PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 11, November 2009, Pages 3575–3583
S 0002-9939(09)09997-3
Article electronically published on June 25, 2009

ON THE "GALOIS CLOSURE" FOR TORSORS

MARCO A. GARUTI

(Communicated by Ted Chinburg)

Abstract. We show that a tower of torsors under affine group schemes can be dominated by a torsor. Moreover, if the base is the spectrum of a field and the structure group schemes are finite, the tower can be dominated by a finite torsor.

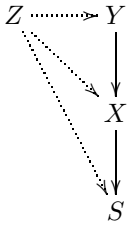
As an application, we show that if X is a torsor under a finite group scheme G over a scheme S which has a fundamental group scheme, then X has a fundamental group scheme too and that this group $\boldsymbol{\pi}(X)$ identifies with the kernel of the map $\boldsymbol{\pi}(S) \to G$.

1. Introduction

The very first result in Galois theory is that any separable extension of a given field K can be embedded in a Galois extension. In particular, if L/K and F/L are Galois extensions, there exists an overfield E which is Galois over K, L and F. In terms of the Galois correspondence, this can be rephrased by saying that the absolute Galois group $Gal(K^{sep}/L)$ can be identified with the kernel of the surjection $Gal(K^{sep}/K) \to Gal(L/K)$.

The same holds for étale covers of schemes. Recall that a finite étale morphism $X \to S$ is a Galois cover with group G if G acts on X without fixed points and S identifies with the quotient of X by this action (cf. [6], §7). This is equivalent to saying that X is a principal homogeneous space (or torsor) over S under G, i.e. that the map $G \times X \to X \times_S X$ given by $(g, x) \mapsto (gx, x)$ is an isomorphism. Then any finite étale cover is dominated by a finite Galois cover. In particular, the following problem has a positive solution for étale torsors (where we can take $B = \operatorname{Spec} \mathbb{Z}$):

Galois closure problem for towers. Let B be a fixed base scheme, $X \to S$ and $Y \to X$ be torsors. Does there there exist a torsor $Z \to S$ dominating X and Y (i.e. all arrows in the commutative diagram below are torsors)?



Received by the editors February 14, 2008, and, in revised form, October 29, 2008.
2000 *Mathematics Subject Classification.* Primary 14L15, 14F20.

In characteristic $p > 0$ or in an arithmetic context it is often necessary to consider not only actions by abstract groups but infinitesimal actions as well. For instance an isogeny between abelian varieties may have an inseparable component (or degenerate to one). One is then led to consider torsors under finite flat group schemes (cf. [6], §12).

In this paper, we solve the Galois closure problem for towers of torsors under finite flat group schemes. We give two versions of this result. The first, Theorem 1, holds for an arbitrary base B and yields a "Galois closure" which is not necessarily finite (even if the intermediate groups are finite). The second, Theorem 2, for schemes over a field, yields a finite "Galois closure".

Except when one can reduce to the case of field extensions (e.g. when all schemes involved are normal), Grothendieck's solution of the Galois closure problem for towers of étale torsors is indirect and relies on his theory of the fundamental group. Namely, in the construction of [5] V §4, one first proves the existence of a "universal cover" $\tilde{S} \to S$ with group $\pi_1(S)$ (step c) and then that any Galois cover $X \to S$ is dominated by an S-morphism $\tilde{S} \to X$, equivariant under a homomorphism $\pi_1(S) \to Gal(X/S)$ (step g). As a consequence, one gets an exact sequence

$$1 \longrightarrow \pi_1(X) \longrightarrow \pi_1(S) \longrightarrow Gal(X/S) \longrightarrow 1 \tag{1}$$

(cf. [5], V §7). As in the case of fields, this sequence allows us to compare finite and infinite Galois theory for schemes.

The arithmetic fundamental group $\pi_1(S)$ "classifies" finite Galois covers of schemes: it is the profinite limit of all Galois groups over S. If S is given over a base scheme B, Grothendieck ([5], X 2.5) suggested to look for a profinite B-group scheme classifying torsors over S under finite flat B-group schemes: it should be the projective limit of all finite group schemes occurring as structure groups of torsors over S. However, the category of torsors under finite flat group schemes is much less well behaved than its étale subcategory: while an S-morphism $Y \to X$ between étale S-schemes is automatically étale, a morphism between S-torsors does not even need to be flat (for instance it can be a closed immersion). As a consequence, one can prove that the projective limit of all structure groups exists only under quite restrictive assumptions on S and B.

For a reduced scheme S, such a *fundamental group scheme* $\boldsymbol{\pi}(S/B)$ has been constructed by Nori [7] (when B is the spectrum of a field) and Gasbarri [4] (when B is a Dedekind scheme). Much progress has been made recently on the fundamental group scheme, thanks to work by Mehta, Subramanian and Esnault among others. This is especially true in the case of proper reduced schemes over a field, where the fundamental group scheme has a Tannakian interpretation in terms of vector bundles and thus a connection with motivic fundamental groups.

