

# Monogenous Algebras. Back to Kronecker.

Daniel Ferrand

October 17, 2003

## Introduction

In this note we develop some properties of those  $A$ -algebras  $B$  which can be generated by a single element after, if need be, some faithfully flat base change  $A \rightarrow A'$ . Here they are called *locally simple*, instead of the less euphonious "monogenous". For a finite algebra this condition is satisfied as soon as the geometric fibers are single generator algebras. This property appears to be commonly satisfied. In particular the morphisms between rings of algebraic integers are locally simple.

A theme we insist on expands an idea Kronecker introduced at the early beginning of the algebraic theory of numbers, namely that many properties of a finite free  $A$ -algebra  $B$  can be read through the characteristic polynomial of the *generic* element of  $B$ . To be precise, let  $e_1, \dots, e_n$  be a basis of  $B$  as an  $A$ -module, and denote  $S = A[T_1, \dots, T_n]$ . The generic element, which may be written as  $\sum T_i e_i \in S \otimes_A B = B[T_1, \dots, T_n]$ , is a root of its characteristic polynomial  $F(X) \in S[X]$ . Therefore we dispose of a canonical morphism, called here the *Kronecker morphism*

$$S[X]/(F) \rightarrow S \otimes_A B.$$

We show that this morphism is universally injective if and only if  $B$  is locally simple over  $A$ .

In the context of rings of algebraic integers the idea of Kronecker was introduced and used by Hilbert in his *Zahlbericht*. We finally interpret some results of this famous memoir from the point of view previously introduced.

*In this note, all the rings are assumed to be commutative and to possess a unit element, and all the ring morphisms are assumed to map unit element to unit element.*

## 1. Locally simple morphisms.

**Definition 1.1** *A morphism  $A \rightarrow B$  between rings is called simple if  $B$  can be generated, as an  $A$ -algebra, by a single element, in other words if there exists a surjective morphism of  $A$ -algebras  $A[X] \rightarrow B$ .*

*A morphism  $A \rightarrow B$  is called locally simple if there exists a faithfully flat morphism  $A \rightarrow A'$  such that  $A' \rightarrow A' \otimes_A B$  is simple.*

Below we will give some specific properties of these morphisms. Let us first recall how crucial they are to the theory of the norm functor (see [F]). With any finite and locally free morphism  $A \rightarrow B$  of rank  $d$  is associated a covariant functor

$$N_{B/A} : B - \mathbf{Mod} \longrightarrow A - \mathbf{Mod},$$

which extends the usual one defined for invertible  $B$ -modules  $L$  (roughly speaking, by taking the norm of a cocycle of  $L$ ). One has  $N_{B/A}(B) = A$  but this functor is far from being additive. Let  $F$  be a locally free  $B$ -module of rank  $n$ . If  $B$  is locally simple over  $A$  then  $N_{B/A}(F)$  is a locally free  $A$ -module of rank  $n^d$ . But, in general, this  $A$ -module may have torsion, even if  $B$  is a complete intersection over  $A$  (see [F] 4.3.4 and 4.4).

**Examples 1.2** Consider a ring  $A$  and the diagonal morphism  $A \rightarrow A^n$ . An element  $x = (x_1, \dots, x_n) \in A^n$  is a generator of that  $A$ -algebra if and only if the powers  $1, x, x^2, \dots, x^{n-1}$  form a basis of the  $A$ -module  $A^n$ . Writing down these powers in the canonical basis of  $A^n$ , one sees that  $x$  is a generator of the  $A$ -algebra  $A^n$  if and only if the Van der Monde determinant

$$\prod_{i < j} (x_j - x_i)$$

is invertible in  $A$ .

The existence of a sequence  $(x_1, \dots, x_n)$  with this property is clear if  $A$  contains an infinite field. It is also clear that such a sequence cannot exist if  $A$  is too small; thus,  $\mathbb{F}_p \rightarrow \mathbb{F}_p^n$  is *not* simple if  $n > p$ . This remark, when  $p = 2$ , implies that  $\mathbb{Z} \rightarrow \mathbb{Z}^n$  is *not* simple if  $n \geq 3$ .

On the other hand, there is a canonical way to adjoin to any ring  $A$  a sequence of  $n$  elements  $(x_1, \dots, x_n)$  making the Van der Monde determinant invertible. Just take the ring of fractions  $A' = A[X_1, \dots, X_n]_V$ , where  $V = \prod_{i < j} (X_j - X_i)$  and, for  $x_i$ , take the image in  $A'$  of  $X_i$ ; the morphism  $A \rightarrow A'$  is faithfully flat (and smooth), and the morphism  $A' \rightarrow A'^n$  is simple; thus for any  $n$  and any ring  $A$ , the morphism  $A \rightarrow A^n$  is locally simple.

A slight generalization implies that any finite étale morphism  $A \rightarrow B$  is locally simple, because it is locally of the form  $A \rightarrow A^n$ .

**Example 1.3** More generally, let  $A$  be a ring, and let  $B_1, \dots, B_s$  be a sequence of finite and locally simple  $A$ -algebras. The product  $B_1 \times \dots \times B_s$  is locally simple over  $A$ .

To see this, it is enough, by induction on  $s$ , to prove the result for two factors which we now denote by  $B$  and  $C$ . Let us choose generators  $b \in B$  and  $c \in C$  and monic polynomials  $P(T)$  and  $Q(T)$  in  $A[T]$  such that  $P(b) = 0$  and  $Q(c) = 0$ ; one then has a surjective morphism

$$A[T]/(P) \times A[T]/(Q) \rightarrow B \times C,$$

and it is enough to prove that the product  $A[T]/(P) \times A[T]/(Q)$  is locally simple over  $A$ . Consider the ring of fractions  $A' = A[X]_{R(X)}$  where we have made invertible the *resultant* ([A] IV 6.6)

$$R(X) = \text{res}_T(P(T+X), Q(T)).$$

Let  $x$  be the image of  $X$  in  $A'$ . The standard property of the resultant (see e.g [A] IV 6.6 Cor.1 to Prop. 7), implies that the polynomials  $P(T+x)$  and  $Q(T)$  are co-maximal in  $A'[T]$  (i.e. they generate the unit ideal). Therefore, the "Chinese remainder theorem" shows that the morphism

