# Monogenous Algebras. Back to KRONECKER

DANIEL FERRAND

*August 2019*

ABSTRACT. - This Note develops some properties of the finite $A$-algebras $B$ which can be generated by a single element, after, if need be, some faithfully flat base change ; they are called *locally monogenous.* Several characterisations of this notion show it appears to be commonly satisfied ; in particular, the morphisms between rings of algebraic integers are locally monogenous.

For a finite locally free $A$-algebra $B$, we have to consider its *ring of parameters* $\mathrm{Sym}_A(B^\vee)$, now denoted by $S$, and its *generic element* $\xi_B \in S \otimes_A B$ ; they are both immediately definable when $B$ is free with a basis $e_1, \ldots, e_n$ : in fact one then has an isomorphism $S \simeq A[T_1, \cdots, T_n]$, and we may write $\xi_B = \sum T_i e_i \in S \otimes_A B$.

The norm map $B \to A$ extends to norm maps $S \otimes_A B \to S$, and $S[X] \otimes_A B \to S[X]$, both still denoted by N ; the *generic characteristic polynomial* is $F_{B/A}(X) = \mathrm{N}(X - \xi_B) \in S[X]$.

Guided by the point of view of torsors, we bring to the fore front a (non conventional) morphism $\mu_B : S \to S[T]$ which induces a smooth morphism

$$S/\mathrm{N}(\xi_B)S \to S[X]/(F_{B/A}(X)).$$

It relates, in a sense, $\mathrm{N}(\xi_B)$ and $F_{B/A}(X)$.

Then we update an idea KRONECKER introduced at the early beginning of the algebraic theory of numbers : namely that some properties of a finite free $A$-algebra $B$ can be read through the generic characteristic polynomial $F = F_{B/A}(X)$ ; in fact, since $\xi$ is a root of $F$ (Hamilton-Cayley) we dispose of a canonical morphism, called the *Kronecker morphism*

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

We show that this morphism is $A$-universally injective if and only if $B$ is locally monogenous over $A$. Thus this injectivity property is true in the context of the theory of numbers ; that is thoroughly, though implicitly, used by HILBERT in the *Zahlbericht* ; besides, the very beginning of this memoir was an inspiration to us for this Note.

In particular, we extend to locally monogenous algebra $A \to B$ the fact, quoted by HILBERT, that the discriminant of $B/A$ is equal to the content (relative to $A \to S$) of the discriminant of $F$.

*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. A ring morphism $A \to B$ is said to be finite locally free if it makes $B$ a projective $A$-module of finite type ; the map $\mathfrak{p} \to \mathrm{rank}_{\kappa(\mathfrak{p})}(B \otimes_A \kappa(\mathfrak{p}))$ is then locally constant (for the Zariski topology) on* Spec$(A)$ *; in other words, $A$ is the finite product of rings $A_r$ such that $B \otimes_A A_r$ is locally free of constant rank $r$ as $A_r$-module.*

**Contents**



## 1. Locally monogenous morphisms

**Definition 1.1** A morphism $A \to B$ between rings is called *monogenous* 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 $A[X] \to B$.

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

Before giving some examples and characterizations of these morphisms, we first recall the central rôle they play in the theory of the norm functor (see [F]) : to any finite and locally free morphism $A \to B$, is associated a covariant functor

$$\mathrm{N}_{B/A} : \mathbf{Mod}_B \longrightarrow \mathbf{Mod}_A,$$

which extends the usual one defined for invertible $B$-modules $L$ (roughly speaking, by then taking the norm of a cocycle associated to $L$) ; for a $B$-algebra $B \to C$, there exists a morphism to the Weil restriction $\mathrm{N}_{B/A}(C) \to \mathbf{R}_{B/A}(C)$ which is an isomorphism if $B/A$ is étale. The point is that the norm of a locally free $B$-module is a locally free $A$-module when $B$ is étale over $A$, or, more generally if $B$ is locally monogenous over $A$ ; but that may fail to be true in general, 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 $A \to A^n$. 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 with respect to 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, but $\mathbf{F}_p \to \mathbf{F}_p^n$ is *not* monogenous if $n > p$. It is also clear that such a sequence cannot exist if the group $A^\times$ of invertible elements is too small, i.e. if $\mathrm{Card}(A^\times) < \frac{n(n-1)}{2}$ ; thus $\mathbf{Z} \to \mathbf{Z}^n$ is *not* monogenous 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 $A \to A'$ is faithfully flat (and smooth), and the morphism $A' \to A'^n$ is monogenous ; thus for any $n$ and any ring $A$, the morphism $A \to A^n$ is locally monogenous.

A slight generalization :
*A finite étale morphism $A \to B$ is locally monogenous.*

If $A \to B$ is of constant rank $r$, then $B$ is locally isomorphic to $A^r$, and thus it is locally monogenous. We can reduce to this case by considering the finite decomposition $A = A_0 \times A_1 \times \cdots \times A_m$ defined by the condition that $B_r := B \otimes_A A_r$ be locally free of constant rank $r$ over $A_r$ ; it is thus locally isomorphic to $A_r^r$ ; the $A$-algebra $B = B_0 \times \cdots \times B_m$, is clearly locally monogenous.

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

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

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

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

Let $x$ be the image of $X$ in $A'$. Using the standard property of the resultant (see e.g [A] IV 6.6 Cor.1 to Prop. 7), we see 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 $A \to A'$ is faithfully flat ; as it 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 $A \to K$ 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 $A' = A[X]_{R(X)}$. Considering the images in $K[T]$ of the two monic polynomials $P(T)$ and $Q(T)$ and their roots in $K$, it is clear that 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 a morphism $A' = A[X]_{R(X)} \to K$.

**Proposition 1.4** (Characterizations). *Let $B$ be a finite $A$-algebra.The following conditions are equivalent :*
*i) The morphism $A \to B$ is locally monogenous.*
*ii) There exists a morphism $A \to A'$ such that $A' \to A' \otimes_A B$ is monogenous, and* Spec$(A')$ →Spec$(A)$ *surjective (i.e the flatness of the base change is superfluous).*
*iii) For any morphism $A \to K$ where $K$ is an algebraically closed field, each local factor of $K \otimes_A B$ is a monogenous $K$-algebra.*
*iv) For any prime ideal $\mathfrak{p}$ of $A$, there exists a finite extension $\kappa(\mathfrak{p}) \to k$ such that $k \otimes_A B$ is monogenous over $k$.*
*v) The $B$-module $\Omega^1_{B/A}$ is monogenous.*
*vi) $\Omega^2_{B/A} = 0$.*

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 in the sequel the *local factors* of $R$.

All the ingredients used in the following proof come from EGA IV, but, for the convenience of the reader, they are given in some detail instead of scattered references.