The hypothesis that S is reduced is rather unpleasant: in particular, a torsor over S may not have a fundamental group scheme. As pointed out by Nori in the introduction of [7], this would be a serious limitation of the theory. As an application of our result, we show (Theorem 3) that this does not occur: if S has a fundamental group scheme and if X is a torsor over S under a finite flat group scheme G, then X has a fundamental group scheme too. Moreover (Theorem 4), we can generalize the fundamental sequence (1) above: $\boldsymbol{\pi}(X/B)$ identifies with the kernel of the map $\boldsymbol{\pi}(S/B) \to G$.

Even when a fundamental group scheme exists, Grothendieck's template for solving the Galois closure problem for towers of torsors does not apply when one drops

the étaleness assumption. If S is a connected scheme and $X \to S$ is an étale Galois cover with group G, then G is a quotient of $\pi_1(S)$ if and only if X is connected. This criterion, used several times in Grothendieck's construction of [5] V §4, obviously fails for infinitesimal group schemes: even the trivial torsor is connected.

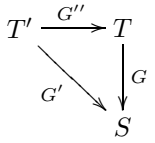
We therefore give a direct construction of the Galois closure: if $X \to S$ and $Y \to X$ are torsors under finite flat B-group schemes G and H respectively, we will explicitly construct from these data an affine group scheme $\Phi = \Phi(G, H)$, equipped with an action of G and a scheme $Z = Z(X, Y, G)$ such that Z is simultaneously a $\Phi \rtimes G$-torsor over S and a Φ-torsor over X dominating Y.

To illustrate the construction, let us describe it in the case of field extensions. Let L/K be a Galois extension of group G and F/L a Galois extension of group H. For $g \in G$ let $F^g = L \otimes_L F$, the tensor product being taken via $g : L \to L$. The algebra $T = \bigotimes_{g \in G} F^g$ can be identified with the set of functions $Fun(G, F)$ made into an L-algebra via the product on the second factor; it is Galois over L and K with $Gal(T/L) = Fun(G, H)$ and $Gal(T/K) = Fun(G, H) \rtimes G$. The Galois algebra T clearly contains the Galois closure of F/K: it is of course far too big, but depends only on L, F and G and thus lends itself to be generalized to a wider context.

2. The Galois closure of a tower of torsors

Notation and conventions. All schemes are assumed locally noetherian. We denote by B a fixed base scheme. When the fibred product is taken over B, we will write $V \times W$ instead of $V \times_B W$. If V and W are schemes over U, we write W_V for the V-scheme $p_1 : V \times_U W \to V$.

Definition 1. If T (resp. T') is a torsor over S under the group scheme G (resp. G'), we say that T' *dominates* T if $T' \to S$ factors through T and T' is a torsor over T for a suitable subgroup $G'' \subseteq G'$:



Theorem 1. *Let S be a B-scheme of finite presentation, G a finite, locally free B-group scheme and H an affine B-group scheme of finite presentation. Let X be a G-torsor over S and Y an H-torsor over X. There exists a scheme Z and an affine B-group scheme of finite presentation $\Phi(G, H)$ such that:*

1. *G acts on $\Phi(G, H)$ and H is a quotient of $\Phi(G, H)$;*
2. *Z is a $\Phi(G, H)$-torsor over X dominating Y (in fact a trivial torsor over Y);*
3. *Z is a $\Phi(G, H) \rtimes G$-torsor over S dominating X.*

The proof rests on the following classical construction (e.g. [2] XI.3.12(b)).

Lemma 1. *Let V be a finite, locally free B-scheme and W an affine B-scheme of finite presentation. Then the functor $U \mapsto \mathrm{Hom}_U(V_U, W_U)$ on B-schemes is representable by a B-scheme of finite presentation $\underline{Hom}_B(V, W)$. Moreover:*

1. *If V is étale and W is finite over B, $\underline{Hom}_B(V, W)$ is finite over B.*

(2) *If B is the spectrum of a field k and G and H are infinitesimal group schemes, then $\underline{Hom}(G,H)$ is connected.*

Proof of Lemma 1. The problem is local, so we may assume that $B = \operatorname{Spec} R$ is affine and $V = \operatorname{Spec} E$ is free of rank r. If $W = \mathbb{A}^s_R$, the functor is represented by $\mathbb{A}^{rs} = \operatorname{Spec} R[x_{i,j}]$ for $i = 1,\dots,s$ and $j = 1,\dots,r$. Indeed, if $\{e_1,\dots,e_r\}$ is an R-basis of E, for any R-algebra A, a map $V_A \to W_A$ is given by a map

$$\begin{aligned} A[t_1,\dots,t_s] &\longrightarrow A \otimes_R E \\ t_i &\longmapsto \textstyle\sum_{j=1}^r x_{i,j} \otimes e_j. \end{aligned} \tag{2}$$