$$A'[T] \longrightarrow A'[T]/(P(T+x)) \times A'[T]/(Q(T))$$

is surjective. Moreover, the  $A'$ -algebras  $A'[T]/(P(T))$  and  $A'[T]/(P(T+x))$  are clearly isomorphic. Therefore, it remains to show that the morphism  $A \rightarrow A'$  is faithfully flat. Since this morphism is clearly flat we have to show that any prime ideal  $\mathfrak{p}$  of  $A$  is the restriction of a prime ideal of  $A'$ . Let  $A \rightarrow K$  be the morphism of  $A$  to an algebraic closure  $K$  of the residue field  $\kappa(\mathfrak{p})$ ; it is enough to see that this morphism factors through  $A'$ . Let us consider the images in  $K[T]$  of the two monic

polynomials  $P(T)$  and  $Q(T)$ . Since  $K$  is algebraically closed these polynomials split, and we can translate the roots of  $P(T)$  away from those of  $Q(T)$ . Thus, there exists  $x \in K$  such that  $P(T+x)$  and  $Q(T)$  have no common root, i.e. such that the resultant  $R(x)$  is non zero in  $K$ . This element  $x$  gives rise to the required morphism  $A' = A[X]_{R(X)} \rightarrow K$ .

**Proposition 1.4** *Let  $B$  be a finite  $A$ -algebra. The following conditions are equivalent:*

- i) *The morphism  $A \rightarrow B$  is locally simple.*
- ii) *There exists a morphism  $A \rightarrow A'$  such that  $A' \rightarrow A' \otimes_A B$  is simple, and such that  $\text{Spec}(A') \rightarrow \text{Spec}(A)$  surjective (i.e the flatness of the base change is superfluous).*
- iii) *For any morphism  $A \rightarrow K$  where  $K$  is an algebraically closed field, each local factor of  $K \otimes_A B$  is a simple  $K$ -algebra.*
- iv) *For any prime ideal  $\mathfrak{p}$  of  $A$ , there exists a finite extension  $\kappa(\mathfrak{p}) \rightarrow k$  such that  $k \otimes_A B$  is simple over  $k$ .*

Recall that a finite algebra  $R$  over a field is the direct product of the local rings  $R_{\mathfrak{m}}$ , where  $\mathfrak{m}$  runs through the (finite) set of the maximal ideals; these local rings are called the *local factors* of  $R$ .

The ingredients used in the following proof all come from EGA IV, but, for the convenience of the reader, I will give some details instead of scattered references.

**Lemma 1.4.1** *Let  $A \rightarrow B$  be a finite morphism. We suppose an  $A$ -algebra  $A \rightarrow E$  exists with the property that  $E \otimes_A B$  is simple over  $E$ . Then, there exists a sub- $A$ -algebra  $F \subset E$  of finite type such that  $F \otimes_A B$  is simple over  $F$ .*

Proof : Let  $x = \sum_{i=1}^n x_i \otimes b_i \in E \otimes_A B$  be a generator as  $E$ -algebra; the sub- $A$ -algebra  $E' = A[x_1, \dots, x_n] \subset E$  is of finite type. Let us consider the morphism

$$E'[X] \longrightarrow E' \otimes_A B,$$

which maps  $X$  to  $x$ ; its cokernel  $M$  is an  $E'$ -module of finite type, as  $E' \otimes_A B$  is, and we have  $E \otimes_{E'} M = 0$ . We shall enlarge  $E'$  inside  $E$  in order to get a finite type algebra  $F$  such that  $F \otimes_{E'} M = 0$ . By induction on the number of generators of  $M$ , (and by looking at the *quotients* of  $M$ ) we are reduced to the case where  $M$  is monogenous, i.e where  $M$  is isomorphic to a quotient  $E'/I$ . The hypothesis,  $E \otimes_{E'} M = 0$ , reads then as  $E = IE$ , i.e as a relation:  $1 = \sum_{j=1}^m a_j y_j$  with  $a_j \in I$  and  $y_j \in E$ . This relation is already true in the  $A$ -algebra of finite type  $E'[y_1, \dots, y_m]$ .

**Lemma 1.4.2** *Let  $\mathfrak{p}$  be a prime ideal in a ring  $A$ , and let  $\kappa(\mathfrak{p}) \rightarrow k$  be a finite field extension. There exist  $t \in A - \mathfrak{p}$ , a finite free morphism  $A_t \rightarrow C$  and an isomorphism  $\kappa(\mathfrak{p}) \otimes_A C \xrightarrow{\sim} k$ .*

Proof : We write  $S = A - \mathfrak{p}$ . By induction on the number of generators of the  $\kappa(\mathfrak{p})$ -algebra  $k$ , we are reduced to proving the following.

Let  $A_t \rightarrow C$  be a finite free morphism such that  $k = \kappa(\mathfrak{p}) \otimes_A C$  is a field, and let  $k \rightarrow k' = k[x]$  be a finite *simple* field extension. Then there exist  $s \in S$  and a finite free morphism  $C_s \rightarrow C'$  such that  $\kappa(\mathfrak{p}) \otimes_A C' \simeq k'$ .

In fact, let  $F(X) \in S^{-1}C[X]$  be a monic polynomial whose image modulo  $\mathfrak{p}$  is the minimal polynomial of  $x$  (such a polynomial  $F$  exists because the morphism  $S^{-1}C \rightarrow S^{-1}C/\mathfrak{p}S^{-1}C \simeq k$  is surjective). If  $s \in S$  denotes the product of the denominators of the coefficients of  $F$ , one has  $F \in C_s[X]$ . The morphism

$$A_{st} \rightarrow C_s \rightarrow C' = C_s[X]/(F)$$

is then free, and one gets an isomorphism  $\kappa(\mathfrak{p}) \otimes_A C' \simeq k'$ .