**Lemma 1.4.1** *Let $A \to B$ be a finite morphism. We suppose an $A$-algebra $A \to E$ exists such that $E \otimes_A B$ is monogenous over $E$. Then, there exists a sub-$A$-algebra $F \subset E$* of finite type *such that $F \otimes_A B$ is monogenous 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 $E' = A[x_1, \ldots, x_n] \subset E$ 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 $E \otimes_{E'} M = 0$. 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 $E'[y_1, \ldots, y_m]$. □

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

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

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 $S^{-1}C \to S^{-1}C/\mathfrak{p}S^{-1}C \simeq k$ 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

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

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 $\mathrm{Spec}(A') \to \mathrm{Spec}(A)$ 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 monogenous over $F$. Let $A \to K$ 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 $\kappa(\mathfrak{p}) \to K$ factors through $\kappa(\mathfrak{p}) \otimes_A F$. But the morphism $\kappa(\mathfrak{p}) \otimes_A F \longrightarrow \kappa(\mathfrak{p}) \otimes_A F \otimes_A B$ is monogenous. Therefore, the $K$-algebra $K \otimes_A B$ is monogenous, 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 monogenous; by lemma 1.4.1, there exists a finite sub-extension $k \subset K$ such that $k \otimes_A B$ is a monogenous $k$-algebra.

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

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

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

For proving $x$ is a generator of the $S^{-1}C$-algebra $S^{-1}(C \otimes_A B)$ consider the following diagram :

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

The cokernel of the injective map $j : S^{-1}C[x] \to S^{-1}(C \otimes_A B)$, is a finitely generated module over $S^{-1}A = A_{\mathfrak{p}}$, which is zero modulo $\mathfrak{p}$. The Nakayama lemma thus implies this cokernel be zero, showing that $j$ is an isomorphism, and that $x$ is a generator of the $S^{-1}C$-algebra $S^{-1}(C \otimes_A B)$. 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 $C_{s's''}[x] \to C_{s's''} \otimes_A B$ is an isomorphism. The morphism $A_{s's''t} \to C_{s's''}$ has the required properties.

*i)* $\Rightarrow$ *v)* $\Rightarrow$ *vi)*. If $B$ is monogenous over $A$, then the $B$-module $\Omega^1_{B/A}$ is generated by one element, namely the differential $d_{B/A}(x)$ of any generator $x$ of the $A$-algebra $B$. Therefore its square wedge is zero. The same conclusion is true if $B$ is locally monogenous because of the isomorphism $A' \otimes_A \Omega^1_{B/A} \simeq \Omega^1_{A' \otimes_A B/A'}$.

*vi)* $\Rightarrow$ *iii)*. Suppose that $\Omega^2_{B/A} = 0$. Let $A \to K$ be a morphism to an algebraically closed field $K$. Let $R$ be a local factor of $K \otimes_A B$. By assumption, one has $\Omega^2_{R/K} = 0$. We write $\Omega = \Omega^1_{R/K}$, and we denote by $\mathfrak{m}$ be 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, $K \to R/\mathfrak{m}$ is an isomorphism. Now the well-known (see below) $K$-linear isomorphism

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

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 monogenous $K$-algebra.

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

**Corollary 1.5** *Let $A \xrightarrow{u} B \xrightarrow{v} C$ be finite morphisms. Then the composite $vu$ is locally monogenous if either :*

- *$u$ is locally monogenous and $v$ is net (i.e unramified), or*
- *$u$ is net and $v$ is locally monogenous.*

This result, which generalizes **1.3**, is easily deduced from the equivalence $i) \Leftrightarrow v)$ of the above proposition and from the exact sequence

$$\Omega^1_{B/A} \otimes_A C \to \Omega^1_{C/A} \to \Omega^1_{C/B} \to 0.$$

**Corollary 1.6** *Let $A$ be a Dedekind domain, $K \to L$ 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 (This is the case if $A = \mathbf{Z}$). Then $A \to B$ is locally monogenous.*

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 $\Omega^1_{\kappa(\mathfrak{n})/\kappa(\mathfrak{m})} = 0$. Therefore, the exact sequence

$$\mathfrak{n}/\mathfrak{n}^2 \to \Omega^1_{B/A} \otimes_B B/\mathfrak{n} \to \Omega^1_{\kappa(\mathfrak{n})/\kappa(\mathfrak{m})} \to 0$$

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

## 2. Tschirnhaus morphisms

I am indebted to the late Dan Laksov (KTH) for discussing this subject together, few years ago.

**2.1. Definition** *Let $A$ be a ring. A morphism $u : B \to C$ between locally free $A$-algebras of the same constant rank is said a* **Tschirnhaus morphism** *if it is "universally norm compatible"; that means that for any morphism $A \to A'$ the following triangle is commutative*

(2.1.1)
$$\begin{array}{ccc} A' \otimes_A B & \xrightarrow{1 \otimes u} & A' \otimes_A C \\ & {\scriptstyle N_{B'}} \searrow \quad \swarrow {\scriptstyle N_{C'}} & \\ & A' & \end{array}$$

*where $N_{B'}$ is a shortland for the norm map $N_{A' \otimes_A B/A'}$, and idem for $N_{C'}$.*

See (**2.4**) below for a justification of the choice of this patronymic instead of the adjective *universally norm compatible.*

(**2.1.2**) An isomorphism, and even an injective morphism, are Tschirnhaus morphisms. With $A' = A[X]$, we see that a Tschirnhaus morphism is compatible with the characteristic polynomials (and in particular with traces) : for any $b \in B$, one has

$$\mathrm{Pol.char}_{B/A}(X, b) = \mathrm{Pol.char}_{C/A}(X, u(b)).$$

Note that the norm maps being *polynomial laws* the squares

$$\begin{array}{ccc} B & \longrightarrow & A' \otimes_A B \\ {\scriptstyle N_B} \downarrow & & \downarrow {\scriptstyle N_{B'}} \\ A & \longrightarrow & A' \end{array}$$

are commutative for any base change $A \to A'$ ; thus, we have the following descent property : if $A \to A'$ is only injective and if the above triangle (**2.1.1**) is commutative, then the original one is also commutative, i.e. $N_B = N_C \circ u$.

(**2.1.3**) Let $u : B \to C$ be a Tschirnhaus morphism between locally free $A$-algebras of rank $n$. Then $\mathrm{Ker}(u)$ is a nilideal in $B$.

In fact, let $b \in B$ such that $u(b) = 0$ ; one has $\mathrm{Pol.char}_{B/A}(X, b) = \mathrm{Pol.char}_{C/A}(X, u(b)) = X^n$, and from Hamilton-Cayley we deduce $b^n = 0$. □

The main source of Tschirnhaus morphisms is given by the following classical result (cf. e.g. [F], 4.3.1).

