Smooth profinite groups, III: the Smoothness Theorem.

Charles De Clercq, Mathieu Florence

Abstract. Let p be a prime. The goal of this article is to prove the Smoothness Theorem 5.1, which notably asserts that a $(1, \infty)$-cyclotomic pair is $(n, 1)$-cyclotomic, for all $n \geq 1$. In the particular case of Galois cohomology, the Smoothness Theorem provides a new proof of the Norm Residue Isomorphism Theorem. Using the formalism of smooth profinite groups, this proof presents it as a consequence of Kummer theory for fields.

Contents

1. Introduction.

Let G be a profinite group and p be a prime. Five years ago, we began working on a mathematical project rooted in the following belief.

(B): The (surjectivity part of the) Norm Residue Isomorphism Theorem is a consequence of Kummer theory for fields.

Recall that the Norm Residue Isomorphism Theorem, also known as the Bloch-Kato Conjecture, was proved by Rost, Suslin, Voevodsky and Weibel, by applying motivic cohomology to norm varieties [18].

With the two previous articles of this series in hand, we can now show that belief (B) is correct, even beyond Galois cohomology: it is accurate in the broader context of $(1, \infty)$-cyclotomic pairs.

We build on these ealier works to achieve its proof: applying the Uplifting Theorem [12, Theorem 14.1], we provide lifting statements for mod p cohomology of a smooth profinite group. Notably, we show with the *Filtered Lifting Theorem*

(Theorem 4.5) that, given a $(1,1)$-smooth profinite group G and a perfect $(\mathbb{F}_p, G)$-algebra A, filtered exact sequences of G-bundles over A lift to their analogues over $\mathbf{W}_2(A)$. A key ingredient here is a process developed in [9], to parametrize higher cohomology groups $H^n(G, .)$ with abelian coefficients, by cohomology sets $H^1(G, .)$ with non-abelian coefficients.

We can then derive from the *Filtered Lifting Theorem* our *Smoothness Theorem* (Theorem 5.1). It states that $(1,1)$-smooth profinite groups are $(n,1)$-smooth and that if $(G, \mathbb{Z}_p(1))$ is a $(1, \infty)$-cyclotomic pair, it is $(n,1)$-cyclotomic, for any $n \geq 1$.

Denote by $G = \mathrm{Gal}(F_s/F)$ "the" absolute Galois group of a field F of characteristic not p. Let $\mathbb{Z}_p(1)$ stand for its Tate module of p-primary roots of unity. Recall that the pair $(G, \mathbb{Z}_p(1))$ is $(1, \infty)$-cyclotomic, so that G is $(1, \infty)$-smooth (see [5]). The Smoothness Theorem then implies the sought-for proof of the Norm Residue Isomorphism Theorem, using the equivalent formulation of the Bloch-Kato conjecture given by Merkurjev for $p = 2$ [22] and for arbitrary p by Gille [15].

Note that we provide in [5, §3] wide classes of smooth profinite groups, arising from geometry. For instance, étale fundamental groups of semilocal $\mathbb{Z}[\frac{1}{p}]$-schemes, of affine $\mathbb{F}_p$-schemes and of smooth curves over algebraically closed fields fit into $(1, \infty)$-cyclotomic pairs. The Smoothness Theorem therefore broadens the cohomological content of the Norm Residue Isomorphism Theorem to these groups.

2. Notation and conventions.

In this text, we assume familiarity with the following notions, developed in the first two articles of this series: $(1, e)$-cyclotomic pairs, $(1, e)$-smooth profinite groups, $(G, \mathbf{W}_r)$-bundles and their complete flags, over an $(G, \mathbb{F}_p)$-scheme S. Here, $\mathbf{W}_r$ stands for p-typical truncated Witt vectors of length r. We focus on the case $r = 2$, with a high degree of generality. We keep notation and conventions of [6] and [12]. In particular, actions of profinite groups on algebro-geometric structures where $p^2 = 0$ are naive, i.e. factor through open normal subgroups. Note also that, in the present text, all schemes are affine.

Let $\mathbf{B}_n \subset \mathbf{GL}_n$ be the Borel subgroup of upper triangular matrices, and let $\mathbf{U}_n$ be its unipotent radical. These are linear algebraic groups, defined over $\mathbb{Z}$. Throughout, the letter G denotes a profinite group, which will often be assumed to be, at least, $(1,1)$-smooth (relatively to p). By definition, this means that for every perfect $(\mathbb{F}_p, G)$-algebra A, the natural arrow

$$H^1(G, \mathbf{B}_2(\mathbf{W}_2(A))) \longrightarrow H^1(G, \mathbf{B}_2(A))$$

is surjective (see [6, Definition 11.9]). Our starting point is the Uplifting Theorem [12, Theorem 14.1].

2.1. Greenberg transfer of linear algebraic groups.

Let A be a commutative $\mathbb{F}_p$-algebra and $\mathbf{G}$ be a smooth affine group scheme over $\mathbf{W}_2(A)$. We denote by $\overline{\mathbf{G}}/A$ its reduction, to a smooth group scheme over A. There is an exact sequence of A-group schemes

$$\mathcal{E}(\mathbf{G}) : 1 \longrightarrow \mathbf{Lie}(\overline{\mathbf{G}})^{(1)} \longrightarrow R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{G}) \xrightarrow{\rho_{\mathbf{G}}} \overline{\mathbf{G}} \longrightarrow 1,$$

where $R_{\mathbf{W}_2/\mathbf{W}_1}$ stands for the Greenberg transfer, from (affine) $\mathbf{W}_2(A)$-schemes to A-schemes (see [1]). Keeping in mind the functorial bijection, between functors of points,

$$R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{G})(R) \xrightarrow{\sim} \mathbf{G}(\mathbf{W}_2(R)),$$

valid for every (commutative) A-algebra R, the arrow $\rho_{\mathbf{G}}$ is given by the reduction

$$\mathbf{G}(\mathbf{W}_2(R)) \longrightarrow \mathbf{G}(R) = \overline{\mathbf{G}}(R).$$

3. Extensions of Kummer type.

DEFINITION 3.1. *(Split unipotent group scheme)*
Let S be a scheme and U/S be a smooth group scheme of dimension m.
Proceeding by induction on m, we say that U/S is split unipotent, if either $U = 1$, or $m \geq 1$, and there exists a central extension (of smooth group schemes over S)

$$1 \longrightarrow U_1 \simeq \mathbb{G}_a \longrightarrow U \longrightarrow U^1 \longrightarrow 1,$$

such that U^1 is split unipotent.

Remark 3.2. If $S = \mathrm{Spec}(k)$, with k a field, then a smooth connected linear k-group U is split unipotent if, and only if, U can be embedded (over k) in $\mathbf{U}_n$, for some $n \geq 1$.

DEFINITION 3.3. *(Exact sequences of Kummer type)*
Let

$$\mathcal{E} : 1 \longrightarrow U \longrightarrow L_2 \xrightarrow{\pi} L_1 \longrightarrow 1$$

be an extension of linear algebraic groups over $\mathbb{F}_p$, whose kernel U is split unipotent. We say that $\mathcal{E}$ is of Kummer type, or simply that π is of Kummer type, if the following lifting property holds.
For every $(1,1)$-smooth profinite group G and for every perfect $(\mathbb{F}_p, G)$-algebra A, the natural map

$$h^1(\pi) : H^1(G, L_2(A)) \longrightarrow H^1(G, L_1(A)),$$

induced by π, is surjective.

Example 3.4. The fundamental example of an extension of Kummer type is given as follows. Consider the Borel subgroup $\mathbf{B}_2 \subset \mathbf{GL}_2$, over $\mathbb{Z}/p^2$. Form the associated extension, of linear algebraic groups over $\mathbb{F}_p$,

$$\mathcal{E}(\mathbf{B}_2) : 1 \longrightarrow \mathbf{Lie}(\overline{\mathbf{B}_2})^{(1)} \longrightarrow R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{B}_2) \xrightarrow{\pi} \overline{\mathbf{B}_2} \longrightarrow 1.$$

Then, $h^1(\pi)$ reads as

$$H^1(G, \mathbf{B}_2(\mathbf{W}_2(A))) \longrightarrow H^1(G, \mathbf{B}_2(A)),$$

which is surjective, for any $(1,1)$-smooth profinite group G and any perfect $(\mathbb{F}_p, G)$-algebra A, by the very definition of $(1,1)$-smoothness (see [6, §11]).
Equivalently, instead of $\mathbf{B}_2$, one can use $\mathbb{G}_a \rtimes \mathbb{G}_m$, the automorphism group scheme of the one-dimensional affine space $\mathbb{A}^1$.

