TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 352, Number 2, Pages 595–608
S 0002-9947(99)02361-2
Article electronically published on May 3, 1999

AUTOMORPHISM SCHEME OF A FINITE FIELD EXTENSION

PEDRO J. SANCHO DE SALAS

ABSTRACT. Let $k \to K$ be a finite field extension and let us consider the automorphism scheme $Aut_k K$. We prove that $Aut_k K$ is a complete k-group, i.e., it has trivial centre and any automorphism is inner, except for separable extensions of degree 2 or 6. As a consequence, we obtain for finite field extensions K_1, K_2 of k, not being separable of degree 2 or 6, the following equivalence:

$$K_1 \simeq K_2 \Leftrightarrow Aut_k K_1 \simeq Aut_k K_2.$$

1. INTRODUCTION

The aim of this paper is to study the automorphism scheme of any finite field extension $k \to K$. In the separable case, the k-group $Aut_k K$ is quite simple; in fact, after a base change, the k-group $Aut_k K$ becomes isomorphic to the symmetric group S_n, where n denotes the degree of K over k. Hence, for finite separable extensions, the k-group $Aut_k K$ is finite and étale. Surprisingly, the facts are quite different for non-separable extensions. In such a case $Aut_k K$ is a large group (it has positive dimension) and it is not smooth.

In any case, it is not difficult to prove that $\operatorname{Spec} K$ is a homogeneous k-scheme under the natural action of the k-group $Aut_k K$. This is a standard property of any classical transformation group. Hence, it seems natural to consider $Aut_k K$ as a new example of such groups (even if $Aut_k K$ is not smooth and has few rational points). Traditionally, the great interest of transformation groups is due to the fact that a transformation group encloses the essential structure of the geometric space in which it acts. The same holds for the group $Aut_k K$ and its geometric space $\operatorname{Spec} K$; in fact, it is possible to recover the extension $k \to K$ from the group $Aut_k K$.

The main result of this paper states that $Aut_k K$ is a complete group, i.e., it has trivial centre and any automorphism is inner. Specifically:

Theorem 1.1. *Let $k \to K$ be a finite field extension. Then we have:*

1. *$Z(Aut_k K) = Id$, except for a separable extension of degree 2.*
2. *The natural morphism defined by conjugation*

$$Aut_k K \to Aut_{k-gr}(Aut_k K)$$

is an isomorphism of k-groups, except for separable extensions of degree 2 or 6.

Received by the editors October 31, 1997.
1991 *Mathematics Subject Classification.* Primary 14L27.
Key words and phrases. Finite field extension, automorphism, complete.
This paper is part of the author's dissertation at the Universidad de Salamanca under the supervision of J. B. Sancho de Salas.

For separable extensions, the above theorem is a reformulation of the classical Hölder's theorem on the completeness of symmetric groups S_n. Hence, our result may be regarded as a broad extension of Hölder's theorem for non-separable extensions.

An interesting consequence of the above theorem is the following result, stating that the automorphism scheme fully determines the field extension.

Theorem 1.2. *Let K_1 and K_2 be finite extensions of a field k. Let us further assume that K_1 and K_2 are not separable extensions of degree 2 or 6 over k. Then we have*

$$K_1 \simeq K_2 \Leftrightarrow Aut_k K_1 \simeq Aut_k K_2.$$

In a forthcoming paper we shall provide an explicit construction of the given field extension $k \to K$ from the k-group $Aut_k K$.

Finally, let us remark that the group $Aut_k K$, as well as its subgroups, have been studied by several authors (Begueri [1], Shatz [15], Chase [2],[3], etc.) in order to extend Galois Theory to non-separable extensions.

2. Preliminary section

Let $\bar{k}$ be the algebraic closure of a field k of characteristic $p > 0$. Our starting point is the following theorem stating the local structure of finite field extensions (the term "local" refers to the f.p.p.f. topology).

Theorem 2.1. *Let $k \to K$ be a finite field extension. There exists an isomorphism of $\bar{k}$-algebras*

$$K \otimes_k \bar{k} = \prod^m \bar{k}[x_1, \ldots, x_n]/(x_1^{p^{e_1}}, \ldots, x_n^{p^{e_n}})$$

where $e_1 \geq e_2 \geq \cdots \geq e_n$.

In the purely inseparable extensions case, the above theorem is a direct consequence of a result of Pickert [11]. The general case is stated in Rasala [12], Chapter II, Theorem 6 and Lemma 4 (see also Pauer [10]). A more general result for finite generated algebras is obtained in Sancho [14].

The integer m is clearly the separability degree of K. The sequence $\varepsilon = \{e_1 \geq e_2 \geq \cdots \geq e_n\}$ may be easily determined from the ranks of the K^{p^r}-modules $\Omega^1_{K^{p^r}/k}$; in fact, we have $e_i = Min\ \{r \in \mathbb{N} \ : \ rank\ \Omega^1_{K^{p^r}/k} < i\}$. Hence, the sequence $\varepsilon = \{e_1 \geq e_2 \geq \cdots \geq e_n\}$ is an invariant of K.

In this paper we study the automorphism scheme of finite field extensions and, in general, of finite algebras satisfying Theorem 2.1. Specifically, we consider the following class of finite k-algebras.

Definition 2.2. Let k be a ring of prime characteristic $p > 0$. A finite k-algebra A is said to be of type (m, ε) if there exists a faithfully flat morphism $k \to \bar{k}$ and an isomorphism of $\bar{k}$-algebras

$$A \otimes_k \bar{k} = \prod^m \bar{k}[x_1, \ldots, x_n]/(x_1^{p^{e_1}}, \ldots, x_n^{p^{e_n}})$$

where $\varepsilon = \{e_1 \geq e_2 \geq \cdots \geq e_n\}$.

Note that finite field extensions of type $(m, 0)$ are separable ones, while those of type $(1, \varepsilon)$ are purely inseparable.

Finite k-algebras with the splitting property stated in 2.1 may be characterized as finite k-algebras whose modules of r-jets $J^r_{A/k}$ are projective for $r \geq 0$ (see Sancho [14]). This characterization will not used here.

Now we shall recall some concepts about the functor of points of a scheme that we shall use systematically in this paper.

Given a k-scheme X, we denote by $X^{\cdot}$ the corresponding functor of points defined on the category of k-schemes:

$$X^{\cdot}(S) = Hom_{k-sch}(S, X).$$

Any element of $X^{\cdot}(S)$, i.e., any morphism $x : S \to X$, will be said to be a point of X (parametrized by S). We shall not use the set theoretic concept of point, denoted by the notation $x \in X$. The statement "point x of X"will be always used in the sense of the functor of points, i.e., it will denote a morphism $x : S \to X$ for some k-scheme S.