**2.2. Proposition** *Let $A \to C$ be a finite and locally free morphism of rank $n$. Let $c \in C$, and let $F(X) = N_{C/A}(X - c)$ be the characteristic polynomial of the map $C \to C$, $t \mapsto tc$. The Hamilton-Cayley theorem gives a morphism of $A$-algebras*

$$A[X]/(F) \to C, \quad X \mapsto c.$$

*This is a Tschirnhaus morphism. In particular, for $c = a \in A$, $A[X]/((X - a)^n) \to C$, $x \mapsto a$ is a Tschirnhaus morphism.*

Proof. Let $B = A[X]/(F)$ and let $u : B \to C$ be the morphism which sends the class $x$ of $X$ to $c$. Since the hypotheses are preserved by any base change, it is enough to proving that $N_C \circ u = N_B$. One has $N_B(X - x) = F(X)$ [1] $= N_C(X - u(x))$, thus for $a \in A$, $N_B(a - x) = N_C(a - u(x))$. Due to the multiplicativity of norms, we are reduced to proving that any $b \in B$ may be written as a product of elements of the form $a - x$ ; but $b = Q(x)$ for some polynomial $Q$ with $\deg Q(X) < \deg F(X)$ ; $b$ may also be written as $b = G(x)$, where $G = Q + F$ is now a monic polynomial in $A[X]$ ; thus there exists a free extension $A'$ of $A$ such that, in $A'[X]$, one has $G(X) = \Pi_i(X - a_i)$, showing that in $A' \otimes_A B$ one has $b = (x - a_1) \cdots (x - a_n)$. □

**2.3. Corollary** *Let $A$ be a ring and $\xi = (\xi_1, \cdots, \xi_n)$ be an element of $A^n$. Let $F(X) \in A[X]$ be a monic polynomial of degree $n$ such that $F(\xi_i) = 0$ for all $i$. Then the morphism of $A$-algebras*

$$A[X]/(F) \to A^n$$

*which sends the class of $X$ to $\xi$, is a Tschirnhaus morphism if and only if $F(X) = \Pi_i(X - \xi_i)$.* □

**2.4** (Tschirnhaus transformation)

Let $G(X) \in A[X]$ be a monic polynomial, and let $P(X) \in A[X]$ be any polynomial. Recall that the traditional *Tschirnhaus transfomation of $G$ by $P$* is the polynomial whose roots are the images by $P$ of those of $G$ ; precisely, let introduce a finite free extension $A'$ of $A$ such that $G$ splits in $A'[X]$ as $G(X) = \Pi_i(X - \xi_i)$ ; then the coefficients of $F(X) = \Pi_i(X - P(\xi_i))$ are symmetric expressions of the roots of $G$, thus $F \in A[X]$ ; it is the transformation of $G$ by $P$. But one can define $F$ without any reference to the roots of $G$ as follows : let $y$ be the class of $Y$ in the free $A$-algebra $C = A[Y]/(G(Y))$ ; then $F(X)$ is nothing but the characteristic polynomial of $c \mapsto cP(y)$, i.e. the norm

$$F(X) = N_{C[X]/A[X]}(X - P(y))$$

From (**2.2**), the morphism which sends $X$ to $P(y)$ induces a Tschirnhaus morphism

$$A[X]/(F) \to A[Y]/(G).$$

Conversely, given two monic polynomials $F, G \in A[X]$ of the same degree, and a Tschirnhaus morphism $u : A[X]/(F) \to A[Y]/(G)$, then $F$ is the Tschirnhaus transformation of $G$ by (any) polynomial $P$ such that $u(x) \equiv P(Y) \mod G$.

**2.5** To pay a tribute to L. Kronecker, and also to show the power of the property of norms from being polynomial laws, we give the following criterium ; it will not be used below.

**2.5.1 Proposition** *Let $A$ be a ring and let $u : B \to C$ be a morphism between locally free $A$-algebras of the same rank $r$. For $u$ to be a Tschirnhaus morphism it is necessary and sufficient that $u \otimes 1_{A[T]} : B[T] \to C[T]$ be norm compatible.*

1. As any undergraduate student knows, the matrix of $b \mapsto xb$ relative to the basis $(1, x, \cdots, x^{n-1})$ is the "companion matrix" of the polynomial $F$, which thus appears as the characteristic polynomial of the matrix.

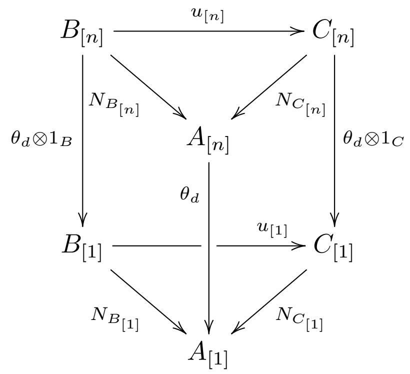
Proof. In this proof we lighten notations by letting $A_{[n]} = A[T_1, \cdots, T_n]$. For proving sufficiency we first show that if $u_{[1]} : A_{[1]} \otimes_A B \to A_{[1]} \otimes_A C$ is norm compatible, then for any positive integer $n$, $u_{[n]}$ is norm compatible. For doing so we use the *Kronecker substitution* : let $d > 1$ be an integer ; the Kronecker substitutions (relative to $d$) $\theta_d : A_{[n]} \to A_{[1]}$, is the morphism of $A$-algebras

$$\theta_d : A[T_1, \cdots, T_n] \longrightarrow A[T], \quad \text{defined by} \quad \theta(T_i) = T^{d^{i-1}}.$$

The image of a monomial $T_1^{m_1} \cdots T_n^{m_n}$ is equal to $T^m$ with $m = m_1 + m_2 d + \cdots + m_n d^{n-1}$ ; under the condition that $0 \leq m_i < d$ for all $i$, this expression of $m$ is its "$d$-adic expansion", and thus it is unique. In other words, if $\Theta \subset A[T_1, \cdots, T_n]$ denotes the set of polynomials whose all partial degrees are $< d$, then the restriction of $\theta_d$ gives an *injective* map (designated by the same letter)

$$\theta_d : \Theta_d \longrightarrow A[T].$$

Now let $x \in B_{[n]} = A_{[n]} \otimes_A B$, and let $u_{[n]}(x)$ its image in $C_{[n]}$ ; we have to check that the polynomials $N_{B_{[n]}}(x)$ and $N_{C_{[n]}}(u_{[n]}(x))$ in $A_{[n]}$ are equal. Choose an integer $d$ strictly greater than all the partial degrees in the variables $T_i$ in both these polynomials ; thus $N_{B_{[n]}}(x)$ and $N_{C_{[n]}}(u_{[n]}(x))$ are inside the subset $\Theta_d \subset A_{[n]}$. Consider the following diagram.




The two front faces of the prism are commutative diagrams because norms are polynomial laws ; the third is also commutative because it is nothing but a base change ; the lower triangle is commutative by assumption, and $\theta_d$ is an injective map when restricted to $\Theta_d$ ; thus $N_{B_{[n]}}(x) = N_{C_{[n]}}(u_{[n]}(x))$.