Of course, we could allow arbitrary extensions of linear algebraic groups over $\mathbb{F}_p$ in the preceding definition, but we stick to those with split unipotent kernel to ensure the pleasant properties of Lemma 3.7. In practice, the extensions of Kummer type considered in this paper often have a commutative kernel $U \simeq \mathbb{G}_a^n$.

The following definition is now natural.

DEFINITION 3.5. *(Group scheme of Kummer type)*
Let $\mathbf{G}$ *be a smooth affine group scheme over* $\mathbb{Z}/p^2$. *We say that* $\mathbf{G}$ *is of Kummer type, or simply Kummer, if the extension of linear algebraic groups over* $\mathbb{F}_p$,

$$1 \longrightarrow \mathbf{Lie}(\overline{\mathbf{G}})^{(1)} \longrightarrow R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{G}) \longrightarrow \overline{\mathbf{G}} \longrightarrow 1$$

is of Kummer type.

Exercise 3.6. Assume that $p = 2$ and denote by $\mathbf{B}$ a Borel subgroup of $\mathbf{SL}_2$. Show that $\mathbf{B}$ is not Kummer.

The following elementary useful Lemma states that being an exact sequence of Kummer type is preserved under pullbacks and pushforwards of extensions. Note that pushforwards of extensions of (non-commutative) algebraic groups do not exist in general; their formation requires a few assumptions, which we recall below. For details on the yoga of extensions of algebraic groups, see [11].

LEMMA 3.7. *Let*

$$\mathcal{E} : 1 \longrightarrow U \longrightarrow L_2 \longrightarrow L_1 \longrightarrow 1$$

be an extension of linear algebraic groups over $\mathbb{F}_p$, *with split unipotent kernel. Let* $\pi : L_1' \longrightarrow L_1$ *be a homomorphism of linear algebraic groups over* $\mathbb{F}_p$. *One can form the pullback extension*

$$\pi^*(\mathcal{E}) : 1 \longrightarrow U \longrightarrow L_2 \times_{L_1} L_1' \longrightarrow L_1' \longrightarrow 1.$$

Then, if $\mathcal{E}$ *is of Kummer type,* $\pi^*(\mathcal{E})$ *is of Kummer type, as well.*

Assume that π *is a surjection with split unipotent kernel, which is of Kummer type. Then, if* $\pi^*(\mathcal{E})$ *is of Kummer type,* $\mathcal{E}$ *is of Kummer type as well.*

Assume now that U *is commutative. It is then naturally endowed with an algebraic action of* L_1, *by group automorphisms.*

Let V *be another commutative split unipotent linear algebraic group over* $\mathbb{F}_p$, *endowed with an algebraic action of* L_1, *by group automorphisms. Let* $\iota : U \longrightarrow V$ *be an* L_1-*equivariant homomorphism of linear algebraic groups over* $\mathbb{F}_p$. *One can form the pushforward extension*

$$\iota_*(\mathcal{E}) : 1 \longrightarrow V \longrightarrow \iota_*(L_2) \xrightarrow{\pi} L_1 \longrightarrow 1.$$

Here

$$\iota_*(L_2) := (V \rtimes L_2)/U,$$

where the semi-direct product is taken w.r.t. the natural action of L_2 *on* V, *via* $L_2 \longrightarrow L_1$, *and where* U *is diagonally embedded in* $V \rtimes L_2$, *as a normal subgroup. Then, if* $\mathcal{E}$ *is of Kummer type,* $\iota_*(\mathcal{E})$ *is of Kummer type as well.*

Proof. This is an elementary diagram chase, left to the reader. $\square$

3.1. AN EQUIVALENT FORMULATION OF THE UPLIFTING THEOREM.
The Uplifting Theorem ([12], 14.1 and 14.2) clearly implies that the algebraic group $\mathbf{B}_n$ is Kummer, for all $n \geq 2$. We are going to be more precise, and translate its step-by-step formulation in terms of extensions of Kummer type.

Let

$$\nabla_n^0 : V_0 \subset V_1 \subset \ldots \subset V_n$$

be a complete flag of free $\mathbb{Z}/p^2$-modules, whose graded pieces are denoted by $L_i = V_i/V_{i-1}$. These are free $\mathbb{Z}/p^2$-modules of rank one.

Denote by
$$\nabla^0_{n-1} := \tau_{n-1}(\nabla^0_n) : V_0 \subset V_1 \subset \ldots \subset V_{n-1}$$
the truncation.

Denote by $\mathrm{Aut}(\nabla^0_n)$ the group scheme (over $\mathbb{Z}/p^2$) of linear automorphisms of V_n, respecting the flag ∇^0_n. It is isomorphic to $\mathbf{B}_n$ and we have a natural exact sequence of group schemes over $\mathbb{Z}/p^2$ (actually defined over $\mathbb{Z}$)
$$1 \longrightarrow \mathbf{K}_n \longrightarrow \mathrm{Aut}(\nabla^0_n) \overset{\pi}{\longrightarrow} \mathrm{Aut}(\nabla^0_{n-1}) \longrightarrow 1,$$
where $\mathbf{K}_n$ is defined as the kernel of π. It is is a disguise of the sequence
$$1 \longrightarrow \mathbb{G}_a^{n-1} \rtimes \mathbb{G}_m \longrightarrow \mathbf{B}_n \overset{\pi}{\longrightarrow} \mathbf{B}_{n-1} \longrightarrow 1,$$
where $\mathbb{G}_a^{n-1} \rtimes \mathbb{G}_m$ stands for the normal subgroup
$$\begin{pmatrix} 1 & 0 & \cdots & 0 & * \\ 0 & 1 & \ddots & \vdots & * \\ \vdots & \ddots & \ddots & 0 & * \\ 0 & \cdots & 0 & 1 & * \\ 0 & \cdots & \cdots & 0 & ** \end{pmatrix} \subset \mathbf{B}_n,$$
where the $*$'s belong to $\mathbb{G}_a$, and where $**$ lies in $\mathbb{G}_m$.

Applying the Greenberg transfer, we may consider this exact sequence as an exact sequence of linear algebraic groups over $\mathbb{F}_p$, reading as
$$1 \longrightarrow R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{K}_n) \longrightarrow R_{\mathbf{W}_2/\mathbf{W}_1}(\mathrm{Aut}(\nabla^0_n)) \longrightarrow R_{\mathbf{W}_2/\mathbf{W}_1}(\mathrm{Aut}(\nabla^0_{n-1})) \longrightarrow 1.$$

Form the exact sequence
$$1 \longrightarrow \mathbf{Lie}(\overline{\mathbf{K}_n})^{(1)} \longrightarrow R_{\mathbf{W}_2/\mathbf{W}_1}(\mathrm{Aut}(\nabla^0_n)) \longrightarrow \mathrm{Aut}_{*,n}(\Delta^0_n) \longrightarrow 1,$$
fitting into a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbf{Lie}(\overline{\mathbf{K}_n})^{(1)} & \longrightarrow & R_{\mathbf{W}_2/\mathbf{W}_1}(\mathrm{Aut}(\nabla^0_n)) & \overset{\rho}{\longrightarrow} & \mathrm{Aut}_{*,n}(\Delta^0_n) & \longrightarrow & 1 \\ & & \downarrow & & \| & & \downarrow & & \\ 1 & \longrightarrow & R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{K}_n) & \longrightarrow & R_{\mathbf{W}_2/\mathbf{W}_1}(\mathrm{Aut}(\nabla^0_n)) & \longrightarrow & R_{\mathbf{W}_2/\mathbf{W}_1}(\mathrm{Aut}(\nabla^0_{n-1})) & \longrightarrow & 1. \end{array}$$

Note that this diagram serves as the definition of $\mathrm{Aut}_{*,n}(\Delta^0_n)$.

