ALGEBRA AND NUMBER THEORY :(2008)

On the algebra of some group schemes

Daniel Ferrand

The algebra of a finite group over a field k of characteristic zero is known to be a projective separable k-algebra; but these separable algebras are of a very special type, characterized by Brauer and Witt.

In contrast with that, we prove that *any* projective separable k-algebra is a quotient of the group algebra of a suitable *group scheme*, finite étale over k. In particular, any finite separable field extension $K \subset L$, even a noncyclotomic one, may be generated by a finite étale K-group scheme.

Introduction

Following Wedderburn and Brauer, the rational group algebra $\mathbb{Q}\langle\Gamma\rangle$ of a finite group Γ may be described as follows: its center is a product $K_1 \times \cdots \times K_s$ of fields, each isomorphic to a subfield of the cyclotomic extension $\mathbb{Q}(\zeta_m)$, where m is the exponent of Γ, and the group algebra itself is a product $A_1 \times \cdots \times A_s$, where A_i is a central simple K_i-algebra.

In general, the factors K_i of the center are not *equal* to cyclotomic extensions of $\mathbb{Q}$, i.e., they cannot be generated themselves by a finite group, as shown by the following example (which I owe to Vincent Beck). Let p be a prime; denote by $L = \mathbb{Q}(\zeta_p)$ the cyclotomic extension of level p. Let $S \subset \mathbb{F}_p^\times \simeq \mathrm{Gal}(L/\mathbb{Q})$ be any subgroup, and write $K = L^S$ for its invariant subfield. Then one has an isomorphism of $\mathbb{Q}$-algebras

$$\mathbb{Q}\langle\mathbb{F}_p \rtimes S\rangle \to \mathbb{Q}\langle S\rangle \times \mathrm{End}_K(L).$$

MSC2000: primary 20C05; secondary 14L15, 16S34, 16S35, 16W30.
Keywords: group algebra, finite étale group scheme, Weil restriction, separable algebra.

(The map $\mathbb{Q}\langle \mathbb{F}_p \rtimes S\rangle \to \mathrm{End}_K(L)$ is defined by $(a,s) \mapsto (\zeta_p^i \mapsto \zeta_p^{a+si})$). The center of this group algebra is thus equal to $\mathbb{Q}\langle S\rangle \times K$; for a suitable choice of S, the extension $\mathbb{Q} \to K$ is not cyclotomic.

The question of characterizing which algebras may occur as a quotient of the algebra of a finite group was already raised by Schur, but solved only around 1950, by Brauer and Witt. Even then, they got a characterization only up to Morita equivalence; see [Fontaine 1971; Yamada 1974].

In this paper, we shift this problem a little: the base ring k is now a semilocal ring, containing the field $\mathbb{Q}$, and we are dealing with projective separable k-algebras; this notion is the natural generalization of the "absolute semisimplicity" which is used when k is a field, and it is equivalent, for commutative algebras, to being étale.

We prove in Section 5 that *any* projective separable k-algebra is a quotient of the group algebra of a suitable *group scheme*, finite étale over k. In particular, we prove that any finite separable field extension $K \subset L$, even a noncyclotomic one, may be generated by a finite étale K-group scheme. Roughly speaking, a separable algebra is a finite product of matrix algebras twisted by some étale torsor; the group scheme we propose is a finite group generating the split form of the algebra, but twisted by the same torsor.

Despite a formal analogy with the Brauer–Witt theory, our result does not add much to it: even in the simplest case, that of the quaternions, our method gives a *nonconstant* group scheme for generating this $\mathbb{R}$-algebra, in fact a group which is a definitely twisted form of the dihedral group D_4.

Notation. The categories in use will be denoted by the following symbols:

Gp stands for the category of groups.

For a commutative ring k,

k-Al denotes the category of k-algebras; its objects are thus the ring morphisms $k \to A$ such that the image of k is contained in the center of A.

k-Alc denotes the category of *commutative* k-algebras.

We say that a commutative ring k is connected if its spectrum $\mathrm{Spec}(k)$ is connected; that is, if k is not isomorphic to a proper finite product of rings.

Local rank. In this paper, most of the k-modules are locally free, but the base rings are seldom connected, and the rank of these modules seldom constant. Moreover, the constructions we have in mind, because they use the Weil restriction relative to a finite flat morphism $X \to S$, cannot be done locally on X. Thus we can't avoid introducing and using the *local* rank of a locally free k-module M of finite type,

which is the map

$$n : \mathrm{Spec}(k) \to \mathbb{N}, \qquad \mathfrak{p} \mapsto \mathrm{rank}_{k_\mathfrak{p}}(M_\mathfrak{p}).$$

This map is constant on each connected component of $\mathrm{Spec}(k)$. We need words to refer to these things; we propose the terms

- *k-integer* for a locally constant map $\mathrm{Spec}(k) \to \mathbb{N}$, and
- *k-rank* (of a locally free k-module M of finite type) for the local rank alluded to above.

For a k-integer n, we can define the k-algebra $\mathbf{M}_n(k)$, the k-group scheme $\mu_{n,k}$, and any other object which may be defined locally on $\mathrm{Spec}(k)$ for the Zariski topology. We have to be careful with the connected components where the k-integer vanishes: $\mathbf{M}_0(k) = 0$ (endomorphisms of the null space), but $\mu_{0,k} = \mathbf{G}_{m,k}$, since for every invertible element x, one has $x^0 = 1$.

1. The algebra of a group scheme

1.1. ***The algebra of a constant group.*** At first, let us recall, in the case of a *constant* group scheme, the well known constructions of its ring of functions (also called its representing algebra), and the construction of the algebra of such a group. Compare [Waterhouse 1979, Chapter 2].

1.1.1. Let k be a commutative ring. For a finite group Γ, we let $\prod_\Gamma k$ denote the ring of the maps from the set Γ to k (we reserve the notation k^Γ for the ring of invariants when is given an action of Γ on k); it is contravariant in Γ. The product in Γ induces a morphism of commutative k-algebras

$$\prod_\Gamma k \to \prod_{\Gamma\times\Gamma} k \simeq \prod_\Gamma k \otimes_k \prod_\Gamma k.$$

More explicitly, let $(\delta_\rho)_{\rho\in\Gamma}$ be the basis made up with the usual Kronecker maps $\delta_\rho : \Gamma \to k$; then the morphism above is given by

$$\delta_\rho \mapsto \sum_{\sigma\tau=\rho} \delta_\sigma \otimes \delta_\tau .$$

We thus get what is sometimes called a k-Hopf-algebra, but we prefer to emphasize the scheme point of view: $\mathrm{Spec}\big(\prod_\Gamma k\big)$ is a k-group scheme; it is called the constant k-group Γ, and it is denoted by Γ_k.

1.1.2. The group algebra of Γ over k will be denoted by $k\langle\Gamma\rangle$, instead of $k[\Gamma]$, because the symbol with brackets $k[V]$ often denotes also the commutative ring of algebraic, or regular, functions on the scheme V; see [Waterhouse 1979, 4.5], for example.

Recall that the group algebra $k\langle\Gamma\rangle$ is the free k-module based on the set Γ, with multiplication induced by that of Γ. It is equipped with a commutative coproduct given by the map

$$k\langle\Gamma\rangle \to k\langle\Gamma\rangle \otimes_k k\langle\Gamma\rangle, \qquad \sum_\sigma a_\sigma \sigma \mapsto \sum_\sigma a_\sigma \sigma \otimes \sigma$$

The dual of this ring is isomorphic to the ring of functions on Γ; namely, consider the k-linear isomorphism

$$\prod_\Gamma k \to \mathrm{Hom}_k(k\langle\Gamma\rangle, k), \qquad \delta_\rho \mapsto \big(\sum_\sigma a_\sigma \sigma \mapsto a_\rho\big). \tag{1-1}$$

The right-hand side (the dual as a k-module) may be endowed with the multiplication coming from dualizing the coproduct mentioned above; then this k-linear map is an isomorphism of k-algebras, as one can check immediately.

By dualizing the preceding morphism, we get the isomorphism

$$\mathrm{Hom}_k\big(\prod_\Gamma k,\ k\big) \to k\langle\Gamma\rangle, \qquad \xi \mapsto \sum_{\sigma\in\Gamma} \xi(\delta_\sigma)\sigma.$$

In Section 1.3, we will proceed along the same lines to define the algebra of a k-group scheme, and to get, in Proposition 1.3.2, an analogue of this well-known result:

Lemma 1.1.1. *Let Γ be a finite group, and let $k \to A$ be a k-algebra, whose multiplicative group is denoted by $A^\times$. Then one has an isomorphism of bifunctors*

$$\mathrm{Hom}_{k\text{-}\mathsf{Al}}(k\langle\Gamma\rangle, A) \xrightarrow{\sim} \mathrm{Hom}_{\mathsf{Gp}}(\Gamma, A^\times).$$

1.2. ***The multiplicative group functor.*** Let $k \to A$ be a k-algebra; recall that the ring A is not assumed to be commutative, but the morphism is required to send k into the center of A.

We will denote by $\mathbf{G}_{m,A/k}$ the multiplicative group functor of A, namely the functor

$$\mathbf{G}_{m,A/k} : k\text{-}\mathsf{Alc} \to \mathsf{Gp}, \qquad k' \mapsto \mathbf{G}_{m,A/k}(k') = (k' \otimes_k A)^\times.$$

It is also written $\mathrm{GL}_1(A)$ by Borel, and μ^A by Demazure and Gabriel.

Lemma 1.2.1 [Waterhouse 1979, 7.5; Demazure and Gabriel 1970, p. 149]. *Suppose that the k-algebra A is a projective (i.e., locally free) k-module of finite type. Then the functor $\mathbf{G}_{m,A/k}$ is representable by an affine k-group scheme of finite type.*

Sketch of proof. Let $A^D = \mathrm{Hom}_k(A, k)$ be the linear dual of A, and let

$$S = \mathrm{Sym}_k(A^D)$$

be the symmetric algebra of that module. Let $\xi \in A^D \otimes_k A$ be the element that corresponds to the identity of A under the canonical isomorphism $A^D \otimes_k A \xrightarrow{\sim} \mathrm{End}_k(A)$.

(If you prefer more explicit things, you can choose a basis (e_i) of A, and the dual basis (X_i) of A^D; this allows you to write $\xi = \sum X_i \otimes e_i$.) We must consider this element

$$\xi \in A^D \otimes_k A \subset S \otimes_k A$$

as the *generic element* of A, since each specification $S \to k'$ of the parameters towards a commutative k-algebra k', gives rise to an element in $k' \otimes_k A$, namely the image of ξ.

Since $S \otimes_k A$ is a finite and locally free S-module, we dispose of the usual norm $N : S \otimes_k A \to S$, namely, $N(x) = \det(y \mapsto xy)$. Then we can check easily that the algebra of fractions $S_{N(\xi)}$ represents $\mathbf{G}_{m,A/k}$ as a functor from k-Alc to the category of sets.