Proof of the proposition. It is clear that *i*) implies *ii*). Let us prove that *ii*) implies *iii*). Let  $A'$  be an  $A$ -algebra such that  $A' \otimes_A B$  is generated by one element and such that the map  $\text{Spec}(A') \rightarrow \text{Spec}(A)$  is surjective. By the above lemma 1.4.1 there exists a sub- $A$ -algebra  $F \subset A'$ , of finite type, such that  $F \otimes_A B$  is simple over  $F$ . Let  $A \rightarrow K$  be a morphism where  $K$  is an algebraically closed field, and denote by  $\mathfrak{p}$  its kernel. By hypothesis, the prime ideal  $\mathfrak{p}$  is the restriction to  $A$  of a prime ideal  $\mathfrak{p}'$  of  $A'$ ; it is also the restriction of the prime ideal  $\mathfrak{q} = \mathfrak{p}' \cap F$  of  $F$ , therefore  $\kappa(\mathfrak{p}) \otimes_A F \neq 0$ . Then, as  $K$  is algebraically closed, the "Hilbert Nullstellensatz" ([AC] V 3.3 Prop.1) implies that the given morphism  $\kappa(\mathfrak{p}) \rightarrow K$  factors through  $\kappa(\mathfrak{p}) \otimes_A F$ , i.e. that  $A \rightarrow K$  factors through  $F$ .

$$\begin{array}{ccccc} A & \longrightarrow & F & \longrightarrow & F \otimes_A B \\ \downarrow & & \downarrow & & \downarrow \\ \kappa(\mathfrak{p}) & \longrightarrow & K & \longrightarrow & K \otimes_A B \end{array}$$

But the morphism  $F \rightarrow F \otimes_A B$  is simple. Therefore, the  $K$ -algebra  $K \otimes_A B$  is simple, and a fortiori each of its factors is.

*iii*)  $\Rightarrow$  *iv*). Let  $K$  be an algebraic closure of a residue field  $\kappa(\mathfrak{p})$  of  $A$ . By the hypothesis *iii*) and the example 1.3, the  $K$ -algebra  $K \otimes_A B$  is simple; by lemma 1.4.1, there exists a finite sub-extension  $k \subset K$  such that  $k \otimes_A B$  is a simple  $k$ -algebra.

*iv*)  $\Rightarrow$  *i*). Suppose first we have already shown that for each prime ideal  $\mathfrak{p}$  of  $A$  there exist an element  $t \in A - \mathfrak{p}$  and a finite free morphism  $A_t \rightarrow C$  such that  $C \rightarrow C \otimes_A B$  is simple.

Then the image of the morphism  $\text{Spec}(C) \rightarrow \text{Spec}(A)$  is the open set  $D(t)$ , and it contains  $\mathfrak{p}$ . As  $\text{Spec}(A)$  is quasi-compact, a finite number of such morphisms  $A \rightarrow C_i, i = 1, \dots, n$ , are enough for covering  $\text{Spec}(A)$ . Hence we can take  $A' = C_1 \times \dots \times C_n$ ; it is faithfully flat over  $A$ , and  $A' \rightarrow A' \otimes_A B$  is simple.

It remains to prove the existence of those required morphisms  $A_t \rightarrow C$ . So let  $\mathfrak{p}$  be a prime ideal in  $A$ . According to *iv*), there exists a finite extension  $\kappa(\mathfrak{p}) \rightarrow k$  such that  $k \rightarrow k \otimes_A B$  is simple. By lemma 1.4.2, one can choose a  $t \in S = A - \mathfrak{p}$ , a finite free morphism  $A_t \rightarrow C$  and an isomorphism  $\kappa(\mathfrak{p}) \otimes_A C \xrightarrow{\sim} k$ . The morphism  $C \rightarrow \kappa(\mathfrak{p}) \otimes_A C \simeq k$  is the composite of the surjection  $S^{-1}C \rightarrow S^{-1}(C/\mathfrak{p}C)$  and of the localization  $C \rightarrow S^{-1}C$ . Then, a generator  $\xi$  of  $k \otimes_A B = S^{-1}(C/\mathfrak{p}C) \otimes_A B$  may be lifted as an element  $x \in S^{-1}(C \otimes_A B)$ . It is a generator of the  $S^{-1}C$ -algebra  $S^{-1}(C \otimes_A B)$ .

$$\begin{array}{ccccc} S^{-1}C & \longrightarrow & S^{-1}C[x] & \longrightarrow & S^{-1}C \otimes_A B \\ \downarrow & & \downarrow & & \downarrow \\ k & \longrightarrow & k[\xi] & \xlongequal{\quad} & k \otimes_A B \end{array}$$

In fact the cokernel of the injective map  $S^{-1}C[x] \hookrightarrow S^{-1}(C \otimes_A B)$ , is a finitely generated module over  $S^{-1}A = A_{\mathfrak{p}}$ , which is zero modulo  $\mathfrak{p}$ . The Nakayama lemma implies this cokernel is zero.

Finally, there is a  $s' \in S$  such that  $x \in C_{s'} \otimes_A B$ . Using again the above finiteness property of the cokernel, we can find a  $s'' \in S$  such that the map  $C_{s's''}[x] \rightarrow C_{s's''} \otimes_A B$  is an isomorphism. The morphism  $A_{s's''t} \rightarrow C_{s's''}$  has the required properties.

**Corollary 1.5** *A finite  $A$ -algebra  $B$  is locally simple if and only if  $\Omega_{B/A}^2 = 0$ .*

Proof. If  $B$  is simple over  $A$ , then the  $B$ -module  $\Omega_{B/A}^1$  is generated by one element, namely the differential  $d_{B/A}(x)$  of a generator  $x$ . Therefore its square wedge is zero. The same conclusion is true if  $B$  is locally simple because of the isomorphism  $A' \otimes_A \Omega_{B/A}^1 \simeq \Omega_{A' \otimes_A B/A'}$ .

Conversely, suppose that  $\Omega_{B/A}^2 = 0$ . We shall prove that the condition *iii*) of 1.4 is satisfied. So let  $A \rightarrow K$  be a morphism to an algebraically closed field  $K$ . Let  $R$  be a local factor of  $K \otimes_A B$ .

By assumption, one has  $\Omega_{R/K}^2 = 0$ . We write  $\Omega = \Omega_{R/K}^1$ , and we denote by  $\mathfrak{m}$  the maximal ideal of  $R$ . Since  $\wedge^2(\Omega/\mathfrak{m}\Omega) = 0$  the dimension of the  $R/\mathfrak{m}$ -vector space  $\Omega/\mathfrak{m}\Omega$  is  $\leq 1$ . As  $K$  is algebraically closed,  $K \rightarrow R/\mathfrak{m}$  is an isomorphism. We will use now the well-known (see below)  $K$ -linear isomorphism

$$\delta : \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\cong} \Omega/\mathfrak{m}\Omega.$$

It implies that  $\mathfrak{m}/\mathfrak{m}^2$  is a  $K$ -vector space of dimension  $\leq 1$ . From the Nakayama lemma we then deduce that the ideal  $\mathfrak{m}$  may be generated by one element. Thus  $R$  is a simple  $K$ -algebra.