If $W \subseteq \mathbb{A}^s$ is defined by the equations $F_h = 0$, $h = 1,\dots,n$, the map defined in (2) factors through W_A iff $F_h(\sum_j x_{i,j} \otimes e_j) = \sum_j F_{h,j}(x_{i,j}) \otimes e_j = 0$ for suitable polynomials $F_{h,j} \in R[x_{i,j}]$. Hence $R[x_{i,j}]/(F_{h,j})$ represents $\underline{Hom}_B(V,W)$.

Statement 1) can be checked over an étale base change $B' \to B$ such that $V_{B'}$ is a finite disjoint union of copies of B', where it is obvious: $\underline{Hom}(\coprod B', W_{B'}) = \prod \underline{Hom}(B', W_{B'}) = \prod W_{B'}$.

For 2), let $p > 0$ be the characteristic of k. We may assume that k is perfect. By [1], III 3.6.3, the Hopf Algebra of G is $E = k[y_1,\dots,y_d]/(y_1^{p^{m_1}},\dots,y_d^{p^{m_d}})$. Choose the basis y^J, with $J = (j_1,\dots,j_d) \in M = [0,p^{m_1}-1] \times \cdots \times [0,p^{m_d}-1]$.

Similarly, $H = \operatorname{Spec} k[t_1,\dots,t_s]/(t_1^{p^{n_1}},\dots,t_s^{p^{n_s}})$. With this notation, the map (2) sends t_i to $\sum_{J\in M} x_{i,J} \otimes y^J$ and therefore factors through H_A if and only if

$$\left(\sum_{J\in M} x_{i,J} \otimes y_1^{j_1} \dots y_d^{j_d}\right)^{p^{n_i}} = \sum_{J\in M} x_{i,J}^{p^{n_i}} \otimes y_1^{p^{n_i} j_1} \dots y_d^{p^{n_i} j_d} = 0.$$

Hence, if we put $M_i = \{(j_1,\dots,j_d) \in M \,|\, (p^{n_i}j_1,\dots,p^{n_i}j_d) \in M\}$, $\underline{Hom}(G,H)$ is represented by $k\left[x_{i,J}\,|\,i = 1,\dots,s, J \in M\right]/(x_{i,J}^{p^{n_i}}\,|\,i = 1,\dots,r, J \in M_i)$ and is therefore connected. □

Proof of Theorem 1. Let $\Phi(G,H)$ be the B-scheme representing morphisms from G to H (forgetting the group structure). We regard it as a group scheme via the product on the target. G acts on $\Phi(G,H)$ by multiplication on the source; we denote this action by $\varphi \mapsto {}^g\varphi$ on points with values in B-schemes.

The map evaluation at $1 \in G$ is a group homomorphism $\Phi(G,H) \to H$ which has a retraction given by the subgroup of constant functions. Therefore $\Phi(G,H) = \Phi^1(G,H) \rtimes H$, where $\Phi^1(G,H)$ is the subgroup of functions taking $1 \in G$ to $1 \in H$. In particular, $\Phi(G,H)$ satisfies condition 1 in the theorem.

Denote by G_μ the scheme $G \times X$ viewed as an X-scheme via the map $\mu : G \times X \to X$ giving the group action. As above, the functor $U \mapsto \operatorname{Hom}_U(G_{\mu,U}, Y_U)$ on X-schemes is representable by an X-scheme of finite presentation $\underline{Hom}_X(G_\mu, Y)$.

We shall prove that $Z = \underline{Hom}_X(G_\mu, Y)$ is a $\Phi(G,H)$-torsor over X dominating Y, over which it is a trivial $\Phi^1(G,H)$-torsor. Moreover, Z will be a $\Phi(G,H) \rtimes G$-torsor over S.

Step 1. $\Phi(G,H)$ acts on $Z = \underline{Hom}_X(G_\mu, Y)$ in the following way:

$$\Phi(G,H) \times \underline{Hom}_X(G_\mu, Y) = \underline{Hom}_X(G_\mu, H \times_X Y) \longrightarrow \underline{Hom}_X(G_\mu, Y),$$

where the second map is induced by the group action $\nu : H \times Y \to Y$. In terms of points with values in an X-scheme V, $\varphi \in \operatorname{Hom}_V(G_V, H_V)$ sends $f \in \operatorname{Hom}_V(G_{\mu,V}, Y_V)$ to

$$\nu(\varphi, f) : G_{\mu,V} \to H_V \times_V Y_V \to Y_V. \tag{3}$$

Step 2. This action makes $Z = \underline{Hom}_X(G_\mu, Y)$ into a $\Phi(G,H)$-torsor over X. Indeed:

$$\begin{aligned} \Phi(G,H) \times \underline{Hom}_X(G_\mu, Y) &= \underline{Hom}_X(G_\mu, H \times Y) \\ &\cong \underline{Hom}_X(G_\mu, Y \times_X Y) \\ &= \underline{Hom}_X(G_\mu, Y) \times_X \underline{Hom}_X(G_\mu, Y), \end{aligned} \tag{4}$$

where the middle isomorphism is induced by the isomorphism $\nu \times id_Y : H \times Y \to Y \times_X Y$.