Finally, let $A \to A'$ be any algebra, and let $y = \sum_1^n a'_i \otimes b_i$ be an element in $A' \otimes_A B$ ; consider the morphism of $A$-algebras $A_{[n]} \to A'$ defined by $T_i \mapsto a'_i$, and let $z \in A_{[n]} \otimes_A B$ be defined by $z = \sum T_i \otimes b_i$ ; the preceding step shows that the norm of $z$ and the norm of $u_{[n]}(z) \in C_{[n]}$ are equal in $A_{[n]}$ ; so the norm of $y$ and the norm of its image in $A' \otimes_A C$ are equal. □

## 3. The generic element

**3.1** *The generic element of a projective $A$-module $M$ of finite type*

Denote by $M^\vee = \mathrm{Hom}_A(M, A)$ the dual of the $A$-module $M$. We define an isomorphism

$$M^\vee \otimes_A M \quad \widetilde{\longrightarrow} \quad \mathrm{End}_A(M)$$

by sending $u \otimes x \in M^\vee \otimes_A M$ to the endomorphism $y \mapsto u(y)x$. We let

$$\xi_M \in M^\vee \otimes_A M$$

be the element corresponding to the identity map of $M$ via the above isomorphism ; explicitely, let $(x_1, \cdots, x_n)$ be a generating system for $M$, and let $v : A^n \to M$ be the surjective linear map associated to it ; since $M$ is projective, one has a map $u : M \to A^n$ such that $vu = 1_M$ ; by writing $u = (u_1, \cdots, u_n)$, we have $\xi_M = \sum u_i \otimes x_i$.

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

$$\gamma_x : \mathrm{Sym}_A(M^\vee) \to A.$$

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

$$\gamma_x \otimes 1 : \mathrm{Sym}_A(M^\vee) \otimes_A M \to M.$$

More generally,

**3.1.2. Lemma** *For any $A$-algebra $A'$, consider the maps*

$$A' \otimes_A M \quad \longrightarrow \quad \mathrm{Hom}_A(M^\vee, A') \quad \longrightarrow \quad \mathrm{Hom}_{A-\mathrm{Alg}}(\mathrm{Sym}_A(M^\vee), A')$$

*where the first one is given by $a' \otimes x \longmapsto (u \mapsto u(x)a')$, and the second map comes from the definition of the symmetric algebra. Then the composite map defines an isomorphism of functors $\mathbf{Alg}_A \to \mathbf{Ens}$. In the opposite direction, a morphism of $A$-algebras $\gamma : \mathrm{Sym}_A(M^\vee) \to A'$ induces a morphism $\gamma \otimes 1_M$ : $\mathrm{Sym}_A(M^\vee) \otimes_A M \to A' \otimes_A M$, from which we get the element $(\gamma \otimes 1_M)(\xi_M) \in A' \otimes_A M$.*

**3.1.3.** If $M$ is a free $A$-module with basis $(e_i)$, and if $(e_i^\vee)$ denotes the dual basis, one has :

$$\xi_M = \sum_i e_i^\vee \otimes e_i.$$

The ring of parameters $\mathrm{Sym}_A(M^\vee)$ is then isomorphic to the polynomial ring $A[T_1, ..., T_n]$, where $T_i$ stands for the linear form $e_i^\vee$ ; with these notations, $\mathrm{Sym}_A(M^\vee) \otimes_A M$ is isomorphic to the $A[T_1, ..., T_n]$-module $M[T_1, \cdots, T_n]$, and the generic element may be written as

$$\xi_M = \sum_i e_i T_i \in M[T_1, \cdots, T_n].$$

### 3.2 *The generic element of a locally free algebra $A \to B$*

Applying the above construction to the $A$-module $B$, we get the generic element

$$\xi_B \in \mathrm{Sym}_A(B^\vee) \otimes_A B.$$

Writing $\xi_B = \sum \beta_i \otimes x_i$, with $\beta_i \in B^\vee$ and $x_i \in B$, one has by definition, for $b \in B$, $b = \sum \beta_i(b) x_i$, and, in particular

$$1_B = \sum \beta_i(1_B) x_i.$$

**3.2.1 Lemma.** *Let $f : A \to B$ be a finite locally free algebra. If the linear map $f$ is injective, it admits a* retraction, *that is a $A$-linear map $\tau : B \to A$ such that $\tau(1_B) = 1_A$ ; in other words, the sequence of $A$-modules $0 \to A \to B \to B/A \to 0$ is split, where we write $B/A$ for the cokernel of $f$ ; it is a projective $A$-module.*

Proof. This is stated in [AC, II §5, Exerc.4], but it may be given a direct proof, as follows. First note that the linearity of $\tau$ means that, for $a \in A$ and $b \in B$, one has $\tau(f(a)b) = a\tau(b)$ ; that implies, with $b = 1_B$, that $\tau \circ f = \mathrm{Id}_A$ ; so $\tau$ is indeed a retraction of $f$. Now, keeping the notations of the beginning of (**3.2**), let $I$ be the ideal in $A$ generated by the elements $\beta_i(1_B)$ ; since $B = IB$ the usual Nakayama trick implies the existence of $a \in I$ such that $(1_A - a)1_B = 0$ ; but $f$ is injective, so $1_A = a$ ; since $I$ is generated by the $\beta_i(1_B)$, one has $1_A = \sum a_i \beta_i(1_B)$, so $\tau = \sum a_i \beta_i$ is a retraction of $f$. □

**3.2.2 Remark.** Let $f : A \to B$ a finite locally free algebra ; let $J = \mathrm{Ker}(f)$. We will show that there exists an idempotent $e \in A$, such that $J$ is generated by $1 - e$, and such that $B = eB$.

In fact, for any $A/J$-module $M$, one has $\mathrm{Hom}_{A/J}(B, M) = \mathrm{Hom}_A(B, M)$, thus $B$ is projective also as an $A/J$-module. From the above lemma there exists a retraction $\tau : B \to A/J$ ; the projectivity of $B$ as an $A$-module implies the existence of a $A$-linear map $\tau'$ and a commutative triangle

$$\begin{array}{ccc} & & B \\ & \swarrow^{\tau'} & \downarrow \tau \\ A & \longrightarrow & A/J \end{array}$$

Let $e = \tau'(1_B)$ ; one has $1_A - e \in J$, so $0 = f(1_A - e) = 1_B - f(e)$ ; that implies $B = eB$ ; but $\tau'$ is $A$-linear thus $eJ = \tau'(1_B J) = 0$, hence $e$ is an idempotent, and $1 - e$ generates $J$.

*In conclusion, $f$ is injective if and only if, for each prime ideal $\mathfrak{p}$ of $A$, the rank of $B$ at $\mathfrak{p}$ is $> 0$, i.e. $\kappa(\mathfrak{p}) \otimes_A B \neq 0$, or, equivalently, if and only if the map $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ be surjective ; it is the case when $B$ is of constant rank $> 0$.*

**3.2.3.** Below we shall introduce a morphism $\mu : \mathrm{Sym}_A(B^\vee) \to \mathrm{Sym}_A(B^\vee)[T]$ - not the canonical one-, which will appears "natural" from the point of view of vector bundles, in the sense of [EGA I, (9.4.9)].

Recall that, for an $A$-module $M$, $\mathbf{V}(M)$ denotes the *vector bundle associated to* $M$, that is the covariant functor from the category of $A$-algebras to the category of groups,

$$A' \mapsto \mathrm{Hom}_{A-\mathrm{Mod}}(M, A') = \mathrm{Hom}_{A-\mathrm{Alg}}(\mathrm{Sym}_A(M), A').$$

Thus this functor is represented by $\mathrm{Sym}_A(M)$.