(For lack of an elementary reference, we briefly recall that  $\delta$  is induced by the differential  $d_{R/K} : \mathfrak{m} \rightarrow \Omega$ , and that the inverse of  $\delta$  is defined as follows. Let  $s : R \rightarrow R/\mathfrak{m} \simeq K$  be the canonical morphism. The map  $R \rightarrow \mathfrak{m}/\mathfrak{m}^2$ ,  $x \mapsto \text{class of } x - s(x) \text{ mod. } \mathfrak{m}^2$ , is a derivation. By the universal property of  $\Omega$ , this derivation extends to a linear map  $\Omega/\mathfrak{m}\Omega \rightarrow \mathfrak{m}/\mathfrak{m}^2$ , which is easily seen to be the inverse of  $\delta$ .)

**Corollary 1.6** *Let  $A \xrightarrow{u} B \xrightarrow{v} C$  be finite morphisms. Then the composite  $vu$  is locally simple if either:*

- $u$  is locally simple and  $v$  is net (i.e unramified).
- $u$  is net and  $v$  is locally simple.

This result, which generalizes **1.3**, is easily deduced from the previous corollary and from the exact sequence

$$\Omega_{B/A}^1 \otimes_A C \rightarrow \Omega_{C/A}^1 \rightarrow \Omega_{C/B}^1 \rightarrow 0.$$

**Corollary 1.7** *Let  $A$  be a Dedekind domain,  $K \rightarrow L$  a finite separable extension of its field of fractions, and let  $B$  be the integral closure of  $A$  in  $L$ . Suppose that all the residue field extensions are separable. Then  $A \rightarrow B$  is locally simple.*

Proof. Let  $\mathfrak{n}$  be a maximal ideal of  $B$ , and let  $\mathfrak{m} = A \cap \mathfrak{n}$ . As  $B_{\mathfrak{n}}$  is a discrete valuation ring, the  $\kappa(\mathfrak{n})$ -vector space  $\mathfrak{n}/\mathfrak{n}^2$  is of dimension 1. Since  $\kappa(\mathfrak{n})$  is supposed to be separable over  $\kappa(\mathfrak{m})$  one has  $\Omega_{\kappa(\mathfrak{n})/\kappa(\mathfrak{m})}^1 = 0$ . Therefore, the exact sequence

$$\mathfrak{n}/\mathfrak{n}^2 \rightarrow \Omega_{B/A}^1 \otimes_B B/\mathfrak{n} \rightarrow \Omega_{\kappa(\mathfrak{n})/\kappa(\mathfrak{m})}^1 \rightarrow 0$$

shows that  $\Omega_{B/A}^1 \otimes_B B/\mathfrak{n}$  is a vector space of rank  $\leq 1$ . Hence for each maximal ideal  $\mathfrak{n}$  one has  $\Omega_{B/A}^2 \otimes_B B/\mathfrak{n} = 0$ , and the Nakayama lemma gives  $(\Omega_{B/A}^2)_{\mathfrak{n}} = 0$ . Since this is true for each maximal ideal of  $B$ , we may conclude that  $\Omega_{B/A}^2 = 0$ .

## 2. The Kronecker morphism.

**2.1. The generic element.** Let  $A \rightarrow B$  be a finite and locally free morphism. Denoting by  $B^\vee = \text{Hom}_A(B, A)$  the dual of  $B$ , we let

$$\xi \in B^\vee \otimes_A B$$

be the element corresponding to the identity map of  $B$  via the isomorphism

$$B^\vee \otimes_A B \xrightarrow{\sim} \text{End}_A(B)$$

which sends  $\beta \otimes x \in B^\vee \otimes_A B$  to the map  $b \mapsto \beta(b)x$ . If we write  $\xi = \sum \beta_i \otimes b_i$ , then, for all  $b \in B$ , one has  $b = \sum \beta_i(b)b_i$ .

When viewing it as an element of  $\text{Sym}_A(B^\vee) \otimes_A B$ , we call  $\xi$  the *generic element* of  $B$ , and we call  $\text{Sym}_A(B^\vee)$  the *ring of parameters* for the elements of  $B$ . In fact, an element  $x$  in  $B$  uniquely determines the  $A$ -linear map  $B^\vee \rightarrow A$  given by  $u \mapsto u(x)$ . This map extends to a morphism of  $A$ -algebras

$$\gamma_x : \text{Sym}_A(B^\vee) \rightarrow A.$$

The morphism  $\gamma_x$  has to be seen as the *specialization of parameters* associated with  $x$  because we recover  $x$  as the image of the generic element  $\xi$  by the morphism

$$\gamma_x \otimes 1 : \text{Sym}_A(B^\vee) \otimes_A B \rightarrow B.$$

If  $(e_i)$  is a basis of  $B$  (as  $A$ -module), and if  $(e_i^\vee)$  denotes the dual basis, one has :  $\xi = \sum_i e_i^\vee \otimes e_i$ . The ring of parameters  $\text{Sym}_A(B^\vee)$  is then isomorphic to the polynomial ring  $A[T_1, \dots, T_n]$ , where  $T_i$  stands for  $e_i^\vee$ , and the generic element is usually written

$$\xi = \sum_i T_i e_i.$$

But introducing variables may hide the important fact that the ring of parameters for  $B$  is *contravariant* in  $B$ . Understanding the functoriality of  $\xi$  is thus easier if one keeps its intrinsic definition and uses the following remark.

Let  $u : B \rightarrow C$  be a morphism of  $A$ -algebras. Suppose  $C$  to be finite and locally free over  $A$ . Under the canonical maps

$$\text{Hom}_A(B, B) \longrightarrow \text{Hom}_A(B, C) \longleftarrow \text{Hom}_A(C, C)$$

the images of  $\text{id}_B$  and of  $\text{id}_C$  are both equal to  $u \in \text{Hom}_A(B, C)$ . In order to extend this to the generic elements let us consider the morphisms of  $A$ -algebras

$$\text{Sym}_A(B^\vee) \otimes_A B \xrightarrow{1 \otimes u} \text{Sym}_A(B^\vee) \otimes_A C \xleftarrow{v \otimes 1} \text{Sym}_A(C^\vee) \otimes_A C,$$

where  $v = \text{Sym}_A(u^\vee)$ . Then, the images of the generic elements  $\xi_B \in \text{Sym}_A(B^\vee) \otimes_A B$  and  $\xi_C \in \text{Sym}_A(C^\vee) \otimes_A C$  are equal in the ring  $\text{Sym}_A(B^\vee) \otimes_A C$ .

