Smooth profinite groups, I: geometrizing Kummer theory

Charles De Clercq, Mathieu Florence

Abstract. In this series of three articles, we study structural properties of smooth profinite groups, a class designed to extend classical Kummer theory for fields, with coefficients in p-primary roots of unity. Enhancing coefficients to arbitrary G-linearized line bundles in Witt vectors, smooth profinite groups provide a powerful formalism which sheds light on several conjectures in Galois cohomology, Galois representations and local systems.

In this first article, we introduce our main protagonists: cyclotomic pairs, smooth profinite groups, Witt modules and (G, S)-cohomology. With this robust axiomatic, we prove a first lifting theorem for G-linearized torsors under line bundles (Theorem A). It leads, in the second article, to the proof of the existence of mod p^2 liftings of mod p Galois representations, of all fields and of all dimensions (Theorem B). With this in hand, we prove in the third article Theorem D, the smoothness theorem, stating that mod p cohomology of a smooth profinite group lifts mod p^2, in all cohomological degrees. In the particular case of Galois cohomology, we obtain a new proof of the Norm Residue Isomorphism Theorem.

Contents

1. Introduction.

Let m be a positive integer and let F be a field, of characteristic prime to m. Fix a separable closure F_s/F and denote by μ_m the Galois module of m-th roots of unity in F_s. Kummer theory, in its most elementary and purest form, states the following. Consider the Kummer exact sequence

$$1 \longrightarrow \mu_m \longrightarrow F_s^\times \xrightarrow{(\cdot)^m} F_s^\times \longrightarrow 1.$$

Then, the Bockstein homomorphism, i.e. the associated boundary map

$$\delta^1_{F,m} : F^\times \longrightarrow H^1(F, \mu_m),$$

is surjective by Hilbert's Theorem 90, with kernel $F^{\times m}$.

For cohomology groups $H^n(F, \mu_m^{\otimes n})$ of degree $n > 1$, producing a description of this kind, through tensor products of copies of $F^\times$ with appropriate relations, is a much more difficult problem. For this purpose, inspired by the Steinberg relations appearing in Matsumoto's description of the K_2 of fields, Milnor introduces in the sixties his K-groups, denoted by $K_n^M(F)$. Milnor, Bass and Tate then extend the Bockstein $\delta^1_{F,m}$ above to morphisms

$$h^n_{F,m} : K_n^M(F) \longrightarrow H^n(F, \mu_m^{\otimes n})$$

called Galois symbol (or norm residue map). Without stipulating it explicitly, they then question whether these could yield isomorphisms

$$K_n^M(F)/m \xrightarrow{\sim} H^n(F, \mu_m^{\otimes n})$$

for any field F of characteristic prime to m, a statement later known as the Bloch-Kato conjecture.

A major breakthrough towards this conjecture was achieved in 1982 by Merkurjev and Suslin, who solved it for $n = 2$ [23]. In 1996, Voevodsky proved the case where m is a power of 2. He was awarded the Fields Medal in 2002 for this achievement. After tremendous efforts, a proof of the whole conjecture, then known as the Norm Residue Isomorphism Theorem, was completed in 2008 by Rost, Suslin, Voevodsky, and Weibel [18].

In this series of three articles, we are interested in studying structural properties of *smooth profinite groups*, leading notably to a proof of the following statement, known to be equivalent to the Norm Residue Isomorphism Theorem (see [15], [22]).

Bloch-Kato conjecture, an equivalent formulation.
Let F be a field and let p be a prime, invertible in F. Then, the Bockstein

$$H^n(F, \mu_p^{\otimes n}) \longrightarrow H^{n+1}(F, \mu_p^{\otimes n})$$

associated with the exact sequence

$$1 \longrightarrow \mu_p^{\otimes n} \longrightarrow \mu_{p^2}^{\otimes n} \longrightarrow \mu_p^{\otimes n} \longrightarrow 1$$

is trivial, for any positive integer n.
Equivalently, the induced map

$$H^n(\mathrm{Gal}(F_s/F), \mu_{p^2}^{\otimes n}) \longrightarrow H^n(\mathrm{Gal}(F_s/F), \mu_p^{\otimes n})$$

is surjective.

A sleek aspect of this statement is that it only involves Galois cohomology: forgetting K-theoretic considerations, the only characters on stage are the profinite group $\mathrm{Gal}(F_s/F)$, together with its module μ_{p^2}. Moreover, the statement holds for finite separable extensions E/F as well– replacing $\mathrm{Gal}(F_s/F)$ by the open subgroup $\mathrm{Gal}(F_s/E) \subset \mathrm{Gal}(F_s/F)$. This fact is the initial motivation for introducing the notion of a cyclotomic pair, that we now discuss.