A linear map $\varphi : M \to N$ induces, by composition on the right, $v \mapsto v\varphi$, a morphism of functors $\mathbf{V}(N) \xrightarrow{\mathbf{V}(\varphi)} \mathbf{V}(M)$, and a morphism of $A$-algebras $\mathrm{Sym}_A(M) \xrightarrow{\mathrm{Sym}_A(\varphi)} \mathrm{Sym}_A(N)$.

Let $0 \to M' \to M \xrightarrow{p} M'' \to 0$ be an exact sequence of $A$-modules. We have a morphism of functors

$$\mathbf{V}(M'') \times \mathbf{V}(M) \longrightarrow \mathbf{V}(M) \times_{\mathbf{V}(M')} \mathbf{V}(M), \quad (u'', u) \longmapsto (u''p + u, u). \tag{3.2.3.1}$$

It is clearly an isomorphism and thus it allows one to see $\mathbf{V}(M)$ as a torsor in the category of functors over $\mathbf{V}(M')$ under the additive group $\mathbf{V}(M'')$. Note that the projection onto the left hand factor of the fiber product over $\mathbf{V}(M')$, namely

$$\mathbf{V}(M'') \times \mathbf{V}(M) \longrightarrow \mathbf{V}(M) \tag{3.2.3.2}$$

is associated to the linear map

$$M \longrightarrow M'' \times M, \quad x \longmapsto (px, x)$$

**3.2.4** Suppose now that the morphism $f : A \to B$ is injective ; from lemma (**3.2.1**), the following sequence of $A$-modules is exact :

$$0 \to (B/A)^\vee \to B^\vee \xrightarrow{\beta \mapsto \beta_{|A}} A^\vee \to 0. \tag{3.2.4.1}$$

We write $S = \mathrm{Sym}_A(B^\vee)$, and $S_0 = \mathrm{Sym}_A((B/A)^\vee)$ for this $A$-subalgebra of $S$.

We now apply the construction from **3.2.3.** to the above sequence. The map $p : M \to M''$ is here the map $B^\vee \to A^\vee, \beta \mapsto \beta_{|A}$ "restriction to $A$" ; denoting by $T$ the canonical basis of the $A$-module $A^\vee$, we have a canonical isomorphism $\mathrm{Sym}_A(A^\vee) = A[T]$, and the morphism $B^\vee \to A^\vee$ may be written as $\beta \mapsto \beta(1)T$. The projection (3.2.3.2) induces on the $A$-algebras representing the involved functors the morphism of $S_0$-algebras

$$\mu : S = \mathrm{Sym}_A(B^\vee) \longrightarrow \mathrm{Sym}_A(A^\vee) \otimes_A \mathrm{Sym}_A(B^\vee) \simeq A[T] \otimes_A \mathrm{Sym}_A(B^\vee) = S[T];$$

it is given by extending to the symmetric algebra the map defined, for $\beta \in B^\vee$, by

$$\beta \longmapsto \beta(1)T + \beta.$$

This morphism $\mu : S \to S[T]$ is clearly *not* the usual canonical morphism of $S$-algebras ; however it is faithfully flat and smooth. In fact, from lemma **3.2.1** we may choose a retraction $\tau : B \to A$ of $f$, in order to get a linear bijection $(B/A)^\vee \oplus A^\vee \xrightarrow{\sim} B^\vee$, and thus an isomorphism of algebras

$$\mathrm{Sym}((B/A)^\vee) \otimes \mathrm{Sym}(A^\vee) = S_0[T] \xrightarrow{\sim} S = \mathrm{Sym}(B^\vee).$$

This isomorphism depends on the choice of $\tau$ (and it should have been referred to by the slogan : « a torsor with a rational point is trivial ») ; at any rate we get from it a morphism $\varphi : S_0 \to S_0[T] \simeq S$ which is faithfully flat and smooth.

**3.2.5.** Now, the isomorphism (3.2.3.1) between functors implies that the following square is cocartesian :

$$\begin{array}{ccc} S & \xrightarrow{\mu} & S[T] \\ {\scriptstyle\varphi}\uparrow & & \uparrow{\scriptstyle\mathrm{can}} \\ S_0 & \xrightarrow[\varphi]{} & S \end{array} .$$

From this square it is clear that $\mu$ is faithfully flat and smooth.

**(3.3)** *Norm of the generic element*

The morphism of $S_0 \otimes_A B$-algebras $\mu_B := \mu \otimes 1_B : S \otimes_A B \to S[T] \otimes_A B$ is faithfully flat and smooth ; one has

$$\mu_B(\xi_B) \;=\; T \otimes 1 + \xi_B.$$

In fact, if we write $\xi_B = \sum \beta_i \otimes x_i$, with $\beta_i \in B^\vee$ and $x_i \in B$, one has $\mu_B(\sum \beta_i \otimes x_i) = \sum(\beta_i(1)T + \beta_i) \otimes x_i = T \otimes (\sum \beta_i(1)x_i) + \xi_B = T \otimes 1 + \xi_B$.

*In the sequel, we shall write $T$ instead of $T \otimes 1 \in S[T] \otimes B$.*

To lighten the expression of the norm maps, we write, for any $A$-algebra $A \to A'$,

$$\mathrm{N}_{B;A'} \;:=\; \mathrm{N}_{A' \otimes_A B/A'};$$

so the second index indicates the target of the norm map. The polynomial $F_{B/A}(T) = \mathrm{N}_{B;S[T]}(T - \xi_B) \in S[T]$ is the generic characteristic polynomial discussed in the next paragraph (cf. **4.1**).

**Proposition 3.3.1.** *Let $A \to B$ be a locally free morphism of rank $n$. With the notations above, one has :*

1. *The generic element $\xi_B$ is regular in $S \otimes_A B$, and the quotient of that ring by the ideal generated by $\xi_B$ is smooth over $B$ ;*
2. *the morphism $\mu$ induces a faithfully flat morphism*

$$S/\mathrm{N}_{B;S}(\xi_B)S \longrightarrow S[T]/(F),$$

*where $F = F_{B/A}(T)$ ; this morphism is smooth of relative dimension 1 ;*

3. *the $S_0$-algebra $S/\mathrm{N}_{B;S}(\xi_B)S$ is locally free of rank $n$.*

Recall that an element $s$ in a ring $S$ is said to be *regular* (= nonzerodivisor) if the map $S \to S,\ x \mapsto sx$ is injective.

*Proof* : 1) The morphism $\mu_B : S \otimes B \to S[T] \otimes B$ is faithfully flat, hence injective, and we have $\mu_B(\xi_B) = T + \xi_B$ ; thus the regularity of $\xi_B$ follows from the regularity of $T + \xi_B$ in $S[T] \otimes B$.