**2.2 The Kronecker morphism.** Let again  $A \rightarrow B$  be a finite and locally free morphism. Let

$$F_{B/A}(X) \in \text{Sym}_A(B^\vee)[X]$$

be the characteristic polynomial of the generic element of  $B$ . From now on this polynomial will be called the *generic characteristic polynomial*.

The relation  $F_{B/A}(X) = 0$  is called by Hilbert (*Zahlbericht*, ch.IV, §10) the *fundamental equation* of the  $A$ -algebra  $B$ . The generic element is a root of this equation (Hamilton-Cayley theorem). Therefore there exists a morphism of  $\text{Sym}_A(B)$ -algebras

$$\text{Sym}_A(B)[X]/(F_{B/A}) \longrightarrow \text{Sym}_A(B) \otimes_A B,$$

which maps (the class of)  $X$  to  $\xi$ ; it will be called the *Kronecker morphism* of  $B/A$ .

**2.2.1** Suppose  $B = A^n$ , and choose the canonical basis  $(e_i)$  for  $A^n$ . The ring of parameters  $\text{Sym}_A(B)$  is then isomorphic to  $S = A[T_1, \dots, T_n]$ , where  $T_i$  stands for the  $i$ -th projection  $A^n \rightarrow A$ . An immediate calculation gives

$$F_{B/A}(X) = \prod_{i=1}^n (X - T_i),$$

and the Kronecker morphism

$$S[X]/(\prod (X - T_i)) \longrightarrow S^n$$

is defined by  $X \mapsto (T_1, \dots, T_n)$ . It is injective since the Van der Monde determinant is a regular element in  $S$ .

The coefficients of the generic characteristic polynomial  $F_{B/A}$  are symmetric polynomials in the  $T_i$ , i.e they are invariant under the automorphisms of the  $A$ -algebra  $B = A^n$ . Below we will show this to be a general fact.

**2.2.2** Direct calculations are seldom illuminating, even in the simplest cases. Let, for example,  $B = A[Y]/(G)$  be the  $A$ -algebra of rank 3 defined by the polynomial

$$G(Y) = Y^3 + a_2Y^2 + a_1Y + a_0.$$

If we write the generic element of  $B$  as  $\xi = T_0 + T_1y + T_2y^2$ , then

$$\begin{aligned} F_{B/A}(X) &= (X - T_0)^3 + (X - T_0)^2[a_2T_1 + (2a_1 - a_2^2)T_2] \\ &\quad + (X - T_0)[a_1T_1^2 + (3a_0 - a_1a_2)T_1T_2 + (a_1^2 - 2a_0a_2)T_2^2] \\ &\quad + [a_0T_1^3 - a_0a_2T_1^2T_2 + a_0a_1T_1T_2^2 - a_0^2T_2^3]. \end{aligned}$$

From this formula, it is not even clear if the Kronecker morphism is injective. In fact it is (cf **2.4**).

**2.2.3** Let  $B = A[u, v]$  with  $u^2 = v^2 = 0$ . It is a radical  $A$ -algebra of rank 4. Writing the generic element as  $\xi = T_0 + T_1u + T_2v + T_3uv$ , we find

$$F_{B/A}(X) = (X - T_0)^4.$$

Since  $(\xi - T_0)^3 = 0$ , the Kronecker morphism is *not* injective in that case.

**2.3** A few words now on the functoriality of these notions.

Let  $u : B \rightarrow C$  be a morphism between finite and locally free  $A$ -algebras. Denote the rings of parameters by  $S = \text{Sym}_A(B)$ , and  $T = \text{Sym}_A(C)$ , and let

$$v = \text{Sym}_A(u) : T \longrightarrow S$$

be the morphism associated to  $u$ . Finally, let the norm maps relative to  $C/A$  be denoted by  $N_T = N_{T \otimes_A C/T}$ , and  $N_S = N_{S \otimes_A C/S}$ . We have the following commutative diagram

$$\begin{array}{ccccc} S \otimes_A B & \xrightarrow{1 \otimes u} & S \otimes_A C & \xleftarrow{v \otimes 1} & T \otimes_A C \\ & & N_S \downarrow & & \downarrow N_T \\ & & S & \xleftarrow{v} & T \end{array}$$

Let  $F_{B/A}(X) \in S[X]$ , and  $F_{C/A}(X) \in T[X]$  be the generic characteristic polynomials. Since  $1 \otimes u(\xi_B) = v \otimes 1(\xi_C)$ , we see that

$$v(F_{C/A}) = N_S(X - v \otimes 1(\xi_C)) = N_S(X - 1 \otimes u(\xi_B)).$$

We can make this last polynomial explicit in some particular cases.

**2.3.1**  $C = B$  and  $u$  is an automorphism of the  $A$ -algebra  $B$ .

As the norm commutes with any automorphism, we have  $v(F_{B/A}) = F_{B/A}$ . Hence

*The generic characteristic polynomial  $F_{B/A} \in \text{Sym}_A(B)[X]$  is invariant under any automorphism of the  $A$ -algebra  $B$  acting (contra-variantly) on  $\text{Sym}_A(B)$ .*

**2.3.2** Suppose that the morphism  $u : B \rightarrow C$  is locally free of rank  $d$ . Then by transitivity of the norm, we have

$$N_{C/A} = N_{B/A} \circ N_{C/B}.$$

Moreover, for  $b \in B$ ,  $N_{C/B}(u(b)) = b^d$ . Therefore,

$$N_S(X - 1 \otimes u(\xi_B)) = N_{S \otimes_A B/S}(N_{S \otimes_A C/S \otimes_A B}(X - 1 \otimes u(\xi_B))) = F_{B/A}(X)^d,$$

and we get

$$v(F_{C/A}(X)) = F_{B/A}(X)^d.$$

In that case, the morphism  $v : \text{Sym}_A(C) \rightarrow \text{Sym}_A(B)$  is surjective and it may be seen as "sending to 0" the variables relative to the quotient  $C/B$ .