Notation. The composition of a point $x : S \to X$, with a morphism $\bar{S} \to S$ is a new point $\bar{S} \to S \xrightarrow{x} X$ which will also be denoted by x.

Given two points $x_1 : S_1 \to X$ and $x_2 : S_2 \to X$ we may always assume that both points have the same parameter space, since we may consider the compositions $S_1 \times_k S_2 \xrightarrow{\pi_1} S_1 \xrightarrow{x_1} X$ and $S_1 \times_k S_2 \xrightarrow{\pi_2} S_1 \xrightarrow{x_2} X$ where π_1, π_2 are the natural projections.

The identity morphism $Id : X \to X$ is said to be the general point of X.

The following elementary formula is essential:

$$Hom_{k-sch}(X, Y) = Hom_{functor}(X^{\cdot}, Y^{\cdot}).$$

According to this equality, to define a morphism of schemes is equivalent to defining a morphism between the corresponding functors of points (which is often easier).

Finally, recall that the functor of points of a k-scheme X is a sheaf in the f.p.p.f. topology (S.G.A. 3, IV 6.3.1. iii).

Let k be a Noetherian ring and let A be a flat finite k-algebra. The automorphism scheme of A is defined to be the k-group scheme $Aut_k A$ representing the functor of automorphisms of A, i.e., the functor of points of $Aut_k A$ is

$$Hom_{k-sch}(S, Aut_k A) = Aut_{\mathcal{O}_S - alg}(A \otimes_k \mathcal{O}_S)$$

for any k-scheme S.

The existence of the scheme $Aut_k A$ is a particular elementary case of the existence of the automorphism scheme for any flat projective morphism [7]. The scheme $Aut_k A$ may also be constructed as a closed subscheme of the general linear group $Gl(n, k) = Aut_{k-lineal}(A)$ where $n = rank_k A$. Moreover, this construction shows that $Aut_k A$ is an affine scheme. In this paper we shall only consider affine schemes of finite type over a Noetherian ring k.[1]

[1]The Noetherian hypothesis has been introduced for the sake of simplicity.

3. The separable case: Reformulation of Hölder's theorem

Let k be a ring and let A be a flat étale finite k-algebra of constant degree n. It is well known that there exists a faithfully flat base change $k \to \bar{k}$ such that

$$A \otimes_k \bar{k} = \bar{k} \times \overset{n}{\cdots} \times \bar{k}.$$

Since the automorphism scheme commutes with base changes, we have

$$(Aut_k A) \times_k \bar{k} = Aut_{\bar{k}}(A \otimes_k \bar{k}) = Aut_{\bar{k}}(\prod^n \bar{k}) = S_n.$$

Hence, the scheme $Aut_k A$ is locally isomorphic to the symmetric group S_n.

A classical result of Hölder [8] states that the symmetric group S_n has trivial centre (when $n \neq 2$) and that any automorphism of S_n is inner (when $n \neq 6$). As a direct consequence we obtain the following:

Theorem 3.1. *Let A be an étale finite k-algebra of degree n. Then*

(a) *The k-group scheme $Aut_k A$ has trivial centre: $Z(Aut_k A) = \{Id\}$ (when $n \neq 2$).*

(b) *The k-group scheme $Aut_k A$ is complete, i.e., the conjugation morphism*

$$Aut_k A \longrightarrow Aut_{k-group}(Aut_k A)$$

is an isomorphism (when $n \neq 2, 6$).

In the case $n = 2$ it is obvious that $Aut_k K = \mathbb{Z}/2\mathbb{Z}$. When $n = 6$, the corresponding result of Hölder gives us an exact sequence:

$$0 \to Aut_k K \longrightarrow Aut_{k-gr}(Aut_k K) \longrightarrow \mathbb{Z}/2\mathbb{Z} \to 0.$$

4. The purely inseparable case: The group S_ε is complete

Now k will be a Noetherian ring of prime characteristic $p > 0$.

Given a sequence $\varepsilon = \{e_1 \geq \cdots \geq e_n\}$, we shall denote by S_ε the automorphism scheme of the "trivial" k-algebra of type $(1, \varepsilon)$

$$A = k[x_1, \ldots, x_n]/(x_1^{p^{e_1}}, \ldots, x_n^{p^{e_n}}).$$

By 2.1, any purely inseparable finite extension of fields $k \to K$ is locally isomorphic to A for a certain sequence ε. Therefore, the scheme $Aut_k K$ is a k-group locally isomorphic to S_ε.

In this section we shall determine the maximal tori of the k-group S_ε. This study will be necessary to prove that S_ε is complete and, hence, that automorphism schemes of purely inseparable field extensions are complete.

First let us determine S_ε. A basis for A as a free k-module is provided by the monomials $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ where $\alpha = (\alpha_1, \ldots, \alpha_n)$ and $0 \leq \alpha_i < p^{e_i}$. Any automorphism τ of A is fully determined by $\tau(x_i)$,

$$\tau(x_i) = \sum_\alpha \lambda_{i,\alpha} x^\alpha.$$

The fact that τ is a morphism of k-algebras is expressed by the conditions $\tau(x_i)^{p^{e_i}} = 0$ or, equivalently,

$$\lambda_{i,\alpha}^{p^{e_i}} = 0 \text{ for any } \alpha < p^{e - e_i}$$

(the notation $\alpha < p^{e-e_i}$ means that $\alpha_j < p^{e_j - e_i}$ for every $1 \leq j \leq n$). The fact that τ is bijective is expressed by the condition of its determinant being invertible.

Such determinant is a polynomial in the coefficients $\lambda_{i,\alpha}$ that we shall denote by *det*. Hence we have:

Proposition 4.1. *The ring of coordinates of S_ε is*

$$\mathcal{O}_{S_\varepsilon} = (k[\lambda_{i,\alpha}]/I)_{det}$$

where I is the ideal generated by the monomials $\lambda_{i,\alpha}^{p^{e_i}}$, with $\alpha < p^{e-e_i}$.

Remark 4.2. It follows directly from the above proposition that S_ε is a non-smooth k-group with geometrically connected fibres. The same holds for the automorphism scheme of any purely inseparable finite extension of a field.