From **(3.2.5.)** the composite morphism of $S_0 \otimes B$-algebras, induced by $\mu_B$

$$S \otimes B/(\xi_B) \xrightarrow{\overline{\mu_B}} S[T] \otimes B/(T + \xi_B) \xrightarrow{T \mapsto -\xi_B} S \otimes B$$

is faithfully flat and smooth. (If, for example, $A = B$, then $S \otimes B = A[X]$, and $\xi_B = X$ ; so the above map is nothing but the familiar one : $A[X]/(X) \xrightarrow{X \mapsto T+X} A[X+T]/(X+T) \xrightarrow{T \mapsto -X} A[X]$.)

2) The following square with straight arrows is cocartesian

$$\begin{array}{ccc} S \otimes B & \xrightarrow{\mu_B} & S[T] \otimes B \\ {\scriptstyle\mathrm{N}_{B;S}}\downarrow\uparrow & & \uparrow\downarrow{\scriptstyle\mathrm{N}_{B;S[T]}} \\ S & \xrightarrow[\mu]{} & S[T] \end{array}$$

Therefore the curved square with the norm maps is commutative ; thus one has

$$\mu(\mathrm{N}_{B;S}(\xi_B)) = \mathrm{N}_{B;S[T]}(\mu_B(\xi_B)) = \mathrm{N}_{B;S[T]}(T + \xi_B).$$

From this and **(3.2.5)**, we deduce that the following square is cocartesian, where $P(T) = \mathrm{N}_{B;S[T]}(T+\xi_B)$

$$\begin{array}{ccc} S/\mathrm{N}_{B;S}(\xi)S & \longrightarrow & S[T]/(P(T)) \\ \uparrow & & \uparrow \\ S_0 & \xrightarrow[\varphi]{} & S \end{array}$$

3) Since $P(T) = \mathrm{N}_{B;S[T]}(T+\xi_B)$ is a monic polynomial of degree $n$ with coefficients in $S$, and using the faithfull flatness of $\varphi$, one sees that $S/\mathrm{N}_{B;S}(\xi)S$ is locally free of rank $n$ over $S_0$. Finally, $(-1)^n P(-T) = \mathrm{N}_{B;S[T]}(T-\xi_B)$ is the characteristic polynomial of $\xi_B$, which is denoted by $F_{B/A}$ in the next section. □

## 4. The Kronecker morphism

### 4.1 Definition and examples

Let $A \to B$ be a finite and locally free morphism. Let

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

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 $\mathrm{Sym}_A(B^\vee)$-algebras

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

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

**4.1.1** As a first example, consider $B = A^n$, and choose the canonical basis $(e_i)$ for $A^n$. The ring of parameters $\mathrm{Sym}_A(B^\vee)$ is then isomorphic to $S = A[T_1, \ldots, T_n]$, where $T_i$ stands for the $i$-th projection $A^n \to A$. 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 $X \mapsto (T_1, \ldots, T_n)$.

It is injective since the Van der Monde determinant $\prod_{i<j}(T_j - T_i)$ is a regular element in $S$ (but it is not invertible if $n \geq 2$).

More generally, let $A \to B$ be a finite étale morphism of rank $n$ ; its generic characteristic polynomial $F_{B/A}$ is locally isomorphic to $\prod_{i=1}^{n}(X - T_i)$, thus, for $n \geq 2$, the morphism $\mathrm{Sym}_A(B^\vee) \to \mathrm{Sym}_A(B^\vee)[X]/(F_{B/A})$ is **not étale**.

**4.1.2** The next example is not illuminating ! Let $B = A[Y]/(G)$ 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 $\xi_B = T_0 + T_1y + T_2y^2$, then

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

From this, it is not even clear if the Kronecker morphism is injective ; in fact it is (cf. **4.2** below).

**4.1.3** Let $B = A[u, v]$ with $u^2 = v^2 = 0$ ; so $A \to B$ is a complete intersection morphism ; the ideal $J = uB + vB$ is a free $A$-module of rank 3, and $J^3 = 0$ ; thus $B$ is a radicial $A$-algebra of rank 4. Writing the generic element as $\xi = T_0 + T_1 u + T_2 v + T_3 uv$, 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.

**Theorem 4.2** (Injectivity of the Kronecker morphism) *Let $A \to B$ be a finite and locally free morphism of rank $n$. Then the following conditions are equivalent :*

*i) $B$ is locally monogenous 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 it remains injective after any base change $A \to A'$.*

Proof. *i)* ⇒ *ii)*. We can suppose $B$ to be monogenous, hence of the form $A[Y]/(G)$, where $G$ is a monic polynomial of degree $n$. We write $y$ 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

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

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

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

with the $s_i$ in $S$, implies that all the $s_i$ are zero ; in other words, one has to show that the family $(1, \xi, ..., \xi^{n-1})$ 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 nonzerodivisor) element in $S$.
Let $U_{ij} \in S$ be the polynomials defined by

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

Each of the polynomials $U_{ij}$ is homogeneous in $T_0, T_1, \dots, T_{n-1}$, of degree $j$ ; in fact, introducing a new variable $T$, we have to check the equality $U_{ij}(TT_0, TT_1, \cdots, TT_{n-1}) = T^j U_{ij}(T_0, \cdots, T_{n-1})$ ; but the left hand side is nothing but the coefficient of $(T\xi)^j$ on the basis element $y^i$ ; hence the equality. Therefore the determinant $U = \det(U_{ij})$ is a homogeneous polynomial of degree $N = 1 + 2 + \cdots + n - 1$.

On the other hand, one has $U(0, T_1, 0, \dots, 0) = T_1^N$ : in fact consider the morphism of $A$-algebras $S \to S$ defined by $T_i \mapsto 0$ for $i \neq 1$, and its extension to $S \otimes_A B$ ; it sends $\xi$ to $T_1 y$, and thus $\xi^j$ is mapped to $T_1^j y^j$ ; the image of the matrix $(U_{ij})$ is the diagonal matrix $\mathrm{diag}(1, T_1, \dots, T_1^{n-1})$, and thus $U(0, T_1, 0, \dots, 0) = T_1^N$.

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 $A \to A'$.

**4.2.1.** As an explicit example, let us go back to the monogenous algebra of degree 3 in (**4.1.2**) ; some by hand calculations give, as expected, a monic polynomial in $T_1$ for the determinant :

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

Before proving the implication *ii)* ⇒ *i)*, we recall a linear algebra fact.