Given a $(1,1)$-smooth profinite group G and a perfect $(\mathbb{F}_p, G)$-algebra A, the map
$$H^1(G, R_{\mathbf{W}_2/\mathbf{W}_1}(\mathrm{Aut}(\nabla^0_n))(A)) = H^1(G, \mathrm{Aut}(\nabla^0_n)(\mathbf{W}_2(A))) \overset{h^1(\rho)}{\longrightarrow} H^1(G, \mathrm{Aut}_{*,n}(\Delta^0_n)(A))$$
induced by ρ is surjective. Indeed, an element $c \in H^1(G, \mathrm{Aut}_{*,n}(\Delta^0_n)(A))$ is the (isomorphism class of) a complete flag of $(G, \mathbf{W}_1)$-bundles over A,
$$\nabla_{n,1} : 0 = W_{0,1} \subset W_{1,1} \subset \ldots \subset W_{n,1},$$
together with a lift of the truncation $\nabla_{n-1,1} := \tau_{n-1}(\nabla_{n,1})$, to a complete flag of $(G, \mathbf{W}_2)$-bundles over A,
$$\nabla_{n-1,2} : 0 = W_{0,2} \subset W_{1,2} \subset \ldots \subset W_{n-1,2}.$$

The Uplifting Theorem ensures that such a lift can be extended to a complete lift

$$\nabla_{n,2} : 0 = W_{0,2} \subset W_{1,2} \subset \ldots \subset W_{n-1,2} \subset W_{n,2}$$

of $\nabla_{n,1}$.

As a consequence, the class c lifts, via $h^1(\rho)$, to the set

$$H^1(G, \mathrm{Aut}(\nabla_n^0)(\mathbf{W}_2(A)))$$

of isomorphism classes of n-dimensional complete flags of $(G, \mathbf{W}_2)$-bundles over A– whose graded pieces, regarded (without the action of G) as invertible $\mathbf{W}_2(A)$-modules , are trivial.
We have proved the following.

THEOREM 3.8. *(Uplifting Theorem, equivalent reformulation)*
The extension of linear algebraic groups over $\mathbb{F}_p$,

$$\mathcal{K}_n : 1 \longrightarrow \mathbf{Lie}(\overline{\mathbf{K}_n})^{(1)} \longrightarrow R_{\mathbf{W}_2/\mathbf{W}_1}(\mathrm{Aut}(\nabla_n^0)) \longrightarrow \mathrm{Aut}_{*,n}(\Delta_n^0) \longrightarrow 1,$$

also known as

$$1 \longrightarrow \mathbb{G}_a^n \longrightarrow R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{B}_n) \xrightarrow{\pi} \mathbf{B}_{*,n} \longrightarrow 1,$$

is of Kummer type.

Remark 3.9. The normal subgroup $\mathbb{G}_a^n \subset R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{B}_n)$ that appears in the previous statement, is

$$\mathbf{Lie}(\mathbb{G}_a^{n-1} \rtimes \mathbb{G}_m)^{(1)} \subset R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbb{G}_a^{n-1} \rtimes \mathbb{G}_m) \subset R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{B}_n);$$

see the discussion above.

As a direct consequence of Theorem 3.8 and Lemma 3.7, we can construct a wide class of extensions of Kummer type, as follows.

LEMMA 3.10. *Let $\mathcal{K}$ be the smallest class of extensions of linear algebraic groups over $\mathbb{F}_p$*

$$\mathcal{E} : 1 \longrightarrow U \longrightarrow L_2 \xrightarrow{\pi} L_1 \longrightarrow 1,$$

or equivalently of surjections $\pi : L_2 \longrightarrow L_1$, with split unipotent kernel, such that:

(1) *The class $\mathcal{K}$ contains the extensions*

$$1 \longrightarrow \mathbb{G}_a^n \longrightarrow R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{B}_n) \xrightarrow{\pi} \mathbf{B}_{*,n} \longrightarrow 1$$

   of Theorem 3.8, for all $n \geq 2$.

(2) *The class $\mathcal{K}$ is closed under arbitrary pullbacks, by homomorphisms $L_1' \longrightarrow L_1$;*

(3) *If $\pi_1 : L_2 \longrightarrow L_1$ and $\pi_2 : L_3 \longrightarrow L_2$ belong to $\mathcal{K}$, so does $\pi_1 \circ \pi_2$.*

(4) *If $\pi_1 : L_2 \longrightarrow L_1$ and $\pi_2 : L_3 \longrightarrow L_2$ are such that $\pi_1 \circ \pi_2$ belongs to $\mathcal{K}$, so does π_1.*

Then, $\mathcal{K}$ consists of extensions of Kummer type.

4. LIFTING FILTERED EXTENSIONS.

Our objective in this section, is the Filtered Lifting Theorem (Theorem 4.5). Its proof uses the point of view and some techniques of [9]- refined with the extra data of complete filtrations.

4.1. FILTERED EXTENSIONS.

DEFINITION 4.1. *(Filtered exact sequences, a.k.a. filtered n-extensions)*
Let R be a commutative ring. A (completely) filtered extension of R-modules is an extension of locally free R-modules of finite rank

$$0 \longrightarrow A \longrightarrow E \longrightarrow B \longrightarrow 0,$$

together with a complete filtration

$$0 = E_0 \subset E_1 \subset \ldots \subset E_{\mathrm{rk}(E)} = E,$$

whose graded pieces E_i/E_{i-1} are invertible R-modules, and such that $A = E_i$ for some $0 \leq i \leq rk(E)$.

Two filtered extension of R-modules

$$0 \longrightarrow A \longrightarrow E \longrightarrow B \longrightarrow 0$$

and

$$0 \longrightarrow B \longrightarrow F \longrightarrow C \longrightarrow 0$$

are said to be compatible, if the filtration of B, induced by the given filtration on E, equals that induced by the given filtration on F.

A filtered exact sequence of R-modules is an exact sequence, of locally free R-modules of finite rank

$$\mathcal{E} : 0 \longrightarrow E_0 \longrightarrow \ldots \longrightarrow E_{n+1} \longrightarrow 0,$$

together with a system of two-by-two compatible filtrations $(E_{j,i})$, on the induced short exact sequences

$$0 \longrightarrow A_j \longrightarrow E_j \longrightarrow A_{j+1} \longrightarrow 0,$$

$j = 1, \ldots, n$.

Assume that R is equipped with an action of the profinite group G. Then, a filtered exact sequence of (R,G)-modules is a filtered exact sequence of R-modules

$$\mathcal{E} : 0 \longrightarrow E_0 \longrightarrow \ldots \longrightarrow E_{n+1} \longrightarrow 0,$$

equipped with a semi-linear action of G (see [6]). In other words, each E_i is endowed with a semi-linear action of G, compatible with the arrows in $\mathcal{E}$, and respecting the given filtrations $(E_{j,i})$.

A filtered exact sequence $\mathcal{E}$ as above will also be called a filtered n-extension.

4.2. THE AUTOMORPHISM GROUP SCHEME OF A FILTERED EXACT SEQUENCE.

DEFINITION 4.2. *(Automorphism group schemes of filtered n-extensions)*
For $n \geq 1$, consider a filtered n-extension of $\mathbb{Z}$-modules

$$\mathcal{E} : 0 \longrightarrow E_0 \longrightarrow E_1 \longrightarrow \ldots \longrightarrow E_{n+1} \longrightarrow 0,$$

with given filtration $(E_{j,i})$ on E_j. We denote by

$$\mathcal{E}_i : 0 \longrightarrow A_i \longrightarrow E_i \longrightarrow A_{i+1} \longrightarrow 0,$$

$i = 1, \ldots, n$ the associated (filtered) short exact sequences and set

$$e_i = \dim_{\mathbb{Z}} E_i$$

and

$$a_i = \dim_{\mathbb{Z}} A_i.$$

Denote by $\Phi(e_0, \ldots, e_{n+1})$ the group of automorphisms of the extension $\mathcal{E}$, respecting the given filtrations. It naturally bears the structure of a solvable group scheme, over $\mathbb{Z}$. Up to isomorphism, it only depends on $e_0, \ldots, e_{n+1}$. On the level of the functor of points, an element of $\Phi(e_0, \ldots, e_{n+1})$ is the data of automorphisms $\phi_0, \ldots, \phi_{n+1}$, respecting the filtrations, and fitting into a commutative diagram

$$
\begin{array}{ccccccccccc}
0 & \longrightarrow & E_0 & \longrightarrow & E_1 & \longrightarrow & \ldots & \longrightarrow & E_n & \longrightarrow & E_{n+1} & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle \phi_0} & & \downarrow{\scriptstyle \phi_1} & & & & \downarrow{\scriptstyle \phi_n} & & \downarrow{\scriptstyle \phi_{n+1}} & & \\
0 & \longrightarrow & E_0 & \longrightarrow & E_1 & \longrightarrow & \ldots & \longrightarrow & E_n & \longrightarrow & E_{n+1} & \longrightarrow & 0.
\end{array}
$$