The group structure is induced by the algebra morphism $S_{N(\xi)} \to S_{N(\xi)} \otimes_k S_{N(\xi)}$ given by extending to symmetric algebra, and localizing, the linear map

$$A^D \xrightarrow{(\text{mult.})^D} (A \otimes_k A)^D \xleftarrow{\sim} A^D \otimes_k A^D \subset \mathrm{Sym}_k(A^D) \otimes_k \mathrm{Sym}_k(A^D). \qquad \square$$

1.3. ***The group-algebra.*** We now deal with group schemes over k, instead of constant groups; their category will be denoted by k-Gp. We are looking for something like a left adjoint to the multiplicative group functor, that is, a functor which, to a k-group scheme G, would associate a k-algebra $k\langle G\rangle$, endowed with an isomorphism of functors

$$\mathrm{Hom}_{k\text{-Al}}(k\langle G\rangle,\ A) \quad \xrightarrow{\sim} \quad \mathrm{Hom}_{k\text{-Gp}}(G, \mathbf{G}_{m,A}).$$

Fortunately, in what follows, we have available strong enough finiteness assumptions to guarantee that these objects exist.

1.3.1. We will try to stick to the notations and terminology used in [Waterhouse 1979]. We recall some of them:

Let $G = \mathrm{Spec}(R)$ be an affine k-group scheme.

- $u : k \to R$ stands for the canonical map,
- $m : R \otimes_k R \to R$ stands for the multiplication,
- $\Delta : R \to R \otimes_k R$ denotes the coproduct,
- $\varepsilon : R \to k$ denotes the counit,
- S indicates the coinverse.

Suppose that R is finite and locally free as a k-module; let $R^D = \mathrm{Hom}_k(R, k)$ be the linear dual of R; then the k-module R^D may be endowed with a structure of a (usually noncommutative) k-algebra: the product is defined as the map

$$R^D \otimes_k R^D \simeq (R \otimes_k R)^D \xrightarrow{\Delta^D} R^D;$$

the associativity of this multiplication comes from the associativity of the product in the group G, and the map $\varepsilon^D : k \to R^D$ actually defines a morphism of algebras since it corresponds to the unity of G.

Definition 1.3.1. Let $G = \mathrm{Spec}(R)$ be an affine k-group scheme with R finite and locally free as a k-module. We define the *k-algebra of the group G*, and we note $k\langle G\rangle$ the linear dual R^D endowed with the algebra structure given above.

Let $k \to k'$ be a commutative k-algebra. We denote by $G_{k'} = \mathrm{Spec}(k' \otimes_k R)$ the group scheme over k' obtained by base change. For G finite and locally free, there is an isomorphism

$$k\langle G\rangle \otimes_k k' \ \xrightarrow{\sim}\ k'\langle G_{k'}\rangle$$

since one has the following sequence of standard isomorphisms, the first one coming from the local freeness of R over k:

$$k\langle G\rangle \otimes_k k' = \mathrm{Hom}_k(R, k) \otimes_k k' \simeq \mathrm{Hom}_k(R, k') \simeq \mathrm{Hom}_{k'}(k' \otimes_k R, k') = k'\langle G_{k'}\rangle.$$

Proposition 1.3.2. *Let $G = \mathrm{Spec}(R)$ be an affine k-group scheme with R finite and locally free as a k-module.Then, for any finite and locally free k-algebra $k \to A$, there is a bijection of functors in G*

$$\mathrm{Hom}_{k\text{-}\mathsf{Al}}(k\langle G\rangle,\ A)\ \xrightarrow{\sim}\ \mathrm{Hom}_{k\text{-}\mathsf{Gp}}(G, \mathbf{G}_{m,A/k}).$$

Proof. For every k-algebra $k' \in k$-Alc, consider the multiplications in the group $G(k')$ and in the ring $k\langle G\rangle \otimes_k k'$, that is the multiplications in $\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(R, k')$ and in $\mathrm{Hom}_k(R, k')$; they are both given by dualizing the same map $\Delta : R \to R \otimes_k R$; therefore, from the mere inclusion

$$\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(R, k') \subset \mathrm{Hom}_k(R, k')$$

we deduce a morphism of multiplicative monoids

$$G(k') \to k' \otimes_k k\langle G\rangle.$$

Since every element of $G(k')$ has an inverse, its image is invertible in the ring $k' \otimes_k k\langle G\rangle$. We have thus defined a morphism of (ordinary) groups, which is functorial in k',

$$G(k') = \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(R, k')\ \to\ (\mathrm{Hom}_k(R, k'))^\times = \mathbf{G}_{m,k\langle G\rangle/k}(k'),$$

that is a morphism of group functors on k-Alc

$$G \to \mathbf{G}_{m,k\langle G\rangle/k}. \tag{1-2}$$

A morphism of k-algebras $k\langle G\rangle \to A$ clearly induces a morphism of group functors

$$\mathbf{G}_{m,k\langle G\rangle/k} \to \mathbf{G}_{m,A/k}.$$

By composition with (1-2), we get a map which is functorial in G

$$\mathrm{Hom}_{k\text{-}\mathsf{Al}}(k\langle G\rangle,\ A) \to \mathrm{Hom}_{k\text{-}\mathsf{Gp}}(G, \mathbf{G}_{m,A/k}). \tag{1-3}$$

Conversely, let $G \to \mathbf{G}_{m,A/k}$ be a morphism of k-group schemes. We want to produce from it a morphism of k-algebras $k\langle G\rangle \to A$. Since the k-group $\mathbf{G}_{m,A/k}$ is not finite over k (except if $k = A$), the above elementary construction does not allow to define something like $k\langle \mathbf{G}_{m,A/k}\rangle$, nor, of course, a morphism $k\langle \mathbf{G}_{m,A/k}\rangle \to A$. At first sight, we are given, for each commutative k-algebra k', the two solid arrows in the following diagram, and we need to complete it with the dotted one:

$$\begin{array}{ccc} \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(R, k') & \longrightarrow & k' \otimes_k A \\ & \searrow \quad \nearrow & \\ & \mathrm{Hom}_k(R, k') & \end{array}$$

To achieve this, we must use the representability of $\mathbf{G}_{m,A/k}$ (Lemma 1.2.1): since the groups G and $\mathbf{G}_{m,A/k}$ are affine, the given morphism $G \to \mathbf{G}_{m,A/k}$ is associated to a morphism of k-algebras

$$\mathrm{Sym}_k(A^D)_{N(\xi)} \to R.$$

The compatibility with the group laws implies the commutativity of the squares

$$\begin{array}{ccccc} A^D & \longrightarrow & \mathrm{Sym}_k(A^D)_{N(\xi)} & \longrightarrow & R \\ {\scriptstyle (\mathrm{mult.})^D}\downarrow & & \downarrow & & \downarrow{\scriptstyle \Delta} \\ A^D \otimes_k A^D & \longrightarrow & \mathrm{Sym}_k(A^D)_{N(\xi)} \otimes_k \mathrm{Sym}_k(A^D)_{N(\xi)} & \longrightarrow & R \otimes_k R \end{array}$$

By dualizing, one gets a k-linear map

$$R^D \to A$$

(Recall that both R and A are locally free k-modules of finite rank). Now the above diagram shows that this map is compatible with Δ^D and with the multiplication in A. We have thus defined a map

$$\mathrm{Hom}_{k\text{-}\mathsf{Al}}(k\langle G\rangle,\ A) \leftarrow \mathrm{Hom}_{k\text{-}\mathsf{Gp}}(G, \mathbf{G}_{m,A/k}).$$

which we can easily check to be the inverse of (1-3). □

1.4. ***Another approach to the group algebra.*** We now sketch a very general definition of an algebra that looks like a "group algebra", and which may appear to be more natural than the previous one, if less explicit; but, this new algebra can be proven to satisfy the required left adjoint property only when the group is finite étale; and, for these groups, this algebra coincides with the previous one.

1.4.1. Let k be a ring, and let G be a group functor on k-Alc; let $F : k\text{-Alc} \to k\text{-Al}$ be the functor defined by

$$F(k') = k'\langle G(k')\rangle.$$

Thus, $F(k')$ is the usual k'-algebra of the discrete group $G(k')$.

Let $\tilde{F}$ be the sheaf associated to F for the étale topology. The algebra $\tilde{F}(k)$ of global sections of this sheaf is equipped with the map

$$\mathrm{Hom}_{k\text{-Gp}}(G, \mathbf{G}_{m,A/k}) \to \mathrm{Hom}_{k\text{-Al}}(\tilde{F}(k),\ A), \tag{1-4}$$

defined as follows: a morphism of functors $G \to \mathbf{G}_{m,A}$ gives, for each $k' \in k$-Alc, a group homomorphism

$$G(k') \to \mathbf{G}_{m,A}(k') = (k' \otimes_k A)^\times$$

which gives rise to a morphism of k'-algebras

$$F(k') = k'\langle G(k')\rangle \to k' \otimes_k A.$$

We thus get a morphism of sheaves from $\tilde{F}$ to the sheaf $k' \mapsto k' \otimes_k A$, and, finally, taking their global sections, we get a morphism of k-algebras $\tilde{F}(k) \to A$. It is not clear if the map (1-4) should be bijective without strong hypothesis.

Proposition 1.4.1. *For a finite étale k-group G, the group algebra $k\langle G\rangle$, defined in Definition 1.3.1, is canonically isomorphic to the ring of global sections of the étale sheaf associated to the functor $k' \mapsto k'\langle G(k')\rangle$, considered above.*

For the proof, we need the following variant of the Dedekind independence result.

Lemma 1.4.2. *Let $G = \mathrm{Spec}(R)$ be a finite étale k-group, and let $k\langle G\rangle$ be its group algebra in the sense of Definition 1.3.1. Then, for $k' \in k$-Alc, the morphism*

$$k'\langle G(k')\rangle \to k\langle G\rangle \otimes_k k' = \mathrm{Hom}_k(R, k')$$

is injective. In other words, the elements of $G(k') = \mathrm{Hom}_{k\text{-Alc}}(R, k')$ are linearly independent in $\mathrm{Hom}_k(R, k')$.

Moreover, there exists a finite étale k-algebra k' for which this morphism is an isomorphism.

We may suppose that $\mathrm{Spec}(k')$ is connected, and we rewrite k' as k for simplicity. Let $g_1, \ldots, g_s \in G(k)$ be distinct elements, seen as k-morphisms $R \to k$; since R is étale over k, each morphism $g_i : R \to k$ gives a projective R-module structure on k, in other words, each kernel $J_i = \mathrm{Ker}(g_i) \subset R$ is generated by an idempotent $e_i \in R$. These ideals are pairwise comaximal: in fact, the ring $R/J_i \simeq k$ being assumed to be connected, the image of an idempotent e_j is either 0, and then $J_i = J_j$ and $i = j$, or this image is 1, implying that $J_i + J_j = R$.

The Chinese remainder theorem then implies that the morphism induced by the s morphisms g_i,

$$R \to k^s,$$

is surjective. This, in turn, clearly implies that the g_i are linearly independent.

Since R is finite and étale over k, it is split by a finite étale morphism $k \to k'$, i.e one has an isomorphism of k'-algebras

$$k' \otimes_k R \xrightarrow{\sim} \prod_{G(k')} k'.$$

It is now clear that any linear form $R \to k'$ is a linear combination, with coefficients in k', of the projections $k' \otimes_k R \to k'$, which indeed correspond to elements in $G(k')$.

Proof of the proposition. Denote by H the functor given by $H(k') = k\langle G\rangle \otimes_k k' = \mathrm{Hom}_k(R, k')$; it is clearly a sheaf in the étale topology. We have to show that the functor map $F \to H$ induces an isomorphism

$$\tilde{F} \xrightarrow{\sim} H.$$

According to the previous lemma, for any k' étale over k, the map $F(k') \to H(k')$ is injective, and it is even bijective if $k \to k'$ factors trough a k_0 which splits R.