Step 3. There is an action of G on $Z = \underline{Hom}_X(G_\mu, Y)$ lifting that on X:

$$\begin{array}{ccc} G \times \underline{Hom}_X(G_\mu, Y) & \xrightarrow{\mu'} & \underline{Hom}_X(G_\mu, Y) \\ \downarrow & & \downarrow \\ G \times X & \xrightarrow{\mu} & X. \end{array} \tag{5}$$

By [6], pp. 110-111, the datum of such a lifting μ' is equivalent to an isomorphism between the two pullbacks of $\underline{Hom}_X(G_\mu, Y)$ on $G \times X$ via μ and p_2. Notice first that, viewing $G \times G_\mu$ and $G_\mu \times_X G_\mu$ as G_μ-schemes via $id_G \times \mu$ and the first projection respectively,

$$id_G \times \mu \times m_G \times id_X : G \times G_\mu \to G_\mu \times_X G_\mu$$

is an isomorphism of G_μ-schemes, m_G being the multiplication in G. The two pullbacks are then

$$G_\mu \times_X \underline{Hom}_X(G_\mu, Y) = \underline{Hom}_{G_\mu}(G_\mu \times_X G_\mu, G_\mu \times_X Y) \cong \underline{Hom}_{G_\mu}(G \times G_\mu, G_\mu \times_X Y)$$

and

$$G \times \underline{Hom}_X(G_\mu, Y) = \underline{Hom}_{G \times X}(G \times G_\mu, G \times Y).$$

To show they are isomorphic we will use the following commutative diagrams:

$$\begin{array}{ccc} G_\mu \times_X Y & \xrightarrow{id_G \times p_2} & G \times Y \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle id_G \times \pi} \\ G_\mu & \xrightarrow{id_G \times \mu} & G \times X \end{array} \qquad \begin{array}{ccc} G \times G \times X & \xrightarrow{id_G \times m_G \times id_X} & G \times G \times X \\ {\scriptstyle id_G \times \mu}\downarrow & & \downarrow{\scriptstyle id_G \times \mu} \\ G \times X & \xrightarrow{id_G \times \mu} & G \times X \end{array}$$

where $\pi : Y \to X$ is the structure morphism. Notice that the horizontal arrows in both diagrams are isomorphisms. Put $\alpha = id_G \times p_2$ and $\beta = id_G \times m_G \times id_X$. Then $f \mapsto \alpha \circ f \circ \beta^{-1}$ gives the desired isomorphism

$$\gamma : \underline{Hom}_{G_\mu}(G \times G_\mu, G_\mu \times_X Y) \longrightarrow \underline{Hom}_{G \times X}(G \times G_\mu, G \times Y). \tag{6}$$

Therefore $\mu' = p_2 \circ \gamma$ is an action of G lifting μ as in diagram (5).

In terms of points with values in an X-scheme, $g \in G(V)$ acts on functions $G_{\mu,V} \to Y_V$ by multiplication on the source.

Step 4. $\Phi(G,H) \rtimes G$ acts on $Z = \underline{Hom}_X(G_\mu, Y)$. Indeed, it is straightforward to check that the map

$$\lambda : \Phi(G,H) \rtimes G \times \underline{Hom}_X(G_\mu, Y) \longrightarrow \underline{Hom}_X(G_\mu, Y) \tag{7}$$

defined by $\lambda(\varphi, g, f) = \nu({}^g\varphi, \mu'(g, f))$ satisfies the requirements.

Step 5. Under this action, $Z = \underline{Hom}_X(G_\mu, Y)$ is a $\Phi(G,H) \rtimes G$-torsor over S. Indeed

$$\begin{aligned}
&\underline{Hom}_X(G_\mu, Y) \times_S \underline{Hom}_X(G_\mu, Y) \\
&\quad = \underline{Hom}_X(G_\mu, Y) \times_X (X \times_S X) \times_X \underline{Hom}_X(G_\mu, Y) \\
&\quad \cong \underline{Hom}_X(G_\mu, Y) \times_X (G \times X) \times_X \underline{Hom}_X(G_\mu, Y) \\
&\quad \cong (\underline{Hom}_X(G_\mu, Y) \times G) \times X \times_X \underline{Hom}_X(G_\mu, Y) \\
&\quad = (\Phi(G,H) \rtimes G) \times \underline{Hom}_X(G_\mu, Y),
\end{aligned}$$

where the first isomorphism is induced by $\mu \times id_X : G \times X \to X \times_S X$ and the second is the isomorphism (6) between the two pullbacks of $\underline{Hom}_X(G_\mu, Y)$ to $G \times X$. We have thus established condition 3 in the statement of Theorem 1.