We have a natural exact sequence of smooth solvable $\mathbb{Z}$-group schemes

$$1 \longrightarrow \Psi(e_0, \ldots, e_{n+1}) \longrightarrow \mathbf{B}_N \longrightarrow \Phi(e_0, \ldots, e_{n+1}) \longrightarrow 1.$$

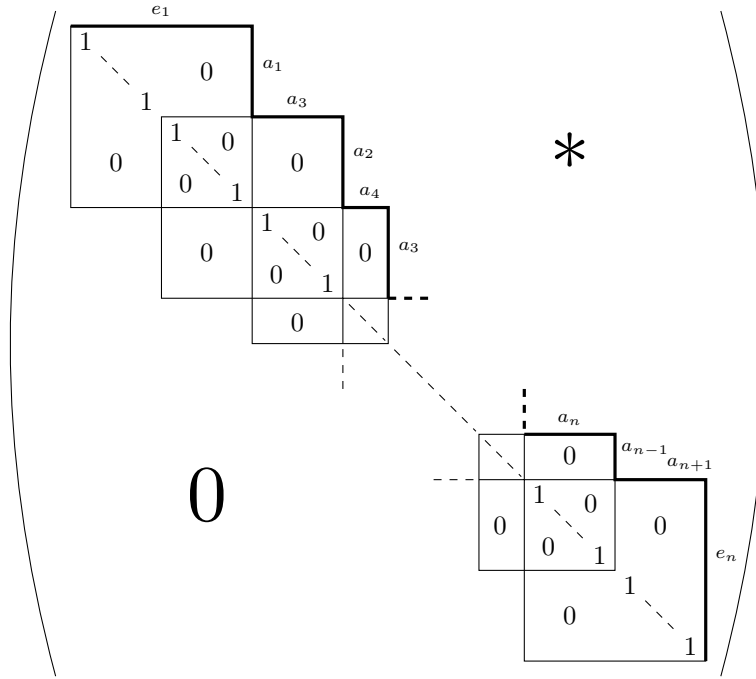*Here*

$$N = e_1 + e_3 + \ldots + e_{n-1} + e_{n+1}$$

if n is even, or

$$N = e_1 + e_3 + \ldots + e_{n-2} + e_n$$

if n is odd. The normal subgroup $\Psi(e_0, \ldots, e_{n+1})$ consists of invertible matrices of the shape
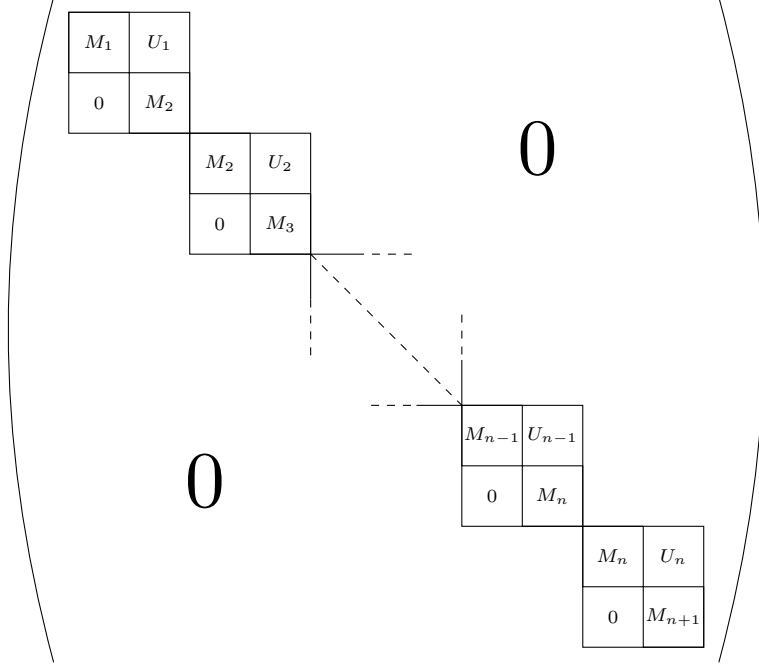
$$
\left(
\begin{array}{c}
\begin{smallmatrix}
1 & & 0 & & a_1 \\
 & 1 & & & a_3 \\
0 & & 1 & 0 & a_2 \\
 & & 0 & 1 & a_4 \\
 & & & 1 & 0 & a_3 \\
 & & & 0 & 1 \\
\end{smallmatrix} \qquad *
\\[2em]
\mathbf{0} \qquad
\begin{smallmatrix}
a_n \\
0 \\
1 & 0 & a_{n-1}\ a_{n+1} \\
0 & 1 & 0 \\
1 \\
0 & & 1
\end{smallmatrix}
\end{array}
\right)
$$

Denoting by

$$0 = F_0 \subset F_1 \subset \ldots \subset F_N = \mathbb{Z}^N$$

a complete flag on the $\mathbb{Z}$-module $\mathbb{Z}^N$, these matrices are the filtered automorphisms, that act trivially on the subquotients

$$F_{a_1+a_2+\ldots+a_{i+1}}/F_{a_1+a_2+\ldots+a_{i-1}},$$

for $i = 1,\ldots,n$. Note that $\Phi(e_0,\ldots,e_{n+1})$ also occurs as the subgroup of $\mathbf{B}_{e_1+e_2+\ldots+e_n}$, consisting of block matrices of the shape

$$\left(\begin{array}{c}\begin{array}{|c|c|}\hline M_1 & U_1 \\\hline 0 & M_2 \\\hline\end{array} & & & \mathbf{0} \\ & \begin{array}{|c|c|}\hline M_2 & U_2 \\\hline 0 & M_3 \\\hline\end{array} & & \\ & & \ddots & \\ & & \begin{array}{|c|c|}\hline M_{n-1} & U_{n-1} \\\hline 0 & M_n \\\hline\end{array} & \\ \mathbf{0} & & & \begin{array}{|c|c|}\hline M_n & U_n \\\hline 0 & M_{n+1} \\\hline\end{array}\end{array}\right)$$

where $M_i \in \mathbf{B}_{a_i}$ corresponds to $A_i \subset E_i$, and $U_i = \mathbb{G}_a^{a_i a_{i+1}}$.

PROPOSITION 4.3. *We keep the notation of the preceding Definition. Then, the mod p^2 reduction of $\Phi(e_0, \ldots, e_{n+1})$ is a Kummer group scheme, over $\mathbb{Z}/p^2$.*

Proof. Put $s := e_1 + e_2 + \ldots + e_n$ and $t = s + (s-1) + (s-2) + \ldots + (s - e_{n+1} + 1)$. Set

$$\mathbf{B}_{s,e_{n+1}} := \mathrm{Ker}(\mathbf{B}_s \longrightarrow \mathbf{B}_{s-e_{n+1}});$$

it consists of matrices of the shape

$$\left(\begin{array}{ccccc|ccc} 1 & 0 & \cdots & 0 & * & \cdots & * \\ 0 & 1 & \ddots & \vdots & * & \cdots & * \\ \vdots & \ddots & \ddots & 0 & * & \cdots & * \\ \vdots & \cdots & \ddots & 1 & * & \cdots & * \\ 0 & \cdots & \cdots & 0 & ** & \ddots & * \\ \vdots & \cdots & \cdots & \vdots & 0 & \ddots & * \\ 0 & \cdots & \cdots & 0 & 0 & \cdots & ** \end{array}\right) \subset \mathbf{B}_s.$$

Notation is $* \in \mathbb{G}_a$, $** \in \mathbb{G}_m$, and there are $e_{n+1} = a_{n+1}$ columns containing $*$'s. Using the embedding $\Phi(e_0, \ldots, e_{n+1}) \longrightarrow \mathbf{B}_s$ given in Definition 4.2, we get a commutative diagram of extensions of linear algebraic groups over $\mathbb{F}_p$,

$$
\begin{array}{ccccccccc}
\mathcal{E} : 0 & \longrightarrow & \mathrm{Lie}(U_n \rtimes M_{n+1})^{(1)} & \longrightarrow & R_{\mathbf{W}_2/\mathbf{W}_1}(\Phi(e_0, \ldots, e_{n+1})) & \overset{\phi}{\longrightarrow} & \Phi'(e_0, \ldots, e_{n+1}) & \longrightarrow & 0 \\
& & \downarrow{\iota} & & \downarrow & & \downarrow & & \\
\mathcal{F} : 0 & \longrightarrow & \mathrm{Lie}(\overline{\mathbf{B}}_{s,e_{n+1}})^{(1)} & \longrightarrow & R_{\mathbf{W}_2/\mathbf{W}_1}(\mathbf{B}_s) & \overset{\psi}{\longrightarrow} & \mathbf{B}'_{s,e_{n+1}} & \longrightarrow & 0,
\end{array}
$$

which serves as the definition of $\Phi'(e_0, \ldots, e_{n+1})$ and of $\mathbf{B}'_{s,e_{n+1}}$.

