) one now checks that $F_B(\Omega_{B/\mathcal{O}})$ equals the principal ideal $B\cdot d$, where d is as in Lemma 1. The equality $\mathrm{Tr}_{B/\mathcal{O}}=d\lambda$ from Lemma 1 implies that $\mathrm{Tr}_{B\otimes B/B}=(d\otimes 1)(\lambda\otimes 1)$. This is used to show that $\eta_\mu\subset B\cdot d$, as in the second half of the proof of (7). Hence the inclusion $\eta_\mu\subset F_B(\Omega_{B/\mathcal{O}})$ holds, and by (6) one has equality. This proves the "only if" part.

The proof of the "if" part depends on the following generalization of Lemma 3. Let a finite flat local algebra over a noetherian local ring C be defined in the same way as for $C=\mathcal{O}$.

Lemma 11. *Let C be a one-dimensional local noetherian ring, let A and B be finite flat local C-algebras, and let $\varphi\colon A\to B$, $\pi\colon B\to C$ be surjective C-algebra homomorphisms. Suppose that* $\mathrm{Hom}_C(A,C)$ *is free of rank* 1 *as an A-module, that $\eta_{\pi\varphi}=\eta_\pi$, and that η_π is free of rank* 1 *as a C-module. Then φ is an isomorphism.*

Proof. If $\eta_\pi=C$ then $\pi\varphi$ and π are both isomorphisms, so φ is an isomorphism as well. For the rest of the proof we assume that $\eta_\pi\neq C$, so that $\eta_\pi\subset\mathfrak{m}_C$. Since η_π is C-free of rank 1, we have $\eta_\pi=Ca$, where a is a non-zero-divisor of C. The proof of (2) now carries through. Hence π induces an isomorphism $\mathrm{Ann}_B\ker\pi\to\eta_\pi$.

Let $\mathfrak{p}$ be a minimal prime ideal of C. Then $C_\mathfrak{p}$ is an Artin ring, and $(\eta_\pi)_\mathfrak{p}$ is a $C_\mathfrak{p}$-ideal that is free of rank 1. Since $C_\mathfrak{p}$ has finite length as a module over itself, this implies that $(\eta_\pi)_\mathfrak{p}=C_\mathfrak{p}$, so $\eta_\pi\not\subset\mathfrak{p}$. Because C is one-dimensional, this implies that the only prime ideal of the ring C/η_π is $\mathfrak{m}_C/\eta_\pi$. It follows that C/η_π is a local Artin ring. Therefore there exists $c\in C$, $c\notin\eta_\pi$, such that $c\mathfrak{m}_C\subset\eta_\pi$.

Next we prove that $B/\,\mathrm{Ann}_B\ker\pi$ is free as a C-module. Write $I=\mathrm{Ann}_B\ker\pi$, so that $I\cong\eta_\pi$ Both B and I are C-free, so it suffices to prove that a basis for I can be supplemented to a basis for B. By Nakayama's lemma, this can be done if the natural map $I/\mathfrak{m}_CI\to B/\mathfrak{m}_CB$ is injective, i.e., if $\mathfrak{m}_CI=I\cap\mathfrak{m}_CB$. Let $x\in I\cap\mathfrak{m}_CB$. Then $cx\in I\cap c\mathfrak{m}_CB\subset I\cap\eta_\pi B=I\cap aB$. Since a acts as a non-zero-divisor on the free C-module B, it follows from the definition of I that $I\cap aB=aI$, which equals $\eta_\pi I$. Hence x is an element of I with $cx\in\eta_\pi I$. Since I is C-free and $c\notin\eta_\pi$, this implies that $x\in\mathfrak{m}_CI$, as required.

Once (2) and the fact that $B/\,\mathrm{Ann}_B\ker\pi$ is C-free are known, the proof that we gave for Lemma 3 generalizes easily to a proof for Lemma 11. □

Let now B and μ be as in the Proposition, and suppose that the congruence ideal η_μ is principal and equal to $F_B(\Omega_{B/\mathcal{O}})$. We wish to prove that B is a complete intersection.

View $B\otimes_{\mathcal{O}}B$ as a B-algebra via the second factor. We start by constructing a finite flat local B-algebra A of the form $A=B[[X_1,\dots,X_n]]/(f_1,\dots,f_n)$ together with a surjective B-algebra homomorphism $\varphi\colon A\to B\otimes_{\mathcal{O}}B$ for which the induced map $(\ker\mu\varphi)/(\ker\mu\varphi)^2\to(\ker\mu)/(\ker\mu)^2$ is an isomorphism. This is done as in the proof of Lemma 9, with $B \otimes_{\mathcal{O}} B$, μ, and B in the roles of B, π, and $\mathcal{O}$. There are two changes.