Then, following [Artin 1962, chapter II], we use the construction $F \rightsquigarrow F^+$ to get the associated sheaf $\tilde{F}$; roughly speaking, a section of $F^+(U)$ "is" a coherent family of sections of F given locally on U, that is, an element of the kernel

$$F(U') \rightrightarrows F(U' \times_U U') \ ,$$

where $U' \to U$ is an étale covering. Since F is a subfunctor of the sheaf H, it is a "separated" presheaf, or, with Artin's notations, F satisfy the property $(+)$; therefore, by [Artin 1962, II.1.4], F^+ is already the associated sheaf $\tilde{F}$. But the injectivity of $F \to H$, and the definition of F^+, alluded to above, imply that the map $\tilde{F} \to H$ is still injective. Now, over the "covering" $\mathrm{Spec}(k_0) \to \mathrm{Spec}(k)$, the morphism $F \to H$ becomes an isomorphism, thus also the morphism $\tilde{F} \to H$; as $\tilde{F}$ and H are sheaves, the map $\tilde{F} \to H$ is an isomorphism everywhere. □

1.5. ***Galois description.*** We now translate essentially the same considerations to the more concrete situation of Galois extensions. Let $k \to K$ be a finite Galois extension of fields, with Galois group $\pi = \mathrm{Gal}(K/k)$; suppose the k-group scheme G be split by K, i.e., that G_K is isomorphic to the constant (finite) group Γ_K; this group G is thus associated to an action of π on Γ, that is to a morphism

$$\pi \to \mathrm{Aut}_{\mathsf{Gp}}(\Gamma).$$

(See [Waterhouse 1979, 6.3] or [Demazure and Gabriel 1970, II.5.1.7, p. 237].) The ring of polynomial maps on G is then given by

$$R = \Big(\prod_{\Gamma} K\Big)^{\pi},$$

where the action of $\sigma \in \pi$ on an element $x : \Gamma \to K \in \prod_\Gamma K$ is

$${}^{\sigma}x = (\gamma \mapsto \sigma(x(\sigma^{-1}\gamma))).$$

Proposition 1.5.1. *The k-group-algebra of G is the ring*

$$k\langle G\rangle = (K\langle\Gamma\rangle)^{\pi},$$

where both the coefficients in K and the basis Γ are acted on by the Galois group π.

To prove this we go back to the isomorphism (1-1)

$$\varphi : \prod_{\Gamma} K \xrightarrow{\sim} \mathrm{Hom}_K(K\langle\Gamma\rangle, K), \quad \delta_\gamma \mapsto \Big(\sum_{\gamma'} a_{\gamma'}\gamma' \mapsto a_\gamma\Big),$$

and we must see that it induces an isomorphism

$$\Big(\prod_{\Gamma} K\Big)^{\pi} \xrightarrow{\sim} \mathrm{Hom}_k(K\langle\Gamma\rangle^{\pi}, k).$$

The morphism φ may be characterized as follows: Given $(x : \Gamma \to K) \in \prod_\Gamma K$, the K-linear map $\varphi(x)$ is defined on the basis Γ, by $\varphi(x)(\gamma) = x(\gamma)$. It is clear that φ is π-equivariant (if $\mathrm{Hom}_K(K\langle\Gamma\rangle, K)$ is acted on by π, both on $K\langle\Gamma\rangle$ and on K); taking the invariants, we thus get an isomorphism

$$\Big(\prod_{\Gamma} K\Big)^{\pi} \xrightarrow{\sim} \mathrm{Hom}_K(K\langle\Gamma\rangle, K)^{\pi}.$$

Since $k \to K$ is a Galois extension, one has $k = K^{\pi}$. It remains to produce an isomorphism

$$\mathrm{Hom}_K(K\langle\Gamma\rangle, K)^{\pi} \xrightarrow{\sim} \mathrm{Hom}_{K^{\pi}}((K\langle\Gamma\rangle)^{\pi}, K^{\pi}).$$

We will apply to $V = K\langle\Gamma\rangle$ the following general result: let V be a K-vector space endowed with a *semilinear* action of π; that means that the group V is equipped with a morphism $\pi \to \mathrm{Aut}_{\mathbb{Z}}(V)$ such that, for $\sigma \in \pi$, $x \in V$ and $\lambda \in K$, one has $\sigma(\lambda x) = \sigma(\lambda)\sigma(x)$. The group V^{π} is then a vector space over K^{π}, and we have an isomorphism

$$K \otimes_{K^{\pi}} V^{\pi} \xrightarrow{\sim} V$$

(See [Bourbaki 1981, A V, §10, Prop. 7, p. 61], for example.) From this we deduce the sequence of isomorphisms

$$\mathrm{Hom}_K(V, K)^{\pi} \simeq \mathrm{Hom}_K(K \otimes_{K^{\pi}} V^{\pi}, K)^{\pi} \simeq \mathrm{Hom}_{K^{\pi}}(V^{\pi}, K)^{\pi} \simeq \mathrm{Hom}_{K^{\pi}}(V^{\pi}, K^{\pi}).$$

Remark 1.5.2. It is easy to show an example where $k\langle G\rangle \not\subseteq k\langle\Gamma\rangle$: with notations as above, suppose there exist an element $\gamma \in \Gamma$, and an element $a \in K$, having both a trivial stabilizer for the action of π. Let

$$x = \sum_{\sigma\in\pi} \sigma(a)\sigma(\gamma) \quad \in K\langle\Gamma\rangle.$$

It is clear that x is π-invariant and does not lie in $k\langle\Gamma\rangle$. Thus, in this case, $(K\langle\Gamma\rangle)^\pi \not\subseteq K^\pi\langle\Gamma^\pi\rangle$.

2. Group generation of finite étale algebras

2.1. ***The Weil restriction.*** Let $k \to K$ be a finite étale morphism of (commutative) rings. The direct image, or Weil restriction, or norm, is the functor

$$\mathsf{R}_{K/k} : K\text{-}\mathsf{Alc} \to k\text{-}\mathsf{Alc}$$

which is left adjoint to the base change functor; for any (commutative) k-algebra A, and any (commutative) K-algebra A', we thus have a bijection

$$\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(\mathsf{R}_{K/k}(A'), A) \quad \xrightarrow{\sim} \quad \mathrm{Hom}_{K\text{-}\mathsf{Alc}}(A', K\otimes_k A),$$

which is functorial in A and in A'. The existence and the main properties of this functor are explained in [Demazure and Gabriel 1970, I.1.6.6, p. 30] and in [Bosch et al. 1990, 7.6].

Suppose that K is a product $K = K_1 \times K_2$; then a K-algebra A' also decomposes as a product $A' = A'_1 \times A'_2$, where A'_i is a K_i-algebra, and one has an isomorphism

$$\mathsf{R}_{K/k}(A') \simeq \mathsf{R}_{K_1/k}(A'_1) \otimes_k \mathsf{R}_{K_2/k}(A'_2).$$

In particular, in the split case $K = k^d$, where $A' = \prod_{i=1}^d A_i$, we have

$$\mathsf{R}_{k^d/k}(A_1 \times \cdots \times A_d) = A_1 \otimes_k \cdots \otimes_k A_d.$$

(From a scheme-theoretic viewpoint, the Weil restriction transforms disjoint unions into products.)

We will use this functor only for K-algebras coming from k, that is, for algebras of the form $A' = K \otimes_k B$ for a k-algebra B. The bijection above then reads as

$$\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(\mathsf{R}_{K/k}(K\otimes_k B), A) \xrightarrow{\sim} \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(B, K\otimes_k A).$$

We may regard the ring $\mathsf{R}_{K/k}(K\otimes_k B)$ as the form of the tensor product $B^{\otimes d}$ twisted by the $\mathfrak{S}_d$-torsor P associated to K; this torsor is the functor $P : k\text{-}\mathsf{Alc} \to \mathsf{Ens}$ defined by

$$P(k') = \mathrm{Isom}_{k'\text{-}\mathsf{Alc}}(k'\otimes_k K, k'^d)$$

This point of view, if easy to conceive, is a little hard writing down (but see [Ferrand 1998, 6.2.2 and 7.3.2], and Section 2.2 below). Anyway, it is clear that for the trivial étale algebra $K = k^d$, the k-algebra $\mathsf{R}_{K/k}(K \otimes_k B)$ is indeed isomorphic to $B^{\otimes d}$, due to the above isomorphism, or to the explicit bijections

$$\mathrm{Hom}_{k\text{-}\mathsf{Alc}}(B, K \otimes_k A) \simeq \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(B, A^d) \simeq \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(B, A)^d \simeq \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(B^{\otimes d}, A).$$

We will use the same symbol $\mathsf{R}_{K/k}$ for the Weil restriction of schemes; in particular, if $G' = \mathrm{Spec}(A')$ is an affine K-group, we write $\mathsf{R}_{K/k}(G')$ for the scheme $\mathrm{Spec}(\mathsf{R}_{K/k}(A'))$; letting $G = \mathrm{Spec}(\mathsf{R}_{K/k}(A'))$, one has, for any $k' \in k\text{-}\mathsf{Alc}$,

$$G(k') = \mathrm{Hom}_{k\text{-}\mathsf{Alc}}(\mathsf{R}_{K/k}(A'), k') = \mathrm{Hom}_{K\text{-}\mathsf{Alc}}(A', K \otimes_k k') = G'(K \otimes_k k').$$

(This isomorphism shows, among other properties, that $G = \mathsf{R}_{K/k}(G')$ is a k-group).

The Weil restriction of a constant K-group is usually *not* a constant k-group.

2.2. ***The twisted Klein group*** $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\boldsymbol{\mu}_{\mathbf{2},\mathbb{C}})$**.** As an example which anticipates the next result, and which is also used later, we now compute the Weil restriction from $\mathbb{C}$ to $\mathbb{R}$, of the group $\mu_{2,\mathbb{C}} = \mathrm{Spec}(\mathbb{C}[T]/(T^2 - 1))$; this Weil restriction will also appear as a twisted form of the Klein group $\mu_2 \times \mu_2$. Let A be the $\mathbb{R}$-algebra of regular functions on this Weil restriction; so we have

$$\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}}) = \mathrm{Spec}(A).$$

We find that

$$A = \mathbb{R}[X, Y]/(X^2 - Y^2 - 1, XY).$$

(To see this, the usual trick is to construct the Weil restriction in order for the canonical morphism

$$\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})_{\mathbb{C}} \longrightarrow \mu_{2,\mathbb{C}} \tag{2-1}$$

to exist. So, we start with the map $\mathbb{C}[T] \longrightarrow \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}[X, Y]$ given by

$$T \mapsto 1 \otimes X + i \otimes Y,$$

and we impose the conditions on X and Y for the image of $T^2 - 1$ to be zero; that immediately gives the required relations.)