Step 6. $Z = \underline{Hom}_X(G_\mu, Y)$ dominates Y, over which it is a trivial $\Phi^1(G,H)$-torsor: the map evaluation at $1 \in G_\mu$ gives an X-morphism $\underline{Hom}_X(G_\mu, Y) \to Y$, with a retraction given by the constant functions. Moreover, the restriction to $\Phi^1(G,H)$ of the action (3) of $\Phi(G,H)$ is a Y-morphism

$$\Phi^1(G,H) \times \underline{Hom}_X(G_\mu, Y) \longrightarrow \underline{Hom}_X(G_\mu, Y).$$

Under this action $\underline{Hom}_X(G_\mu, Y)$ is a $\Phi^1(G,H)$-torsor over Y. Indeed, for any pair $f_1, f_2 \in \mathrm{Hom}_V(G_{\mu,V}, Y_V)$ there is a unique $\varphi \in \Phi(G,H)(V)$ such that $\varphi f_1 = f_2$, because $\underline{Hom}_X(G_\mu, Y)$ is a $\Phi(G,H)$-torsor over X. Hence $\varphi(1) f_1(1) = f_2(1)$; thus $\varphi \in \Phi^1(G,H)$ if $f_1(1) = f_2(1)$.

Having a retraction, Z is a trivial $\Phi^1(G,H)$-torsor over Y. □

Remark 1. With notation as in Theorem 1, we have decompositions

$$\Phi = \Phi^1 \rtimes H \qquad \text{and} \qquad Z = \underline{Hom}_X(G_\mu, Y) = \Phi^1 \times Y.$$

Let us spell these out in terms of points with values in a given S-scheme U: any $\varphi \in \Phi(U)$ can be written uniquely as

$$\varphi = \psi h \qquad \text{with} \qquad \psi \in \Phi^1(U),\ h \in H(U), \tag{8}$$

the latter viewed as a constant function. Similarly, any $f \in \mathrm{Hom}_U(G_{\mu,U}, Y_U)$ can be written uniquely as

$$f = \xi y \qquad \text{with} \qquad \xi \in \Phi^1(U),\ y \in Y(U), \tag{9}$$

the latter viewed as a constant function. An element $g \in G(U)$ acts on these decompositions in the following way:

$$^g\varphi = (^g\psi / \psi(g))\,(\psi(g) h)\,, \qquad ^g f = (^g\xi / \xi(g))\,(\xi(g) y)\,. \tag{10}$$

Theorem 2. *Let B be the spectrum of a field k. Under the assumptions of Theorem* 1*, suppose H is a finite group scheme. Then there exists a finite group scheme $\Phi(G,H)$ satisfying the conditions of Theorem* 1*.*

Proof. By Lemma 1(1), if G is étale, and in particular if k has characteristic zero, then $\Phi(G,H)$ is finite. In positive characteristic, using the étale-connected sequence, we are reduced to the case that G is connected.

Let $\Phi = \Phi(G,H)$ be as in the proof of Theorem 1 and H^0 the connected component of H. Notice that $\Phi^1 = \Phi^1(G,H) = \Phi^1(G,H^0)$, the subgroup of functions taking $1 \in G$ to $1 \in H$, is connected, though not necessarily finite.

As in the proof of Theorem 1, let G_μ be $G \times X$ viewed as a scheme over X via the action μ. Recall that $\Phi = \Phi^1 \rtimes H$ and that $\underline{Hom}_X(G_\mu, Y)$ is a trivial Φ^1-torsor over Y, a Φ-torsor over X and a $\Phi \rtimes G$-torsor over S.

Fix an integer n such that the connected component H^0 of H is of height $\leq n$ and let ${}_{F^n}\Phi^1$ be the kernel of the n-th iterate of the Frobenius morphism: by [1], II 7.1.6, it is a finite group scheme. We will show that the subscheme $Z = {}_{F^n}\Phi^1 \times Y \subset \Phi^1 \times Y \simeq \underline{Hom}_X(G_\mu, Y)$ satisfies the hypotheses of Theorem 1 with the finite group ${}_{F^n}\Phi^1 \rtimes H$ replacing $\Phi(G, H)$. Notice that ${}_{F^n}\Phi^1 \rtimes H^0 = {}_{F^n}\left({}_{F^n}\Phi^1 \rtimes H\right)$ is a characteristic subgroup of Φ and thus so is ${}_{F^n}\Phi^1 \rtimes H$.