The subgroup $T = G_m \times_k \overset{n}{\cdots} \times_k G_m$ of S_ε defined by the equations $\{\lambda_{i,\alpha} = 0,\ \alpha \neq (0,..,1_i,..,0)\}$ is said to be the standard torus of S_ε. The action $T \times_k \operatorname{Spec} A \xrightarrow{*} \operatorname{Spec} A$ transforms any two points $(t_1,\dots,t_n) :\ S \to T = (G_m)^n$, $(x_1,\dots,x_n) :\ S \to \operatorname{Spec} A \subset \mathbb{A}^n$ into the point

$$(t_1,\dots,t_n) * (x_1,\dots,x_n) = (t_1x_1,\dots,t_nx_n).$$

Proposition 4.3. *The centralizer of the standard torus T in S_ε coincides with T, i.e.,*

$$C(T) = T.$$

Proof. Let $t = (t_1,\dots,t_n)$ be the general point of T and let g be any point of $C(T)$. Write

$$g(x_i) = \sum_\alpha \mu_{i,\alpha} x^\alpha.$$

By definition of $C(T)$ we have $g \circ t = t \circ g$. Applying this equality to x_i we have

$$\sum_\alpha \mu_{i,\alpha} t_i x^\alpha = \sum_\alpha \mu_{i,\alpha} t^\alpha x^\alpha$$

so that $\mu_{i,\alpha}(t_i - t^\alpha) = 0$. Since $t_1,\dots,t_n$ are algebraically independent, we conclude that $\mu_{i,\alpha} = 0$ for any $\alpha \neq (0,..,1_i,..,0)$. Hence g is a point of T. □

Theorem 4.4. *The centre of the k-group S_ε is trivial: $Z(S_\varepsilon) = \{Id\}$.*

Proof. It is clear that $Z(S_\varepsilon) \subseteq C(T) \overset{4.3}{=} T$, so that it is enough to prove that if a point $t = (t_1,\dots,t_n)$ of T belongs to the centre, then it is the identity. Let g be the general point of S_ε, defined by

$$g(x_i) = \sum_\alpha \lambda_{i,\alpha} x^\alpha$$

where $\lambda_{i,\alpha}^{p^{e_i}} = 0$ for any $\alpha < p^{e-e_i}$.

Applying the equality $g \circ t = t \circ g$ to x_i, we obtain

$$\sum_\alpha \lambda_{i,\alpha} t_i x^\alpha = \sum_\alpha \lambda_{i,\alpha} t^\alpha x^\alpha$$

so that $\lambda_{i,\alpha}(t_i - t^\alpha) = 0$. Since $\lambda_{i,\alpha}^{p^{e_i}} = 0$ (with $\alpha < p^{e-e_i}$) are the only relations between the variables $\lambda_{i,\alpha}$, it follows that $t_i = t^\alpha$ for any $\alpha < p^e$. In particular, taking $\alpha = (0,\dots,0)$, we obtain that $t_i = 1$. □

Let us recall the concept of homogeneous scheme. Consider the action of a k-group G on a k-scheme X. We say that X is homogeneous under the G-action if for any two points $x_1, x_2 \in X^{\cdot}(S)$ there exists a faithfully flat morphism $\bar{S} \to S$ and a point $g \in G^{\cdot}(\bar{S})$ such that $g * x_1 = x_2$.

Proposition 4.5. *Consider the trivial k-algebra $A = k[x_1, \dots, x_n]/(x_1^{p^{e_1}}, \dots, x_n^{p^{e_n}})$ of type $(1, \varepsilon)$. Then* $\operatorname{Spec} A$ *is a homogeneous scheme under the natural action of the k-group $S_\varepsilon = Aut_k A$.*

Proof. Let us consider two (affine) points $\phi, \bar{\phi} : \operatorname{Spec} B \to \operatorname{Spec} A$ that will be defined by two k-algebra morphisms $\phi, \bar{\phi} : A \to B$. Then we have $\phi(x_i) = b_i$, $\bar{\phi}(x_i) = \bar{b}_i$, where $b_i^{p^{e_i}} = \bar{b}_i^{p^{e_i}} = 0$. It is easy to check that the automorphism g of $A_B = A \otimes_k B$ defined by $g(x_i) = x_i - b_i + \bar{b}_i$ satisfies $g * \phi = \bar{\phi}$. □

Now, let us consider the action of a k-group G on a k-scheme X. Given a point $x : S \to X$, the isotropy subgroup of x is defined to be the subgroup H_x of $G_S = G \times_k S$ whose functor of points is

$$H_x^{\cdot}(\bar{S}) = \{g \in G^{\cdot}(\bar{S}) \ : g * x = x\}$$

for any S-scheme $\bar{S}$.

This subgroup is the fibre over x of the S-morphism $G_S \xrightarrow{*} X_S$, $g \mapsto g * x$. This fact proves the existence of H_x.

Let $x\colon \operatorname{Spec} k \to \operatorname{Spec} A$ be a point.

Corollary 4.6. *The quotient S_ε / H_x exists (in the f.f.p.f. topology) and is isomorphic to* $\operatorname{Spec} A$. *Moreover, the natural morphism $S_\varepsilon \to S_\varepsilon / H_x = \operatorname{Spec} A$ has a section.*

Proof. Since $\operatorname{Spec} A$ is homogeneous, we may assume that x is the "origin", i.e., the point defined by the ideal $\mathfrak{m} = (x_1, \dots, x_n)$ of A. The morphism $S_\varepsilon^{\cdot} \to \operatorname{Spec} A^{\cdot}$, $g \mapsto g * x$ is an epimorphism of sheaves by 4.5. It is clear that the quotient sheaf $S_\varepsilon^{\cdot} / H_x^{\cdot}$ (associated to the presheaf quotient) is isomorphic to $\operatorname{Spec} A^{\cdot}$. Hence, $S_\varepsilon^{\cdot} / H_x^{\cdot}$ is representable and $S_\varepsilon / H_x = \operatorname{Spec} A$.

A section s of the morphism $S_\varepsilon \to \operatorname{Spec} A$, $g \mapsto g * x$ may be defined as follows: Given a point $a = (a_1, \dots, a_n)$ of $\operatorname{Spec} A$ (i.e., $(a_1, \dots, a_n)$ is the point defined by the ideal $(x_1 - a_1, \dots, x_n - a_n)$ of A), $s(a) = \tau_a$ is the point of S_ε defined by $\tau_a(x_i) = x_i + a_i$. □

Let $G \times_k X \xrightarrow{*} X$ be an action of a k-group G on a k-scheme X. A point $x \in X^{\cdot}(S)$ is said fixed by G when for any base change $\bar{S} \to S$ and any point $g \in G^{\cdot}(\bar{S})$ we have $g * x = x$.