Let x and y be the classes in A, of X and Y respectively. We will then show that A is an $\mathbb{R}$-vector space of rank 4, and that the set $\{x, y\}$ may be included in a basis; the simplest way for doing so is to introduce the element $s = x + y \in A$, whose powers are $s^2 = x^2 + y^2$, $s^3 = x - y$ and $s^4 = 1$; it is then clear that one gets a morphism

$$\mathbb{R}[S]/(S^4 - 1) \longrightarrow A$$

which is easily checked to be an isomorphism. Despite this isomorphism, the group $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$ is obviously not isomorphic to $\mu_{4,\mathbb{R}}$. In fact, the group law on $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$ is associated to the morphism $\Delta : A \to A \otimes_{\mathbb{R}} A$ given by

$$\Delta(x) = x \otimes x - y \otimes y, \quad \Delta(y) = x \otimes y + y \otimes x.$$

The conjugation in $\mathbb{C}$ induces an involution of the functor $\mathsf{R}_{\mathbb{C}/\mathbb{R}}$, and thus an involution u on A, compatible with Δ; it is given by $u(x) = x, u(y) = -y$. By composing with (2-1), we thus get another morphism $\mathbb{C}[T]/(T^2 - 1) \to \mathbb{C} \otimes_{\mathbb{R}} A$; putting both together, we get

$$\mathbb{C}[T_1, T_2]/(T_1^2 - 1, T_2^2 - 1) \longrightarrow \mathbb{C} \otimes_{\mathbb{R}} A, \quad t_1 \mapsto 1 \otimes x + i \otimes y, t_2 \mapsto 1 \otimes x - i \otimes y$$

It is clearly an isomorphism; moreover, the conjugation in $\mathbb{C}$ induces on $\mathbb{C} \otimes_{\mathbb{R}} A$ an automorphism which corresponds, in the left hand algebra, to the transposition of T_1 and T_2: this is the algebraic meaning of the statement that the Weil restriction $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$ is a twisted form of the Klein group $\mu_2 \times \mu_2$.

We now define a *surjective* morphism from the $\mathbb{R}$-algebra of the Weil restriction, to $\mathbb{C}$

$$\mathbb{R}\langle \mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}}) \rangle \longrightarrow \mathbb{C}.$$

(This is the simplest example for Theorem 2.3 below.) Actually, since $\{x, y\}$ is part of a basis of A, the map

$$\mathbb{R}\langle \mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}}) \rangle = A^D = \mathrm{Hom}_{\mathbb{R}}(A, \mathbb{R}) \to \mathbb{C}, \quad \alpha \mapsto \alpha(x) + i\alpha(y),$$

is surjective; it is also a morphism of algebras, as one can check from the definition of Δ given above.

But, if, instead of the nonconstant group $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$, you prefer to generate $\mathbb{C}$ with a constant one, you can, as everybody does, use the cyclic group of order four $\{\pm 1, \pm i\}$.

Theorem 2.3. *Let $k \to K$ be a finite étale morphism. Let $n : \mathrm{Spec}(K) \to \mathbb{N}$ be an K-integer which is invertible in k. Then the Weil restriction*

$$G = \mathsf{R}_{K/k}(\mu_{n,K}) = \mathrm{Ker}(\mathbf{G}_{m,K/k} \xrightarrow{n} \mathbf{G}_{m,K/k})$$

is a finite étale group scheme over $\mathrm{Spec}(k)$. *According to Proposition 1.3.2, the inclusion $G \subset \mathbf{G}_{m,K/k}$ induces a morphism of k-algebras*

$$k\langle G \rangle \to K. \tag{2-2}$$

This morphism is surjective.

Recall form Section 1.2 that $\mathbf{G}_{m,K/k}$ denotes the group scheme over $\mathrm{Spec}(k)$ given by the multiplicative group of K; since K is commutative one has, here, $\mathbf{G}_{m,K/k} = \mathsf{R}_{K/k}(\mathbf{G}_{m,K})$.

Proof. The hypothesis on n means that we are given a decomposition as a product $K = K_1 \times \cdots \times K_s$, and a family $(n_1, \ldots, n_s)$ of integers, each of which is invertible in k; the K-group $\mu_{n,K}$ is equal, over the open-closed set $\mathrm{Spec}(K_i)$, to μ_{n_i,K_i}.

The properties of the Weil restriction do not allow to reduce to the case where n is constant, but we may suppose $\mathrm{Spec}(k)$ to be connected; then there exists a faithfully flat étale morphism $k \to k'$, with $\mathrm{Spec}(k')$ connected, a finite set I and an isomorphism of k'-algebras

$$k' \otimes_k K \simeq \prod_I k'.$$

The decomposition of K as the product associated to n gives the surjective map

$$\alpha : I \to \{1, 2, \ldots, s\}$$

such that, for $j = 1, \ldots, s$, one has

$$k' \otimes_k K_j = \prod_{\alpha^{-1}(j)} k'.$$

The definition of the direct image now gives

$$G(k') = \mu_n(k' \otimes_k K) = \prod_{i \in I} \mu_{n_{\alpha(i)}}(k').$$

This last group will be noted as $\prod_I \mu_{n\alpha}(k')$. Since n is supposed to be invertible in k, the group schemes μ_{n_j} are étale and finite; this shows that G is finite and étale over k.

Now the surjectivity of the morphism (2-2) can be checked after any faithfully flat base change $k \to k'$; so we may suppose that the ring k', connected as above, is big enough so that it contains, for all $i \in I$, an $n_{\alpha(i)}$-th root of unity ζ_i different from 1; by connectedness, $1 - \zeta_i$ is invertible.[1]

We have to show that every idempotent of $\prod_I k'$ is in the image of the morphism

$$k'\Big\langle \prod_I \mu_{n\alpha}(k') \Big\rangle \to \prod_I k'.$$

[1] A quick proof I learned from Pascal Autissier: Let R be a connected ring containing two roots u an v of a separable polynomial $P(T)$; then either $u - v$ is zero, or it is invertible in R. In fact, letting $P(T) = (T - u)Q(T)$, one has $P' = (T - u)Q' + Q$, so $(T - u)P' = (T - u)^2 Q' + P$, and then $(v - u)P'(v) = (v - u)^2 Q'(v)$; since P is separable, $P'(v)$ is invertible in R, and thus, the ideal $(v - u)R$ is equal to its square; it is therefore generated by an idempotent. But, by assumption, R doesn't contain any nontrivial idempotent.

Fix $i_0 \in I$, and let $e = (e_i) \in \prod_I k' = k' \otimes_k K$, be the idempotent given by $e_{i_0} = 1$, and $e_i = 0$ for $i \neq i_0$. Consider the element $f = (f_i) \in \prod_I \mu_{n\alpha}(k')$, with $f_{i_0} = \zeta_{i_0}$, and for $i \neq i_0$, $f_i = 1$. One has

$$(1 - \zeta_{i_0})e = 1 - f.$$

But $1 - \zeta_{i_0}$ is invertible in the base ring k'. So we are done. □

2.4. ***The case of a Galois field extension.*** By using the Galois descent machinery, we now generalize Section 2.2 to a Galois extension of fields $k \to K$, with Galois group π, and where 2 is invertible in k; we take $n = 2$.

One has the inclusion

$$\mu_2 = \{\pm 1\} \to K^\times \subset K$$

Extend it as

$$\prod_\pi \mu_2 \to \prod_\pi K.$$

The elements of these sets will be seen as maps from π to μ_2, and to K respectively. We define a left action of π on these maps: for $\sigma, \tau \in \pi$,

$$({}^\sigma u)(\tau) = u(\tau\sigma).$$

(Note that, for this action, π acts on the source ($= \pi$), but not the target ($= K$).)

We consider the ring $\prod_\pi K$ as a K-algebra via the morphism $K \to \prod_\pi K$ given by $x \mapsto (\sigma \mapsto \sigma(x))$; this morphism is π-equivariant, and taking the invariants gives back the initial morphism

$$k = K^\pi \to K \simeq \Big(\prod_\pi K\Big)^\pi.$$

The group scheme G is now defined by the abstract group $G(K) = \prod_\pi \mu_2$, equipped with the given above action of π. We thus have a π-equivariant map

$$G(K) \to \Big(\prod_\pi K\Big)^\times \subset \prod_\pi K.$$

It induces a morphism of K-algebras

$$K\langle G(K)\rangle \to \prod_\pi K.$$

To be explicit: for $x \in K$, and $g \in G(K)$, the image of $xg \in K\langle G(K)\rangle$ is the map $\pi \to K$ given by $\sigma \mapsto \sigma(x)g(\sigma)$; this morphism is π-equivariant for π acting on $K\langle G(K)\rangle$ by the rule ${}^\tau(xg) = \tau(x)\,{}^\tau g$; it is also surjective since the Kronecker idempotent $\delta_\sigma \in \prod_\pi K$ is the image of $\frac{1}{2}(1 + g)$, where $g(\tau) = -1$ if $\tau \neq \sigma$, and

$g(\sigma) = 1$. Taking the invariants, one gets the surjective morphism

$$k\langle G\rangle \overset{1.5.1}{=} \left(K\langle G(K)\rangle\right)^{\pi} \to K = \left(\prod_{\pi} K\right)^{\pi}.$$

3. Some properties of separable algebras

Let k be a commutative ring. A k-algebra $k \to A$ is said to be *separable* if A is a projective $A \otimes_k A^{\mathrm{opp}}$-module, for the module structure given by

$$A \otimes_k A^{\mathrm{opp}} \times A \to A, \quad (x \otimes y, a) \mapsto xay.$$

This notion was introduced and studied by Auslander and Goldman [Auslander and Goldman 1960] (or see [Knus and Ojanguren 1974]); it generalizes what is called *absolutely semisimplicity* when k is a field. Nowadays, separable algebras are as ubiquitous as their commutative counterparts, the étale algebras.

The definition above is equivalent to the more explicit following one:

Definition 3.1. Let $p : A \otimes_k A \to A$ be the product map, given by $p(a \otimes b) = ab$; this map is $A \otimes_k A^{\mathrm{opp}}$-linear. The separability is equivalent to the existence of an element $e \in A \otimes_k A$ such that $p(e) = 1$, and, for all $c \in A$, $c \otimes 1 \cdot e = e \cdot 1 \otimes c$. To avoid any doubt on which product is used in this equality, we write $e = \sum_i a_i \otimes b_i$; then one must have $\sum a_i b_i = 1$, and for any $c \in A$, $\sum ca_i \otimes b_i = \sum a_i \otimes b_i c$.

Such an element e is called a *separability idempotent* for A.

Lemma 3.2. *Let $k \to A$ be a separable algebra, and let M be a left A-module. If M is k-projective, then it is A-projective as well.*

We give the proof from [Orzech and Small 1975, p. 13], because it shows how the product by e acts as taking the mean value, which is usual when dealing with finite groups. So let $u : P \to M$ be a surjective map of left A-modules, and let $v : M \to P$ be a k-linear right inverse ($uv = 1$). Look at $\mathrm{Hom}_k(M, P)$ as a left $A \otimes_k A^{\mathrm{opp}}$-module, by letting

$$(x \otimes y \cdot v)(m) = xv(ym).$$

Then it makes sense to consider the map ev; we check that it is an A-linear right inverse of u. It is A-linear since, for $c \in A$, one has

$$c(ev) = (c \otimes 1 \cdot e)v = (e \cdot 1 \otimes c)v,$$

and then

$$c(ev)(m) = (\sum a_i v(b_i cm)) = (ev)(cm)$$

Moreover, it is easy to check that $u(ev) = 1$. Therefore, M is A-projective.

3.3. In the following, we only consider separable algebras which in addition are projective k-modules of finite type; since a projective separable algebra must be a finitely generated k-module (see [Knus and Ojanguren 1974, p. 82] or [Orzech and Small 1975, p. 13]), we call such algebras simply *projective separable*. The main examples of projective separable algebras are

- finite étale (commutative) k-algebras;
- k-algebras $\mathrm{End}_k(P)$ of endomorphisms of a projective k-module of finite type; if P is free, and denoting by (e_{ij}) the usual basis of the ring of matrices, the element $\sum_{i,j} e_{ij} \otimes e_{ji}$ is a separability idempotent;
- the algebra $k\langle\Gamma\rangle$ of a finite group Γ whose order n is invertible in k; for a separability idempotent one may then take $\frac{1}{n}\sum_{\sigma\in\Gamma} \sigma \otimes \sigma^{-1}$.