**2.3.3** Consider the case where  $C = B/J$  is a quotient by a nilpotent ideal  $J$  such that the successive quotients  $J^s/J^{s+1}$  are locally free  $C$ -modules of constant rank; let  $e$  be the sum of these ranks. According to ([A] III 9.4 Prop. 5), we have in  $S[X]$

$$F_{B/A}(X) = N_S(X - 1 \otimes u(\xi_B))^e,$$

whence the equality

$$F_{B/A}(X) = v(F_{C/A}(X))^e.$$

**2.3.4** Let us give a precise meaning to the intuitively clear following sentence:

*The generic characteristic polynomial of a product of rings is the product of the generic characteristic polynomials of the factors.*

Let  $B = \prod B_i$  be a decomposition in a finite product of  $A$ -algebras. Denote by  $p_i : B \rightarrow B_i$  the projections, and let

$$q_i = \text{Sym}(p_i) : S_i = \text{Sym}_A(B_i) \longrightarrow S = \text{Sym}_A(B)$$

be the injective morphism associated to  $p_i$ . The decomposition  $S \otimes_A B \simeq \prod S \otimes_A B_i$  shows that

$$F_{B/A}(X) = \prod N_{S \otimes_A B_i/S}(X - 1_S \otimes p_i(\xi_B)),$$

If we now apply the remark above with  $p_i : B \rightarrow B_i$  instead of  $u : B \rightarrow C$ , we get

$$N_{S \otimes_A B_i/S}(X - 1_S \otimes p_i(\xi_B)) = q_i(F_{B_i/A}(X)).$$

Putting these equalities together, we find the expected formula for the product :

$$F_{B/A}(X) = \prod q_i(F_{B_i/A}(X)).$$

**Theorem 2.4** (Injectivity of the Kronecker morphism) *Let  $A \rightarrow B$  be a finite and locally free morphism. Then the following conditions are equivalent:*

- i)  $B$  is locally simple over  $A$ .*
- ii) The Kronecker morphism*

$$\mathrm{Sym}_A(B^\vee)[X]/(F_{B/A}) \longrightarrow \mathrm{Sym}_A(B^\vee) \otimes_A B,$$

*is injective, and remains injective after any base change  $A \rightarrow A'$ .*

Let us show the implication  $i) \Rightarrow ii)$ . We can clearly suppose  $B$  to be simple, hence of the form  $A[Y]/(G)$ , where  $G$  is a monic polynomial of degree  $n$ . We write  $y$  for the class of  $Y$  in  $B$ , and we choose the basis  $(1, y, \dots, y^{n-1})$  for  $B$ . The ring of parameters  $\mathrm{Sym}_A(B^\vee)$  will then be seen as the polynomial ring  $S = A[T_0, T_1, \dots, T_{n-1}]$ , in such a way that the generic element would be written as

$$\xi = T_0 + T_1 y + \dots + T_{n-1} y^{n-1}.$$

Checking the injectivity of the Kronecker morphism amounts to proving the following: any relation of the form

$$s_0 + s_1 \xi + \dots + s_{n-1} \xi^{n-1} = 0$$

with the  $s_i$  in  $S$ , implies that all the  $s_i$  are zero; in other words, one has to show that the family  $(1, \xi, \dots, \xi^{n-1})$  of elements of  $S \otimes_A B$  is free over  $S$ . For doing so, we consider the determinant of the matrix of the  $\xi^j$  on the basis  $(y^i)$ , and we show it is a regular (i.e not a zero divisor) element of  $S$ .

Let  $U_{ij} \in S$  be the polynomials defined by

$$\xi^j = U_{0,j} + U_{1,j} y + \dots + U_{n-1,j} y^{n-1},$$

and let  $U = \det(U_{ij})$ .

An explicit example will perhaps give the flavor of the situation. When  $G(Y) = Y^3 + a_2 Y^2 + a_1 Y + a_0$  some by hand calculations give

$$U = T_1^3 - 2a_2 T_1^2 T_2 + (a_1 + a_2^2) T_1 T_2^2 + (a_0 - a_1 a_2) T_2^3.$$

In this example, a fact is to be noticed:  $U$  is a monic polynomial in  $T_1$ . We will check this to be a general fact.

Each of the polynomials  $U_{ij}$  is homogeneous in  $T_0, T_1, \dots, T_{n-1}$ , of degree  $j$ . Therefore the determinant  $U$  is a homogeneous polynomial of degree  $N = 1 + 2 + \dots + n - 1$ . On the other hand,

$U(0, T_1, 0, \dots, 0) = T_1^N$ . In fact if we map  $\xi$  to  $T_1 y$  then  $\xi^j$  is mapped to  $T_1^j y^j$ , and the matrix involved becomes the diagonal matrix  $\text{diag}(1, T_1, \dots, T_1^{n-1})$ . These two facts together imply that  $U$  is a monic polynomial in  $T_1$ . Hence  $U$  is a regular element in  $S$ , and it remains regular after any base change  $A \rightarrow A'$ .

To prove the implication  $ii) \Rightarrow i)$  let us first simplify the notations and write the Kronecker morphism as

$$u : S[X]/(F) \longrightarrow S \otimes_A B.$$

The cokernel  $M$  of  $u$  is an  $S$ -module of finite presentation, therefore the set  $V \subset \text{Spec}(S)$  of those prime ideals  $\mathfrak{n}$  of  $S$  such that  $M_{\mathfrak{n}} = 0$  is open and quasi-compact (Hence  $V$  may be covered by a finite family  $(V_i)$  of affine open subsets, and someone who dislikes schemes could replace  $V$  by the ring  $A' = \prod_i \Gamma(V_i)$ ). The injectivity assumption implies that  $\mathfrak{n}$  is in  $V$  if and only if  $u_{\mathfrak{n}}$  is an isomorphism. Thus for such an  $\mathfrak{n}$  the  $S_{\mathfrak{n}}$ -algebra  $S_{\mathfrak{n}} \otimes_A B$  is simple. As the morphism  $V \rightarrow \text{Spec}(A)$  is clearly flat, we have only to check that it is surjective. So, let  $k = \kappa(\mathfrak{p})$  be the residue field at a prime ideal  $\mathfrak{p}$  of  $A$ . The ring  $k \otimes_A S$  is isomorphic to a polynomial ring over  $k$ ; thus it is an integral domain, and we denote its fraction field by  $K$ . By assumption, the  $k \otimes_A S$ -linear map  $1_k \otimes u$  is injective; by localization, the  $K$ -linear map  $u_K : K[X]/(F) \rightarrow K \otimes_A B$  is still injective. But both sides are  $K$ -vector spaces of the same dimension; therefore  $u_K$  is bijective. Hence the generic point of  $k \otimes_A S$  is a point of  $V$ , and it lies over  $\mathfrak{p}$ .

