SPLITTING FAMILIES IN GALOIS COHOMOLOGY

CYRIL DEMARCHE AND MATHIEU FLORENCE

Abstract. Let k be a field, with absolute Galois group Γ. Let A/k be a finite étale group scheme of multiplicative type, i.e. a discrete Γ-module. Let $n \geq 1$ be an integer, and let $x \in H^n(k, A)$ be a cohomology class. We show that there exists a countable set I, and a familiy $(X_i)_{i \in I}$ of (smooth, geometrically integral) k-varieties, such that the following holds. For any field extension l/k, the restriction of x vanishes in $H^n(l, A)$ if and only if (at least) one of the X_i's has an l-point. This is Theorem 4.1, which we state in a slighty more general context, using Yoneda extensions. In the case where A is of p-torsion for a prime number p, we moreover show that the X_i's can be made into an ind-variety, cf. Proposition 5.1. In the case $n = 2$, we note that one variety is enough.

Introduction

Let k be a field, and let p be a prime number, which is invertible in k. The notion of a norm variety was introduced in the study of the Bloch-Kato conjecture. It is a key tool in the proof provided by Rost, Suslin and Voevodsky. The norm variety $X(s)$ of a pure symbol

$$s = (x_1) \cup (x_2) \cup \ldots \cup (x_n) \in H^n(k, \mu_p^{\otimes n}),$$

where the x_i's are elements of $k^\times$, was constructed by Rost (cf. [6] or [3]). The terminology 'norm variety' reflects that it is defined through an inductive process involving the norm of finite field extensions of degree p. It has the remarkable property that, if l/k is a field extension, then the restriction of s vanishes in $H^n(l, \mu_p^{\otimes n})$ if and only if the l-variety $X(s)_l$ has a 0-cycle of degree prime-to-p. It enjoys nice geometric features, which we will not mention here. For $n \geq 3$, norm varieties are, to the knowledge of the authors of this paper, known to exist for pure symbols only. In this paper, we shall be interested in the following closely related problem. Let A/k be a finite étale group scheme of multiplicative type, that is to say, a discrete Γ-module. Consider a class $x \in H^n(k, A)$. Does there exists a *countable* family of smooth k-varieties $(X_i)_{i \in I}$, such that, for every field extension l/k, the presence of a l-point in (at least) one of the X_i's is equivalent to the vanishing of x in $H^n(l, A)$? If such a family exist, can it always be endowed with the structure of an ind-variety?

We provide answers to those questions. The main results of the paper are the following:

Date: November 20, 2017.

2000 *Mathematics Subject Classification.* Primary .

The first author acknowledges the support of the Agence Nationale de la Recherche under reference ANR-15-CE40-0002.

The second author acknowledges the support of the Agence Nationale de la Recherche under reference GeoLie (ANR-15-CE40-0012).

Theorem 0.1 (Corollary 4.2, Theorem 5.1 and Corollary 5.4)**.** *Let A/k be a finite étale group scheme of multiplicative type and let $\alpha \in H^n(k, A)$.*

- *There exists a countable family $(X_i)_{i \in I}$ of smooth geometrically integral k-varieties, such that for any field extension l/k with l infinite, α vanishes in $H^n(l, A)$ if and only if $X_i(l) \neq \emptyset$ for some i.*
- *If $n = 2$, the family (X_i) can be replaced by a single smooth geometrically integral k-variety.*
- *If A is p-torsion for some prime number p and n is arbitrary, then there is such a family (X_i) which is an ind-variety.*

Note that our main "non formal" tool, as often (always?) in this context, is Hilbert's Theorem 90.

1. Notation and definitions.

In this paper, k is a field, with a given separable closure k^s. We denote by $\Gamma := \mathrm{Gal}(k^s/k)$ the absolute Galois group. The letters d and n denote two positive integers. We assume d to be invertible in k.

We denote by $\mathcal{M}_d$ the Abelian category of finite $\mathbf{Z}/d\mathbf{Z}$-modules, and by $\mathcal{M}_{\Gamma,d}$ that of finite and discrete Γ-modules of d-torsion. The latter is equivalent to the category of finite k-group schemes of multiplicative type, killed by d. We denote this category by $\mathcal{M}_{k,d}$. When no confusion can arise, we will identify these categories without further notice. We have an obvious forgetful functor $\mathcal{M}_{\Gamma,d} \to \mathcal{M}_d$.

1.1. **Groups and cohomology.** Let G be a linear algebraic k-group; that is, an affine k-group scheme of finite type. We denote by $H^1(k, G)$ the set of isomorphism classes of G-torsors, for the fppf topology. It coincides with the usual Galois cohomology set if G is smooth. Let $\varphi : H \to G$ be a morphism of linear algebraic k-groups. It induces, for every field extension l/k, a natural map $H^1(l, H) \to H^1(l, G)$, which we denote by $\varphi_{l,*}$.

1.2. **Yoneda Extensions.** Let $\mathcal{A}$ be an Abelian category. For all $n \geq 0$, $A, B \in \mathcal{A}$, we denote by $\mathbf{YExt}^n_{\mathcal{A}}(A, B)$ (or $\mathbf{YExt}^n(A, B)$) the (additive) category of Yoneda n-extensions of B by A, and by $\mathrm{YExt}^n_{\mathcal{A}}(A, B)$ (or $\mathrm{YExt}^n(A, B)$) the Abelian group of Yoneda equivalence classes in $\mathbf{YExt}^n(A, B)$.