3.4. Let A be a k-algebra. Then A is projective separable if and only if there exists a faithfully flat morphism $k \to k'$ (even an étale one), a finite family $(n_i)_{i\in I}$ of k'-integers n_i, and an isomorphism of k'-algebras

$$k' \otimes_k A \simeq \prod_{i\in I} \mathrm{M}_{n_i}(k')$$

This characterization, or a direct proof, shows:

Proposition. *Let A be a projective separable k-algebra. Then the center K of A is finite étale over k and A is projective separable over K* [Knus and Ojanguren 1974, III, 5.5].

A K-algebra that is projective separable and *central* is called an Azumaya K-algebra.

In this paper, we shall not consider the Morita equivalence between Azumaya algebra, nor the Brauer group.

3.5. ***Existence of a maximal étale subalgebra.*** A careful reading of the proof given in [Auslander and Goldman 1960, p. 384] or in [Knus and Ojanguren 1974, III,6.4], which both concern a local base ring, leads to the following very slight generalization:

Proposition. *Let k be a semilocal ring and $k \to A$ a projective separable algebra, with center K. Then there exists a maximal commutative subalgebra $L \subset A$, which is finite étale over the center K, and then also finite étale over k. Moreover, if the rank of A as a K-module is constant, equal to n^2, then the rank of L over K is n.*

3.6. Let L be a maximal étale subalgebra of A. From the inclusion $L \subset A$ come two structures of L-module on A: we note respectively by ${}_LA$ and A_L the L-modules given by multiplication of "scalars" in L on the left, and on the right. Since L is étale over K, both these L-modules are projective (Lemma 3.2).

Proposition 3.7 [Knus and Ojanguren 1974, III.6.1]. *The morphism from $A \otimes_K L$ to $\mathrm{End}_L(A_L)$ given by $a \otimes \lambda \mapsto (a' \mapsto aa'\lambda)$, is an isomorphism.*

4. Construction of the group G

For this section, we fix the following notations:

- $k \to A$ is a projective separable k-algebra;
- K denotes the center of A;
- L denotes a chosen maximal étale subalgebra $L \subset A$;
- ${}_L A$ is the L-module for the law given by the multiplication on the left; it is a locally free L-module.

We thus have the algebra inclusions

$$k \subset K \subset L \subset A.$$

4.1. ***Introducing the "normalizer" of L in A.*** The inclusion of k-algebras $L \subset A$ gives rise to a closed immersion of multiplicative group functors

$$\mathbf{G}_{m,L/k} \subset \mathbf{G}_{m,A/k}.$$

Denote the normalizer of this subgroup by

$$\mathsf{N} = \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k})$$

Let us be more explicit. For $k' \in k\text{-}\mathsf{Alc}$, one has

$$\mathsf{N}(k') = \left\{a \in (k' \otimes_k A)^\times \mid a(k' \otimes_k L)^\times a^{-1} = (k' \otimes_k L)^\times\right\}.$$

We show, by the standard Lie-type argument, that $\mathsf{N}(k')$ acts, in fact, on the whole algebra $k' \otimes_k L$, and not only on its invertible elements. Let, as usual, $k'[\varepsilon]$ be the ring of dual numbers over k' ($\varepsilon^2 = 0$); one has an exact sequence of groups

$$0 \longrightarrow k' \otimes_k L \xrightarrow{x \mapsto 1+\varepsilon x} \mathbf{G}_{m,L/k}(k'[\epsilon]) \longrightarrow \mathbf{G}_{m,L/k}(k'),$$

where the first term $k' \otimes_k L$ stands for the additive underlying group of that ring. As the group functor $\mathbf{G}_{m,L/k}$ is acted upon by N, one sees that N also acts on the above kernel, that is on the functor in additive groups $k' \mapsto k' \otimes_k L$; to be precise, a section $a \in \mathsf{N}(k')$ induces the inner automorphism $x \mapsto axa^{-1}$ of the group $(k' \otimes_k L)^\times$, and thus it defines an automorphism w of the k'-algebra $k' \otimes_k L$, characterized by

$$ax = w(x)a \quad \text{for all } x \in k' \otimes_k L. \tag{4-1}$$

By its very definition, this automorphism w is the identity on the subalgebra $k' \otimes_k K$.

Therefore we get a morphism of group functors

$$\mathsf{N} = \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k}) \to \mathsf{Aut}(L/K),$$

where $\mathsf{Aut}(L/K)$ is the functor on the category of commutative k-algebras given by

$$\mathsf{Aut}(L/K)(k') \;=\; \mathrm{Aut}_{(k'\otimes_k K)\text{-}\mathsf{Alc}}(k'\otimes_k L)$$

(Technically, the base ring k should appear in the symbol $\mathsf{Aut}(L/K)$, but it is clear from the context that this functor, like most of the others under consideration, is defined on the category of commutative k-algebras.)

Let us introduce the local rank of A as a K-module; since A is locally a matrix algebra, this rank is a square; so, let $n : \mathrm{Spec}(K) \to \mathbb{N}$ be the map defined by

$$\mathrm{rank}_{K_\mathfrak{q}}(A_\mathfrak{q}) = n(\mathfrak{q})^2.$$

Since L is étale over K the L-module ${}_L A$ is locally free by Lemma 3.2. As the K-rank of L is n, the L-rank of ${}_L A$ is also n — with a slight abuse of notation, this last n being the composite map

$$\mathrm{Spec}(L) \to \mathrm{Spec}(K) \xrightarrow{n} \mathbb{N}.$$

Denote by $\mathscr{L}$ the determinant of the L-module ${}_L A$, that is the invertible L-module defined by

$$\mathscr{L} = \det_L({}_L A) = \bigwedge\nolimits^n {}_L A$$

Fix $k' \in k\text{-}\mathsf{Alc}$, and consider a section $a \in \mathsf{N}(k')$; as above, we write w for the inner automorphism of $k'\otimes_k L$ defined by a — see (4-1). The product by a on the left in $k'\otimes_k A$ is thus a w-semilinear map, that we may write as a $k'\otimes_k L$-linear map

$$k'\otimes_k A \to w_\star(k'\otimes_k A), \quad a' \mapsto aa'$$

The n-th exterior power of this map gives a $k'\otimes_k L$-linear map

$$\det(a) : k'\otimes_k \mathscr{L} \to w_\star(k'\otimes_k \mathscr{L})$$

(The notation $\det(a)$, usually reserved for endomorphisms, is a bit improper here; but it cannot cause any confusion.)

4.2. ***Constructing the group functor*** G**.** Because k is supposed to be semilocal, the ring L is also semilocal since it is finite over k; hence, the invertible L-module $\mathscr{L}$ is isomorphic to L; we *choose* a basis $e \in \mathscr{L}$, i.e., an isomorphism

$$L \xrightarrow{\sim} \mathscr{L}, \qquad x \mapsto xe.$$

We now define the group functor G as the stabilizer of the basis e of $\mathscr{L}$, for its action through det; more precisely,

$$\mathsf{G}(k') = \big\{a \in \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k})(k') \mid \det(a)(1\otimes e) = 1\otimes e\big\}.$$

(Although the map det is not a morphism, G is indeed a group.)

Proposition 4.3. *We maintain the assumptions and notation at the beginning of Section 4, and we suppose in addition that the ring k is semilocal and that the K-integer n is invertible in k. Then the group functor* G, *defined above, fits into the following commutative diagram, whose rows are exact sequences of sheaves on* $\mathrm{Spec}(k)$ *for the étale topology*:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathsf{R}_{L/k}(\mu_{n,L}) & \longrightarrow & \mathsf{G} & \longrightarrow & \mathsf{Aut}(L/K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \| & & \\
1 & \longrightarrow & \mathbf{G}_{m,L/k} & \longrightarrow & \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k}) & \longrightarrow & \mathsf{Aut}(L/K) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle n} & & & & & & \\
 & & \mathbf{G}_{m,L/k} & & & & & &
\end{array}$$

In particular, G *is finite étale over* k.

The proof occupies Sections 4.4–4.5.

4.4. *The sequence* $1 \to \mathbf{G}_{m,L/k} \to \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L}) \to \mathsf{Aut}(L/K) \to 1$ *is exact.*

(a) *Exactness at* $\mathsf{N} = \mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k})$. The property of L being a "maximal commutative" subalgebra may be interpreted as the exactness of the following sequence of K-modules

$$0 \to L \to A \to \mathrm{Hom}_K(L, A),$$

where the map on the right associates to $a \in A$ the K-linear map $x \mapsto ax - xa$. Such exactness is preserved by any flat base change.

Now, consider a section $a \in \mathsf{N}(k')$, where k' is flat over k; suppose that the conjugation by a gives the identity in $\mathsf{Aut}(L/K)(k')$; this means that $axa^{-1} = x$ for all $x \in k' \otimes_k L$; thus a commutes with all the elements of the *maximal commutative* subalgebra $k' \otimes_k L$; therefore, one has $a \in \mathbf{G}_{m,L/k}(k')$.

(b) The proof of the (local) *surjectivity of* $\mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k}) \to \mathsf{Aut}(L/K)$ needs several steps.

4.4.1. We begin with the "split" case where $A = \mathrm{End}_K(L)$, the inclusion $L \subset A$ being isomorphic to the map $m : L \to \mathrm{End}_K(L)$ given by the multiplication. Then each automorphism of K-algebras $w : L \to L$ is the restriction to L of the conjugation by w in $\mathrm{End}_K(L)$, as the formula $wm(x)w^{-1} = m(w(x))$ shows. That implies the surjectivity in this case.

We will now show that the general case is "locally" isomorphic to this split one.

4.4.2. There is an isomorphism of algebras $\omega : A \otimes_K L \xrightarrow{\sim} \mathrm{End}_K(L) \otimes_K L$ making the following diagram commutative (it is an isomorphism of L-algebras for the product *on the right* by elements of L).

$$\begin{array}{ccc} L \otimes_K L & \xrightarrow{\iota \otimes 1} & A \otimes_K L \\ \| & & \downarrow \omega \\ L \otimes_K L & \xrightarrow[m \otimes 1]{} & \mathrm{End}_K(L) \otimes_K L \end{array}$$

Proof. Look at A as an $L \otimes_K L$-module via the law $(x \otimes y, a) \mapsto xay$; since $L \otimes_K L$ is étale over K, and since A is locally free over K, A is locally free as a $L \otimes_K L$-module (Lemma 3.2); as both A and $L \otimes_K L$ have the same rank n^2 over K, the module A is of rank 1 over $L \otimes_K L$. But the ring $L \otimes_K L$ is finite over the semilocal ring k; therefore it is also semilocal, and then any rank one projective module over $L \otimes_K L$ is isomorphic to $L \otimes_K L$. Thus we can find $\varepsilon \in A$ such that the map

$$L \otimes_K L \to A, \quad x \otimes y \mapsto x\varepsilon y,$$

is an isomorphism. On considering both $L \otimes_K L$ and A as L-modules for the product on the right, we get an isomorphism of L-algebras

$$\mathrm{End}_L(A_L) \xrightarrow{\sim} \mathrm{End}_L(L \otimes_K L).$$

We obtain the isomorphism ω by composing the above one with the isomorphism indicated in Proposition 3.7:

$$A \otimes_K L \xrightarrow{3.7} \mathrm{End}_L(A_L) \xrightarrow{\sim} \mathrm{End}_L(L \otimes_K L) \xrightarrow{\sim} \mathrm{End}_K(L) \otimes_K L.$$

The required commutativity of the square is easy to check. □

4.4.3. There exist a finite injective étale morphism $k \to k'$ and an isomorphism of k'-algebras

$$\omega' : A \otimes_k k' \xrightarrow{\sim} \mathrm{End}_K(L) \otimes_k k'$$

making commutative the diagram

$$\begin{array}{ccc} L \otimes_k k' & \xrightarrow{\iota \otimes 1} & A \otimes_k k' \\ \| & & \downarrow \omega' \\ L \otimes_k k' & \xrightarrow[m \otimes 1]{} & \mathrm{End}_K(L) \otimes_k k' \end{array}$$

(The difference with the previous diagram is that the tensor products are now taken over k.)