**Remark 2.5** An other proof of the implication  $ii) \Rightarrow i)$  uses the condition  $iii)$  of the proposition 1.4. We will now give its main step because it seems to be of interest in itself.

Let  $K$  be an algebraically closed field, and  $R$  a finite local  $K$ -algebra. We suppose that there exist a non zero  $K$ -algebra  $S$ , a monic polynomial  $F(X) \in S[X]$  of degree  $n = \text{rank}_K(R)$ , and an injective morphism of  $S$ -algebras  $u : S[X]/(F) \rightarrow S \otimes_K R$ . Then  $R$  is a simple  $K$ -algebra.

Proof : We write  $R = K + J$  where  $J$  is nilpotent. Let  $m$  be the lowest integer such that  $J^m = 0$ ; hence, in the filtration

$$R \supset J \supset J^2 \supset \dots \supset J^{m-1} \supset J^m = 0$$

all those  $K$ -subspaces are distinct. Therefore, we have  $m \leq \dim_K(R) = n$ . Let  $x$  denote the class of  $X$  in  $S[X]/(F)$ . We write  $u(x) = s + \eta \in S \otimes_K R = S + S \otimes_K J$ , with  $s \in S$  and  $\eta \in S \otimes_A J$ . Since  $u((x-s)^m) = \eta^m = 0$ , the injectivity of  $u$  implies that  $F(X)$  divides  $(X-s)^m$ . Therefore  $m = n$  because  $\deg(F) = n \geq m$ . Thus,  $J^{n-1} = J^{m-1} \neq 0$ . But  $J$  is a vector space of dimension  $n-1$ , and the filtration above is strict; therefore the vector space  $J/J^2$  is of rank one, i.e the ideal  $J$  is generated by one element (Nakayama) and we conclude that  $R$  is simple.

The following consequence has most probably been already noticed, at least in its polynomial setting.

**Corollary 2.6** Let  $A \rightarrow B$  be a finite and locally free morphism. Suppose  $A$  and  $B$  to be domains. If  $B$  is locally simple over  $A$ , then the norm of the generic element of  $B$  generates a prime ideal in  $\text{Sym}_A(B^\vee)$ . In particular, let  $L/K$  be a finite simple field extension; choose any  $K$ -basis  $(e_1, \dots, e_n)$  for  $L$ . Then the polynomial

$$F(T_1, \dots, T_n) = \text{Norm}_{L/K}(T_1 e_1 + \dots + T_n e_n)$$

is irreducible in  $K[T_1, \dots, T_n]$ .

Proof : We write  $\text{Sym}_A(B^\vee) = S$ , and we consider the morphism of  $A$ -algebras  $u : S \rightarrow S[X]$  extending the linear map  $B^\vee \rightarrow S[X]$  given by  $\beta \mapsto \beta(1)X - \beta$ . If we denote by  $v : S[X] \rightarrow S$

the morphism of  $S$ -algebras which sends  $X$  to 0, then  $v \circ u$  is clearly an automorphism of  $S$ . Let  $\xi \in S \otimes_A B$  be the generic element of  $B$ . Its image  $u \otimes 1(\xi)$  in  $S[X] \otimes_A B$  is easily seen to be  $X - \xi$ . The commutativity of the square

$$\begin{array}{ccc} S \otimes_A B & \xrightarrow{u \otimes 1} & S[X] \otimes_A B \\ \text{Norm} \downarrow & & \downarrow \text{Norm} \\ S & \xrightarrow{u} & S[X] \end{array}$$

shows that  $u(\text{Norm}_{B/A}(\xi)) = F_{B/A}(X)$ . Therefore,  $u$  induces a morphism

$$\bar{u} : S/\text{Norm}(\xi)S \longrightarrow S[X]/(F).$$

Using the morphism  $v$ , we see that  $\bar{u}$  is injective. The conclusion now follows from the implication  $i) \Rightarrow ii)$  of the theorem, and from the fact that  $S \otimes_A B$  is a domain.

**Remark 2.7** The simplest non simple (!) field extension is

$$K = \mathbb{F}_2(X, Y) \subset L = \mathbb{F}_2(U, V),$$

given by  $X = U^2, Y = V^2$ . It is a radical extension of degree 4. The norm of the generic element  $T_0 + T_1U + T_2V + T_3UV$  is  $(T_0^2 + T_1^2X + T_2^2Y + T_3^2XY)^2$ . It is a reducible polynomial.

### 3. Reading some pages of Hilbert.

The today reader of the beginning of the *Zahlbericht* of Hilbert ([H]) has to face at least two difficulties. The first one is clearly pointed out in the introduction of the English edition; it comes from the deliberate avoiding by Hilbert of any "abstract algebra" concept, even the more useful ones among those he already had at hand (e.g the notion of quotient group). The reader is thus driven through heavy periphrases. In other places, the constraint of rigour is less clear, for example when Hilbert defines something as the product of the (more or less mysterious) "conjugates" of some expression, where today one understands simply a norm, etc.

The second difficulty is much more interesting because it is connected to the debate, at that time, on the best way to "save" the factoriality (or, to say it better, to get around the non-factoriality) of the rings of integers (see the book by H. Weyl [W], or the Historical Note at the end of [AC]). By oversimplifying this debate we may personify the two positions by Dedekind and Kronecker. The idea of Kronecker was to associate polynomials to the objects under consideration, in order to work inside polynomial rings over  $\mathbb{Z}$ , or  $\mathbb{F}_p$ , which are indeed factorial. The idea of Dedekind was to create the notion of ideal. It prevails.

In what follows, I should like to show how the language and the results of the preceding paragraphs enlighten some of the statements of the *Zahlbericht*, mainly those which involve the Kronecker construction. I think this construction deserves to be better known even if it became useless in the algebraic theory of numbers.