Remark 1.1. The groups $\mathrm{YExt}^n_{\mathcal{A}}(A, B)$ can also be defined as $\mathrm{Hom}_{\mathcal{D}(\mathcal{A})}(A, B[n])$, where $\mathcal{D}(\mathcal{A})$ denotes the derived category of $\mathcal{A}$.

Given $A, B \in \mathcal{M}_d$, we put $\mathbf{YExt}^n_d(A, B) := \mathbf{YExt}^n_{\mathcal{M}_d}(A, B)$. Given $A, B \in \mathcal{M}_{k,d}$, we put $\mathbf{YExt}^n_{k,d}(A, B) := \mathbf{YExt}^n_{\mathcal{M}_{k,d}}(A, B)$.

Remark 1.2. Let A be a finite discrete Γ-module.
Let d be the exponent of A. Then there is a canonical isomorphism

$$\mathrm{YExt}^n_{k,d}(\mathbf{Z}/d\mathbf{Z}, A) \xrightarrow{\sim} H^n(\Gamma, A)$$

where $H^n(\Gamma, A)$ denotes the usual n-th cohomology group.

Remark 1.3. Let l/k be any field extension. For $A, B \in \mathcal{M}_{k,d}$, we have a restriction map

$$\mathrm{Res}_{\mathrm{l/k}} : \mathbf{YExt}^n_{k,d}(A, B) \longrightarrow \mathbf{YExt}^n_{l,d}(A, B).$$

1.3. **Lifting triangles.** Let $\varphi : H \to G$ be a morphism of linear k-algebraic groups. A lifting triangle (relative to φ) is a commutative triangle

$$\begin{tikzcd} T : Q \arrow[r, "f"] \arrow[dr, "H_X"'] & P \arrow[d, "G_X"] \\ & X\,, \end{tikzcd}$$

where X is a k-scheme, $Q \longrightarrow X$ (resp. $P \longrightarrow X$) is an H_X-torsor (resp. a G_X-torsor), and where f is an H-equivariant morphism (formula on the functors of points: $f(h.x) = \varphi(h).f(x)$).
Note that such a diagram is equivalent to the data of an isomorphism between the G_X-torsors P and $\varphi_*(Q)$.
The k-scheme X is called the *base* of the lifting triangle T.
We have an obvious notion of isomorphism of lifting triangles.
Moreover, if $\eta : Y \longrightarrow X$ is a morphism of k-schemes, we can form the pullback $\eta^*(T)$; it is a lifting triangle, over the base Y.

1.4. **Lifting varieties.** Let $\varphi : H \to G$ be a morphism of linear k-algebraic groups. Let $P \to \mathrm{Spec}(k)$ be a torsor under the group G.

A geometrically integral k-variety X will be called a *lifting variety* (for the pair (φ, P)) if it fits into a lifting triangle $\mathcal{T}$:

$$\begin{tikzcd} \mathcal{Q} \arrow[r, "F"] \arrow[dr, "H_X"'] & P \times_k X \arrow[d, "G_X"] \\ & X\,, \end{tikzcd}$$

such that the following holds:

For every field extension l/k, with l infinite, and for every lifting triangle t:

$$\begin{tikzcd} Q \arrow[r, "f"] \arrow[dr, "H_l"'] & P \times_k l \arrow[d, "G_l"] \\ & \mathrm{Spec}(l)\,, \end{tikzcd}$$

the set of l-rational points $x : \mathrm{Spec}(l) \longrightarrow X$ such that the pullback $\mathcal{T}_x := x^*(\mathcal{T})$ is isomorphic to t (as a lifting triangle over $\mathrm{Spec}(l)$) is Zariski-dense in X, hence non-empty.

In particular, the variety X has an l-point if and only if the class of the G-torsor P in $H^1(l, G)$ is in the image of the map $\varphi_{l,*} : H^1(l, H) \to H^1(l, G)$.

1.5. **Splitting families.** Let A, B be objects of $\mathcal{M}_{k,d}$. Pick a class $x \in \mathbf{YExt}^n_{k,d}(A, B)$.

A countable set $(X_i)_{i \in I}$ of (smooth, geometrically integral) k-varieties will be called a *splitting family* for x if the following holds:

For every field extension l/k, with l infinite, $\mathrm{Res}_{l/k}(x)$ vanishes in $\mathbf{YExt}^n_{l,d}(A,B)$ if and only if (at least) one of the l-varieties X_i possesses a l-point.

Whenever a splitting family exists, it is natural to ask whether it can be made into an ind-variety. By this, we mean here that $I=\mathbb{N}$ and that, for each $i \geq 0$, we are given a closed embedding of k-varieties $X_i \longrightarrow X_{i+1}$.

2. Existence of lifting varieties.

This section contains the non formal ingredient of this paper, which may have an interest on his own.

Let $\varphi : H \to G$ be a morphism of linear k-algebraic groups; that is, of affine k-group schemes of finite type.
Let $P \to \mathrm{Spec}(k)$ be a torsor under the group G.