**4.2.2. Lemma** *Let $R$ be a ring, and let $u : M \to N$ be a $R$-linear map between projective $R$-modules of the same rank $n$. The $R$-modules $\wedge^n M$ and $\wedge^n N$ are invertible (i.e. of rank 1), and so is*

$$L = \mathrm{Hom}_R(\wedge^n M, \wedge^n N).$$

*Consider the image of $\lambda = \wedge^n u$ in $\mathrm{Sym}_R(L)$, and the quotient $R_\lambda = \mathrm{Sym}_R(L)/(\lambda - 1)$. Then*

*(a) The morphism $R \to R_\lambda$ is flat, and the image of $\mathrm{Spec}(R_\lambda) \to \mathrm{Spec}(R)$ is the open set $\mathcal{U}$ of the primes $\mathfrak{p}$ such that $M_\mathfrak{p} \to N_\mathfrak{p}$ is bijective.*

*(b) The map $u$ is injective if and only if $\wedge^n u$ is, and this is also equivalent to $R \to R_\lambda$ being injective; in particular, the open set $\mathcal{U}$ is then non empty (if $R \neq 0$).*

The notation $R_\lambda$ is indeed unusual since $\lambda$ is not an element in $R$; but if it were, then the usual fractions ring $R_\lambda$ would have been written as $R[T]/(\lambda T - 1)$, which is exactly $\mathrm{Sym}_R(L)/(\lambda - 1)$ when $L$ is free with basis noted $T$. Since the $R$-module $L$ is locally isomorphic to $R$, to check the lemma, we can suppose that $M$ and $N$ are free, but then the part (a) rests on the well known relations between a square matrix and its determinant; the equivalence in part (b) comes from [A], III, §8.2, Prop. 3, p.524. □

**Proof of the implication** *ii*) ⇒ *i*) of **Theorem 4.2**. Suppose now that the Kronecker morphism is injective; we will define a faithfully flat morphism $A \to A'$ such that the $A'$-algebra $A' \otimes_A B$ be monogenous. Simplify the notation as

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

Both sides are projective $S$-modules of the same rank $n$, so we can apply the above lemma whose we adopt the notations; now the symbol $\wedge^n$ denotes the wedge power as $S$-module. We introduce the invertible $S$-module $L = \mathrm{Hom}_S(\wedge^n(S[X]/(F)), \wedge^n(S \otimes_A B))$, and its element $\lambda = \wedge^n u$; the spectrum of $S_\lambda$ defines the open set $\mathcal{U} \subset \mathrm{Spec}(S)$ where $u$ is an isomorphism. So the morphism

$$u_\lambda : S_\lambda[X]/(F) \longrightarrow S_\lambda \otimes_A B$$

is an isomorphism; in particular, the $S_\lambda$-algebra on the right is monogenous. It remains to check that the morphisme $A \to S_\lambda$ is faithfully flat, i.e. that the morphism $\mathcal{U} \to \mathrm{Spec}(A)$ is surjective; but it is an immediate consequence of the hypothesis that $u$ remains injective after any base change $A \to A'$. □

**4.2.3.** (Back to the *Zahlbericht* of HILBERT ) In the §§10 and 11 of this memoir, the base ring is $A = \mathbf{Z}$ and the algebra $B$ is the ring of integers of a number field $K$, hence it is a monogenous $\mathbf{Z}$-algebra. The generic element $\xi$ is called by Hilbert the *fundamental form*, and the generic characteristic polynomial is denoted by $F$; the relation $F = 0$ is said the fundamental equation of the ring.

The theorem 34 of the *Zahlbericht* says :

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

It is an other way for stating the injectivity property *ii*) of ( **4.2.2**), when the base ring is $\mathbf{Z}$.

**Remark 4.2.4.** An alternative proof of the implication *ii*) ⇒ *i*) of (**4.2**) 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 $n = \mathrm{rank}_K(R)$, and an* injective *morphism of $S$-algebras $u : S[X]/(F) \to S \otimes_K R$. Then $R$ is a monogenous $K$-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

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

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, $J^{n-1} \neq 0$. 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 monogenous.

**Corollary 4.2.5.** *Let $A \to B$ be a finite locally free and locally monogenous morphism. If the ring $B$ is reduced (resp. a domain, a connected ring) then the same is true for the ring $S/\mathrm{N}_{B;S}(\xi_B)S$.*

Proof. By composing the Kronecker morphism (**4.2**) with the morphism $\mu$ from the proposition (**3.3**), we get a morphism of $A$-algebras

$$S/\mathrm{N}_{B;S}(\xi_B)S \quad \longrightarrow \quad S \otimes_A B$$

which is injective, even after any base change $A \to A'$ ; moreover, the properties of the ring $B$ taken into account in the statement are transfered to the ring $S \otimes_A B$, and also to its subring $S/\mathrm{N}_{B;S}(\xi_B)S$. $\square$

This result has most probably been noticed already, at least for field extension, as the sentence : *If $K \to L$ is a monogenous field extension of degree $n$, the norm of the generic element is an irreducible polynomial in $K[T_1, \cdots, T_n]$.*

**Remark 4.2.6.** The simplest non monogenous field extension is

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

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

**Remark 4.3.** (O. Loos) The injectivity of the Kronecker morphism means that the characteristic polynomial $F_{B/A}$ is also the minimum polynomial of the generic element, as already pointed out by Hilbert. The following remarks, which elaborate this idea, are essentially due to O. Loos.

First suppose that $A = K$ is a field ; let $L$ be the field of fractions of the polynomial ring $S = \mathrm{Sym}_K(B^\vee)$ ; denote by $\xi_L \in L \otimes_A B$ the image of the generic element of $S \otimes_A B$. Let $\mu[X] \in L[X]$ be the monic minimum polynomial of $\xi_L$ ; since the characteristic polynomial $F_{B/A}(X) \in S[X]$ is a multiple of $\mu(X)$, a classical result (Dedekind ?) asserts that the coefficients of $\mu(X)$ are in the integrally closed ring $S$. This polynomial $\mu(X) \in S[X]$ will be called the *generic minimum polynomial.*

In the paper [L] on Jordan algebras, O. Loos gives a statement (lemma (2.8)), which looks close to the above theorem, whose we keep the notations. Instead of the characteristic polynomial $F_{B/A}$, Loos consider a monic polynomial $G \in S[X]$ of degree $n$ whose the generic element $\xi$ is a root ; let

$$v : S[X]/(G) \longrightarrow S \otimes_A B$$

be the associated morphism of $S$ algebras. Loos does not assume the injectivity of $v$ but only the injectivity of the maps $v_K = v \otimes_A 1_K$ for all morphisms $A \to K$ to a field ; in other words, he supposes that, for all $K$, $G_K$ is the generic minimum polynomial over $K$. He proves that such a polynomial $G$ exists if and only if $B$ is locally monogenous . Assuming that such a polynomial $G$ exists, Loos consider the open set $\mathcal{V} \subset \mathrm{Spec}(S)$ of those primes $\mathfrak{n}$ such that $v_{\kappa(\mathfrak{n})}$ is bijective ; he then uses [EGA III] 11.10.10, to deduce that $\mathcal{V}$ is schematically dense in $\mathrm{Spec}(S)$, and so that $B$ is locally monogenous, as in the end of the proof of (**4.3**).

Conversely, if $B$ is locally monogenous, Loos proves that one can take for $G(X)$ the generic characteristic polynomial.

## 5 Discriminant of the generic characteristic polynomial

**5.1** The Theorem 35 of the *Zahlbericht* [H] states that

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

Hilbert pointed out that this property is a consequence of the injectivity of the Kronecker morphism. The discriminant of $F(X)$ is an element of the ring containing the coefficients of $F$, namely $\mathrm{Sym}_A(B^\vee)$ ; in the context of the *Zahlbericht*, this ring is isomorphic to the factorial ring $\mathbf{Z}[T_1, \ldots, T_n]$, 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*).