First, we need a new argument, in the second paragraph, to show that the kernel of any surjective B-linear map $f\colon B^n \to (\ker \mu)/(\ker \mu)^2$ is generated by n elements. This depends on the hypothesis that the ideal $F_B((\ker \mu)/(\ker \mu)^2)$ is *principal*, say with generator a. Since the module $(\ker \mu)/(\ker \mu)^2$ is supposed to be of finite length, its Fitting ideal contains a power of a prime element of $\mathcal{O}$, and therefore a is not a zero-divisor. This implies that $F_B((\ker \mu)/(\ker \mu)^2)$ is B-free of rank 1. By Nakayama's lemma, any set of generators for $F_B((\ker \mu)/(\ker \mu)^2)$ contains a basis, so one can choose the element a to be of the form $\det(v_1, \dots , v_n)$, where $v_1, \dots , v_n \in \ker f$. Let $v \in \ker f$, and replace, for some $1 \le i \le n$, the ith column of the matrix $(v_1, \dots , v_n)$ by v. The determinant of the resulting matrix belongs to $F_B((\ker \mu)/(\ker \mu)^2)$, and is therefore equal to $b_i a$ for some uniquely determined $b_i \in B$. One now verifies in a straightforward way that $v = \sum_{i=1}^{n} b_i v_i$ ("Cramer's rule"), so that $v_1, \dots , v_n$ span $\ker f$.

Second, we need a new proof that A is finite flat as a B-algebra. For this one can apply a version of Lemma 1 that is valid for general base rings (as in [**2**]), or one uses R. Pink's argument that we sketched above. In the same way one proves that $\operatorname{Hom}_B(A, B)$ is A-free of rank 1 and that the analogue of (7) is valid for A, that is, $F_B((\ker \mu\varphi)/(\ker \mu\varphi)^2) = \eta_{\mu\varphi}$.

Having constructed A, one shows that the map

$$\varphi\colon A = B[[X_1, \dots , X_n]]/(f_1, \dots , f_n) \to B \otimes_{\mathcal{O}} B$$

is an isomorphism of B-algebras. To do this one simply copies the proof of Corollary 10, replacing Lemma 3 by Lemma 11 (applied to $B \otimes_{\mathcal{O}} B$ and B in the roles of B and C).

We now know that B becomes a "relative complete intersection" after base extension with itself. To finish the proof of the Proposition we descend to $\mathcal{O}$.

Let, generally, C be a complete local noetherian ring, and R a complete local noetherian C-algebra with the same residue class field k as C. Then there exists m *such that* $C[[X_1, \dots , X_m]]$ has an ideal J for which $R \cong C[[X_1, \dots , X_m]]/J$ as C-algebras. The minimal number of generators of the ideal J equals $\dim_k J/\mathfrak{m}J$, where $\mathfrak{m}$ denotes the maximal ideal of $C[[X_1, \dots , X_m]]$. The number $m - \dim_k J/\mathfrak{m}J$ only depends on the C-algebra R, and not on the presentation $R \cong C[[X_1, \dots , X_m]]/J$; this is proved by a straightforward argument, which resembles the proof, given above, that the Fitting ideal is well-defined. Write $\epsilon(R, C) = m - \dim_k J/\mathfrak{m}J$. If D is a finite flat local C-algebra, then one readily verifies that $\epsilon(R \otimes_C D, D) = \epsilon(R, C)$.

With $C = \mathcal{O}$, $D = R = B$ we now find that $\epsilon(B, \mathcal{O}) = \epsilon(B \otimes_{\mathcal{O}} B, B) \ge 0$, the inequality coming from the isomorphism $B[[X_1, \dots , X_n]]/\ (f_1, \dots , f_n) \cong B \otimes_{\mathcal{O}} B$. It follows that there exist m and $g_1, \dots , g_m \in \mathcal{O}[[X_1, \dots , X_m]]$ such that $\mathcal{O}[[X_1, \dots , X_m]]/(g_1, \dots , g_m) \cong B$ as $\mathcal{O}$-algebras. Hence B is a complete intersection. (One actually has $\epsilon(B, \mathcal{O}) = 0$, by [**3**], Theorem 21.1.) This completes the proof of the Proposition. □

Remark. Under the hypotheses of the Proposition, B is actually a complete intersection if and only if the Fitting ideal $F_B(\Omega_{B/\mathcal{O}})$ is principal. This can be deduced from Theorem 9.5 in E. Kunz, *Kähler differentials* (Vieweg, Braunschweig, 1986).

References

[1] M. F. Atiyah, I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass., 1969.

[2] B. de Smit, H. W. Lenstra, Jr., *Finite complete intersection algebras*, Report 9453/B, Econometric Institute, Erasmus University Rotterdam, The Netherlands, 1994.

[3] H. Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986.

[4] B. Mazur, L. Roberts, *Local Euler characteristics*, Invent. Math. **9** (1970), 201–234.

[5] J. Tilouine, *Théorie d'Iwasawa classique et de l'algèbre de Hecke ordinaire*, Compositio Math. **65** (1988), 265–320.