The aim of this section is to construct a lifting variety for (φ, P). Equivalently, we will build a "nice" k-variety X that is a versal object for H-torsors that lift the G-torsor P, in the sense explained in the previous paragraph.
In particular, recall that $X(l) \neq \emptyset$ if and only if $[P_l]$ lifts to $H^1(l,H)$, for every field extension l/k, with l infinite.
To construct such an X, we mimick the usual construction of versal torsors (see for instance [7], section I.5). We just have to push it slightly further.

There exists a finite dimensional k-vector space V endowed with a generically free linear action of H. There exist a dense open subset $V_0 \subset \mathbf{A}(V)$, stable under the action of H, and such that the geometric quotient

$$V_0 \longrightarrow V_0/H$$

exists, and is an H-torsor, which we denote by $\mathcal{Q}$.

Form the quotient

$$X_{\varphi,P} := (P \times_k V_0)/H,$$

where H acts on P via φ, and on V_0 in the natural way. Projecting onto V_0 induces a morphism

$$\pi : X_{\varphi,P} \longrightarrow V_0/H,$$

which can also be described as the twist of P by the H-torsor $\mathcal{Q}$, over the base V_0/H.

Note that $X_{\varphi,P}$ depends on the choice of V.

If we denote by $\mathcal{Q}'$ the pullback via π of the H-torsor $\mathcal{Q}$, there is a natural lifting triangle $\mathcal{T}_{\varphi,P}$:

$$\begin{tikzcd} \mathcal{Q}' \arrow[r] \arrow[dr, "H"'] & X_{\varphi,P} \times_k P \arrow[d, "G"] \\ & X_{\varphi,P} \end{tikzcd}$$

Its existence is explained by the following key fact. If $Y := V_0/H$, then for any Y-scheme S, a point

$$s \in X_{\varphi,P}(S) = \mathrm{Hom}_{Y-\mathrm{sch}}(S, X_{\varphi,P})$$

is exactly the same as an H-equivariant morphism between $\mathcal{Q} \times_Y S$ and $X_{\varphi,P} \times_k S$, over the base S (see for instance [2], théorème III.1.6.(ii)), i.e. it is the same as a lifting triangle relative to φ over the base S, i.e. an isomorphism of G-torsors between $\varphi_* \mathcal{Q} \times_Y S$ and $X_{\varphi,P} \times_k S$. We shall refer to this property as the universal property of $X_{\varphi,P}$.

Proposition 2.1. *The k-variety $X_{\varphi,P}$ is a lifting variety for the pair (φ, P).*
In particular, $X_{\varphi,P}(l) \neq \emptyset$ if and only if $[P_l]$ lifts to $H^1(l, H)$.

Proof. Let l/k be a field extension with l infinite. Let

$$\begin{tikzcd} t : Q \arrow[r, "f"] \arrow[dr, "H_l"'] & P \times_k l \arrow[d, "G_l"] \\ & \mathrm{Spec}(l) \end{tikzcd}$$

be a lifting triangle, over l. By Hilbert's Theorem 90 (for $\mathbf{GL}_k(V)$), the set of l-rational points

$$x \in (V_0/H)(l) = \mathrm{Hom}_{k-\mathrm{sch}}(\mathrm{Spec}(l), V_0/H)$$

such that $x^*(\mathcal{Q})$ is isomorphic to Q (as G-torsors over l) is Zariski-dense. Let x be such a point. Then the lifting triangle t corresponds to an isomorphism of G-torsors between $\varphi_*(Q)$ and P, over the base $\mathrm{Spec}(l)$. Since Q is isomorphic to $x^*(\mathcal{Q})$, the universal property of $X_{\varphi,P}$ implies that the lifting triangle t is isomorphic to the fiber of $\mathcal{T}_{\varphi,P}$ at an l-rational point of $X_{\varphi,P}$. This finishes the proof. □

Lemma 2.2. *The k-variety $X_{\varphi,P}$ is smooth and geometrically unirational if $\varphi : H \to G$ is surjective, or if G is smooth and connected.*

Proof. To prove this, we can assume that $k = \bar{k}$, in which case the torsor P is trivial. Then $X_{\varphi,P} = (G \times V_0)/H$. If G is smooth and connected, then it is k-rational. Hence $G \times V_0$ is smooth, connected and k-rational as well. The quotient morphism

$$G \times V_0 \longrightarrow X_{\varphi,P}$$

is an H-torsor, and smoothness and geometrical unirationality of its total space implies that of its base.
Now, assume that φ is surjective. Denoting by K its kernel, we see that $X_{\varphi,P} = V_0/K$, which implies the result. □

3. Triviality of Yoneda extensions in Abelian categories.

Let $\mathcal{A}$ be an Abelian category.
The following lemma is well-known.