Let n, e be positive integers and let G be a profinite group. Given a free $\mathbb{Z}/p^{e+1}\mathbb{Z}$-module $\mathcal{T}$ of rank 1, endowed with a continuous action of G, we say that the pair $(G, \mathcal{T})$ is (n, e)-cyclotomic if for any open subgroup $H \subset G$, the natural morphism

$$H^n(H, \mathcal{T}^{\otimes n}) \longrightarrow H^n(H, (\mathcal{T}/p)^{\otimes n})$$

is surjective (Definition 6.2).

The analogy with the discussion above is quite direct: Kummer theory readily implies that, taking

$$\mathcal{T} := \varprojlim_r \mu_{p^r}$$

to be the usual Tate module, the pair $(\mathrm{Gal}(F_s/F), \mathcal{T})$ is $(1, \infty)$-cyclotomic. Thenceforward, the above formulation of the Bloch-Kato conjecture can be rephrased, for cyclotomic pairs, as

(∗) “ If $(G, \mathcal{T})$ is a $(1, \infty)$-cyclotomic pair, then it is $(n, 1)$-cyclotomic.”

This statement fleshes out the common belief that the keystone of the Norm Residue Isomorphism Theorem is Hilbert Theorem 90 for fields.

In this work, we prove statement $(*)$ (Theorem D below), thus settling a new proof of the Norm Residue Isomorphism Theorem. Not only does this result flesh out the belief that the Norm Residue Isomorphism Theorem follows from Kummer theory, but also, Theorem D applies to a much broader context than Galois cohomology. Indeed, étale fundamental groups of smooth curves over algebraically closed fields and of semilocal rings also give rise to $(1,\infty)$-cyclotomic pairs [5, §4].

1.1. Our pathway. In this series of three articles, we provide a self contained proof of the Norm Residue Isomorphism Theorem by raising a bridge between it and the conjectural existence of mod p^2-liftings of mod p Galois representations. More precisely, let F be a field, with separable closure F_s. Let

$$\rho_1 : \mathrm{Gal}(F_s/F) \longrightarrow GL_d(\mathbb{F}_p)$$

be a Galois representation. One can ask wether ρ_1 lifts to p^2-torsion, that is to say, whether there is a mod p^2 Galois representation ρ_2 such that the diagram

$$\begin{tikzcd}
\mathrm{Gal}(F_s/F) \arrow[r, "\rho_2"] \arrow[dr, "\rho_1"'] & GL_d(\mathbb{Z}/p^2\mathbb{Z}) \arrow[d] \\
& GL_d(\mathbb{F}_p)
\end{tikzcd}$$

commutes, the vertical arrow being induced by the usual reduction.

This problem also fits very well in the framework of cyclotomic pairs. In the second article of this series, we prove a very general lifting statement, our so-called Uplifting Theorem. It implies that, if $(G, \mathcal{T})$ is a $(1,1)$-cyclotomic pair, then all continuous mod p semi-linear representations of G lift, to their mod p^2 analogue. This is a decisive step towards $(*)$. The Uplifting Theorem not only applies to mod p Galois representations as above, but also to mod p representations of algebraic fundamental groups of many schemes of interest- including smooth curves, proper or not, over algebraically closed fields.

For the sake of proving our lifting results, a crucial point is, as often, to allow more flexible objects. Indeed, as stated above, Kummer theory has an obvious weakness: whereas it holds for any field F (and actually over a much larger class of base schemes), its coefficients are forever fixed: for $m = p^r$, they are μ_{p^r}, merely an étale sheaf of one-dimensional free $\mathbb{Z}/p^r$-modules. A way to have it gain robustness and versatility, is to extend these coefficients to a G-linearized line bundle in p-typical Witt vectors of length r, on a G-scheme S of characteristic p. This should be done in such a way that, replacing μ_p by a G-linearized line bundle L, the analogue of μ_{p^r} should be the Teichmüller lift $\mathbf{W}_r(L)$ (up to a twist). The concepts of Witt vector bundles and of their extensions, whose systematic study was initiated in [8], will thus play a key role in our approach.

In this first article, we state and prove a lifting theorem, which is thought of as a generalization of classical Kummer theory– μ_p being replaced by an arbitrary G-line bundle, over a G-scheme S of characteristic p. For simplicity, we formulate it here in the particular case, where S is affine and perfect.

Theorem A (§9). *Let $(G, \mathbb{Z}/p^{1+e}(1))$ be a (n,e)-cyclotomic pair, for numbers $n \in \mathbb{N}^*$ and $e \in \mathbb{N}^* \cup \{\infty\}$.*

Pick an integer $1 \leq r \leq e$. Let S be a perfect affine $(G, \mathbb{F}_p)$-scheme and let L be a G-linearized line bundle over S. Then, the natural arrow

$$H^n((G,S), \mathbf{W}_{1+e}(L)(n)) \longrightarrow H^n((G,S), \mathbf{W}_r(L)(n))$$

is onto. Therefore, G is (n,e)-smooth.