Proof. Let $k' = \mathsf{R}_{K/k}(L)$ be the Weil restriction of L from Section 2.1; it is a finite étale k-algebra, and by its very definition, it is equipped with a morphism of K-algebras

$$L \;\to\; K \otimes_k k'.$$

Now, for any K-module V, we have the isomorphisms

$$(V \otimes_K L) \otimes_L (K \otimes_k k') \simeq V \otimes_K (K \otimes_k k') \simeq V \otimes_k k'.$$

It is now clear that the required square is obtained from the square of the step 4.4.2 by the base change $L \to K \otimes_k k'$.

One can interpret this step by saying that the inclusion $\iota : L \to A$ is a twisted form, for the finite étale topology on k, of the map $m : L \to \mathrm{End}_K(L)$, given by the product in L.

That ends the proof that the map $\mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k}) \to \mathsf{Aut}(L/K)$ is locally surjective. □

4.5. *The sequence* $\mathbf{1} \to \mathsf{R}_{L/k}(\boldsymbol{\mu}_{n,L}) \to \mathsf{G} \to \mathsf{Aut}(L/K) \to \mathbf{1}$ *is exact.*

(a) *Exactness at* G. Due to the exactness of the bottom row of the diagram of Proposition 4.3, we have to check the equality

$$\mathsf{G} \cap \mathbf{G}_{m,L/k} \;=\; \mathsf{R}_{L/k}(\mu_{n,L}).$$

But, for k' over k, a section $a \in \mathbf{G}_{m,L/k}(k') = (k' \otimes_k L)^\times$ has to be seen as a scalar for the $k' \otimes_k L$-module $k' \otimes_k A$, which is of rank n; therefore, one has $\det(a) = a^n$; since $e \in \mathscr{L}$ is a basis over L, the equality $\det(a)(1 \otimes e) = 1 \otimes e$ is equivalent to $a^n = 1$.

(b) We now check that the morphism $\mathsf{G} \longrightarrow \mathsf{Aut}(L/K)$ is "locally" surjective: given k' finite étale over k, and given an automorphism $w \in \mathsf{Aut}(L/K)(k')$, we have to find a finite étale morphism $k' \to k''$, and a section $a \in \mathsf{G}(k'')$ such that w induces on $k'' \otimes_k L$ the conjugation by a. We already know this to be true for the bottom morphism $\mathsf{Norm}_{\mathbf{G}_{m,A/k}}(\mathbf{G}_{m,L/k}) \to \mathsf{Aut}(L/K)$; we have thus to show the following: given k' finite étale over k and $a \in \mathsf{N}(k')$, there exists a finite étale morphism $k' \to k''$, and a section $y \in \mathbf{G}_{m,L/k}(k'')$ such that $y^{-1}a \in \mathsf{G}(k'')$. But, in any case, since $e \in \mathscr{L}$ is a basis over L, there exists $x \in (k' \otimes_k L)^\times$ such that

$$\det(a)(1 \otimes e) \;= x \cdot 1 \otimes e.$$

Let $k' \to k'_1$ be finite étale morphism which "splits" $k' \otimes_k L$. Thus, there exists a finite set I and an isomorphism

$$k'_1 \otimes_k L \;\xrightarrow{\sim}\; \prod_I k'_1.$$

To the element $x \in (k' \otimes_k L)^\times$ there corresponds a family $(x_i)_{i\in I}$ of invertible elements of k'_1; since the integer n is supposed invertible in k, each of the polynomials $Y^n - x_i \in k'_1[Y]$ is separable; therefore, there exists a finite étale morphism $k'_1 \to k''$, and a family $(y_i) \in \prod_I k''$ such that $y_i^n = x_i$. Going back to $k'' \otimes_k L$ via its isomorphism with $\prod_I k''$, we get an element $y \in k'' \otimes_k L$ such that $y^n = x$; therefore $y^{-1}a \in \mathsf{G}(k'')$.

5. Group generation of separable algebras

Recall the result we want to prove.

Theorem 5.0. *Let k be a semilocal ring containing the field $\mathbb{Q}$. Let $k \to A$ be a projective separable algebra. Then, there exists a finite étale k-group G and a surjective morphism of k-algebras*

$$k\langle \mathsf{G} \rangle \to A.$$

5.1. ***Fixed points.*** We begin by recalling the few facts we need about the fixed points under the action of a group functor.

Let $k \subset K \subset L$ be two finite injective étale morphisms of rings. Let $W \subset \mathsf{Aut}(L/K)$ be a subgroup functor (it is a functor on k-Alc). We will denote by $L^W \subset L$ the subring of the elements which are *absolutely* invariant under W, that is the set of those $x \in L$ such that for all k-algebra k', the image of x in $k' \otimes_k L$ is invariant under the group $W(k')$. Suppose that W is affine and flat over k; let $u : k \to R$ be its (commutative) algebra of functions, so that $W = \mathrm{Spec}(R)$; then the action of W on L is given by a morphism of k-algebras

$$\delta : L \longrightarrow L \otimes_k R$$

The ring of invariants L^W is then characterized by the exactness of the sequence

$$L^W \longrightarrow L \underset{\delta}{\overset{1\otimes u}{\rightrightarrows}} L \otimes_k R \ .$$

In fact, fix $k' \in k$-Alc; an automorphism $w \in W(k')$ may be seen as a morphism of k-algebras $w : R \to k'$; it leads to the commutative diagram

$$\begin{array}{ccc} L & \underset{\delta}{\overset{1\otimes u}{\rightrightarrows}} & L \otimes_k R \\ \downarrow & & \downarrow{\scriptstyle 1\otimes w} \\ L \otimes_k k' & \underset{w'}{\overset{\mathrm{Id}}{\rightrightarrows}} & L \otimes_k k' \end{array}$$

where w' is induced from $(1 \otimes w) \circ \delta$; this is nothing but the automorphism given by w, acting on $L \otimes_k k'$. That shows the claim.

The relevance of using group functors (instead of constant groups) appears again in the following result: in a weak sense, any finite étale morphism is "galoisian".

Lemma 5.1.1. *Let $k \subset K \subset L$ be two finite injective étale morphisms of rings. Then*

$$L^{\mathrm{Aut}(L/K)} = K.$$

To make notations lighter, let $W = \mathrm{Aut}(L/K)$. The inclusion $K \subset L^W$ comes from the definition.

For the converse, it is enough to show the inclusion $k' \otimes_k L^W \subset k' \otimes_k K$ for a faithfully flat morphism $k \to k'$. Remark first that for any such morphism, the canonical morphism

$$k' \otimes_k (L^W) \longrightarrow (k' \otimes_k L)^{W(k')}$$

is clearly injective. Let us now take for $k \to k'$ a finite étale morphism which splits the finite étale algebras K and L; the inclusion $k' \otimes_k K \subset k' \otimes_k L$ is then isomorphic to the inclusion $\prod_I k' \subset \prod_J k'$ associated to some surjective map $\alpha : J \to I$ of finite sets; in this situation, the group $W(k')$ is isomorphic to the subgroup $\Gamma \subset \mathfrak{S}_J$ of all the bijections σ of J such that $\alpha \circ \sigma = \alpha$; precisely, one has $\Gamma = \prod_{i \in I} \mathfrak{S}_{\alpha^{-1}(i)}$. As the map α clearly induces a bijection $J/\Gamma \simeq I$, the elements of $k' \otimes_k L = \prod_J k'$ which are invariants under the automorphisms in Γ are those of $\prod_I k' = k' \otimes_k K$.

5.2. ***Proof of the theorem.*** As in Section 4, we denote by K the center of A, and by n^2 the K-rank of A as a locally free K-module. We again choose an étale maximal subalgebra $L \subset A$, and a generator of the invertible L-module $\mathscr{L} = \det_L({}_L A) = \bigwedge^n {}_L A$.

According to Proposition 4.3 we can define a sequence of morphisms between finite étale groups

$$1 \longrightarrow \mathsf{R}_{L/k}(\mu_{n,L}) \longrightarrow \mathsf{G}_0 \longrightarrow \mathrm{Aut}(L/K) \longrightarrow 1$$

which is exact as a sequence of sheaves for the étale topology.

5.2.1. Now suppose given a k-subgroup $W \subset \mathrm{Aut}(L/K)$, which is finite étale over k, and such that $L^W = K$ (according to Lemma 5.1.1, W may be the whole $\mathrm{Aut}(L/K)$, but it may also be the (constant) Galois group of L/K in case this morphism is galoisian).

We then define the group G for the theorem as the pull-back of G_0, as shown in the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathsf{R}_{L/k}(\mu_{n,L}) & \longrightarrow & \mathsf{G} & \longrightarrow & W & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \mathsf{R}_{L/k}(\mu_{n,L}) & \longrightarrow & \mathsf{G}_0 & \longrightarrow & \mathrm{Aut}(L/K) & \longrightarrow & 1
\end{array}$$

Consider the canonical morphism

$$f : k\langle \mathsf{G} \rangle \to A$$

associated, via Proposition 1.3.2, to the inclusion $\mathsf{G} \subset \mathsf{G}_0 \subset \mathsf{N} \subset \mathbf{G}_{m,A/k}$. We will prove it to be surjective.

5.2.2. The first step is to prove that an element $a \in A$ which commutes with any "local" section of G is in fact in the center K of A.

Let a be such an element; the hypothesis means that for each commutative algebra $k \to k'$, the image of a in $k' \otimes_k A$ commutes with the elements of $\mathsf{G}(k') \subset k' \otimes_k A$.

First, we show that $a \in L$. By assumption, $af(b) = f(b)a$ for all $b \in k\langle \mathsf{G} \rangle$. By Theorem 2.3, the k-algebra L is generated by the subgroup $\mathsf{R}_{L/k}(\mu_{n,L}) \subset \mathsf{G}$; thus, the element a must commute with all the elements of L; but L is a *maximal* commutative subalgebra; therefore, $a \in L$.

Next we show that $a \in K = L^W$. Let $w \in W(k')$; since the morphism of sheaves $\mathsf{G} \to W$ is surjective, we may find a faithfully flat extension k'' of k' and a section $g \in \mathsf{G}(k'')$, such that

$$w(1 \otimes a) = g(1 \otimes a)g^{-1}$$

The hypothesis on a then implies that $w(1 \otimes a) = 1 \otimes a$.