Lemma 3.1. *Let $\mathcal{E} = (0 \to B \xrightarrow{f_0} E_1 \xrightarrow{f_1} \cdots \to E_{n-1} \xrightarrow{f_{n-1}} E_n \xrightarrow{f_n} A \to 0)$ be an object in $\mathbf{YExt}^n(A, B)$, and let E denotes its class in $\mathrm{YExt}^n(A, B)$.*

Then $E = 0$ in $\mathrm{YExt}^n(A, B)$ if and only if there exists $\mathcal{F}$ in $\mathbf{YExt}^{n-1}(E_n, B)$ and a morphism of complexes $\phi : \mathcal{E} \to \mathcal{F}$ inducing the identity on B and E_n, i.e. a commutative diagram (with exact rows)

$$
\begin{tikzcd}
0 \arrow[r] & B \arrow[r, "f_0"] \arrow[d, "\mathrm{id}"] & E_1 \arrow[r, "f_1"] \arrow[d, "\phi_1"] & \dots \arrow[r] & E_{n-1} \arrow[r, "f_{n-1}"] \arrow[d, "\phi_{n-1}"] & E_n \arrow[r, "f_n"] \arrow[d, "\mathrm{id}"] & A \arrow[r] & 0 \\
0 \arrow[r] & B \arrow[r] & F_1 \arrow[r, "g_1"] & \dots \arrow[r] & F_{n-1} \arrow[r, "g_{n-1}"] & E_n \arrow[r] & 0 & .
\end{tikzcd}
\tag{3.1}
$$

Proof. By [5], section 2 (see also [1], section 7.5, theorem 1, in the case of categories of modules), $E = 0$ is and only if there exists a commutative diagram

$$
\begin{tikzcd}
0 \arrow[r] & B \arrow[r] \arrow[d] & E_1 \arrow[r] \arrow[d] & \dots \arrow[r] & E_{n-1} \arrow[r] \arrow[d] & E_n \arrow[r] \arrow[d] & A \arrow[r] \arrow[d, "="] & 0 \\
0 \arrow[r] & B \arrow[r] & G_1 \arrow[r] & \dots \arrow[r] & G_{n-1} \arrow[r] & G_n \arrow[r] & A \arrow[r] & 0 \\
0 \arrow[r] & B \arrow[r, "\mathrm{id}"] \arrow[u] & B \arrow[r] \arrow[u] & 0 \dots 0 \arrow[r] & 0 \arrow[r] \arrow[u] & A \arrow[r, "\mathrm{id}"] \arrow[u] & A \arrow[r] \arrow[u, "="'] & 0 .
\end{tikzcd}
\tag{3.2}
$$

Assume $E = 0$. In the previous diagram, let $K' := \mathrm{Ker}(G_n \to A)$. Since we are given a splitting s of $G_n \to A$, there is a natural map $E_n \to K'$ defined via the retraction of $K' \to G_n$ associated to s. Define $\mathcal{F}$ to be the pull-back of the exact sequence

$$0 \to B \to G_1 \to \cdots \to G_{n-1} \to K' \to 0$$

by the aforementionned morphism $E_n \to K'$. It is now clear that $\mathcal{F}$ satisfies the statement of the Lemma.

To prove the converse, assume the existence of $\mathcal{F}$ and ϕ as in the Lemma. Define $F_i := G_i$ for all $i \leq n-1$, and $G_n := E_n \oplus A$. Consider the maps $h_i := g_i$ for $i \leq n-2$, and let $h_{n-1} := g_{n-1} \oplus 0 : G_{n-1} \to G_n = E_n \oplus A$ and $h_n : G_n = E_n \oplus A \to A$ be the natural projection. Then the morphism ϕ together with the map $\mathrm{id} \oplus f_n : E_n \to G_n = E_n \oplus A$ defines a commutative diagram of the shape (3.2), hence $E = 0$. □

Definition 3.2. Given $\mathcal{E} \in \mathbf{YExt}^n(A, B)$ as in Lemma 3.1, a $\mathcal{E}$-diagram is a pair $(\mathcal{F}, \phi)$, where $\mathcal{F} \in \mathbf{YExt}^{n-1}(E_n, B)$ and $\phi : \mathcal{E}_{n-1} \to \mathcal{F}$ is a morphism of complexes inducing the identity on B and E_n (see diagram (3.1)).

We denote by $\mathbf{Diag}(\mathcal{E})$ (or $\mathbf{Diag}_{\mathcal{A}}(\mathcal{E})$) the category of $\mathcal{E}$-diagrams, where a morphism between $(\mathcal{F}, \phi)$ and $(\mathcal{F}', \phi')$ is a morphism between the commutative diagrams associated (as in Lemma 3.1) to both $\mathcal{E}$-diagrams, and by $\mathrm{Diag}(\mathcal{E})$ the set of isomorphism classes in $\mathbf{Diag}(\mathcal{E})$.

Note that, given $\mathcal{D} = (\mathcal{F}, \phi) \in \mathbf{Diag}(\mathcal{E})$, there is a natural group homomorphism $\mathrm{Aut}(\mathcal{D}) \to \mathrm{Aut}(\mathcal{E})$.

Example 3.3. Consider the particular case when $\mathcal{A}$ is the category $\mathcal{M}_{k,d}$. Recall the obvious functor $\mathcal{M}_{k,d} \to \mathcal{M}_d$.

Then an object $\mathcal{E}$ of the category $\mathbf{YExt}^n_{k,d}(A, B)$ is exactly the same as an object $\mathcal{E}'$ in $\mathbf{YExt}^n_d(A, B)$ together with a group homomorphism $p : \Gamma \to \mathrm{Aut}(\mathcal{E}')$.