Obviously, the action of Φ on $\underline{Hom}_X(G_\mu, Y)$ restricts to an action of ${}_{F^n}\Phi^1 \rtimes H$ on Z. To show that Z is a ${}_{F^n}\Phi^1 \rtimes H$-torsor over X we use the decompositions (8) and (9) above. For any X-scheme V and any pair $f_1, f_2 \in \mathrm{Hom}_V(G_{\mu,V}, Y_V)$ there is a unique $\varphi \in \Phi(V)$ such that $\varphi f_1 = f_2$, because $\underline{Hom}_X(G_\mu, Y)$ is a Φ-torsor over X. Writing $f_1 = \xi_1 y_1$, $f_2 = \xi_2 y_2$ and $\varphi = \psi h$ we get $\psi h \xi_1 y_1 = \psi h \xi_1 h^{-1} h y_1 = \xi_2 y_2$. Since Φ^1 is normal, $\psi h \xi_1 h^{-1} \in \Phi^1(V)$; since the decomposition (9) is unique, we must have $h y_1 = y_2$ and $\psi h \xi_1 h^{-1} = \xi_2$ and thus $\psi = h \xi_1 h^{-1} \xi_2$. Therefore, if $f_1, f_2 \in Z(V)$, then $\xi_1, \xi_2 \in {}_{F^n}\Phi^1(V)$ and so $\psi \in {}_{F^n}\Phi^1(V)$, because also ${}_{F^n}\Phi^1$ is normal. Hence $\varphi \in \left({}_{F^n}\Phi^1 \rtimes H\right)(V)$.

The action of G on $\underline{Hom}_X(G_\mu, Y)$ restricts to an action of G on Z. Indeed, let U be any S-scheme and take $g \in G(U)$ and $f = \xi y \in Z(U)$. Since ${}_{F^n}\Phi^1 \rtimes H$ is characteristic, ${}^g\xi \in \left({}_{F^n}\Phi^1 \rtimes H\right)(U)$ and ${}^g\xi(1) = \xi(g)$, so ${}^g\xi/\xi(g) \in {}_{F^n}\Phi^1(U)$.

Finally, Z is a $\left({}_{F^n}\Phi^1 \rtimes H\right) \rtimes G$-torsor over S. Indeed, for any S-scheme U and any pair $f_1, f_2 \in \mathrm{Hom}_U(G_U, Y_U)$ there is a unique pair $\varphi \in \Phi(U)$ and $g \in G(U)$ such that ${}^g\varphi {}^g f_1 = f_2$, because $\underline{Hom}_X(G_\mu, Y)$ is a $\Phi \rtimes G$-torsor over S. Writing $f_1 = \xi_1 y_1$, $f_2 = \xi_2 y_2$ and $\varphi = \psi h$ we get

$$ {}^g\psi h\, {}^g\xi_1 y_1 = {}^g\psi h\, {}^g\xi_1 \left(\psi(g) h \xi_1(g)\right)^{-1} \left(\psi(g) h \xi_1(g)\right) y_1 = \xi_2 y_2. $$

Since the decomposition (9) is unique, we must have ${}^g\psi h\, {}^g\xi_1 \left(\psi(g) h \xi_1(g)\right)^{-1} = \xi_2$ and therefore

$$ {}^g\psi/\psi(g) = \xi_2 \hat{h} \left({}^g\xi_1/\xi_1(g)\right)^{-1} \hat{h}^{-1}, $$

where $\hat{h} = \psi(g) h$. Therefore, if $f_1, f_2 \in Z(U)$, then $\xi_1, \xi_2 \in {}_{F^n}\Phi^1(U)$ and so ${}^g\psi/\psi(g) \in {}_{F^n}\Phi^1(U)$; thus ${}^g\psi$ belongs to the characteristic subgroup ${}_{F^n}\Phi^1 \rtimes H$. Hence $\psi \in \left({}_{F^n}\Phi^1 \rtimes H\right) \cap \Phi^1 = {}_{F^n}\Phi^1$. □

3. An exact sequence for the fundamental group scheme

Let B be a fixed base scheme, S a flat B-scheme and $b \in S(B)$ a marked rational point. We consider the category $\mathfrak{C}(S, b)$ whose objects are triples (X, G, x) consisting of a finite flat B-group scheme G, a G-torsor $f : X \to S$ and a rational point $x \in X(B)$ such that $f(x) = b$. A morphism $(X', G', x') \to (X, G, x)$ in $\mathfrak{C}(S, b)$ is the datum of an S-morphism $\alpha : X' \to X$ such that $\alpha(x') = x$ and a B-group scheme homomorphism $\beta : G' \to G$ making the following diagram commute:

$$ \begin{array}{ccc} G' \times X' & \xrightarrow{\mu'} & X' \\ {\scriptstyle \beta \times \alpha}\downarrow & & \downarrow{\scriptstyle \alpha} \\ G \times X & \xrightarrow{\mu} & X \end{array} $$

where the horizontal arrows are the group actions. Notice that α is not required to be flat, and in particular X' does not necessarily dominate X in the sense of Definition 1. This is in marked contrast with the case of étale Galois coverings.