A word of explanation is needed, concerning the new notion of a (n,e)-smooth profinite group G, given in Definition 6.8. At its core lies even more flexibility. We say that G is (n,e)-smooth if the following holds. Let L_1 be a G-linearized line bundle, over a perfect affine $(G, \mathbb{F}_p)$-scheme S. Let

$$c_1 \in H^n((G,S), L_1)$$

be a cohomology class. Then, it lifts to a class

$$c_{e+1} \in H^n((G,S), L_{e+1}[c_1]),$$

for *some* G-linearized invertible $\mathbf{W}_{e+1}(A)$-module $L_{e+1}[c_1]$, *depending* on c_1. This notion thus dismisses the cyclotomic module $\mathbb{Z}/p^{1+e}(1)$: it is intrinsic to G.

If $(G, \mathbb{Z}/p^{1+e}(1))$ is a (n,e)-cyclotomic pair, Theorem A thus shows that G is (n,e)-smooth. Indeed, assuming for simplicity that $\mathbb{F}_p(1) = \mathbb{F}_p$ has the trivial action of G, we can then take

$$L_{e+1}[c_1] := \mathbf{W}_{1+e}(L_1)(n),$$

which is the same for all c_1's.
In particular, if p is invertible in the field F, then $G = Gal(F_s/F)$ is $(1,\infty)$-smooth and the following lifting result, proved in the second article, implies that mod p Galois representations of F lift to p^2-torsion.

Theorem B ([12, §14]). *Let G be a $(1,1)$-smooth profinite group, A be a perfect $(\mathbb{F}_p, G)$-algebra and $d \geq 1$ be an integer. Denote by $\mathbf{B}_d \subset \mathbf{GL}_d$ the Borel subgroup of upper triangular matrices.*
Then, the natural arrow

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

given by reduction, is surjective.
Moreover, liftings of triangular semi-linear representations of G can be constructed step-by-step.

In the third article, we derive from Theorem B the following general lifting theorem, for filtered exact sequences of G-linearized vector bundles.

Theorem C ([7, §4]). *Let G be a $(1,1)$-smooth profinite group and 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-linearized vector bundles over A.
Then, $\mathcal{E}$ admits a lift to a filtered exact sequence of $(G, \mathbf{W}_2)$-bundles over A.

Casting Theorem C and considering the interplay between (G,S)-cohomology and Yoneda extensions of G-linearized Witt vector bundles, we can then settle our smoothness theorem, from which we derive a new proof of the Norm Residue Isomorphism Theorem.

Theorem D ([7, §5]). *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.

We give a Leitfaden, connecting significant results of our three papers. For simplicity, we stick to Galois cohomology. Note that the same diagram holds, replacing absolute Galois groups (resp. Galois representations) by $\pi_1(X)$, where X is a smooth curve over an algebraically closed field, or a semilocal scheme (resp. étale local systems on X).

$$\begin{tikzcd}
\text{Theorem A} \arrow[rr, Rightarrow] & & \boxed{\begin{array}{c}\text{Absolute Galois groups}\\ \text{are } (1,\infty)\text{-smooth}\end{array}} \arrow[dll, equal, bend right] \arrow[d, equal] \arrow[drr, equal, bend left] & & \\
\text{Theorem B} \arrow[rr, Rightarrow] \arrow[d, Rightarrow] & & \text{Theorem C} \arrow[rr, Rightarrow] & & \text{Theorem D} \arrow[d, Rightarrow] \\
\boxed{\begin{array}{c}\text{mod } p \text{ Galois reps}\\ \text{lift to } p^2\text{-torsion}\end{array}} & & & & \boxed{\begin{array}{c}\text{Norm residue}\\ \text{isomorphism Theorem}\end{array}}
\end{tikzcd}$$

In this first article, we introduce the main protagonists of our work and prove Theorem A. Sections 1 to 5 provide the needed geometrization of the flagbearers of classical Kummer theory, introducing G-Witt modules and (G,S)-cohomology, using (G,S)-affine spaces and Yoneda extensions. Smooth profinite groups, cyclotomic pairs and their Laurent extensions are defined and studied in Sections 6 and 7. Theorem A is proved in section 9. Among other results of independent interest, the last sections provide material required for Theorem B, proved in the second article of this work. Our smoothness theorem (Theorem D) is proved in the third article.

To ensure a pleasant reading, we took care to add at the end of the third article an index, which tables the notions introduced in this work.