Moreover, a $\mathcal{E}$-diagram $\mathcal{D}$ in the category $\mathcal{M}_{k,d}$ is the same as a $\mathcal{E}'$-diagram $\mathcal{D}'$ in the category $\mathcal{M}_d$ together with a homomorphism $q : \Gamma \to \mathrm{Aut}(\mathcal{D}')$ lifting p.

Note that in this context, the groups $\mathrm{Aut}(\mathcal{D}')$ and $\mathrm{Aut}(\mathcal{E}')$ are finite.

4. Splitting families

The following statement is the main result of the paper:

Theorem 4.1. *Let A, B be objects of $\mathcal{M}_{k,d}$. Pick a class $e \in \mathrm{YExt}^n_{k,d}(A, B)$.*

Then, there exists a countable family $(X_i)_{i\in I}$ of smooth geometrically integral k-varieties, which is a splitting family for e.

Proof. Let $\mathcal{E} \in \mathbf{YExt}^n_{k,d}(A, B)$ be an element representing e. The n-extension $\mathcal{E}$ defines a group homomorphism $p : \Gamma \to \mathrm{Aut}(\mathcal{E}) := \mathrm{Aut}_{\mathcal{M}_d}(\mathcal{E})$ (see example 3.3). Consider the finite group $G := \mathrm{Im}(p)$: then p corresponds to a $\mathrm{Spec}(k)$-torsor $P_{\mathcal{E}}$ under G.

Then Example 3.3 relates the triviality of the class e to the existence of a $\mathcal{E}$-diagram $\mathcal{D}$ in the category $\mathcal{M}_d$ together with a lifting of the torsor $P_{\mathcal{E}}$ to a subgroup H of $\mathrm{Aut}_{\mathcal{M}_d}(\mathcal{D})$. Since we are interested in splitting families satisfying nice geometric properties, we have to make sure that the corresponding morphism $H \to G$ is surjective (see lemma 2.2). To this end, we have to consider subgroups H of $\mathrm{Aut}_{\mathcal{M}_d}(\mathcal{D})$ surjecting to G.

Consider the category I of pairs $(\mathcal{D}, H)$ where $\mathcal{D} \in \mathrm{Diag}_{\mathcal{M}_d}(\mathcal{E})$ is a diagram (involving only finite Abelian groups of d-torsion), and H is a (finite) subgroup of $\mathrm{Aut}_{\mathcal{M}_d}(\mathcal{D})$ surjecting to G. For any $i = (\mathcal{D}, H) \in I$, we define X_i to be the k-variety $X_{H\to G,P_q}$ defined in Proposition 2.1, where H and G are considered as finite constant algebraic groups over k.

Then the result is a consequence of Proposition 2.1 and Lemma 3.1. □

Corollary 4.2. *Let A be a finite Γ-module and let $\alpha \in H^n(k, A)$.*

Then there exists a countable family $(X_i)_{i\in I}$ of smooth geometrically integral k-varieties, which is a splitting family for α.

Proof. Combine the previous theorem and remark 1.2. □

In general, the countable family $(X_i)_{i\in I}$ is in fact a functor from the category I of pairs $(\mathcal{D}, H)$ introduced in the proof of Proposition 4.1 to the category of k-varieties.

As we will see below, at least in the case where A is p-torsion (for a prime number p), one can assume that the varieties X_i form an ind-variety.

5. Examples

5.1. **p-torsion coefficients.** Let us now focus on the special case where $d = p$ is prime. In this context, we have a more precise statement:

Theorem 5.1. *Let A, B be p-torsion Γ-modules and $E \in \mathrm{YExt}^n_{k,p}(A, B)$ (resp. $\alpha \in H^n(k, A)$).*

Then there exists a smooth geometrically integral ind-variety $(X_i)_{i\in\mathbf{N}}$, which is a splitting family for E (resp. α).

Proof. Let $\mathcal{E}(a, b, m)$ denote the following n-extension of $\mathbf{F}_p$-vector spaces:

$$\mathcal{E}(a, b, m) := (0 \to F_0 \xrightarrow{g_0} F_1 \xrightarrow{g_1} \cdots \to F_{n-1} \xrightarrow{g_{n-1}} F_n \xrightarrow{g_n} F_{n+1} \to 0)\,,$$

where $F_0 := \mathbf{F}_p^b$, $F_1 := \mathbf{F}_p^b \oplus \mathbf{F}_p^m$, $F_2 = \cdots = F_{n-1} = \mathbf{F}_p^m \oplus \mathbf{F}_p^m$, $F_n = \mathbf{F}_p^m \oplus \mathbf{F}_p^a$, $F_{n+1} = \mathbf{F}_p^a$, and $g_0(x) := (x, 0)$, $g_i(x, y) = (y, 0)$ for $1 \le i \le n-1$ and $g_n(x, y) := y$.