We shall denote by X^G the subscheme of X representing the functor of fixed points, i.e.,

$$(X^G)^{\cdot}(S) = \{\text{points } x \in X^{\cdot}(S) \text{ fixed by } G\}.$$

For the existence of the scheme of fixed points we refer to (S.G.A. 3; VIII 6.5d)

Corollary 4.7. *For any point $x : S \to \operatorname{Spec} A$, we have*

$$S \overset{x}{=} (\operatorname{Spec} A_S)^{H_x}.$$

Proof. Since $\operatorname{Spec} A$ is homogeneous, we may assume that x is the "origin", i.e., the point defined by the ideal $\mathfrak{m} = (x_1, \ldots, x_n)$ of $A_S = \bar{k}[x_1, \ldots, x_n]/(x_1^{p^{e_1}}, \ldots, x_n^{p^{e_n}})$ (where $\bar{k}$ denotes the affine ring of S). In this case the standard torus T, which acts on $\operatorname{Spec} A_S$ by the formula

$$(t_1, \ldots, t_n) * (x_1, \ldots, x_n) = (t_1 x_1, \ldots, t_n x_n),$$

is contained in H_x. It is clear that the unique fixed point of T is the "origin". Therefore

$$S \overset{x}{\subseteq} (\operatorname{Spec} A_S)^{H_x} \subseteq (\operatorname{Spec} A_S)^T = S$$

and the corollary follows. □

Remark 4.8. Let us consider the functor of isotropy subgroups

$$F(S) = \{\text{Isotropy groups } H_x \text{ of points } x : \ S \to \operatorname{Spec} A\}.$$

The above corollary shows that this functor is isomorphic to the functor of points of $\operatorname{Spec} A$: any point x of $\operatorname{Spec} A$ defines an isotropy subgroup H_x and, conversely, any subgroup H_x determines a unique point $(\operatorname{Spec} A)^{H_x} \to \operatorname{Spec} A$.

The action of S_ε on itself by conjugation, defines a natural action of S_ε on $T_{Id}S_\varepsilon$ (where Id is the unity section of S_ε). Let us denote the action of S_ε on $T_{Id}S_\varepsilon$ by $*$.

Corollary 4.9. *H_x is the subgroup of S_ε which stabilizes the k-sub-bundle $T_{Id}H_x \subset T_{Id}S_\varepsilon$.*

Proof. Since $\operatorname{Spec} A$ is homogeneous, we may assume that x is the "origin". Recall ([4] II §4 2.4) that $T_{Id}S_\varepsilon = T_{Id}Aut_k A$ is identified to $Der_k(A, A)$ and with this identification $T_{Id}H_x$ is equal to the set of derivations of A leaving $\mathfrak{m} = (x_1, \ldots, x_n)$ stable, i.e., it is equal to the set of derivations of A vanishing at x. Then, given a point τ of S_ε, $\tau * (T_{Id}H_x)$ is the set of derivations of A vanishing at $\tau * x$. The derivations of A vanishing at x, do not vanish at any other point (for example, take $\{x_i\partial_{x_1}\}_{1\le i\le n}$). Therefore, $\tau * (T_{Id}H_x) = T_{Id}H_x \Leftrightarrow \tau * x = x \Leftrightarrow \tau$ is a point of H_x. □

Let $\mathcal{O}_{S_\varepsilon}$ be the affine ring of S_ε and let $\tilde{\mathfrak{m}}$ be the ideal corresponding to the unity section of S_ε. Let $G_{\tilde{\mathfrak{m}}}\mathcal{O}_{S_\varepsilon} = \bigoplus_{n=0}^{\infty} \tilde{\mathfrak{m}}^n/\tilde{\mathfrak{m}}^{n+1}$. It is clear from 4.1 that we have an isomorphism of graduate algebras

$$G_{\tilde{\mathfrak{m}}}\mathcal{O}_{S_\varepsilon} = k[\lambda_{i,\alpha}]/I^2$$

where I is the ideal generated by the monomials $\lambda_{i,\alpha}^{p^{e_i}}$ with $\alpha < p^{e-e_i}$. Given $\bar{f} \in \tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2 \subset G_{\tilde{\mathfrak{m}}}\mathcal{O}_{S_\varepsilon}$, we say that the exponent of $\langle \bar{f} \rangle$ is n if $\bar{f}^{\,n-1} \neq 0$ and $\bar{f}^{\,n} = 0$.

Lemma 4.10. *Assume that k is a field and write $e_1 = \cdots = e_r > e_{r+1} \ge \cdots \ge e_n$. Then $\langle \lambda_{i,0} \rangle$, $0 < i \le r$, are the unique T-line k-sub-bundles of $\tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2$ of exponent p^{e_1}.*

Proof. Let $t = (t_1, \ldots, t_n)$ be a general point of T. Remark that $t * \lambda_{i,\alpha} = t^{1_i - \alpha}\lambda_{i,\alpha}$. Then $\lambda_{i,0}$ is the unique T-line sub-bundle of $\tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2$ where T acts by the character t_i, i.e., $t * \lambda_{i,0} = t_i\lambda_{i,0}$. If L is a sub-bundle in the conditions of the lemma, we have to prove that T acts over L by the character t_i, for some i such that $0 < i \le r$.

[2]Instead of the term $\lambda_{i,(0,..,1_i,..,0)}$, we should write $\lambda_{i,(0,..,1_i,..,0)} - 1$, but we shall maintain the formula as we write it for the sake of simplicity .

It is clear that the exponent of $\lambda_{i,\alpha} \in \tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2$ is p^{e_i} if $\alpha < p^{e-e_i}$, and it does not have a finite exponent if $\alpha \not< p^{e-e_i}$. Note that $\lambda_{i,\alpha}$ has exponent finite p^{e_1} if and only if $0 < i \leq r$ and $\alpha = 0$. Let $E_i = \{\text{elements of } \tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2 \text{ of exponent} \leq e_i\}$. Obviously, E_i is a T-sub-bundle of $\tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2$ and we have that $E_1/E_{r+1} = \langle \lambda_{i,0} \rangle_{0<i\leq r}$. The natural morphism $L \to E_1/E_{r+1}$ is injective, therefore T acts over L by the character t_i, $0 < i \leq r$. □

Lemma 4.11. *Let x be the "origin" of* $\operatorname{Spec} A$*, and H_x the associated isotropy subgroup in $Aut_k A$ of x. Then the incident $T_{Id}H_x^\circ \subset \tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2$ of $T_{Id}H_x$ verifies*

$$T_{Id}H_x^\circ = \langle \lambda_{1,0}, \ldots, \lambda_{n,0} \rangle.$$

Proof. A point g, $g(x_i) = \sum_\alpha \lambda_{i,\alpha} x^\alpha$ of $Aut_k A$ is a point of H_x if and only if g stabilizes the ideal $(x_1, \ldots, x_n)$ of A; that is, if and only if $\lambda_{1,0} = \cdots = \lambda_{n,0} = 0$. Hence, H_x is the subgroup of $Aut_k A$ defined by the ideal $(\lambda_{1,0}, \ldots, \lambda_{n,0})$. The conclusion follows easily. □

Theorem 4.12. *H_x is the unique flat and closed k-subgroup of S_ε, up to conjugation, such that*

1. *the quotient S_ε/H_x exists (in the f.f.p.f. topology) and is isomorphic to* $\operatorname{Spec} A$*;*
2. *the natural morphism $S_\varepsilon \to S_\varepsilon/H_x$ has a section.*

Proof. H_x verifies these conditions by 4.6.