5.2.3. Let C be the center of the group algebra $k\langle \mathsf{G} \rangle$. We prove that

$$f(C) = K.$$

Take $c \in C$; since the image $f(c)$ commutes with the local sections of G, the previous step shows that $f(c) \in K$. Conversely, let us check the inclusion $K \subset f(C)$. The group $\mathsf{R}_{K/k}(\mu_{n,K})$ is clearly a subfunctor of G, and we have, by Theorem 2.3,

$$f(k\langle \mathsf{R}_{K/k}(\mu_{n,K}) \rangle) = K.$$

Moreover, since $\mathsf{R}_{K/k}(\mu_{n,K})$ is a subgroup of $\mathbf{G}_{m,K/k}$, it is included in the center of $\mathsf{G} \subset \mathbf{G}_{m,A/k}$; therefore $k\langle \mathsf{R}_{K/k}(\mu_{n,K}) \rangle \subset C$, and we are done.

5.2.4. We now conclude the proof of the surjectivity of f. The k-algebra $B = k\langle \mathsf{G} \rangle$ is separable since the order of the étale group G is invertible in k (recall that $\mathbb{Q} \subset k$); it is thus an Azumaya C-algebra. Since $f(C)$ is contained in the center K of A, the K-algebra A can be seen as a C-algebra, and f as a morphism of C-algebras from the Azumaya C-algebra B to A. According to [Knus and Ojanguren 1974, III.5.3, p. 95], f induces an isomorphism

$$B \otimes_C A^B \quad \xrightarrow{\sim} \quad A,$$

where $A^B = \{a \in A \mid af(b) = f(b)a \text{ for all } b \in B\}$; but this ring is equal to K, as seen in 5.2.2, and the map $C \to K$ is surjective, by 5.2.3. Therefore the morphism $f : B \to A$ is surjective.

6. Examples

Let K be a field of characteristic zero.

6.1. ***Some finite groups generating a matrix algebra.*** We begin with the "standard" representation of the symmetric group

$$K\langle \mathfrak{S}_{n+1}\rangle \longrightarrow \mathbf{M}_n(K) \tag{6-1}$$

More generally, let Γ be a group acting transitively on the set $I = \{0, 1, \dots, n\}$; consider the $K\langle\Gamma\rangle$-module $U = \mathsf{M}(I, K) \simeq K^{n+1}$ whose elements are the maps $u : I \to K$; it is the direct sum $U = U_0 \oplus U_1$, of the submodules $U_0 = \{u \mid \sum_i u(i) = 0\}$, and $U_1 = U^\Gamma$; this last module is a K-vector space of rank one, generated by the constant map with value 1. The algebra $\mathrm{End}_{K\langle\Gamma\rangle}(U)$ decomposes as the product $\mathrm{End}_{K\langle\Gamma\rangle}(U_0) \times \mathrm{End}_{K\langle\Gamma\rangle}(U_1)$, and the second factor is isomorphic to K. On the other hand, by expressing the elements of $\mathrm{End}_K(U)$ as matrices indexed by $I \times I$, one can check that the K-vector space $\mathrm{End}_{K\langle\Gamma\rangle}(U) \subset \mathrm{End}_K(U)$ has a basis indexed by the quotient set $(I \times I)/\Gamma$; the factor $\mathrm{End}_{K\langle\Gamma\rangle}(U_1)$ is generated by the class of the diagonal which is one orbit in $I \times I$; therefore, the morphism $K \to \mathrm{End}_{K\langle\Gamma\rangle}(U_0)$ is an isomorphism if and only if Γ has just one more orbit on the product, that is if Γ is 2-transitive on I; by the Wedderburn double centralizer theorem we finally get the following well-known characterization (for a proof using character theory, see [Serre 1977, §2.3, exercise 2]):

Proposition 6.1.1. *The morphism $K\langle\Gamma\rangle \to \mathrm{End}_K(U_0)$ is surjective if and only if the action of Γ is 2-transitive on I.*

We return to (6-1). The matrix algebra $\mathbf{M}_n(K) \simeq \mathrm{End}_K(U_0)$ is thus shown to be generated by the symmetric group $\mathfrak{S}_{n+1}$, but this group is far from being of the type we introduced in Section 4. Let us try to get close to these constructions.

We define a commutative étale maximal subalgebra of $\mathrm{End}_K(U_0)$ coming from a commutative subgroup of $\mathfrak{S}_{n+1}$: namely, let $H \subset \mathfrak{S}_{n+1}$ be the subgroup generated by the cyclic permutation $\rho = (0, 1, 2, \dots, n)$, and let $L \subset \mathrm{End}_K(U_0)$ be the subalgebra it generates; since the composite map

$$K\langle H\rangle \to \mathrm{End}_K(U_0) \times \mathrm{End}_K(U_1) \to \mathrm{End}_K(U)$$

is injective, we readily get an isomorphism

$$K[X]/(X^n + X^{n-1} + \cdots + 1) \xrightarrow{\sim} L$$

showing that L is étale of rank n (recall that $\mathbb{Q} \subset K$). Let $N \subset \mathfrak{S}_{n+1}$ be the normalizer of ρ; this group is isomorphic to the semidirect product

$$\Gamma = \mathbb{Z}/(n+1)\mathbb{Z} \rtimes (\mathbb{Z}/(n+1)\mathbb{Z})^{\times};$$

consider the morphism

$$K\langle\Gamma\rangle \to \mathrm{End}_K(U_0);$$

according to Proposition 6.1.1, this morphism is surjective if and only if the integer $n+1$ is prime. If it is not, we may follow the method of Section 4; it leads to a nonconstant group scheme (see also Section 6.3).

In any case, it is easy — and this is certainly well known — to get smaller finite (constant) subgroups of $\mathrm{GL}_n(K)$ which generate $\mathbf{M}_n(K)$; for example, choose a transitive group W of permutations of the canonical basis of K^n, say the group generated by a cycle of length n, and let $D \subset \mathrm{GL}_n(K)$ be the group of diagonal matrices with coefficients ± 1; then the morphism

$$K\langle D \rtimes W\rangle \to \mathbf{M}_n(K)$$

is easily seen to be surjective.

6.2. ***Back to quaternions.*** For the following remarks, it is useful to define the $\mathbb{R}$-algebra of quaternions as a subring of the ring of complex 2×2 matrices

$$\mathbb{H} = \left\{ \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \,\middle|\, a, b \in \mathbb{C} \right\}.$$

We choose the maximal étale subalgebra $L \subset \mathbb{H}$ consisting of the matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & \bar{a} \end{smallmatrix}\right)$; we denote by $\delta : \mathbb{C} \to L$ the isomorphism given by $\delta(a) = \left(\begin{smallmatrix} a & 0 \\ 0 & \bar{a} \end{smallmatrix}\right)$.

Recall that the choice of a generator $i \in \mathbb{C}$ leads to an isomorphism of $\mathbb{R}$-group functors

$$\mu_{2,\mathbb{R}} \xrightarrow{\sim} \mathsf{Aut}(\mathbb{C}/\mathbb{R}).$$

Namely, to an $\mathbb{R}$-algebra K and an element $u \in K$ such that $u^2 = 1$, one associates the K-automorphism of $K \otimes_{\mathbb{R}} \mathbb{C}$, given by $1 \otimes i \mapsto u \otimes i$. For the sequel, it is better to describe $\mathsf{Aut}(\mathbb{C}/\mathbb{R})$ without any choice, as follows: let $\epsilon = \frac{1}{2}(1+u)$; this is an idempotent of K, and the automorphism associated to u may be rewritten as $z \mapsto \epsilon z + (1-\epsilon)\bar{z}$; that only involves the automorphism $z \mapsto \bar{z}$ induced by the conjugation on the factor $\mathbb{C}$. Similarly, we denote by $W = \mathsf{Aut}(L/\mathbb{R})$ the constant Galois group functor of $L/\mathbb{R}$; the group $W(K)$ contains the involution $c : K \otimes_{\mathbb{R}} L \to K \otimes_{\mathbb{R}} L$ given by $\left(\begin{smallmatrix} a & 0 \\ 0 & \bar{a} \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} \bar{a} & 0 \\ 0 & a \end{smallmatrix}\right)$, and one has

$$W(K) = \mathrm{Gal}(K \otimes_{\mathbb{R}} L/K) = \{\epsilon\,\mathrm{Id} + (1-\epsilon)c \mid \epsilon^2 = \epsilon \in K\}.$$

Set $j = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$; then, $\{1, j\}$ is a basis of the L-module ${}_L\mathbb{H}$ associated to the multiplication on the left. Let K be a commutative $\mathbb{R}$-algebra. For $x \in K \otimes_{\mathbb{R}} L$, we have $jxj^{-1} = c(x)$. Any element of $K \otimes_{\mathbb{R}} \mathbb{H}$ may be written as

$$\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & \bar{a} \end{pmatrix} + \begin{pmatrix} \bar{b} & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \delta(a) + \delta(\bar{b}) \cdot j,$$

with $a, b \in K \otimes_{\mathbb{R}} \mathbb{C}$; an expression which we simplify in $x + yj$, with $x, y \in K \otimes_{\mathbb{R}} L$.

Note that $\det x = a\bar{a} \in K$ for $x = \delta(a)$. One checks that $\det(x+yj) = \det x + \det y$. For $x, y \in K \otimes_{\mathbb{R}} L$, the next formula gives the condition of invertibility, and the inverse.

$$(x + yj)(c(x) - yj) = (\det x + \det y)\, 1.$$

Let $\mathsf{N} = \mathrm{Norm}_{\mathbf{G}_{m,\mathbb{H}/\mathbb{R}}}(\mathbf{G}_{m,L/\mathbb{R}})$ be the normalizer. An invertible element $x + yj$ is in $\mathsf{N}(K)$ if and only if, for any $z \in (K \otimes_{\mathbb{R}} L)^\times$, one has

$$(x + yj)z(c(x) - yj) \in K \otimes_{\mathbb{R}} L.$$

By looking at the coefficient of j, we see that this condition means that, for any $z \in (K \otimes_{\mathbb{R}} L)^\times$, one has

$$xy(z - c(z)) = 0.$$

But, if $z = \left(\begin{smallmatrix} 1\otimes i & 0 \\ 0 & -1\otimes i \end{smallmatrix}\right)$, the element $z - c(z)$ is invertible; therefore the conditions on $x + yj$ for being in $\mathsf{N}(K)$ are $\det x + \det y \in K^\times$ and $xy = 0$.

We now follow Section 4.2 for constructing a group G which will generate $\mathbb{H}$: we take $e = 1 \wedge j$ as a basis of $\mathscr{L} = \bigwedge^2{}_L\mathbb{H}$. Let us compute the "wedge two" of the left product by $x + yj$ (written as $x \cdot 1 + y \cdot j$ for clarity): one finds, since $j^2 = -1$,

$$(x \cdot 1 + y \cdot j) \wedge (x \cdot j - y \cdot 1) = x^2 \cdot 1 \wedge j - (y \cdot j) \wedge (y \cdot 1) = (x^2 + y^2) \cdot 1 \wedge j.$$

Thus, using the isomorphism $\delta : \mathbb{C} \to L$, one has

$$\mathsf{G}(K) \simeq \{(a, b) \in (K \otimes_{\mathbb{R}} \mathbb{C})^2 \mid ab = 0, a^2 + b^2 = 1, a\bar{a} + b\bar{b} \in K^\times\}. \tag{6-2}$$

The group law takes j into account:

$$(a, b).(a', b') = (aa' - b\bar{b'}, ab' + b\bar{a'}). \tag{6-3}$$

Now consider the map $\mathsf{G} \to W$ that sends $x + yj$ to the automorphism

$$z \mapsto (x + yj)\, z\, (x + yj)^{-1}.$$

We check that, with the notation of (6-2), the map $\mathsf{G}(K) \to W(K)$ can be written as

$$(a, b) \;\mapsto\; \Big(\frac{a\bar{a}}{a\bar{a} + b\bar{b}}\Big)\mathrm{Id} + \Big(\frac{b\bar{b}}{a\bar{a} + b\bar{b}}\Big)c.$$

The conditions given in (6-2) imply that the coefficient $\dfrac{a\bar{a}}{a\bar{a} + b\bar{b}}$ is indeed an idempotent of K.