Lemma 5.2. *Let $\mathcal{E} = (0 \to B \xrightarrow{f_0} E_1 \xrightarrow{f_1} \dots \to E_{n-1} \xrightarrow{f_{n-1}} E_n \xrightarrow{f_n} A \to 0)$ be an object in $\mathbf{YExt}^n_{k,p}(A,B)$. Let $a := \dim(A)$ and $b := \dim(B)$. Then there exist an integer m, a Galois action on $\mathcal{E}(a,b,m)$ and a morphism $\phi : \mathcal{E} \to \mathcal{E}(a,b,m)$ in $\mathbf{YExt}^n_{k,p}(A,B)$, i.e. a commutative diagram of n-extensions of $\mathbf{F}_p$-vector spaces with actions of Γ:*

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r, "f_0"] \arrow[d, "\phi_0", "\sim"'] & E_1 \arrow[r, "f_1"] \arrow[d, "\phi_1"] & \dots \arrow[r] & E_{n-1} \arrow[r, "f_{n-1}"] \arrow[d, "\phi_{n-1}"] & E_n \arrow[r, "f_n"] \arrow[d, "\phi_n"] & A \arrow[r] \arrow[d, "\phi_{n+1}", "\sim"'] & 0 \\
0 \arrow[r] & F_0 \arrow[r, "g_0"] & F_1 \arrow[r, "g_1"] & \dots \arrow[r] & F_{n-1} \arrow[r, "g_{n-1}"] & F_n \arrow[r, "g_n"] & F_{n+1} \arrow[r] & 0\,,
\end{tikzcd}$$

such that for all i, ϕ_i is injective.

Moreover, given another morphism $\psi : \mathcal{E} \to \mathcal{E}(a,b,m)$ with the same properties, there exists an automorphism $\epsilon : \mathcal{E}(a,b,m) \to \mathcal{E}(a,b,m)$ in $\mathbf{YExt}^n_p(A,B)$ such that $\psi = \epsilon \circ \phi$.

Proof. Choose m large enough such that $m \geq \dim(E_i)$ for all i. Then construct ϕ_i inductively by choosing suitable basis of the vector spaces E_i.

The second part of the statement is basic linear algebra. □

We now need a second Lemma. Fix once and for all a n-extension $\mathcal{E} = (0 \to B \xrightarrow{f_0} E_1 \xrightarrow{f_1} \dots \to E_{n-1} \xrightarrow{f_{n-1}} E_n \xrightarrow{f_n} A \to 0)$ in $\mathbf{YExt}^n_{k,p}(A,B)$ representing E such that:

- $\dim E_{n-1}$ is minimal.
- $\dim E_{n-2}$ is minimal among n-extensions representing E with minimal $\dim E_{n-1}$.
- $\dim E_{n-3}$ is minimal among n-extensions representing E with minimal $\dim E_{n-1}$ and minimal $\dim E_{n-2}$.
- ...
- $\dim E_1$ minimal among n-extensions representing E with minimal $\dim E_{n-1}$, ..., minimal $\dim E_2$.

Let $e := \dim E_n$ and $b := \dim(B)$.

We now claim the following Lemma:

Lemma 5.3. *The class E is trivial if and only if there exists an integer m and a $\mathcal{E}$-diagram $\phi : \mathcal{E} \to \mathcal{E}(e,b,m)$ in $\mathbf{YExt}^n_{k,p}(A,B)$ as follows:*

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r, "f_0"] \arrow[d, "\phi_0", "\sim"'] & E_1 \arrow[r, "f_1"] \arrow[d, "\phi_1"] & \dots \arrow[r] & E_{n-1} \arrow[r, "f_{n-1}"] \arrow[d, "\phi_{n-1}"] & E_n \arrow[r, "f_n"] \arrow[d, "\phi_n", "\sim"'] & A \arrow[r] & 0 \\
0 \arrow[r] & F_0 \arrow[r, "g_0"] & F_1 \arrow[r, "g_1"] & \dots \arrow[r] & F_{n-1} \arrow[r, "g_{n-1}"] & F_n \arrow[r] & 0 & ,
\end{tikzcd}$$

where all ϕ_i are injective.

Proof. The existence of such a diagram implies the triviality of E, by Lemma 3.1.

Let us now prove the converse. Assume $E = 0$. Then by Lemma 3.1, there exists a $\mathcal{E}$-diagram $\varphi : \mathcal{E} \to \mathcal{G}$ of the following shape:

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r, "f_0"] \arrow[d, "\varphi_0", "\sim"'] & E_1 \arrow[r, "f_1"] \arrow[d, "\varphi_1"] & \dots \arrow[r] & E_{n-1} \arrow[r, "f_{n-1}"] \arrow[d, "\varphi_{n-1}"] & E_n \arrow[r, "f_n"] \arrow[d, "\varphi_n", "\sim"'] & A \arrow[r] & 0 \\
0 \arrow[r] & G_0 \arrow[r, "h_0"] & G_1 \arrow[r, "h_1"] & \dots \arrow[r] & G_{n-1} \arrow[r, "h_{n-1}"] & G_n \arrow[r] & 0
\end{tikzcd} , \tag{5.1}$$

We now prove by induction that all φ_i are injective. By construction, φ_n is injective.