Now, let H' be a flat and closed subgroup of S_ε satisfying conditions (1) and (2).

a) Let us assume that k is a field. Remark that H' contains $(S_\varepsilon)_{\text{red}}$: The rational point $Id \cdot H'$ of $S_\varepsilon/H' \simeq \operatorname{Spec} A$ is defined by a nilpotent ideal, then H', which is the fibre of $Id \cdot H'$ by the morphism $S_\varepsilon \to S_\varepsilon/H'$, is defined by a nilpotent ideal of $\mathcal{O}_{S_\varepsilon}$. The conclusion follows.

If s is a section of the morphism $S_\varepsilon \to S_\varepsilon/H' = \operatorname{Spec} A$, then we have an isomorphism $\operatorname{Spec} A \times H' \simeq S_\varepsilon$ $((x, h') \mapsto s(x) \cdot h$, where x is a point of $\operatorname{Spec} A$ and h' is a point of $H')$.

Thus, via this isomorphism, the function $x_1 \in A = k[x_1, .., x_n]/(x_1^{p^{e_1}}, ..., x_n^{p^{e_n}})$ defines a function $f \in \mathcal{O}_{S_\epsilon}$ vanishing at H', so that its class $\bar{f} \in \tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2$ is an element of exponent p^{e_1} and belongs to the incident $T_{Id}H'^\circ$ of $T_{Id}H'$. Then, there exist elements of exponent p^{e_1} in $T_{Id}H'^\circ$. Note that the standard torus $T \subset (S_\varepsilon)_{\text{red}} \subset H'$ acts on $T_{Id}H'^\circ$. Since T transforms elements of exponent m to elements of exponent m and any T-module is a direct sum of submodules where T acts by means of characters ([4], II 2, 2.5), there exists a T-line sub-bundle in $T_{Id}H'^\circ$ of exponent p^{e_1}. By 4.10, we may assume that $\lambda_{1,0} \in T_{Id}H'^\circ$.

Now, let g be a point of $(S_\varepsilon)_{\text{red}} \subset H'$ defined by $g(x_1) = x_1 + x_i$ and $g(x_j) = x_j$, for any $j \neq 1$. Then

$$g * \lambda_{1,0} = \lambda_{1,0} + \lambda_{i,0} \in T_{Id}H'^\circ$$

Hence, we have $\lambda_{i,0} \in T_{Id}H'^\circ$. Then $T_{Id}H'^\circ = \langle \lambda_{1,0}, ..., \lambda_{n,0} \rangle$ because $\dim_k T_{Id}H'^\circ = \dim_k T_{Id}^* \operatorname{Spec} A = n$. By Lemma 4.11 $T_{Id}H_x{}^\circ = \langle \lambda_{1,0}, \ldots, \lambda_{n,0} \rangle$. In conclusion, $T_{Id}H'^\circ = T_{Id}H_x^\circ$ and $T_{Id}H' = T_{Id}H_x$. By 4.9, $H' \subseteq H_x$ and, since both of them are subgroups of S_ε of the same index, we have $H' = H_x$.

b) Let assume that k is a ring. Let us see that $T \subset H'$, after conjugation if necessary.

Consider the action of T on S_ε/H' by translations. There exists a decomposition $\mathcal{O}_{S_\varepsilon/H'} = k \oplus I$, where I is the direct sum of the T-modules where T acts by means

of some non-trivial character, so that the product of two of these characters is non-trivial (in particular, I is an ideal): It suffices to prove these statements on fibres over k, then we may assume that k is a field. By a) S_ε/H' coincides with $S_\varepsilon/H_x = \operatorname{Spec} A$ and we have that $A = k \oplus \mathfrak{m} = k \oplus (\bigoplus k \cdot x^\alpha)$, $0 < \alpha < p^e$, where the general point $t = (t_1, \ldots, t_n)$ of T verifies that $t(x^\alpha) = t^\alpha x^\alpha$.

Then, T fixes the point $\operatorname{Spec} k \hookrightarrow S_\varepsilon/H'$ defined by I, and T is included in a conjugated group of H'.

Let us now see that $H' = H_x$. Note that $\langle \lambda_{i,0} \rangle$ is the unique line sub-bundle of $\tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2$ such that $t * \lambda_{i,0} = t_i \lambda_{i,0}$, then $T_{Id} H_x^\circ \subset \mathfrak{m}_{Id}/\mathfrak{m}_{Id}^2$ is the unique T-sub-bundle of $\tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2$ such that on fibres over k is equal to $\langle \lambda_{1,0}, ..., \lambda_{n,0} \rangle \subset \tilde{\mathfrak{m}}/\tilde{\mathfrak{m}}^2$. Therefore $T_{Id} H'^\circ = T_{Id} H_x^\circ$. Again as in a) we have that $H' \subseteq H_x$. Since S_ε/H' and S_ε/H_x are finite and flat schemes over k and the natural morphism $S_\varepsilon/H' \to S_\varepsilon/H_x$ is an isomorphism on fibres over k we have that $S_\varepsilon/H' = S_\varepsilon/H_x$ and $H' = H_x$. □

Theorem 4.13. *The k-group S_ε is complete, i.e., the natural morphism defined by conjugation*

$$S_\varepsilon \longrightarrow Aut_{k-gr}(S_\varepsilon)$$

is an isomorphism of k-groups.

Proof. We have to prove that the natural morphism

$$S_\varepsilon^\cdot \longrightarrow Aut_{k-gr}(S_\varepsilon)^\cdot$$

is an isomorphism of sheaves for the f.p.p.f. topology.

The considered morphism is injective because $Z(S_\varepsilon) = \{Id\}$ (see 4.4).

Let us see that it is surjective.

Let τ be a point of $Aut_{k-gr}(S_\varepsilon)$. By 4.12, τ defines an automorphism of the functor of isotropy subgroups of S_ε. Now, this functor is isomorphic to the functor of points of $\operatorname{Spec} A$ (see Remark after 4.7). We conclude that τ defines an automorphism σ of $\operatorname{Spec} A$. By definition, we have

$$(*) \qquad \tau(H_x) = H_{\sigma(x)},$$

and we have to prove that τ is the inner automorphism of S_ε defined by σ.