2. G-equivariant constructions.

2.1. General setting. Let X be an object of a category $\mathcal{C}$, and G be a profinite group. In this text, a *naive action* of G on X is an action of the abstract group G on X, whose kernel G_0 is an open subgroup of G. We denote by $G - \mathcal{C}$ the category whose objects are objects of $\mathcal{C}$, equipped with a naive action of G, and whose morphisms are the same as in $\mathcal{C}$. In $G - \mathcal{C}$, Hom-sets are actually enriched with the structure of G-sets. Thus, G-equivariant morphisms $X \longrightarrow Y$, between objects of $G - \mathcal{C}$, are fixed elements of the G-set $\mathrm{Hom}(X,Y)$. In short:

$$\mathrm{Hom}_{G-equ}(X,Y) = H^0(G, \mathrm{Hom}(X,Y)).$$

An object of $G - \mathcal{C}$ will be called a G-object of $\mathcal{C}$.

Remark 2.1. In the sequel, unless specified otherwise, we shall write "action" for "naive action".

2.2. *G*-LINEARIZED MODULES OVER *G*-SCHEMES. In this work, all schemes are assumed to be quasi-compact. By a sheaf over a scheme, we mean a sheaf for the Zariski topology. We will restrict to "topologically well-behaved" G-actions, in the sense of Definition below.

DEFINITION 2.2. *A G-scheme (or scheme with a G-action) is the data of a scheme S, equipped with a naive action of G, satisfying the property:*

> $(*)$ *S is covered by affine G-invariant open subschemes.*

The collection of all G-schemes form a category $G - Sch$, with morphisms being usual morphisms of schemes.
A $(G, \mathbb{F}_p)$-scheme is a G-scheme of characteristic p.
If S is a given G-scheme, a (G, S)-scheme is a G-equivariant morphism

$$T \longrightarrow S,$$

in $G - Sch$.

Remark 2.3. In general, G may act on a scheme S, in such a way that S is *not* covered by affine G-invariant open subschemes. See, however, the next Exercise (a classical result).

Exercise 2.4. Let S be a scheme, separated over $\mathbb{Z}$, such that every finite set of points of S is contained in an open affine subscheme of S. Show that S has property $(*)$, for any naive action of G on S.

It is clear that a closed subscheme of a G-scheme, given by a G-invariant Ideal, is a G-scheme as well. It is perhaps less obvious that this also holds for open subschemes.

LEMMA 2.5. *Let S be a G-scheme. Let $U \subset G$ be a G-invariant open subscheme. Then, U is a G-scheme as well.*

Proof. We can assume that $S = \mathrm{Spec}(A)$ is affine, and G finite. The complement of U in S is given by a G-invariant ideal $I \subset A$. Pick a point $u \in U$. Denote by $P_1, \ldots, P_n$ the distinct prime ideals of A corresponding to the G-orbit of u. For each $i = 1 \ldots n$, there exists an element $a_i \in I$, not belonging to P_i but belonging to all other P_j's. Put $a := \sum_1^n a_i$. Then, the principal open set $D(a)$ is contained in U, and contains the G-orbit of u. Denoting by

$$f := \prod_{g \in G} g \cdot a$$

the norm of a, we see that $D(f) \subset U$ is an affine G-invariant open, containing u. Thus, U can be covered by affine G-invariant open subschemes. □

Conceptually, the next definition is down-to-earth; however, it is sufficient for our purposes.

DEFINITION 2.6. *Let S be a G-scheme. A G-presheaf on S, with values in a category $\mathcal{D}$, is a contravariant functor, from the category of G-invariant open subsets of S (where morphisms are inclusions), to $\mathcal{D}$. A G-sheaf is a G-presheaf, satisfying the usal sheaf axiom.*
In most applications, $\mathcal{D}$ will actually be $G - \mathcal{C}$, where $\mathcal{C}$ is a category.

Definition 2.7. *Let S be a G-scheme. A G-linearized $\mathcal{O}_S$-Module is the data of a quasi-coherent $\mathcal{O}_S$-Module M, equipped with a continuous semilinear action of G. In concrete terms, such an action is given by isomorphisms of $\mathcal{O}_S$-Modules*

$$\phi_g : M \longrightarrow (g.)^*(M),$$

one for each $g \in G$, such that the following conditions hold :
i) The mapping $g \mapsto \phi_g$ is locally constant on G, i.e. factors through a quotient $G \longrightarrow G/G_0$, by a normal open subgroup.
ii) We have

$$\phi_{gh} = (h.)^*(\phi_g) \circ \phi_h,$$

for each $g, h \in G$.
We will often say $(G, \mathcal{O}_S)$-Module, or (G, S)-Module, instead of G-linearized $\mathcal{O}_S$-Module.
The collection of all $(G, \mathcal{O}_S)$-Modules form an Abelian category, monoidal through the tensor product $\otimes = \otimes_{\mathcal{O}_S}$. We denote it by $(G, \mathcal{O}_S) - Mod$.
If M and N are two $(G, \mathcal{O}_S)$-Modules, the internal Hom of $\mathcal{O}_S$-modules $\underline{\mathrm{Hom}}_{\mathcal{O}_S}(M, N)$ is naturally a $(G, \mathcal{O}_S)$-Module, which we denote simply by $\underline{\mathrm{Hom}}(M, N)$. We put

$$M^\vee := \underline{\mathrm{Hom}}(M, \mathcal{O}_S).$$

A locally free $(G, \mathcal{O}_S)$-Module of finite constant rank as an $\mathcal{O}_S$-module, will be called a G-vector bundle on S.