Assume that φ_i are injective for all $k < i \leq n$. Let us prove that φ_k is also injective. Consider the quotient $\overline{E_k} := E_k/\mathrm{Ker}(\varphi_k)$ and define $\widetilde{E}_{k-2}$ to be the inverse image $h_{k-2}^{-1}(E_{k-1}) \subset G_{k-2}$. Then we have a natural commutative diagram with exact lines:

$$\begin{tikzcd}
\dots \arrow[r] & E_{k-3} \arrow[r] \arrow[d, "\mathrm{id}"] & E_{k-2} \arrow[r] \arrow[d] & E_{k-1} \arrow[r] \arrow[d, "\mathrm{id}"] & E_k \arrow[r] \arrow[d] & E_{k+1} \arrow[r] \arrow[d, "\mathrm{id}"] & \dots \\
\dots \arrow[r] & E_{k-3} \arrow[r] \arrow[d] & \widetilde{E}_{k-2} \arrow[r] \arrow[d] & E_{k-1} \arrow[r] \arrow[d] & \overline{E}_k \arrow[r] \arrow[d] & E_{k+1} \arrow[r] \arrow[d] & \dots \\
\dots \arrow[r] & G_{k-3} \arrow[r] & G_{k-2} \arrow[r] & G_{k-1} \arrow[r] & G_k \arrow[r] & G_{k+1} \arrow[r] & \dots .
\end{tikzcd}$$

In particular, the n-extension

$$0 \to B \xrightarrow{f_0} E_1 \xrightarrow{f_1} \dots \to E_{k-3} \to \widetilde{E}_{k-2} \to E_{k-1} \to \overline{E}_k \to E_{k+1} \to \dots \to E_n \xrightarrow{f_n} A \to 0$$

represents the class E, with $\dim \overline{E}_k \leq \dim E_k$. By minimality of the extension $\mathcal{E}$, we have $\dim \overline{E}_k = \dim E_k$, hence φ_k is injective.

Hence we proved the existence of a diagram (5.1) with injective vertical maps φ_i.

Apply now Lemma 5.2 to the $(n-1)$-extension $\mathcal{G}$, in order to get a commutative diagram of exact sequences of $\mathbf{F}_p$-vector spaces with Γ-action:

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r, "f_0"] \arrow[d, "\varphi_0", "\sim"'] & E_1 \arrow[r, "f_1"] \arrow[d, "\varphi_1"] & \dots \arrow[r] & E_{n-1} \arrow[r, "f_{n-1}"] \arrow[d, "\varphi_{n-1}"] & E_n \arrow[r, "f_n"] \arrow[d, "\varphi_n", "\sim"'] & A \arrow[r] & 0 \\
0 \arrow[r] & G_0 \arrow[r, "h_0"] \arrow[d, "\phi'_0", "\sim"'] & G_1 \arrow[r, "h_1"] \arrow[d, "\phi'_1"] & \dots \arrow[r] & G_{n-1} \arrow[r, "h_{n-1}"] \arrow[d, "\phi'_{n-1}"] & G_n \arrow[r] \arrow[d, "\phi'_n", "\sim"'] & 0 \\
0 \arrow[r] & F_0 \arrow[r, "g_0"] & F_1 \arrow[r, "g_1"] & \dots \arrow[r] & F_{n-1} \arrow[r, "g_{n-1}"] & F_n \arrow[r] & 0
\end{tikzcd} ,$$

where the maps ϕ'_i are injective. To conclude the proof of Lemma 5.3, consider the composed map $\phi := \phi' \circ \varphi : \mathcal{E} \to \mathcal{E}(e, b, m)$. $\square$

Let us now prove Theorem 5.1.

Lemma 5.3 ensures that in order to construct the splitting varieties, it is sufficient to consider only diagrams (of $\mathbf{F}_p$-vector spaces) $\phi : \mathcal{E} \to \mathcal{E}(e, b, m)$, for some $m \in \mathbf{N}$, i.e. diagrams of the following shape (Lemma 5.3 essentially says that such diagrams are cofinal in the category of diagrams):

$$
\begin{tikzcd}
0 \arrow[r] & B \arrow[r, "f_0"] \arrow[d, "\phi_0", "\sim"'] & E_1 \arrow[r, "f_1"] \arrow[d, "\phi_1"] & \dots \arrow[r] & E_{n-1} \arrow[r, "f_{n-1}"] \arrow[d, "\phi_{n-1}"] & E_n \arrow[r, "f_n"] \arrow[d, "\phi_n", "\sim"'] & A \arrow[r] & 0 \\
0 \arrow[r] & F_0 \arrow[r, "g_0"] & F_1 \arrow[r, "g_1"] & \dots \arrow[r] & F_{n-1} \arrow[r, "g_{n-1}"] & F_n \arrow[r] & 0
\end{tikzcd}
\tag{5.2}
$$

,

where all ϕ_i are injective.

In addition, the second part of Lemma 5.2 implies that one only needs to consider one such diagram for each m (since such diagrams with the same m are equivalent up to an automorphism of $\mathcal{E}(e, b, m)$).

Therefore, let us fix, for all $m \in \mathbf{N}$ (sufficiently large), one diagram $\mathcal{D}_m$ of the shape (5.2) in the category of $\mathbf{F}_p$-vector spaces, in a compatible way: the diagram $\mathcal{D}_{m+1}$ for the integer $m+1$ is obtained from the diagram $\mathcal{D}_m$ associated to m by composing the morphism $\phi_m : \mathcal{E} \to \mathcal{E}(e, b, m)$ with the natural (injective) morphism $\mathcal{E}(e, b, m) \to \mathcal{E}(e, b, m+1)$.