The statements in question are in the §§10 and 11; here the base ring is  $A = \mathbb{Z}$  and the algebra  $B$  is the ring of integers of a number field  $K$ . The generic element  $\xi$  is called by Hilbert the *fundamental form*, and the generic characteristic polynomial is denoted by  $F$  (amazingly enough, it is

named in the memoir as "the left hand side of the fundamental equation"). As shown before,  $B$  is locally simple over  $A$ , hence the Kronecker morphism is injective, and it remains injective modulo any prime  $p$ ; this is the content of theorem 34 of the *Zahlbericht* which says:

*The congruence of degree  $n$ ,  $F(X) \equiv 0 \pmod{p}$  is the congruence of lowest degree which is satisfied modulo  $p$  by the fundamental form  $\xi$  (i.e. by the generic element).*

The first part of theorem 33 of Hilbert's memoir gives the correspondence between the factorization of  $F(X) \pmod{p}$  (that is in  $\mathbb{F}_p[T_1, \dots, T_n, X]$ ) and the (now) usual factorization of the ideal  $pB$  as a product of prime ideals in  $B$ . Namely:

*If  $p$  factorizes in  $B$  as  $pB = \mathfrak{p}^e \mathfrak{p}'^{e'} \dots$  then  $F$  decomposes modulo  $p$  in the form*

$$F \equiv \Pi^e \Pi'^{e'} \dots \pmod{p},$$

*where  $\Pi, \Pi', \dots$  represent distinct polynomials which are irreducible modulo  $p$ .*

The proof in the memoir is preceded by three lemmas we may nowadays easily circumvent by some functoriality considerations. In fact, the factorization of  $pB$  gives a decomposition of  $\mathbb{F}_p$ -algebras:

$$B/pB = B/\mathfrak{p}^e \times B/\mathfrak{p}'^{e'} \times \dots$$

Using the remarks 2.3.3 and 2.3.4 (and without mentioning the base field  $\mathbb{F}_p$  any more), we may write

$$F = v(G^e) v'(G'^{e'}) \dots$$

where  $G$  is the generic characteristic polynomial of  $B/\mathfrak{p}$ , and where  $v, v' \dots$  denote the injective morphisms between rings of parameters

$$v : \text{Sym}((B/\mathfrak{p})^\vee) \rightarrow \text{Sym}((B/pB)^\vee)$$

associated with the quotients  $B/\mathfrak{p}, B/\mathfrak{p}' \dots$ . Since these morphisms may be seen as just "adding the variables corresponding to a basis of the kernel", they preserve the irreducibility of polynomials. But the generic characteristic polynomial  $G$  is irreducible in  $\text{Sym}((B/\mathfrak{p})^\vee[X])$  (2.4). Therefore its image  $v(G)$  is still irreducible in  $\text{Sym}((B/pB)^\vee[X])$ . This is the required polynomial  $\Pi$ .

Theorem 35 of the *Zahlbericht* is also, as Hilbert pointed out, a consequence of the injectivity of the Kronecker morphism :

*The content of the discriminant of  $F(X)$  is equal to the discriminant of  $B$  (or of  $K$ ).*

The discriminant of  $F(X)$  is an element of the ring containing the coefficients of  $F$ , i.e. here  $\text{Sym}(B)^\vee$ . This ring is isomorphic to  $\mathbb{Z}[T_1, \dots, T_n]$ , therefore that makes sense to look at the gcd of the coefficients of the discriminant, i.e. at its *content* (Hilbert writes: *the greatest numerical factor*). Let us also recall what the discriminant of an algebra is. Let  $S \rightarrow E$  be a finite morphism, locally free of rank  $n$ . The discriminant of  $E/S$  is the ideal of  $S$  image of the  $S$ -linear map

$$d_{E/S} : (\wedge^n E)^\otimes 2 \longrightarrow S,$$

defined as the extension to the  $n$ -th exterior power of the bilinear map

$$E \times E \longrightarrow S, \quad (x, y) \mapsto \text{Tr}_{E/S}(xy).$$

If  $F(X) \in S[X]$  is a monic polynomial, the discriminant of the  $S$ -algebra  $S[X]/(F)$  is the ideal generated by the discriminant of the polynomial  $F$ . In the situation under consideration, it can be checked that the Kronecker morphism

$$u : E := S[X]/(F) \longrightarrow S \otimes_A B$$

is compatible with the traces (see e.g [F], lemma 4.3.1 ), namely :

$$\mathrm{Tr}_{E/S} = \mathrm{Tr}_{S \otimes_A B/S} \circ u.$$

Since  $\mathrm{Tr}_{S \otimes_A B/S} = \mathrm{Tr}_{B/A} \otimes \mathrm{id}_S$ , we get

$$d_{E/S} = (d_{B/A} \otimes \mathrm{id}_S) \circ (\wedge^n u)^{\otimes 2}.$$

The Kronecker morphism  $u$  is universally injective (2.4). Therefore  $\wedge^n u$  is injective, and remains injective modulo any prime  $p$  ([A] III 8.2 Prop.3). Hence, the content of  $\wedge^n u$  is 1, and the assertion follows.

## References

- [A] N. BOURBAKI, Algebra, vol. I: ch.1-3; vol.II: ch.4-7, Springer-Verlag (1989 and 1990).
- [AC] N. BOURBAKI, Commutative Algebra, Ch. 1-7, Springer-Verlag (1989)
- [F] D. FERRAND, *Un foncteur norme*, Bull. Soc. Math. France, 126 (1998) p.1-49
- [H] D. HILBERT, *Zahlbericht, Jahresber. der D.M.V.*, 4 (1897), pp.175-546
  - Translated into French by A. Lévy and Th. Got under the title " *Théorie des corps de nombres algébriques*", Paris (Hermann),1913 ; reprinted by J. Gabay (1991)
  - Translated into English by I. T. Adamson, with an Introduction by F. Lemmermeyer and N. Schappacher, Berlin, etc. (Springer) 1998
- [W] H. WEYL, Algebraic Theory of Numbers, *Ann. of Math. Studies, no 1*, Princeton (1940)

IRMAR, UNIVERSITÉ DE RENNES 1, CAMPUS DE BEAULIEU, F-35040 RENNES CEDEX  
*E-mail address:* `daniel.ferrand@univ-rennes1.fr`