Let g be a point of $S_\varepsilon = Aut_k A$. For any point x of $\operatorname{Spec} A$ we clearly have

$$(**) \qquad g \cdot H_x \cdot g^{-1} = H_{g(x)}.$$

Applying τ to this equality and using $(*)$ we obtain

$$\tau(g) \cdot H_{\sigma(x)} \cdot \tau(g)^{-1} = H_{\sigma(g(x))}$$

and, by $(**)$, it follows that $\tau(g)(\sigma(x)) = \sigma(g(x))$; that is, $\tau(g) \circ \sigma = \sigma \circ g$ and we obtain that $\tau(g) = \sigma \circ g \circ \sigma^{-1}$. □

5. The General Case

Let k be a Noetherian ring of prime characteristic $p > 0$ and let A be the trivial k-algebra of type (m, ε)

$$A = \prod^m k[x_1, \ldots, x_n]/(x^{p^{e_1}}, \ldots, x^{p^{e_n}}).$$

We denote by $S_{m,\varepsilon}$ the automorphism scheme of A.

5.1. **Structure of the group $S_{m,\varepsilon}$.** Let $e = e_1$ be the greatest exponent of A. It is obvious that $A^{p^e} = \prod^m k$ is the maximal étale subalgebra of A.

Since p-th powers commute with base changes (because the morphisms $A^{p^n} \to A$ are faithfully flat), there exists a restriction morphism

$$S^{\cdot}_{m,\varepsilon} = (Aut_k A)^{\cdot} \longrightarrow (Aut_k A^{p^e})^{\cdot} = S^{\cdot}_m.$$

This morphism has an obvious section $S^{\cdot}_m \hookrightarrow S^{\cdot}_{m,\varepsilon}$. On the other hand, the kernel of the restriction morphism is just the sheaf

$$F(S) = \{\tau \in (Aut_k A)^{\cdot}(S) \ : \ \tau(a \otimes 1) = a \otimes 1 \text{ for any } a \otimes 1 \in A^{p^e} \otimes_k \mathcal{O}_S\}.$$

It is easy to verify that $F = \prod^m S^{\cdot}_{\varepsilon}$, so that we obtain:

Proposition 5.1. *There exists an isomorphism of k-groups*

$$S_{m,\varepsilon} = \left(\prod^m S_\varepsilon\right) \rtimes S_m$$

where S_m acts on $\prod^m S_\varepsilon$ in the obvious way, permuting factors.

Corollary 5.2. *When $(m, \varepsilon) \neq (2, 0)$, we have*

$$Z(S_{m,\varepsilon}) = \{Id\}.$$

Proof. Let us consider an abstract group G with more than one element. It is an elementary exercise in group theory to verify that

$$Z\left(\left(\prod^m G\right) \rtimes S_m\right) = Z(G).$$

Therefore, if $\varepsilon \neq 0$, we have

$$Z(S_{m,\varepsilon}) \overset{5.1}{=} Z\left(\left(\prod^m S_\varepsilon\right) \rtimes S_m\right) = Z(S_\varepsilon) \overset{4.4}{=} \{Id\}.$$

If $\varepsilon = 0$, then $S_{m,\varepsilon} = S_m$ and the conclusion follows because $Z(S_m) = \{Id\}$ when $m \neq 2$ (see Rotman [13], 7.4). □

5.2. **The group $S_{m,\varepsilon}$ is complete.** In this section we shall assume that $\operatorname{Spec} k$ is connected.

Proposition 5.3. *The group S_ε is not a direct product of non-trivial subgroups.*

Proof. (1) First we assume that k is a field.

Let us consider a decomposition $S_\varepsilon = G_1 \times_k G_2$ and let τ be the general point of the standard torus T of S_ε, so that

$$\tau(x_i) = t_i x_i.$$

Then $\tau = g_1 \cdot g_2$ where g_1, g_2 are points of G_1, G_2 respectively. Since g_1 and g_2 commute, it follows that g_1 and g_2 commute with τ. It then follows that g_1,g_2 are points of $C(T) \overset{4.3}{=} T$ and we have

$$g_1(x_i) = \alpha_i x_i, \quad g_2(x_i) = \beta_i x_i$$

where α_i, β_i are elements of the ring $\mathcal{O}_T = k[t_1, t_1^{-1}, \ldots, t_n, t_n^{-1}]$ such that $\alpha_i \beta_i = t_i$.

For any index j, we consider the conjugate $\bar{g}_1$ of g_1 defined after a suitable base change by

$$\bar{g}_1(y_i) = \alpha_i y_i$$

where $y_i = x_i$ when $i \neq j$ and $y_j = x_j + a$, where a is a new variable that is independent of t_i satisfying $a^{p^{e_j}} = 0$. The point $\bar{g}_1$ belongs to G_1 because it is a conjugate of g_1, hence it commutes with g_2, so that

$$(\bar{g}_1 \cdot g_2)(x_j) = (g_2 \cdot \bar{g}_1)(x_j)$$

and we obtain

$$(\alpha_j - 1)(\beta_j - 1) = 0.$$

Since $\mathcal{O}_T$ is a domain, we conclude that $\alpha_j = 1$ (and $\beta_j = t_j$) or $\beta_j = 1$ (and $\alpha_j = t_j$).

Assume that $\alpha_1 = t_1$ (so that $\beta_1 = 1$). For any index $j \neq 1$ we consider the conjugate g_1' of g_1 defined by

$$g_1'(z_i) = \alpha_i z_i$$

where $z_1 = x_1 + x_j$, and $z_i = x_i$ when $i \neq 1$. By the above argument, g_1' commutes with g_2, so that

$$(g_1' \cdot g_2)(x_1) = (g_2 \cdot g_1')(x_1)$$

and we obtain

$$t_1 - \alpha_j = t_1\beta_j - t_j.$$

Of the two possible cases ($\alpha_j = t_j,\ \beta_j = 1$) and ($\alpha_j = 1,\ \beta_j = t_j$), only the first one satisfies the above condition. Therefore we obtain that $g_1 = \tau$. Since the general point of T is a point of G_1, it follows that $T \subset G_1$. Now, G_2 commutes with G_1 and, in particular, it commutes with T. Hence $G_2 \subset C(T) = T \subset G_1$ so that $G_2 = \{Id\}$.

(2) Now let k be a ring with connected spectrum.