Remark 2.8. In the previous Definition, the largest open subgroup through which $g \mapsto \phi_g$ factors may be much smaller than the kernel of the action of G on S.

Remark 2.9. In short, a $(G, \mathcal{O}_S)$-Module is the data of a quasi-coherent $\mathcal{O}_S$-Module, equipped with a semilinear (naive) action of G.
For G finite, a G-line bundle is a G-linearized line bundle over S, in the sense of Mumford's Geometric Invariant Theory.

Remark 2.10. Assume that $X = \mathrm{Spec}(A)$ is an affine G-scheme. In other words, A is a commutative ring, endowed with a naive action of G. We then use the denomination (G, A)-module (resp. (G, A)-bundle) for a $(G, \mathcal{O}_S)$-module (resp. a $(G, \mathcal{O}_S)$-bundle). A (G, A)-module is the data of an A-module M, equipped with a semilinear (naive) action of G. Formula for the "semi" part of linearity:

$$g.(am) = g(a).g(m),$$

for all $g \in G$, $a \in A$ and $m \in M$.
In particular, if G is "the" absolute Galois group of a field F, and if $A = \mathbb{F}_p$, a (G, A)-Module is then a Galois representation of the field F, with $\mathbb{F}_p$ coefficients.

Remark 2.11. Assume that G is a finite group, acting on the commutative ring A. There are two extreme cases.

- The group G acts trivially on A. Then, a (G, A)-Module M, such that $M = A^d$ as an A-module, is a representation

$$\rho : G \longrightarrow \mathbf{GL}_d(A),$$

  in the usual sense.
- The group G acts freely on $\mathrm{Spec}(A)$. Set $B := H^0(G, A)$. Then, B/A is a G-Galois algebra, and by Speiser's Lemma, the category of (G, A)-modules is equivalent to that of B-modules, via the assignment

$$\{B - Mod\} \longrightarrow \{(G, A) - Mod\},$$

$$N \mapsto A \otimes_B N,$$

with quasi-inverse

$$\{(G,A) - Mod\} \longrightarrow \{B - Mod\},$$
$$M \mapsto H^0(G,M).$$

When trying to prove a "natural" property of (G,A)-modules, for an arbitrary G-action on A, it is advisable to check first, if it holds true in these two extreme cases. If it does, it is then likely to hold true in general.

Remark 2.12. Let S be a G-scheme, and let M be a quasi-coherent $\mathcal{O}_S$-Module. A necessary condition for G-linearizing M (that is to say, for the existence of a structure of $(G,\mathcal{O}_S)$-Module on M) is that M be G-invariant. In other words, M is isomorphic to $g^*(M)$, for all $g \in G$. Note that G-invariant Modules are not systematically G-linearizable– except, for instance, when G is a free profinite group.

3. Recollections on Witt vectors and Witt modules.

Let A be a ring of characteristic p. We denote by $\mathbf{W}(A)$ the ring of p-typical Witt vectors built out of A. Set-wise, $\mathbf{W}(A)$ is simply $A^{\mathbb{N}}$, and the ring structure on $\mathbf{W}(A)$ is derived from the universal Witt polynomials (see [28]). For a thorough exposition of Witt modules and Witt vector bundles, see [8], where an alternative construction of Witt vectors is provided, using divided powers of abelian groups.

The ring of Witt vectors $\mathbf{W}(A)$ is endowed with a Verschiebung (additive) morphism

$$\begin{array}{cccc} \mathrm{Ver}: & \mathbf{W}(A) & \longrightarrow & \mathbf{W}(A) \\ & (a_0, a_1, a_2, ...) & \longmapsto & (0, a_0, a_1, a_2, ...) \end{array}$$

and the Frobenius morphism $\mathrm{Frob} : (a_0, a_1, ...) \mapsto (a_0^p, a_1^p, ...)$.

For any $r \geq 1$, denote by $\mathbf{W}_r(A)$ the ring of truncated Witt vectors of length r. We have $\mathbf{W}_1(A) = A$, and the ring $\mathbf{W}(A)$ is the projective limit of the $\mathbf{W}_r(A)$ through the quotient maps

$$\begin{array}{cccc} \pi_{r+1,r}: & \mathbf{W}_{r+1}(A) & \longrightarrow & \mathbf{W}_r(A) \\ & (a_0, ..., a_{r+1}) & \longmapsto & (a_0, ..., a_r) \end{array}$$

More generally, for any two integers $r \leq s$, we denote by $\pi_{s,r}$ the quotient map

$$\mathbf{W}_s(A) \longrightarrow \mathbf{W}_r(A).$$

We will often use the following fundamental property: the quotient

$$\mathbf{W}(A) \longrightarrow \mathbf{W}_1(A) = A$$

has a multiplicative section given by the Teichmüller representative

$$\tau : a \mapsto (a, 0, ...),$$

refered to as the multiplicative (or Teichmüller) section.