Here $\Phi(e_0, \ldots, e_{n+1})$, $\mathbf{B}_s$ and $\mathbf{B}_{s,e_{n+1}}$ are considered over $\mathbb{Z}/p^2$. We have

$$\mathbb{G}_a^{t-e_{n+1}(s-e_n)} \simeq \mathrm{Lie}(U_n \rtimes M_{n+1})^{(1)} \subset R_{\mathbf{W}_2/\mathbf{W}_1}(U_n \rtimes M_{n+1}),$$

and

$$\mathbb{G}_a^t \simeq \mathrm{Lie}(\overline{\mathbf{B}_{s,e_{n+1}}})^{(1)} \subset R_{\mathbf{W}_2/\mathbf{W}_1}(\overline{\mathbf{B}_{s,e_{n+1}}}).$$

By induction using Theorem 3.8, we know that ψ, or equivalently the extension $\mathcal{F}$, is of Kummer type. Hence, the extension $\iota_*(\mathcal{E})$ is of Kummer type as well by Lemma 3.10. Now, as a morphism of $\mathbb{F}_p$-representations of $\Phi'(e_0, \ldots, e_{n+1})$, the injection ι has a natural retraction ρ. Indeed, the source of ι has a complement in $\mathrm{Lie}(\overline{\mathbf{B}_{s,e_{n+1}}})^{(1)}$, given by block matrices of the shape

$$\left(\begin{array}{c|c} 0 & * \\ \hline 0 & 0 \end{array} \right) \subset \mathbf{B}_s,$$

where $*$ is a matrix with $(s - e_n)$ rows and e_{n+1} columns. Thus, $\mathcal{E} = \rho_*(\iota_*(\mathcal{E}))$ is of Kummer type as well. Equivalently, ϕ is of Kummer type. We conclude that $\Phi(e_0, \ldots, e_{n+1})$ is Kummer, by induction on n.

$$\square$$

Remembering the definition of a surjection of Kummer type, Proposition 4.3 translates as follows, in the langage of G-linearized extensions.

PROPOSITION 4.4. *(Proposition 4.3, equivalent formulation).*
Let G be a $(1,1)$-smooth profinite group. Let A be a perfect $(\mathbb{F}_p, G)$-algebra. Let

$$\mathcal{E} : 0 \longrightarrow E_0 \longrightarrow E_1 \longrightarrow \ldots \longrightarrow E_n \longrightarrow E_{n+1} \longrightarrow 0$$

be a filtered n-extension of $(G, \mathbf{W}_1)$-bundles over A. Assume that all graded pieces, of the given filtration on each E_i, are trivial (i.e. isomorphic to A), as invertible A-modules.
Then, $\mathcal{E}$ lifts to a filtered n-extension of $(G, \mathbf{W}_2)$-bundles over A

$$\mathcal{E}_2 : 0 \longrightarrow E_{0,2} \longrightarrow E_{1,2} \longrightarrow \ldots \longrightarrow E_{n,2} \longrightarrow E_{n+1,2} \longrightarrow 0,$$

such that all graded pieces, of the given filtration on each $E_{i,2}$, are trivial (i.e. isomorphic to $\mathbf{W}_2(A)$), as invertible $\mathbf{W}_2(A)$-modules.

From the proof of Proposition 4.3, we even get the stronger result, that the lifting of the n-extension $\mathcal{E}$ can be obtained *step-by-step*, lifting its arrows one after another (starting from $E_0 \longrightarrow E_1$).

Our goal in the next Section, is to remove the assumption that all graded pieces are trivial, as invertible A-modules.

4.3. THE FILTERED LIFTING THEOREM.
We can now state one of our main theorems.

THEOREM 4.5. *(Filtered Lifting Theorem)*
Let G be a $(1,1)$-smooth profinite group. Let A be a perfect $(\mathbb{F}_p, G)$-algebra. Let $n \geq 1$ be an integer, and let

$$\mathcal{E} : 0 \longrightarrow E_0 \longrightarrow E_1 \longrightarrow \ldots \longrightarrow E_n \longrightarrow E_{n+1} \longrightarrow 0$$

be a filtered exact sequence of $(G, \mathbf{W}_1)$-bundles over A.
Then, $\mathcal{E}$ admits a lift, to a filtered exact sequence of $(G, \mathbf{W}_2)$-bundles over A.

Proof. Denote by $L_{j,i} := E_{j,i}/E_{j,i-1}$ the graded pieces of the filtrations on $\mathcal{E}$; these are invertible A-modules. As a filtered exact sequence of A-modules, $\mathcal{E}$ is isomorphic to the (split) exact sequence

$$\mathcal{F} : 0 \longrightarrow F_0 \longrightarrow F_1 \longrightarrow \ldots \longrightarrow F_n \longrightarrow F_{n+1} \longrightarrow 0,$$

where

$$F_j := \bigoplus_i L_{j,i}.$$

Here the arrow $F_j \longrightarrow F_{j+1}$ is given by projecting on the (direct sum of) the graded pieces which are common to F_j and F_{j+1}. With the notation of Definition 4.1, these are the graded pieces of A_{j+1}. Clearly, $\mathcal{F}$ naturally lifts to a (split) filtered exact sequence of $\mathbf{W}_2(A)$-modules

$$\mathcal{F}' : 0 \longrightarrow F_0' \longrightarrow F_1' \longrightarrow \ldots \longrightarrow F_n' \longrightarrow F_{n+1}' \longrightarrow 0,$$

where

$$F_j' := \bigoplus_i \mathbf{W}_2(L_{j,i}).$$

Denote by $\mathbf{B}$ the automorphism $\mathbf{W}_2(A)$-group scheme of $\mathcal{F}'$. It is defined as in 4.2, except that we work over $\mathbf{W}_2(A)$ instead of working over $\mathbb{Z}$.

Now, the G-structure on $\mathcal{E}$ is given by a continuous 1-cocycle

$$\rho_1 : G \longrightarrow \mathbf{B}(A).$$

Lifting $\mathcal{E}$ as desired is equivalent to lifting ρ_1 to a continuous 1-cocycle

$$\rho_2 : G \longrightarrow \mathbf{B}(\mathbf{W}_2(A)),$$

which is also equivalent to the vanishing of a class

$$Obs_2 \in H^2(G, \mathrm{Lie}(\overline{\mathbf{B}})^{(1)}),$$

where $\overline{\mathbf{B}}$ is the reduction of $\mathbf{B}$, to an A-group scheme.

We now show that for any i, j, we can assume that $L_{i,j} = A$. Setting

$$R_{j,i} = \bigoplus_{n \in \mathbb{Z}} L_{i,j}^{\otimes n} \text{ and } R := \bigotimes_{i,j} R_{i,j},$$

we see that as the natural arrow $A \longrightarrow R$ is a split monomorphism of (G, A)-modules, the class Obs_2 vanishes if and only if

$$Obs_2 \otimes_A R \in H^2(G, \mathrm{Lie}(\overline{\mathbf{B}})^{(1)} \otimes_A R)$$

vanishes.

Consequently, the existence of a lift of $\mathcal{E} \otimes_A R$ to a filtered exact sequence of $(\mathbf{W}_2(R), G)$-modules ensures that $\mathcal{E}$ lifts to a filtered exact sequence of $(\mathbf{W}_2(A), G)$-modules. We can thus base change from A to R. As the R-modules $L_{j,i} \otimes_A R$ are free of rank one, our reduction step is done.

Under the assumption that all $L_{i,j}$'s are free A-modules of rank one, $\mathcal{E}$ is isomorphic (as a filtered exact sequence of A-modules) to the base-change via $\mathbb{Z} \longrightarrow A$ of a split filtered exact sequence of $\mathbb{Z}$-modules, which we denote by $\mathcal{E}_{\mathbb{Z}}$.