If $S_\varepsilon = G_1 \times_k G_2$, then we denote by I_{G_i} the ideal defining the subgroup G_i in S_ε and we denote by $\mathfrak{m}_{Id}$ the ideal defining the identity element $\operatorname{Spec} k \hookrightarrow S_\varepsilon$. Let us consider the finitely generated $\mathcal{O}_{S_\varepsilon}$-module $\mathfrak{m}_{Id}/I_{G_i}$. Note that $\mathfrak{m}_{Id}/I_{G_i} = 0 \Leftrightarrow G_i = \{Id\}$.

Considering the fibres of $S_\varepsilon \to \operatorname{Spec} k$, the case (1) shows that

$$S_\varepsilon = Sup(\mathfrak{m}_{Id}/I_{G_1}) \cup Sup(\mathfrak{m}_{Id}/I_{G_2}),$$

$$\emptyset = Sup(\mathfrak{m}_{Id}/I_{G_1}) \cap Sup(\mathfrak{m}_{Id}/I_{G_2}),$$

and we obtain that $G_1 = \{Id\}$ or $G_2 = \{Id\}$ because S_ε is connected. □

Corollary 5.4. *Let $\varphi : \prod^m S_\varepsilon \to S_\varepsilon$ be a morphism of k-groups. If φ is surjective (as a morphism of sheaves for the f.p.p.f. topology), then φ factors through the natural projection onto some factor.*

Proof. Let $\phi :\ G_1 \times \cdots \times G_m \to G$ be a surjective morphism between abstract groups and let ϕ_i denote the restriction of ϕ to the subgroup G_i. If G has a trivial centre, it is easy to verify that

$$ker\ \phi = ker\ \phi_1 \times \cdots \times ker\ \phi_m$$

and this result may be readily generalized to the k-groups. Hence we have

$$ker\ \varphi = ker\ \varphi_1 \times_k \cdots \times_k ker\ \varphi_m$$

so that

$$S_\varepsilon = (\prod^m S_\varepsilon)/ker\ \varphi = \prod^m (S_\varepsilon/ker\ \varphi_i).$$

According to 5.3 only one factor $S_\varepsilon/ker\ \varphi_i$ is $\neq 0$ and we may assume that $S_\varepsilon/ker\ \varphi_1 \neq 0$. Then $ker\ \varphi_i = S_\varepsilon$ for $2 \leq i \leq m$, i.e.,

$$\{Id\} \times S_\varepsilon \times \cdots \times S_\varepsilon \subset ker\ \varphi$$

and $\varphi : \prod S_\varepsilon \to S_\varepsilon$ factors through the projection onto the first factor.

This argument uses the existence of quotient groups $S_\varepsilon/ker\ \varphi_i$, which follows from this well-known result: If the product of a finite number of sheaves is representable, then every factor is representable. Applying this result to the product

$$\prod (S_\varepsilon{}^{\cdot}/ker\ \varphi_i{}^{\cdot}) = \left(\prod S_\varepsilon{}^{\cdot}\right)/ker\ \varphi^{\cdot} = S_\varepsilon{}^{\cdot}$$

we obtain the existence of a k-group $S_\varepsilon/ker\ \varphi_i$ representing the quotient sheaf $S_\varepsilon{}^{\cdot}/ker\ \varphi_i{}^{\cdot}$. □

Corollary 5.5. *We have*

$$Aut_{k-gr}\left(\prod^m S_\varepsilon\right) = \left(\prod^m S_\varepsilon\right) \rtimes S_m.$$

Proof. Let τ be a point of $Aut_{k-gr}\,(\prod^m S_\varepsilon)$. Applying the above corollary, it is easy to prove that τ permutes the factors of $\prod^m S_\varepsilon$. Therefore, composing τ with a convenient permutation, we may assume that τ takes each factor of $\prod^m S_\varepsilon$ into itself. The corollary follows, because S_ε is complete (4.13). □

Theorem 5.6. *The k-group $S_{m,\varepsilon}$ is complete, i.e., the natural morphism induced by conjugation*

$$S_{m,\varepsilon} \longrightarrow Aut_{k-gr}(S_{m,\varepsilon})$$

is an isomorphism, except for the types $(m = 2, \varepsilon = 0)$ and $(m = 6, \varepsilon = 0)$.

Proof. If $\varepsilon = 0$, then $S_{m,\varepsilon} = S_m$ and Hölder's theorem proves this case.

Let us assume that $\varepsilon \neq 0$.

Let τ be an automorphism of $S_{m,\varepsilon} \overset{5.1}{=} (\prod^m S_\varepsilon) \rtimes S_m$. This automorphism induces an automorphism of the connected component of the identity $(S_{m,\varepsilon})^0 = \prod^m S_\varepsilon$. By 5.5, composing τ with an inner automorphism we may assume that τ induces the identity on $\prod^m S_\varepsilon$. Let us verify that τ is the identity on $S_{m,\varepsilon}$, then the theorem will follow.

It is enough to prove that τ is the identity on the subgroup S_m. First, it is easy to characterize points of S_m as the only points of $S_{m,\varepsilon}$ which coincide with a permutation of the factors $\prod^m S_\varepsilon$ when acting by conjugation. Now, we consider a point σ of S_m and $(g_1, \ldots, g_n)$ of $\prod^m S_\varepsilon$. We have

$$(*) \qquad \sigma \cdot (g_1, \ldots, g_n) \cdot \sigma^{-1} = (g_{\sigma(1)}, \ldots, g_{\sigma(n)}).$$

Applying τ to this equality, we obtain

$$(**) \qquad \tau(\sigma) \cdot (g_1, \ldots, g_n) \cdot \tau(\sigma)^{-1} = (g_{\sigma(1)}, \ldots, g_{\sigma(n)})$$

because τ acts on $\prod^m S_\varepsilon$ by the identity. From the above mentioned characterization of S_m, it follows that $\tau(\sigma)$ is a point of S_m. Finally, comparing $(*)$ and $(**)$ we obtain that $\tau(\sigma) = \sigma$. □

6. Final results

Theorem 6.1. *Let $k \to K$ be a finite field extension. Then*

(a) *$Z(Aut_k K) = \{Id\}$, except for separable extensions of degree 2.*
(b) *$Aut_k K$ is a complete k-group, i.e., the action by conjugation defines an isomorphism*

$$Aut_k K \longrightarrow Aut_{k-gr}(Aut_k K)$$

except for separable extensions of degree 2 or 6.

Proof. After a base change, we may assume by 2.1 that K is the trivial k-algebra of a certain type (m, ε). In that case, $Aut_k K = S_{m,\varepsilon}$ and the conclusion follows from 5.2 and 5.6. □

Remark 6.2. The proof of the above theorem holds for any finite ring morphism $k \to K$ of type $(2, 0)$ in case (a) and of a type different from $(2, 0)$ and $(6, 0)$ in case (b).