Consider now a scheme S of characteristic p, covered by affine open subschemes $\mathrm{Spec}(A_i)$. We denote by $\mathbf{W}_r(S)$ the scheme of Witt vectors of S of length n. It is defined by gluing the affine schemes $\mathrm{Spec}(\mathbf{W}_r(A_i))$ and is a universal thickening of S of order n, through the nilpotent closed immersions $\mathbf{W}_r(S) \longrightarrow \mathbf{W}_{r+1}(S)$. In particular, the underlying topological space of $\mathbf{W}_r(S)$ agrees with that of S.

The following definition is classical (see [29]).

Definition 3.1. *Let $r \geq 1$ be an integer. The association*

$$U \mapsto \mathbf{W}_r(\mathcal{O}_S(U))$$

defines a sheaf of (commutative) rings on S, denoted by $\mathbf{W}_r(\mathcal{O}_S)$.

By definition, $\mathbf{W}_1(\mathcal{O}_S)$ is simply the structure sheaf $\mathcal{O}_S$ of S and following the previous notations, for $s \geq r$, we denote by

$$\pi_{s,r} : \mathbf{W}_s(\mathcal{O}_S) \longrightarrow \mathbf{W}_r(\mathcal{O}_S)$$

the natural transformation defined by the

$$\pi_{s,r}(U) : \mathbf{W}_s(\mathcal{O}_S(U)) \longrightarrow \mathbf{W}_r(\mathcal{O}_S(U))$$

defined above.

Witt modules mimic quasi-coherent $\mathcal{O}_S$-modules, in higher p-primary torsion.

Definition 3.2. *Assume that $S = \mathrm{Spec}(A)$ is affine. Let $r \geq 1$ be a positive integer. Let M be a $\mathbf{W}_r(A)$-module. The formula*

$$U \mapsto M \otimes_{\mathbf{W}_r(A)} \mathbf{W}_r(\mathcal{O}_S(U))$$

defines a presheaf (for the Zariski topology) on S. We denote by $\tilde{M}$ the associated sheaf. It is a sheaf of $\mathbf{W}_r(\mathcal{O}_S)$-modules.

Definition 3.3 (Witt Modules).
A Witt Module of height $r \geq 1$ over S is a sheaf of $\mathbf{W}_r(\mathcal{O}_S)$-modules, which is locally isomorphic to a sheaf of the shape $\tilde{M}$ (cf. Definition 3.2).
When no reference to its height is necessary, a Witt Module will simply be referred to as a W-Module.
A W-module over S locally isomorphic to $\mathbf{W}_r(\mathcal{O}_S)^d$ for some $d \geq 0$ is called a $\mathbf{W}_r$-bundle of rank d.

3.1. Reduction. Let $0 \leq r \leq s$ be integers. Let $\mathcal{F}$ be a sheaf of $\mathbf{W}_s(\mathcal{O}_S)$-modules over S.
The reduction of $\mathcal{F}$ to p^r-torsion is the sheaf of $\mathbf{W}_r(\mathcal{O}_S)$-modules associated to the presheaf

$$U \mapsto \mathcal{F}(U) \otimes_{\mathbf{W}_s(\mathcal{O}_S(U))} \mathbf{W}_r(\mathcal{O}_S(U)),$$

which we denote by $\mathcal{F} \otimes_{\mathbf{W}_s} \mathbf{W}_r$.

3.2. Frobenius. The absolute Frobenius morphism

$$\mathrm{Frob} : S \longrightarrow S$$

lifts by functoriality to an endomorphism of $\mathbf{W}_r(S)$, the Frobenius endomorphism of $\mathbf{W}_r(S)$, which we still denote by Frob. If $\mathcal{F}$ is a $\mathbf{W}_r$-module over S, and if m is a positive integer, we put

$$\mathcal{F}^{(m)} := (\mathrm{Frob}^m)^*(\mathcal{F});$$

is a $\mathbf{W}_r$-module over S. If $\mathcal{F}$ is a $\mathbf{W}_r$-bundle, then $\mathcal{F}^{(m)}$ is a $\mathbf{W}_r$-bundle as well, of the same rank as $\mathcal{F}$. Note that, throughout this paper, the Frobenius pullback of a W-module is always taken with respect to the Frobenius of the base where the module is defined, thus avoiding confusion.

4. (G, M)-torsors and Yoneda extensions.