Denote by $B_{\mathbb{Z}} = \Phi(e_0, \ldots, e_{n+1})$ the automorphism $\mathbb{Z}$-group scheme of $\mathcal{E}_{\mathbb{Z}}$- see Definition 4.2. Its mod p^2 reduction B is Kummer, by Proposition 4.3. Note that we have $\mathcal{F}' = \mathcal{E}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbf{W}_2(A)$ and $\mathbf{B} = B_{\mathbb{Z}} \times_{\mathbb{Z}} \mathbf{W}_2(A)$. We conclude that ρ_1 indeed lifts, to a continuous 1-cocycle

$$\rho_2 : G \longrightarrow B_{\mathbb{Z}}(\mathbf{W}_2(A)) = \mathbf{B}(\mathbf{W}_2(A)).$$

Twisting $\mathcal{E}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbf{W}_2(A)$ by ρ_2, we get the desired lift of $\mathcal{E}$. $\hfill\square$

5. The Smoothness Theorem.

In this section, we consider a classical problem: lifting the mod p cohomology of a profinite group. Solving by the affirmative part of the Smoothness Conjecture 14.25 of [4], in depth $e = 1$, we achieve it in the framework of $(1,1)$-smooth profinite groups, and give a consequence for cyclotomic pairs.

THEOREM 5.1. *(The Smoothness Theorem)*
Let $n \geq 1$ be an integer.
Let G be a $(1,1)$-smooth profinite group. Then, G is $(n,1)$-smooth.
Let $(G, \mathbb{Z}_p(1))$ be a $(1,\infty)$-cyclotomic pair. Then, it is $(n,1)$-cyclotomic.

Proof. By the standard restriction-corestriction argument, we first reduce to the case where G is a pro-p-group. We start off with the first assertion: let $c_1 \in H^n(G, L_1) = \mathrm{Ext}^n_{(A,G)}(A, L_1)$ be a cohomology class, where L_1 is a (G, A)-module, invertible as an A-module.

Let
$$\mathcal{E}(c_1) : 0 \longrightarrow L_1 \longrightarrow E_1 \longrightarrow \ldots \longrightarrow E_n \longrightarrow A \longrightarrow 0$$
be an exact sequence of $(G, \mathbf{W}_1)$-bundles over A, whose Yoneda cohomology class equals c_1. We now show that since G is a pro-p-group, we can assume that $\mathcal{E}(c_1)$ is filtered, in such a way that the graded pieces of all E_i's are free of rank one, as A-modules. Pick an open subgroup $G_1 \subset G$, such that $\mathrm{Res}(c_1) = 0 \in H^n(G_1, L_1)$ and consider the exact sequence
$$0 \longrightarrow L_1 \xrightarrow{i_1} L_1^{G/G_1} \longrightarrow Q_2 \longrightarrow 0.$$
Using Shapiro's lemma, we see that $(i_1)_*(c_1) = 0$. Hence, c_1 is the Bockstein of a class $c_{1,n-1} \in H^{n-1}(G, Q_2)$. Again, there exists an open subgroup $G_2 \subset G$, such that $(i_2)_*(c_{1,n-1}) = 0$, where
$$0 \longrightarrow Q_2 \xrightarrow{i_2} Q_2^{G/G_2} \longrightarrow Q_3 \longrightarrow 0.$$
Continuing this process, we build an extension of $(G, \mathbf{W}_1)$-bundles over A,
$$\mathcal{E}(c_1) : 0 \longrightarrow L_1 \longrightarrow E_1 := L_1^{G/G_1} \longrightarrow \ldots \longrightarrow E_{n-1} := Q_{n-1}^{G/G_{n-1}} \longrightarrow E_n \longrightarrow A \longrightarrow 0,$$
representing c_1. We claim that this $\mathcal{E}(c_1)$ can be completely filtered, as asserted. To see this, note first that by construction, $\mathcal{E}(c_1)$ is the pullback of the extension
$$\mathcal{E}(G_1, \ldots, G_n) : 0 \longrightarrow L_1 \longrightarrow L_1^{G/G_1} \longrightarrow \ldots \longrightarrow Q_{n-1}^{G/G_{n-1}} \longrightarrow Q_n^{G/G_n} \longrightarrow Q_{n+1} \longrightarrow 0,$$
by an element of $H^0(G, Q_{n+1}) = \mathrm{Hom}_{(A,G)}(A, Q_{n+1})$.

The extension $\mathcal{E}(G_1, \ldots, G_n)$ only depends on the data of L_1 and on the subgroups $G_1, \ldots, G_n$. It does not depend on c_1. Actually, it is canonically isomorphic to
$$\mathcal{E}_0(G_1, \ldots, G_n) \otimes_{\mathbb{F}_p} L_1,$$
where
$$\mathcal{E}_0(G_1, \ldots, G_n) : 0 \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{F}_p^{G/G_1} \longrightarrow \ldots \longrightarrow Q_{0,n}^{G/G_n} \longrightarrow Q_{0,n+1} \longrightarrow 0$$
is the corresponding extension of $(\mathbb{F}_p, G)$-modules, with respect to $G_1, \ldots, G_n$ (i.e. the particular case where $A = \mathbb{F}_p$ and $L_1 = \mathbb{F}_p$).

Since G is a pro-p-group, $\mathcal{E}_0(G_1,\ldots,G_n)$ can be completely filtered. The proof is by induction, using the standard fact that a non-zero $(\mathbb{F}_p, G)$-module has a non-zero G-invariant element. It follows that $\mathcal{E}(G_1,\ldots,G_n)$ supports a complete filtration as well, whose graded pieces are isomorphic to L_1- hence free of rank one as A-modules. Consequently, $\mathcal{E}(c_1)$ supports the same kind of filtration.

Casting Theorem 4.5, this filtered exact sequence then lifts to a filtered exact sequence of $(G, \mathbf{W}_2)$-bundles over A,

$$\mathcal{F} : 0 \longrightarrow F_0 \longrightarrow F_1 \longrightarrow \ldots \longrightarrow F_n \longrightarrow F_{n+1} \longrightarrow 0.$$

Replacing $\mathcal{F}$ by $\mathcal{F} \otimes F_{n+1}^{-1}$, we can assume that $F_{n+1} = \mathbf{W}_2(A)$, without loss of generality. Set $L_2(c_1) := F_0$, and take $c_2 \in H^n(G, L_2(c_1))$ to be the Yoneda class of the n-extension

$$\mathcal{F} : 0 \longrightarrow L_2(c_1) \longrightarrow F_1 \longrightarrow \ldots \longrightarrow F_n \longrightarrow \mathbf{W}_2(A) \longrightarrow 0.$$

Then, c_2 lifts c_1, and we are done: the profinite group G is $(n, 1)$-smooth.

We now move on to the second assertion. Let $(G, \mathbb{Z}_p(1))$ be a $(1, \infty)$-cyclotomic pair. Given a cohomology class $c_1 \in H^n(G, \mathbb{F}_p(n))$, we need to show that c_2 lifts to a class $c_2 \in H^n(G, \mathbb{Z}/p^2(n))$. Let

$$\Gamma := G((t_1))((t_2))\ldots((t_{n+1}))$$

be the $(n+1)$-th iterated Laurent extension of G (see [6, Definition 7.1]). The pair $(\Gamma, \mathbb{Z}_p(1))$ is $(1, \infty)$-cyclotomic, by [6, Proposition 7.2]. For $i = 1,\ldots, n+1$, set

$$x_i = (t_1) \cup (t_2) \cup \ldots \cup \widehat{(t_i)} \cup \ldots \cup (t_{n+1}) \in H^n(\Gamma, \mathbb{F}_p(n)),$$

where $\widehat{(t_i)}$ means that (t_i) is omitted.

As the pair $(\Gamma, \mathbb{Z}_p(1))$ are $(1, \infty)$-cyclotomic, the profinite group Γ is $(1, \infty)$-smooth, by [6, Theorem A]. The first statement of this theorem ensures then that Γ is $(n, 1)$-smooth.