Finally, the group functor G comes within an exact sequence

$$1 \longrightarrow \mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}}) \longrightarrow \mathsf{G} \longrightarrow W \longrightarrow 1,$$

where $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$ denotes the Weil restriction already considered in Section 2.2, and where the left hand map is defined as follows: an element in $a \in \mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})(K)$ is an element in $K \otimes_{\mathbb{R}} \mathbb{C}$ such that $a^2 = 1$; it is mapped to $(a, 0) \in \mathsf{G}(K)$.

This sequence splits locally but not globally. In fact, a splitting of $\mathsf{G}(K) \to W(K)$ must map $c \in W(K)$ to an involution $(a, b) \in \mathsf{G}(K)$, whose image back to $W(K)$ must be c; the last condition implies $a = 0$ and then $b^2 = 1$, and, according to (6-3), the first condition implies $b\bar{b} = -1$. In $\mathbb{R} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}$, such an element b cannot exist; but in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ you can take $b = i \otimes i$. Thus the sequence is split over $\mathbb{C}$, and it is not split over $\mathbb{R}$.

As seen in the Section 2.2, the group scheme $\mathsf{R}_{\mathbb{C}/\mathbb{R}}(\mu_{2,\mathbb{C}})$ is a twisted form of the Klein four group; therefore, the group G constructed above is a twisted form of the dihedral group D_4; it has nothing to do with the (constant) quaternion group Q_8 which, of course, also generates $\mathbb{H}$.

6.3. ***A split case.*** Let $K \to L$ be a finite Galois extension of fields, of degree n, with galois group $W = \mathrm{Gal}(L/K)$. We consider the (Azumaya) algebra $A = \mathrm{End}_K(L)$ equipped with its maximal étale subalgebra L.

In this situation, we will see that different choices for a basis of the invertible sheave $\mathscr{L}$ may lead, following Section 4.2, to nonisomorphic groups G.

6.3.1. The normalizer of $L^\times$ is known to be isomorphic to a semidirect product:

$$\mathrm{Norm}_{A^\times}(L^\times) \xrightarrow{\sim} L^\times \rtimes W, \quad a \mapsto (a(1), a(1)^{-1}a). \tag{6-4}$$

In fact, if an element $a \in A^\times$, seen as a *K-linear* automorphism of L, is assumed to normalize $L^\times$, then for any $x \in L^\times$ there exists $x' \in L^\times$ such that for all $y \in L^\times$,

$$a(xa^{-1}(y)) = x'y;$$

Letting $y = a(1)$, we see that $x' = a(1)^{-1}a(x)$; the above equality then gives

$$a(1)^{-1}a(xy) = a(1)^{-1}a(x)a(1)^{-1}a(y).$$

Therefore,the map $z \mapsto a(1)^{-1}a(z)$ is a *K-algebra* automorphism of L; the map (6-4) is thus well defined. Consider now an element $(x, w) \in L^\times \rtimes W$; the map a defined by $a(y) = xw(y)$ normalizes the (left product by an) element $z \in L^\times$, since $a(za^{-1}(y)) = xw(za^{-1}(y)) = w(z)y$; therefore, (6-4) is an isomorphism.

6.3.2. We now choose a first basis of $\mathscr{L}$, by using the isomorphism

$$L \otimes_K L^D \xrightarrow{\sim} \mathrm{End}_K(L) = A, \qquad x \otimes y^* \mapsto (z \mapsto y^*(z)x)$$

(As before, L^D stands for the K-linear dual $\mathrm{Hom}_K(L,K)$). The structure of L-module on ${}_LA$ corresponds to the structure of L-module on $L\otimes_K L^D$ coming from the first factor. For the sheaf $\mathscr{L}=\bigwedge_L^n A$ introduced in Section 4.1, we thus have the isomorphism

$$\mathscr{L}=\bigwedge\nolimits_L^n(L\otimes_K L^D)=L\otimes_K\bigwedge\nolimits_K^n(L^D).$$

Let $e'\in\bigwedge_K^n(L^D)$ be any basis of this K-vector space of rank one; take $e=1\otimes e'\in L\otimes_K\bigwedge_K^n(L^D)$ as an L-basis of $\mathscr{L}$.

The isomorphism of $L\otimes_K L^D$ corresponding to the left product by $a=xw\in\mathrm{Norm}_{A^\times}(L^\times)$, is given by $y\otimes z^*\mapsto xw(y)\otimes z^*$. Therefore, the "wedge" of this map is

$$\det{}_L(a):\mathscr{L}\longrightarrow w_\star(\mathscr{L}),\qquad y\otimes e'\mapsto x^n w(y)\otimes e'$$

The group scheme G_1 we are looking for, along the lines of Section 4.2, is "locally" given by the set of sections a of N such that $\det_L(a)(e)=e$; thus, for a connected (commutative) K-algebra K', one has

$$\mathsf{G}_1(K')=\{(x,w)\in(K'\otimes_K L)^\times\rtimes W\mid x^n=1\}$$

That is,

$$\mathsf{G}_1=\mathsf{R}_{L/K}(\mu_{n,L})\rtimes W_K,$$

where W_K denotes the constant group scheme on $\mathrm{Spec}(K)$ defined by W.

6.3.3. We choose another basis for $\mathscr{L}$ by using the following consequence from Galois theory: every endomorphism $a\in\mathrm{End}_K(L)$ is writable in a unique way as

$$a=\sum_{w\in W}x_w w,$$

with the x_w in L.

Choose a total ordering $\{w_1,\dots,w_n\}$ on the set W, and let $e=w_1\wedge\cdots\wedge w_n$; it is an L-basis of $\mathscr{L}$.

Consider, as above, the product in A by the element $a=xw\in\mathrm{Norm}_{A^\times}(L^\times)$; the determinant of the matrix, relative to the basis W, of the multiplication on the left by w is nothing but the *sign*, noted $\mathrm{sgn}_W(w)$, of the permutation of the finite set W, given by $w'\mapsto ww'$. We thus have, for $ye\in\mathscr{L}$,

$$\det{}_L(a)(ye)=x^n w(y)\mathrm{sgn}_W(w)e.$$

The group G_2 associated to this new basis is thus given (for K' connected) by

$$\mathsf{G}_2(K')=\{(x,w),x\in(K'\otimes_K L)^\times\mid w\in W,x^n\mathrm{sgn}_W(w)=1\}.$$

This is a subgroup of the semidirect product $(K'\otimes_K L)^\times\rtimes W$, but it is not isomorphic to $\mathsf{G}_1(K')$.

In fact, for $(x, w) \in \mathsf{G}_2(K')$, if $\mathrm{sgn}_W(w) = -1$, then x may be of order $2n$ (Recall that $\mathrm{sgn}_W(w) = 1$ except if W is of even order, and the subgroup generated by w contains a 2-Sylow subgroup of W).

6.4. ***Crossed products.*** Keeping the hypotheses and the notation of Section 6.3, we now consider the Azumaya K-algebra associated to a 2-cocycle θ, that is, a map

$$\theta : W \times W \longrightarrow L^\times$$

satisfying, for $s, t, u \in W$, the relation

$$s(\theta(t,u))\theta(st,u)^{-1}\theta(s,tu)\theta(s,t)^{-1} = 1.$$

We suppose that the cocycle is normalized, in the sense that, for any $s \in W$, one has

$$\theta(s,1) = \theta(1,s) = 1.$$

The algebra $A = (L/K, \theta)$ associated to θ is the free L-module with basis $(e_s)_{s\in W}$, endowed with the product extending linearly the following relations, for $s, t \in W$ and $\lambda \in L$,

$$e_s e_t = \theta(s,t)e_{st} \tag{6-5}$$

and

$$e_s\lambda = s(\lambda)e_s.$$

The identity of A is e_1, and $Le_1 \subset A$ is a maximal étale K-subalgebra of A; the normalizer of its multiplicative group is the set $\{\lambda e_s \mid \lambda \in L^\times, s \in W\}$. According to Equation (6-5), the determinant of the matrix of the map $a \mapsto \lambda e_s a$, relative to the basis (e_t) is

$$\det(a \mapsto \lambda e_s a) = \lambda^n.\Big(\prod_{t\in W} \theta(s,t)\Big).\mathrm{sgn}_W(s).$$

Letting

$$\gamma(s) = \Big(\prod_{t\in W} \theta(s,t)\Big).\mathrm{sgn}_W(s),$$

we find for the group functor $\mathsf{G} \subset \mathbf{G}_{m,L/K} \rtimes W$,

$$\mathsf{G}(K') = \{(\lambda, s) \mid \lambda \in (K' \otimes_K L)^\times, s \in W, \lambda^n\gamma(s) = 1\}.$$

References

[Artin 1962] M. Artin, "Grothendieck topologies", mimeographed notes, Harvard University, 1962. Zbl 0208.48701

[Auslander and Goldman 1960] M. Auslander and O. Goldman, "The Brauer group of a commutative ring", *Trans. Amer. Math. Soc.* **97** (1960), 367–409. MR 22 #12130 Zbl 0100.26304

[Bosch et al. 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergebnisse der Mathematik (3) **21**, Springer, Berlin, 1990. MR 91i:14034 Zbl 0705.14001

[Bourbaki 1981] N. Bourbaki, *Éléments de mathématique*, Masson, Paris, 1981. Algèbre, chapitres IV à VII. MR 84d:00002 Zbl 0498.12001

[Demazure and Gabriel 1970] M. Demazure and P. Gabriel, *Groupes algébriques, I: Géométrie algébrique, généralités, groupes commutatifs*, Masson, Paris, 1970. MR 46 #1800 Zbl 0203.23401

[Ferrand 1998] D. Ferrand, "Un foncteur norme", *Bull. Soc. Math. France* **126**:1 (1998), 1–49. MR 2000a:13018 Zbl 1017.13005

[Fontaine 1971] J.-M. Fontaine, "Sur la décomposition des algèbres de groupes", *Ann. Sci. École Norm. Sup.* (4) **4** (1971), 121–180. MR 47 #1925 Zbl 0215.10003

[Knus and Ojanguren 1974] M.-A. Knus and M. Ojanguren, *Théorie de la descente et algèbres d'Azumaya*, Lecture Notes in Math. **389**, Springer, Berlin, 1974. MR 54 #5209 Zbl 0284.13002

[Orzech and Small 1975] M. Orzech and C. Small, *The Brauer group of commutative rings*, Lecture Notes Pure Appl. Math. **11**, Dekker, New York, 1975. MR 56 #15627 Zbl 0302.13001

[Serre 1977] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics **42**, Springer, New York, 1977. MR 56 #8675 Zbl 0355.20006

[Waterhouse 1979] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Math. **66**, Springer, New York, 1979. MR 82e:14003 Zbl 0442.14017

[Yamada 1974] T. Yamada, *The Schur subgroup of the Brauer group*, Lecture Notes in Math. **397**, Springer, Berlin, 1974. MR 50 #456 Zbl 0321.20004

Communicated by Jean-Louis Colliot-Thélène
Received 2007-12-12 Revised 2008-03-31 Accepted 2008-05-06

daniel.ferrand@univ-rennes1.fr *IRMAR, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes, France*