Let G be a profinite group G. Let A be a G-group, i.e. a group equipped with a (naive) action of G. Then, there is a well-known bijection between the set $H^1(G, A)$, and isomorphism classes of G-equivariant principal homogeneous spaces (torsors) of A. In this section, we provide needed extensions of this fact, especially to the context of G-equivariant torsors under $(G, \mathcal{O}_S)$-modules. Our basic tool (see Proposition 4.20) is Yoneda's smart interpretation of torsors, as equivalence classes of extensions [32].

4.1. Yoneda extensions and operations on them. Let S be a G-scheme, let $n \in \mathbb{N}^*$ be an integer and let A, B be $(G, \mathcal{O}_S)$-Modules over S. As in any Abelian category, we can consider the notion of a Yoneda n-extension of A by B, which we now recall (see [5, §2]). One could use the langage of derived categories instead, but we chose to stick to Yoneda extensions: they are concrete, and easy to learn.

As usual, we set

$$\mathrm{YExt}^0_{(G,\mathcal{O}_S)-Mod}(A, B) := \mathrm{Hom}_{(G,\mathcal{O}_S)-Mod}(A, B).$$

For $n \geq 1$, an n-extension of A by B is an exact sequence of $(G, \mathcal{O}_S)$-Modules

$$\mathcal{E} : 0 \longrightarrow B \longrightarrow A_1 \longrightarrow \ldots \longrightarrow A_n \longrightarrow A \longrightarrow 0.$$

4.2. Morphisms. A morphism

$$\mathcal{E}_1 \longrightarrow \mathcal{E}_2,$$

between two n-extensions of A by B, is a morphism of complexes which is the identity on both A and B. The n-extensions of A by B then form a category $\mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A, B)$.

4.3. Pushforwards and pullbacks. A morphism $f : B \longrightarrow B'$ induces a pushforward functor

$$f_* : \mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A, B) \longrightarrow \mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A, B').$$

Likewise, a morphism $g : A' \longrightarrow A$ induces a pullback functor

$$g^* : \mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A, B) \longrightarrow \mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A', B).$$

The two composite functors

$$f_*g^* : \mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A, B) \longrightarrow \mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A', B')$$

and

$$g^*f_* : \mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A, B) \longrightarrow \mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A', B')$$

are canonically isomorphic.

4.4. Baer sum. One can add two n-extensions

$$\mathcal{E}_1, \mathcal{E}_2 \in \mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A, B),$$

using the Baer sum.
Denoting by

$$\begin{array}{rccc} \delta : & A & \longrightarrow & A \oplus A \\ & a & \longmapsto & (a, a) \end{array}$$

the diagonal, and by

$$\begin{array}{rccc} \alpha : & B \oplus B & \longrightarrow & B \\ & (b_1, b_2) & \longmapsto & b_1 + b_2 \end{array}$$

the addition, our formula is

$$\mathcal{E}_1 + \mathcal{E}_2 := \alpha_*(\delta^*(\mathcal{E}_1 \oplus \mathcal{E}_2)).$$

For this operation, the trivial 1-extension is the direct sum

$$0 \longrightarrow B \longrightarrow B \oplus A \longrightarrow A \longrightarrow 0.$$

If $n \geq 2$, the trivial n-extension is

$$0 \longrightarrow B \xrightarrow{\mathrm{Id}} B \longrightarrow 0 \longrightarrow \ldots \longrightarrow 0 \longrightarrow A \xrightarrow{\mathrm{Id}} A \longrightarrow 0.$$

Baer sum is $\mathcal{O}_S$-linear, in the natural fashion.

4.5. Change of the base. Let

$$h : T \longrightarrow S$$

be a G-equivariant morphism of G-schemes. Let

$$\mathcal{E} : 0 \longrightarrow B \longrightarrow A_1 \longrightarrow \ldots \longrightarrow A_n \longrightarrow A \longrightarrow 0$$

be an n-extension, in $\mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A, B)$. We would like to define

$$h^*(\mathcal{E}) \in \mathbf{YExt}^n_{(G,\mathcal{O}_T)-Mod}(h^*(A), h^*(B)).$$

This can be done in a natural way, in each of the following items.

(1) The morphism h is flat.

(2) When decomposing $\mathcal{E}$ as the cup-product of short exact sequences (indexed by $i = 1, \ldots, n$)

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

all $\mathcal{E}_i$'s are Zariski locally split on S, as exact sequences of $\mathcal{O}_S$-modules. Then, applying usual change of the base indeed yields an exact sequence of $(G, \mathcal{O}_T)$-modules

$$h^*(\mathcal{E}) : 0 \longrightarrow h^*(B) \longrightarrow h^*(A_1) \longrightarrow \ldots \longrightarrow h^*(A_n) \longrightarrow h^*(A) \longrightarrow 0.$$

Note that, in many applications, it happens that A, B and the A_i's are vector bundles, so that the E_i's are also vector bundles, and the assumption above is fulfilled.