Following Nori [7], chap. II, Definition 1, we shall say that S *has a fundamental group scheme* $\boldsymbol{\pi}(S/B;b)$ if the category $\mathrm{Pro}(\mathfrak{C}(S,b))$ has an initial object $(\tilde{S},\boldsymbol{\pi}(S/k;b),\tilde{b})$. Nori [7] (resp. Gasbarri [4]) have shown that if S is reduced and B is the spectrum of a field (resp. a Dedekind scheme), then S has a fundamental group scheme.

The assumption that S is reduced is quite restrictive: in particular, if X is a G-torsor over S, it may not have a fundamental group scheme. In this section, we will show that if B is a Dedekind scheme, this does not occur.

Theorem 3. *Let B be a Dedekind scheme and (S,b) a pointed B-scheme which has a fundamental group scheme. If (X,x) is a marked torsor over S under a finite flat group scheme G, then also (X,x) has a fundamental group scheme.*

Proof. We will apply the following criterion (Nori [7], chap. II, Proposition 1, if $\dim B = 0$; and Gasbarri [4], Proposition 2.1, if $\dim B = 1$): (X,x) has a fundamental group scheme if and only if $\mathfrak{C}(X,x)$ is filtered. By loc. cit., it suffices to show that for any $(Y,H,y) \in \mathfrak{C}(X,x)$ and any pair of morphisms $\alpha_i : (Y_i,H_i,y_i) \to (Y,H,y)$ in $\mathfrak{C}(X,x)$, the triple $(Y_1 \times_Y Y_2, H_1 \times_H H_2, (y_1,y_2))$ belongs to $\mathfrak{C}(X,x)$. Notice that, by Nori [7], chap. II, Lemma 1, $Y_1 \times_Y Y_2$ is in any case an $H_1 \times_H H_2$-torsor over a closed subscheme of X containing x.

It suffices to prove the theorem when B is the spectrum of a field. Indeed, the case of a general Dedekind scheme follows by taking the scheme-theoretic closure of the objects defined over the generic fibre: the proof of [4], Proposition 2.1 goes through verbatim.

Thus let B be the spectrum of a field. By Theorem 2, there exist objects $(Z,\Phi \rtimes G,z)$ and $(Z_i,\Phi_i \rtimes G,z_i)$ of $\mathfrak{C}(S,b)$ dominating (Y,H,y) and (Y_i,H_i,y_i), respectively. Since (S,b) has a fundamental group scheme, $Z_1 \times_Z Z_2$ is a pointed $(\Phi_1 \times_\Phi \Phi_2) \rtimes G$-torsor over S. Moreover, by property 2 of Theorem 1, $Z_1 \times_Z Z_2$ is a trivial $\Phi_1^1 \times_{\Phi^1} \Phi_2^1$-torsor over $Y_1 \times_Y Y_2$.

On the other hand, $Z_1 \times_Z Z_2$ is a $\Phi_1 \times_\Phi \Phi_2$-torsor over X. Indeed, it is a $\Phi_1 \times_\Phi \Phi_2$-torsor over $T = (Z_1 \times_Z Z_2) \wedge^{(\Phi_1 \times_\Phi \Phi_2) \rtimes G} G$; by construction, T is a G-torsor over S and one checks immediately that $Z_1 \times_Z Z_2 \to X$ descends to a G-equivariant morphism $T \to X$. Since both T and X are G-torsors over S, this is an isomorphism.

Since both the first map and the composite $Z_1 \times_Z Z_2 \to Y_1 \times_Y Y_2 \to X$ are faithfully flat, we conclude that $Y_1 \times_Y Y_2 \to X$ is faithfully flat and therefore an $H_1 \times_H H_2$-torsor over the whole of X. □

Remark 2. If S is *proper* and reduced, Nori [7], chap. I, gives an alternative definition of $\boldsymbol{\pi}(S/k;b)$ as the Tannaka fundamental group of a suitable category of vector bundles. H. Esnault, P.H. Hai and X. Sun [3], §2, have recently shown that Nori's Tannakian construction can be extended to G-torsors over S.