We have defined a direct system of diagrams $\mathcal{D}_m$. The n-extension $\mathcal{E}$ defines a homomorphism $q : \Gamma \to \mathrm{Aut}(\mathcal{E})$, hence a $\mathrm{Spec}(k)$-torsor P_q. For all m, let X_m denotes the k-variety $X_{\mathrm{Aut}(\mathcal{D}_m) \to \mathrm{Aut}(\mathcal{E}), P_q}$ defined in Proposition 4.1. By functoriality of the construction of these varieties and by the natural (injective) group homomorphisms $\mathrm{Aut}(\mathcal{D}_m) \to \mathrm{Aut}(\mathcal{D}_{m+1})$, we get a direct system of k-varieties X_m.

In addition, the second part of Lemma 5.2 implies that the morphisms $\mathrm{Aut}(\mathcal{D}_m) \to \mathrm{Aut}(\mathcal{E})$ are surjective, hence the varieties X_m are smooth and geometrically unirational.

To conclude the proof, recall that those varieties X_m are cofinal among the varieties $(X_i)_{i \in I}$ that appear in Proposition 4.1. □

5.2. **2-extensions.** In this section, let d be arbitrary. We restrict to the special case of $\mathrm{YExt}^2_k(A, B)$ and $H^2(k, A)$, where the splitting family is smaller.

Corollary 5.4. *Let A, B be finite d-torsion Γ-modules and $E \in \mathrm{YExt}^2_{k,d}(A, B)$ (resp. $\alpha \in H^2(k, A)$).*

Then, there exists a finite family $X_1, \dots, X_n$ of smooth geometrically integral k-varieties (resp. one smooth geometrically integral k-variety X), which is a splitting family for E (resp. α).

Proof. Let $\mathcal{E} = (0 \to B \to E_1 \to E_2 \to A \to 0)$ be a 2-extension of d-torsion Γ-modules representing E. A $\mathcal{E}$-diagram is a commutative diagram with exact lines in the category of finite d-torsion abelian groups:

$$
\begin{tikzcd}
0 \arrow[r] & B \arrow[r] \arrow[d, "\mathrm{id}", "\sim"'] & E_1 \arrow[r] \arrow[d, "\phi_1"] & E_2 \arrow[r] \arrow[d, "\mathrm{id}", "\sim"'] & A \arrow[r] & 0 \\
0 \arrow[r] & B \arrow[r] & F_1 \arrow[r] & E_2 \arrow[r] & 0
\end{tikzcd}
\tag{5.3}
$$

.

In particular, there are only finitely many such $\mathcal{E}$-diagrams. Therefore Proposition 4.1 gives the required result in the case of Yoneda extensions.

In the Galois cohomology case, one has to consider diagrams (5.3) with $A = \mathbf{Z}/d\mathbf{Z}$. Using Pontryagin duality $\mathrm{Hom}(\cdot, \mathbf{Z}/d\mathbf{Z})$, it is equivalent to consider diagrams (5.3) with $B = \mathbf{Z}/d\mathbf{Z}$. In this case, the last row of the diagram splits, hence such a diagram is unique up to isomorphism (in the category $\mathcal{M}_d$). Which proves that one splitting variety is enough. □

Remark 5.5. In the Galois cohomology case, Corollary 5.4 recovers a result of Krashen (see [4]).

References

1. Bourbaki, Nicolas, *Éléments de mathématique. Algèbre. Chapitre 10. Algèbre homologique.* Masson, Paris, 1980. vii+216 pp.
2. Giraud, Jean, *Cohomologie non abélienne*, Die Grundlehren der mathematischen Wissenschaften, Band 179, Springer-Verlag, Berlin, 1971, ix+467 pp.
3. Suslin, Andrei and Joukhovitski, Seva, *Norm varieties*, J. of Pure and Applied Algebra **206**, 245–276 (2006).
4. Krashen, Daniel, *Period and index, symbol lengths, and generic splittings in Galois cohomology*, to appear in the Bulletin of the London Mathematical Society.
5. Oort, Frans, *Yoneda extensions in abelian categories*, Math. Ann. **153**, 227-235 (1964).
6. Rost, Markus, *Norm Varieties and Algebraic Cobordism*, Available on the author's webpage.
7. Serre, Jean-Pierre, *Cohomological invariants, Witt invariants, and trace forms* Notes by Skip Garibaldi. Univ. Lecture Ser., **28**, *Cohomological invariants in Galois cohomology*, 1–100, Amer. Math. Soc., Providence, RI, 2003.

Sorbonne Universités, UPMC Univ Paris 06 Institut de Mathématiques de Jussieu-Paris Rive Gauche UMR 7586, CNRS, Univ Paris Diderot, Sorbonne Paris Cité, F-75005, Paris, France

Current address: Département de mathématiques et applications, École Normale Supérieure, 45 rue d'Ulm, 75230 Paris Cedex 05, France

E-mail address: `cyril.demarche@imj-prg.fr`

Sorbonne Universités, UPMC Univ Paris 06 Institut de Mathématiques de Jussieu-Paris Rive Gauche UMR 7586, CNRS, Univ Paris Diderot, Sorbonne Paris Cité, F-75005, Paris, France

E-mail address: `mathieu.florence@imj-prg.fr`