Let $C := (c_1, x_1,\ldots,x_{n+1})$, where c_1 is viewed here as a class in $H^n(\Gamma, \mathbb{F}_p(n))$. The profinite group Γ is $(n, 1)$-cyclothymic ([6, Theorem 11.4]). By definition, this means there exists a lift of $\mathbb{F}_p(n)$ to $\mathbb{Z}/p^2[C]$, a free $\mathbb{Z}/p^2$-module with an action of Γ, such that the classes $c_1, x_1,\ldots,x_{n+1}$ all lift to $H^n(\Gamma, \mathbb{Z}/p^2[C])$. We are going to show that

$$\mathbb{Z}/p^2[C] \simeq \mathbb{Z}/p^2(n).$$

This will conclude the proof, for then c_1 lifts to $H^n(G, \mathbb{Z}/p^2(n))$, using the canonical section of the surjection $\Gamma \longrightarrow G$. Consider $\mathbb{Z}/p^2[C]$ and $\mathbb{Z}/p^2(n)$ as extensions

$$\mathcal{E}(C) : 0 \longrightarrow \mathbb{F}_p(n) \longrightarrow \mathbb{Z}/p^2[C] \longrightarrow \mathbb{F}_p(n) \longrightarrow 0$$

and

$$\mathcal{E}(n) : 0 \longrightarrow \mathbb{F}_p(n) \longrightarrow \mathbb{Z}/p^2(n) \longrightarrow \mathbb{F}_p(n) \longrightarrow 0.$$

Form their Baer difference

$$\Delta(n) := \mathcal{E}(C) - \mathcal{E}(n) : 0 \longrightarrow \mathbb{F}_p(n) \longrightarrow \delta(n) \longrightarrow \mathbb{F}_p(n) \longrightarrow 0;$$

it is an extension of $(\mathbb{F}_p, \Gamma)$-modules. Untwisting, it can also be viewed as an extension

$$\Delta : 0 \longrightarrow \mathbb{F}_p \longrightarrow \delta \longrightarrow \mathbb{F}_p \longrightarrow 0,$$

i.e. an element of $H^1(\Gamma, \mathbb{F}_p)$.

The Theorem boils down to showing that Δ splits. As all the t_i's lift to $H^1(\Gamma, \mathbb{Z}/p^2(1))$, the cohomology classes x_i's lift to $H^n(\Gamma, \mathbb{Z}/p^2(n))$. The x_i's lift to both $H^n(\Gamma, \mathbb{Z}/p^2(n))$ and $H^n(\Gamma, \mathbb{Z}/p^2[C])$, from which we infer that

$$\Delta \cup x_i = 0 \in H^{n+1}(\Gamma, \mathbb{F}_p(n)),$$

for all $i = 1, ..., n+1$.

Write $\Gamma_0 = G$ and

$$\Gamma_i = G((t_1)) \ldots ((t_i)),$$

so that $\Gamma = \Gamma_{n+1} = \Gamma_n((t_{n+1}))$. Recall that by [6, Proposition 7.4], we have for any $i \in \{1, ..., n+1\}$, for any $m \geq 1$ and any integer k, a short exact sequence

$$0 \longrightarrow H^m(\Gamma_{i-1}, \mathbb{F}_p(k)) \longrightarrow H^m(\Gamma_i, \mathbb{F}_p(k)) \xrightarrow{\text{Res}_i} H^{m-1}(\Gamma_{i-1}, \mathbb{F}_p(k-1)) \longrightarrow 0.$$

To lighten notation, we denote by Res_i the residue maps: the values of m and k will be clear in the context.

Taking residue with respect to t_{n+1}, we get

$$\text{Res}_{n+1}(\Delta \cup x_{n+1}) = \text{Res}_{n+1}(\Delta) \cup x_{n+1} = 0 \in H^n(\Gamma_n, \mathbb{F}_p(n-1)).$$

Here

$$\text{Res}_{n+1}(\Delta) \in H^0(G, \mathbb{F}_p(-1)),$$

and $x_{n+1} \in H^n(\Gamma_n, \mathbb{F}_p(n))$ is non-zero, therefore $\text{Res}_{n+1}(\Delta) = 0$. In other words, Δ is inflated via $\Gamma \longrightarrow \Gamma_n$: it comes from an extension of $(\mathbb{F}_p, \Gamma_n)$-modules

$$\Delta_n : 0 \longrightarrow \mathbb{F}_p \longrightarrow \delta_n \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

Applying

$$\text{Res}_n \circ \text{Res}_{n+1} : H^{n+1}(\Gamma, \mathbb{F}_p(n)) \longrightarrow H^{n-1}(\Gamma, \mathbb{F}_p(n-2))$$

to the equality $\Delta \cup x_n = 0$, we get

$$\text{Res}_n(\Delta_n) \cup (t_1) \cup \ldots (t_{n-1}) \in H^{n-1}(\Gamma, \mathbb{F}_p(n-2)),$$

whence $\text{Res}_n(\Delta_n) = 0 \in H^0(G, \mathbb{F}_p(-1))$. Consequently, Δ_n is inflated from an extension of $(\mathbb{F}_p, \Gamma_{n-1})$-modules

$$\Delta_{n-1} : 0 \longrightarrow \mathbb{F}_p \longrightarrow \delta_{n-1} \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

Continuing this process, we eventually see that Δ is "constant": it is inflated from an extension of $(\mathbb{F}_p, G)$-modules

$$\Delta_0 : 0 \longrightarrow \mathbb{F}_p \longrightarrow \delta_0 \longrightarrow \mathbb{F}_p \longrightarrow 0.$$

Now we see that

$$\Delta_0 = \text{Res}_1 \circ \ldots \circ \text{Res}_n(\Delta \cup x_{n+1}) = 0.$$

The class Δ is therefore trivial as well, which concludes the proof. $\qquad\square$

Exercise 5.2.

In the last part of the proof of Theorem 5.1, we actually show the following result.

(R): Let $(G, \mathbb{Z}/p^2(1))$ be a $(1, \infty)$-cyclotomic pair. Assume that G is $(n, 1)$-smooth. Then, $(G, \mathbb{Z}/p^2(1))$ is $(n, 1)$-cyclotomic.

We then use (R), to deduce the second assertion of the Theorem from the first.

Our objective is to provide another way to prove (R).

With minor changes, we keep notation introduced in the proof of Theorem 5.1. Let

$$c_1 \in H^n(G, \mathbb{F}_p(n))$$

be a cohomology class. We want to lift it to $H^n(G, \mathbb{Z}/p^2(n))$.

1) Denote by
$$\Gamma_n := G((t_1))((t_2)) \ldots ((t_n))$$
the n-th iterated Laurent extension of G. Set
$$x := (t_1) \cup \ldots \cup (t_n) \in H^n(\Gamma_n, \mathbb{F}_p(n)).$$
By assumption, there exists a lift of $\mathbb{F}_p(n)$ to a $(\mathbb{Z}/p^2, G)$-module $\mathbb{Z}/p^2[c_1, x]$, free of rank one as a $\mathbb{Z}/p^2$-module, such that both c_1 and x lift to $H^n(G, \mathbb{Z}/p^2[c_1, x])$. Consider the exact sequence
$$\mathcal{E}(c_1, x) : 0 \longrightarrow \mathbb{F}_p(n) \longrightarrow \mathbb{Z}/p^2[c_1, x] \longrightarrow \mathbb{F}_p(n) \longrightarrow 0.$$

Set
$$\Delta(n) := \mathcal{E}(c_1, x, n) - \mathcal{E}(n) : 0 \longrightarrow \mathbb{F}_p(n) \longrightarrow \delta(n) \longrightarrow \mathbb{F}_p(n) \longrightarrow 0.$$
We are going to show that $\Delta(n)$ splits, or equivalenty, that
$$\Delta := \Delta(n) \otimes_{\mathbb{F}_p} \mathbb{F}_p(-n)$$
splits.

2) Assume that the G-action on $\mathbb{F}_p(1)$ is non-trivial- which is possible only if $p \neq 2$. Show that inflation
$$H^1(G, \mathbb{F}_p) \longrightarrow H^1(\Gamma_n, \mathbb{F}_p)$$
is an iso. Conclude.

3) Assume that p is odd, and that the G-action on $\mathbb{F}_p(1)$ is trivial. Put
$$G' := \mathbb{F}_p^\times \times G.$$

Denote by $\mathbb{Z}_p(1)'$ the group $\mathbb{Z}_p(1)$, on which G' acts as follows. Its first factor $\mathbb{F}_p^\times$ acts via the Teichmüller character $\mathbb{F}_p^\times \longrightarrow \mathbb{Z}_p^\times$, and its second factor G acts in the given way. Show that $(G', \mathbb{Z}_p(1)')$ is a $(1, \infty)$-cyclotomic pair as well. Conclude using question 2.