Having established that a G-torsor $f : X \to S$ has a fundamental group scheme, we can show that $\boldsymbol{\pi}(X/B,x)$ is the kernel of $\boldsymbol{\pi}(S/B,b) \to G$.

Theorem 4. *Let B be a Dedekind scheme, (S,b) a pointed B-scheme and (X,x) be a marked torsor over S under a finite flat B-group scheme G. Assume that*

both S and X have a fundamental group scheme. Then, if $\boldsymbol{\pi}(S/B,b) \to G$ is an epimorphism, we have an exact sequence of profinite group schemes:

$$1 \longrightarrow \boldsymbol{\pi}(X/B,x) \xrightarrow{\boldsymbol{\pi}(f)} \boldsymbol{\pi}(S/B,b) \longrightarrow G \longrightarrow 1.$$

Proof. The fact that $\boldsymbol{\pi}(f)$ is injective is a direct consequence of Theorem 2 (if $\dim B = 1$ one has to repeat the scheme-theoretic closure argument above). Indeed, for any quotient H of $\boldsymbol{\pi}(X/B,b)$, we have a diagram

$$\begin{array}{ccc} \boldsymbol{\pi}(X/B,x) & \xrightarrow{\boldsymbol{\pi}(f)} & \boldsymbol{\pi}(S/B,b) \\ \downarrow & & \downarrow \\ \Phi(G,H) & \longrightarrow & \Phi(G,H) \rtimes G \\ \downarrow & & \\ H & & \end{array}$$

Since $\boldsymbol{\pi}(X/B,x)$ is the projective limit of such H's and $\Phi(G,H) \to \Phi(G,H) \rtimes G$ is injective, $\boldsymbol{\pi}(f)$ must be injective.

The sequence is exact in the middle if and only if for any $\chi : \boldsymbol{\pi}(S/B,b) \to G'$ such that $\chi \circ \boldsymbol{\pi}(f) = 0$, χ factors through G. The condition $\chi \circ \boldsymbol{\pi}(f) = 0$ means that if (S',b') is the G'-torsor over S corresponding to χ, the G'-torsor $X' = X \times_S S'$ over X is trivial, whence an S-morphism $\alpha : X \to X' \to S'$. Restricting to the fibers at b and composing with the isomorphisms $\mu_x : G \to X_b$ and $\mu'_{b'} : G' \to S'_b$ induced by the marked points, we get a map $\beta : G \to G'$, which is a group morphism because of the commutativity of the diagram:

$$\begin{array}{ccccccccccc} G\times G & \xrightarrow{id\times\mu_x} & G\times X_b & \xrightarrow{\mu\times id} & X_b\times X_b & \xrightarrow{\alpha\times\alpha} & S'_b\times S'_b & \xleftarrow{\mu'\times id} & G'\times S'_b & \xleftarrow{id\times\mu'_{b'}} & G'\times G' \\ {\scriptstyle m_G}\downarrow & & {\scriptstyle\mu}\downarrow & & {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle p_1} & & \downarrow{\scriptstyle\mu'} & & \downarrow{\scriptstyle m_{G'}} \\ G & \xrightarrow{\mu_x} & X_b & = & X_b & \xrightarrow{\alpha} & S'_b & = & S'_b & \xleftarrow{\mu'_{b'}} & G' \end{array}$$

We thus have a morphism $(X,G,x) \to (S',G',b')$ in $\mathfrak{C}(S,b)$, which is the same as saying that χ factors through G. □

References

[1] M. Demazure and P. Gabriel, *Groupes Algébriques*, Masson, Paris (1970). MR0302656 (46:1800)

[2] M. Demazure and A. Grothendieck, *Schémas en Groupes*, Lecture Notes in Math. 151, 152, 153, Springer (1970). MR0274458 (43:223a), MR0274459 (43:223b), MR0274460 (43:223c)

[3] H. Esnault, P. H. Hai, and X. Sun, *On Nori's fundamental group scheme*, Progress in Mathematics 265, 377-398, Birkhäuser (2007). MR2402410 (2009f:14091)

[4] C. Gasbarri, *Heights of vector bundles and the fundamental group scheme of a curve*, Duke Math. J. 117, 287-311 (2003). MR1971295 (2004c:14047)

[5] A. Grothendieck, *Revêtements étales et groupe fondamental*, Lecture Notes in Math. 224, Springer (1971). MR0354651 (50:7129)

[6] D. Mumford, *Abelian Varieties*, Oxford University Press, Oxford (1982). MR0282985 (44:219)

[7] M. Nori, *The fundamental group scheme*, Proc. Indian Acad. Sci. (Math. Sci.) 91, 73-122 (1982). MR682517 (85g:14019)

Dipartimento di Matematica Pura ed Applicata, Università degli Studi di Padova, Via Trieste 63, 35121, Padova, Italy

E-mail address: mgaruti@math.unipd.it