Although it may mean extending the definition of the *content* in non factorial situation, we get the following general result.

**5.2 Proposition** *Let $A \to B$ be a finite locally free and locally monogenous morphism of rank $n$. Then the content of the discriminant of $F_{B/A}(X)$ is equal to the discriminant of $B$.*

**5.2.1** First recall the general definition of the **content** (see, for example [SGA 3], $VI_B$, théorème 6.2.3, p. 374). Let $A \to S$ be an $A$-algebra, and let $u : M \to L$ be a $S$-linear map between $S$-modules. Denote by $\Im$ the set of those ideals $I$ in $A$ such that $u$ induces the zero map $M/IM \to L/IL$. If $\Im$ contains a unique minimal ideal, this ideal is called the *content* of $u$ and it is denoted by $\mathsf{Ct}_{S/A}(u)$, or, simply $\mathsf{Ct}(u)$ when the context is clear.

**5.2.2. Lemma** *Let $A \longrightarrow S$ be a morphism such that, locally for the Zariski topology on* $\mathrm{Spec}(A)$*, the $A$-module $S$ is free, possibly with an infinite basis, and let $u : M \to L$ be a $S$-linear map between $S$-modules where $L$ is an invertible $S$-module. Then $u$ has a content.*

Proof. Let $L^{-1} = \mathrm{Hom}_S(L, S)$ be the inverse of $L$, and let $u' : M \otimes_S L^{-1} \to S$ be the map associated with $u$ ; the set of ideals $\Im$ is the same for $u$ and for $u'$ ; so one can suppose that $L = S$, and we denote by $J \subset S$ the ideal $\mathrm{Im}(u')$ ; moreover an easy gluing consideration reduces to the case where $S$ is free over $A$. Then, choose a basis $(e_\lambda)$ of $S$ as $A$-module ; let $e_\lambda^\vee : S \to A$ be the "coordinate" linear form attached to $e_\lambda$. Consider the ideal in $A$

$$I = \sum_\lambda e_\lambda^\vee(J) \tag{5.2.2.1}$$

generated by the coordinates of the elements in the ideal $J$. It is clear that $I$ is the sought-for content. It is also clear that this construction commutes with any base change $A \to A'$ in the sense that the ideal $\mathsf{Ct}(u)A' \subset A'$ generated by the image in $A'$ of the content of $u$, is the content of the map $u \otimes_A 1_{A'}$ of $A' \otimes_A S$ modules (For details, see *loc. cit.*, end of the proof, p.375). □

**Lemma 5.2.3** *Let $A \to S$ be as in lemma* **5.2.2** *above. Let $N \overset{v}{\to} M \overset{u}{\to} L$ be $S$-linear maps between three invertible $S$-modules. We suppose that $v$ is injective and that it remains injective under any base changes $A \to A'$. Then $Ct(uv) = Ct(u)$.*

Proof. Since the map $v$ is « universally injective as $A$-linear map », the very definition of its content shows that $\mathsf{Ct}(v) = A$. By restricting to affine open sets of $\mathrm{Spec}(A)$, we may suppose that $S$ is free, and using a basis, we dispose, as in the proof of lemma (**5.2.2**), of a family of $A$-linear maps $w_\lambda : M \to N$ such that $\sum_\lambda w_\lambda(M) = \mathsf{Ct}(v)N = N$ ; then, we can introduce the affine open subsets $U_\lambda \subset \mathrm{Spec}(A)$ where $w_\lambda$ is surjective, and thus bijective, since $M$ and $N$ are invertible ; on these open sets, one has $\mathsf{Ct}(uv) = \mathsf{Ct}(u)$ ; but, due to the expression (**5.2.2.1**) of the content, these open sets cover $\mathrm{Spec}(A)$ since $\mathsf{Ct}(v) = A$. □

**5.2.4** Let us recall what the **discriminant** is. Let $S \to E$ be a finite morphism, locally free of rank $n$ ; we let $E^\vee = \mathrm{Hom}_S(E, S)$ ; the $S$-linear map $\mathrm{Tr}_{E/S} : E \to S$ induces a $S$-linear map

$$\alpha : E \to E^\vee, \quad x \mapsto (y \mapsto \mathrm{Tr}_{E/S}(xy));$$

its extension to the $n$-th exterior power $\wedge^n\alpha : \wedge^n E \to \wedge^n(E^\vee) = (\wedge^n E)^\vee$ leads to an $S$-linear map

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

its image is called the discriminant of $E/S$ ([EGA $IV_4$],18.2.7, (ii)).

If $F(X) \in S[X]$ is a monic polynomial, the discriminant of the $S$-algebra $E = S[X]/(F)$ is the ideal generated by the usual discriminant of the polynomial $F$.

**5.2.5** Proof of (**5.2**) In the situation under consideration, the Kronecker morphism

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

is compatible with the traces (**2.2**), 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 $A$-universally injective (**4.3**). Therefore $\wedge^n u$ is also $A$-universally injective ([A] III 8.2 Prop.3), and $\mathsf{Ct}_{S/A}((\wedge^n u)^{\otimes 2}) = A$ ; from lemma (**5.2.3**) we deduce that

$$\mathsf{Ct}_{S/A}(d_{E/S}) = \mathsf{Ct}_{S/A}(d_{B/A} \otimes \mathrm{id}_S) = \mathrm{Im}(d_{B/A}).$$

□

**5.2.6 Remark** From the proposition **5.2**, we see that if $A \to B$ is étale, i.e. if $d_{B/A}$ is an isomorphism, then $\mathsf{Ct}_{S/A}(d_{E/S}) = A$ ; but that does not mean that $S[X]/(F)$ is étale *over* $S$ ; for example, for $B = A^n$, the characteristic polynomial is, as seen in (**4.2.1**), $F(X) = \prod(X - T_i)$ ; it is not separable over $A[T_1, \cdots, T_n]$ if $n \geq 2$.

# Références


[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)

[EGA I] A. Grothendieck, J. Dieudonné *Éléments de Géométrie algébrique, III : Étude cohomologique des faisceaux cohérents*, Publ. Math. IHÉS no 11 (1961) et 17 (1963).

[EGA III] A. Grothendieck, J. Dieudonné *Éléments de Géométrie algébrique, III : Étude cohomologique des faisceaux cohérents*, Publ. Math. IHÉS no 11 (1961) et 17 (1963).

[EGA $IV_4$] A. Grothendieck, J. Dieudonné *Éléments de Géométrie algébrique* Publ. Math. IHÉS no. 32, (1967).

[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

[L] O. LOOS, *Generically algebraic Jordan algebras over commutative rings*, Journ. of Algebra, 297,(2006) 474-529.

[SGA 3] M. Demazure, A. Grothendieck, *Schémas en groupes*, Documents mathématiques n$^o$ 7, Soc. Math. France, (2011).

[W] H. WEYL, Algebraic Theory of Numbers, *Ann. of Math. Studies, no 1*, Princeton (1940)



Sorbonne Université
IMJ-PRG, Case 247
4 place Jussieu, 75252 Paris Cedex 05, France
daniel.ferrand@imj-prg.fr