4) Explain how one can adapt the previous procedure for $p = 2$, by extending scalars to the finite field $\mathbb{F}_4$, and working with $\mathbb{F}_4$ instead of $\mathbb{F}_2$.

Remark 5.3. The preceding Exercise sheds light on the following crucial property. A group of order 2 has trivial automorphism group, whereas if G is a group of (possibly infinite) order ≥ 3, we have a *strict* inclusion
$$H^0(Aut(G), G) \subsetneq G.$$
Checking this is a nice exercise.

Working with $\mathbb{F}_4$ coefficients, instead of $\mathbb{F}_2$ coefficients, thus puts the prime $p = 2$ on an equal footing vis-à-vis all odd primes. Note that we presented a proof of Theorem 5.1, that is the same for every p.

COROLLARY 5.4. *(The Norm Residue Isomorphism Theorem).*
Let F be a field of characteristic not p, with separable closure F_s.
1) For all $n \geq 1$, the natural homomorphism
$$H^n(\mathrm{Gal}(F_s/F), \mu_{p^2}^{\otimes n}) \longrightarrow H^n(\mathrm{Gal}(F_s/F), \mu_p^{\otimes n})$$
is onto. Equivalently, the connecting homomorphism
$$H^n(\mathrm{Gal}(F_s/F), \mu_p^{\otimes n}) \longrightarrow H^{n+1}(\mathrm{Gal}(F_s/F), \mu_p^{\otimes n}),$$
arising from the twisted Kummer sequence
$$0 \longrightarrow \mu_p^{\otimes n} \longrightarrow \mu_{p^2}^{\otimes n} \longrightarrow \mu_p^{\otimes n} \longrightarrow 0,$$

vanishes.
2) The Norm Residue Isomorphism Theorem holds: the Galois symbol

$$K_n^M(F)/p \longrightarrow H^n(\mathrm{Gal}(F_s/F), \mu_p^{\otimes n})$$

is an isomorphism.

Proof. Remember that $(\mathrm{Gal}(F_s/F), \mathbb{Z}_p(1))$ is a $(1, \infty)$-cyclotomic pair, where $\mathbb{Z}_p(1)$ is the Tate module given by roots of unity of p-primary order, by usual Kummer theory- see, for instance, [4]. The first statement is then given by the second part of the Smoothness Theorem.

We give references for proving 1) $\Rightarrow$ 2). When $p = 2$ (Milnor's Conjecture), this is precisely the job done in [22]. When p is arbitrary, use [15, Theorem 0.2]. Note that both papers are short and self-contained. $\qquad\square$

Remark 5.5. In the preceding Corollary, the proof of 1), that we provide in this series of three papers, puts all primes on an equal footing. In particular, the parity of p plays no rôle.

6. The Symbols Conjecture

To conclude, we state a conjecture which sharpens the Smoothness Theorem.

Conjecture. 6.1. *(The Symbols Conjecture)*
Let G be a $(1, 1)$-smooth pro-p group.
Then, the cohomology algebra

$$H^*(G, \mathbb{F}_p) := \bigoplus_{n \in \mathbb{N}} H^n(G, \mathbb{F}_p)$$

is generated in degree one.

Remark 6.2. Applied to absolute Galois groups, the Symbols Conjecture implies, without using any further result, the (surjectivity part of the) Norm Residue Isomorphism Theorem for p-special fields- hence for all fields by a restriction/corestriction argument.

The Symbols Conjecture may be weakened, by demanding that cohomology classes in $H^n(G, \mathbb{F}_p)$ be quasi-symbols instead of symbols; that is, sums of corestrictions of symbols, w.r.t. open subgroups of G. We do, however, believe that it holds as stated, and that it can be proved by an explicit application of the Uplifting Theorem, providing bounds for symbol length.

Index of notation and denomination

Bibliography

[1] A. Bertapelle, C. D. González-Avilés, *The Greenberg functor revisited*, European Journal of Mathematics, Vol. 4, Issue 4, 1340-1389, 2018.

[2] J. Borger, *The basic geometry of Witt vectors. II: Spaces*, Math. Annalen 351, 877-933, 2011.

[3] M. Brion, *Lectures on the Geometry of Flag Varieties*, in Trends in Math.: Topics in Cohomological Studies of Algebraic Varieties, Birkhäuser, 33-85.

[4] C. De Clercq, M. Florence, *Lifting Theorems and Smooth Profinite Groups,* available on the arXiv at https://arxiv.org/abs/1710.10631.

[5] C. De Clercq, M. Florence, *Lifting low-dimensional local systems,* to appear in Mathematische Zeitschrift.

[6] C. De Clercq, M. Florence, *Smooth profinite groups, I: geometrizing Kummer theory,* available on the arXiv at https://arxiv.org/abs/2009.11130.

[7] C. De Clercq, M. Florence, *Smooth profinite groups, III: the Smoothness Theorem,* available on the arXiv at https://arxiv.org/abs/2012.11027.

[8] C. De Clercq, M. Florence, G. Lucchini-Arteche, *Lifting vector bundles to Witt vector bundles,* available on the arXiv at https://arxiv.org/abs/1807.04859.

[9] C. Demarche, M. Florence, *Splitting families in Galois cohomology,* to appear in Ann. Sci. ÉNS.

[10] M. Emmerton, T. Gee, *Moduli stacks of étale (ϕ, Γ)-modules and the existence of crystalline lifts,* available on the arXiv at https://arxiv.org/abs/1908.07185.

[11] M. Florence, G. Lucchini-Arteche, *On extensions of algebraic groups,* L'Enseignement Mathématique 65, 441-455, 2019.

[12] M. Florence, *Smooth profinite groups, II : the Uplifting Theorem,* available on the arXiv at https://arxiv.org/abs/2009.11140

[13] E. M. Friedlander, A. Suslin, *Cohomology of finite groups schemes over a field,* Inv. math. 127, 209-270, 1997.

[14] W. Fulton, *Intersection theory*, Springer, 1996.

[15] P. Gille, *Symbole galoisien l-adique et théorème de Suslin-Voevodsky,* J. Math. Kyoto Univ. 47, 665-690, 2007.

[16] P. Gille, T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge Studies in Advanced Mathematics, 2006.

[17] M. J. Greenberg, *Schemata over local rings,* Ann. of Math. 73, 624-648, 1961.

[18] C. Haesemeyer, C. Weibel *The Norm Residue Theorem in Motivic Cohomology*, Annals of Mathematics Studies, Princeton University Press, 2019.

[19] N. Karpenko, *Torsion in CH^2 of Severi-Brauer varieties and indecomposability of generic algebras,* Manuscripta Math. 88, 109-117, 1995.

[20] C. B. Khare, *Base change, lifting, and Serre's conjecture,* J. of Number Theory 63, no. 2, 387–395, 1997.

[21] C. B. KHARE, M. LARSEN, *Liftable groups, negligible cohomology and Heisenberg representations,* preprint, available on the Arxiv at https://arxiv.org/pdf/2009.01301.pdf.

[22] A. MERKURJEV, *On the norm residue homomorphism for fields,* AMS Transl. 174, 49-71, 1996.

[23] A. MERKURJEV, A. SUSLIN, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Mathematics of the USSR - Izvestija 21, no. 2, 307-340, 1983.

[24] OORT, FRANS, *Yoneda extensions in abelian categories*, Math. Ann. 153, 227-235, 1964.

[25] C. QUADRELLI, T. WEIGEL, *Profinite groups with a cyclotomic p-orientation*, to appear in Doc. Math.

[26] R. RAMAKRISHNA, *Lifting Galois representations,* Inv. Math. 138, 537-562, 1999.

[27] N. ROBY, *Lois polynomes et lois formelles en théorie des modules*, Ann. Sci. École Norm. Sup. (3) 80, 213-348, 1963.

[28] J.-P. SERRE, *Corps locaux*, Hermann, Paris, 1968.

[29] J.-P. SERRE, *Sur la topologie des variétés algébriques en caractéristique p*, Symposium de topologie algébrique, Mexico, 24-53, 1956.

[30] J.-P. SERRE, *Cohomologie galoisienne*, Springer Lecture Notes in Math., 1997.

[31] The Stacks Project, https://stacks.math.columbia.edu/

[32] N. YONEDA, *On the homology theory of modules*, J. Fac. Univ. Tokyo, Sect I.7, 193-227, 1954.