Lemma 6.3. *Let K_1 and K_2 be two finite k-algebras of type (m, ε) and (m', ε') respectively. If $Aut_k K_1 \simeq Aut_k K_2$, then $(m, \varepsilon) = (m', \varepsilon')$.*

Proof. We have to show that the type of any k-algebra K may be determined from the group $Aut_k K$. After a base change we may assume that K is the trivial k-algebra of a certain type (m, ε), so that $Aut_k K = S_{m,\varepsilon}$.

The integer $m!$ (and therefore m) is determined by the degree of the quotient $S_{m,\varepsilon}/S^0_{m,\varepsilon}$ (where $S^0_{m,\varepsilon}$ denotes the connected component of the identity in $S_{m,\varepsilon}$) since, by 5.1,

$$S_{m,\varepsilon}/S^0_{m,\varepsilon} = S_{m,\varepsilon}/(\prod^m S_\varepsilon) = S_m.$$

To determine the sequence ε, first we note that $(S^0_{m,\varepsilon})^{S_m} = (\prod^m S_\varepsilon)^{S_m} = S_\varepsilon$. Then we must prove that the sequence ε is determined by S_ε. We denote by $G^{(p^r)}$ the p^r-th power of $G = S_\varepsilon$, i.e., $G^{(p^r)} = \operatorname{Spec} \mathcal{O}^{p^r}_{S_\varepsilon}$. A straightforward calculation from the equations in 4.1 for S_ε gives us the following formula:

$$rank\ \Omega^1_{G^{(p^{r-1})}/k} = rank\ \Omega^1_{G^{(p^r)}/k} \Leftrightarrow r \neq e_1, \ldots, e_n.$$

This formula shows that the sequence $\varepsilon = (e_1, \ldots, e_n)$ is fully determined by the group S_ε. □

Theorem 6.4. *Let K_1 and K_2 be two finite k-algebras of a type different from $(2, 0)$ and $(6, 0)$. Then*

$$K_1 \simeq K_2 \Leftrightarrow Aut_k K_1 \simeq Aut_k K_2.$$

Proof. If $Aut_k K_1 \simeq Aut_k K_2$, by 6.3, both algebras have the same type, say (m, ε). By definition, k-algebras of type (m, ε) are locally (in the sense of f.p.p.f. topology) isomorphic to the k-algebra

$$A = k[x_1, \ldots . x_n]/(x_1^{p^{e_1}}, \ldots, x_n^{p^{e_n}}).$$

These k-algebras are classified by the first cohomology "group" of automorphisms of A, i.e., by $H^1(k, S^{\cdot}_{m,\varepsilon})$ (see [6], 4, or [9], II 8.1).

On the other hand, both groups $Aut_k K_1$ and $Aut_k K_2$ are locally isomorphic to $S_{m,\varepsilon}$. Moreover, k-groups locally isomorphic to $S_{m,\varepsilon}$ are classified by the first cohomology "group" $H^1(k, Aut_{k-gr}(S_{m,\varepsilon})^{\cdot})$.

By 5.6 we have $S^{\cdot}_{m,\varepsilon} = Aut_{k-gr}(S_{m,\varepsilon})^{\cdot}$ and the conclusion follows. □

Corollary 6.5. *Let K_1 and K_2 be finite extensions of a field k, not being separable extensions of degree 2 or 6. Then*

$$K_1 \simeq K_2 \Leftrightarrow Aut_k K_1 \simeq Aut_k K_2.$$

References

1. L. Begueri. *Schéma d'automorphismes. Application a l'étude d'extensions finies radicielles.* Bull. Soc. Math. **93** (1969) pp. 89-111. MR **41:**1701
2. S. U. Chase. *On the automorphism scheme of a purely inseparable field extension.* Ring Theory (R. Gordon, ed.), Academic Press Inc., New York and London (1972). MR **50:**7107
3. S. U. Chase. *Infinitesimal group scheme actions on finite field extensions.* Amer. Journal of Math. **98**, no 2 (1976) pp. 441-480. MR **54:**12731
4. M. Demazure and P. Gabriel. *Groupes Algébriques. vol. 1, Géométrie Algébrique, Généralités, Groupes Commutatifs.* Masson, Paris (1970). MR **46:**1800
5. M. Demazure and A. Grothendieck. *Séminaire de Géométrie Algébrique du Bois Marie S.G.A. 3.* Lect. Notes in Math. vols. **151, 152** and **153**, Springer-Verlag, Heidelberg (1970). MR **43:**223a; MR **43:**223b; MR **43:**223c
6. A. Grothendieck. *Fondements de la Géométrie Algébrique* (Extraits du Séminaire Bourbaki 1957-1962), Technique de descente et théorèmes d'existence en géométrie algébrique I. Paris (1962).
7. A. Grothendieck. *Fondements de la Géométrie Algébrique* (Extraits du Séminaire Bourbaki 1957-1962), Technique de descente et théorèmes d'existence en géometrie algébrique, IV Les schémas de Hilbert. Paris (1962). MR **26:**3566
8. O. Hölder. *Bildung Zusammengesetzter Gruppen.* Math. Ann. **46** (1895) pp. 321-422.
9. M. A. Knus and M. Ojanguren. *Théorie de la Descente et Algèbres d'Azumaya.* Lect. Notes in Math. vol. **389**, Springer-Verlag, Heidelberg (1974). MR **54:**5209
10. F. Pauer. *Spezielle Algebren und transitive Operationen.* Math. Zeit. **160** (1978) pp. 103-134. MR **58:**27939
11. G. Pickert. *Eine Normalform für endliche rein-inseparable Körpererweiterungen.* Math. Zeit., **53** (1950) pp. 133-135. MR **12:**316a
12. R. Rasala. *Inseparable Splitting Theory.* Trans. Amer. Math. Soc. **162** (1971) pp. 411-448. MR **44:**1648
13. J. J. Rotman. *The Theory of Groups. An Introduction.* (2nd edition) Allyn and Bacon, Inc. (1973). MR **50:**2315
14. P. Sancho. *Differentially homogeneous algebras.* (preprint).
15. S. S. Shatz. *Galois Theory. In: Category Theory, Homology Theory and their Applications I.* Lect. Notes in Math., vol. **86**, Springer-Verlag, Heidelberg (1969). MR **40:**2655

Departamento de Matemáticas, Universidad de Extremadura, Badajoz 06071, Spain
E-mail address: sancho@unex.es