(3) In this last item, we assume there is a morphism of $(G, \mathbb{F}_p)$-schemes

$$h_1 : T_1 \longrightarrow S_1,$$

and an integer $r \geq 1$, such that h is the morphism

$$h = \mathbf{W}_r(h_1) : T = \mathbf{W}_r(T_1) \longrightarrow S = \mathbf{W}_r(S_1)$$

induced on Witt vectors.
We further assume that "$\mathcal{E}$ is schematic, w.r.t. the ring scheme $\mathbf{W}_r$".

Precisely, this means we are given $n+2$ flat, affine and G-linearized commutative S_1-group schemes

$$\mathbf{B}, \mathbf{A}_i, \mathbf{A} \longrightarrow S_1,$$

enjoying the following properties.

- Let $\mathbf{V}$ be one of these group schemes. Forgetting the action of G, there exists an integer $s \in [1, \dots, r]$, and $d \in \mathbb{N}$, such that $\mathbf{V}$ is, Zariski locally over S_1, isomorphic to the group scheme $\mathbf{W}_s^d$. Here s and d depend on $\mathbf{V}$.
- Each of these $\mathbf{V}$'s is endowed with the extra structure of a scheme in $(G, \mathbf{W}_r)$-modules over S_1. Considering $\mathbf{W}_r$ as a scheme of commutative rings over S_1, this means we are given a morphism of (G, S_1)-schemes
$$\mathbf{W}_r \times_{S_1} \mathbf{V} \longrightarrow \mathbf{V},$$
satisfying the axioms which are usual for modules over rings.
- The n-extension of $(G, \mathcal{O}_S)$-modules $\mathcal{E}$ arises from an exact sequence of schemes of $(G, \mathbf{W}_r)$-modules over S_1,
$$\mathbf{E} : 0 \longrightarrow \mathbf{B} \longrightarrow \mathbf{A}_1 \longrightarrow \dots \longrightarrow \mathbf{A}_n \longrightarrow \mathbf{A} \longrightarrow 0.$$
This means that $\mathbf{E}$ is an exact sequence of commutative group schemes over S_1 (for the fppf topology), in which all arrows respect the structures of schemes of $(G, \mathbf{W}_r)$-modules. Using that each of these group schemes is locally isomorphic to a $\mathbf{W}_s^d$, and the triviality of $\mathbf{W}_s$-torsors over an affine base, we get, for every affine G-invariant open $U \subset S_1$, that sections of $\mathbf{E}$ over U, reading as
$$\mathbf{E}(U) : 0 \longrightarrow \mathbf{B}(U) \longrightarrow \mathbf{A}_1(U) \longrightarrow \dots \longrightarrow \mathbf{A}_n(U) \longrightarrow \mathbf{A}(U) \longrightarrow 0,$$
are still exact sequences. Remembering that $S = \mathbf{W}_r(S_1)$, they thus define an n-extension of $(G, \mathcal{O}_S)$-modules, which we require to be isomorphic to $\mathcal{E}$.

If $\mathcal{E}$ comes from an $\mathbf{E}$ as above, we can form

$$h_1^*(\mathbf{E}) : 0 \longrightarrow h_1^*(\mathbf{B}) \longrightarrow h_1^*(\mathbf{A}_1) \longrightarrow \dots \longrightarrow h_1^*(\mathbf{A}_n) \longrightarrow h_1^*(\mathbf{A}) \longrightarrow 0;$$

an exact sequence of schemes of $(G, \mathbf{W}_r)$-modules over T_1. We then define $h^*(\mathcal{E})$ as the n-extension of $(G, \mathcal{O}_T)$-modules arising from $h_1^*(\mathbf{E})$ (through the process explained above). Of course, $h^*(\mathcal{E})$ a priori depends on the choice of $\mathbf{E}$. In applications, this choice will be clear: there will be no ambiguity, as to which $\mathbf{E}$ is used.

Most changes of the base will be performed through the process described in item (2) above. Note that item (1) is not really suitable for our purposes: our arrows h, often arising as in item (3), will almost never be flat! Actually, all changes of the base made in this series of three papers, can be performed following the process of item (3).

4.6. Morphisms of 1-extensions. Morphisms in $\mathbf{YExt}^1_{(G,\mathcal{O}_S)-Mod}(A, B)$ are isomorphisms. Automorphisms of 1-extensions are easily described, as follows.

Lemma 4.1. *Let*

$$\mathcal{E} : 0 \longrightarrow B \xrightarrow{i} E \xrightarrow{\pi} A \longrightarrow 0$$

be an exact sequence of $(G, \mathcal{O}_S)$*-Modules. Then, the assignment*

$$\mathrm{Hom}_{(G,\mathcal{O}_S)-Mod}(A, B) \longrightarrow \mathrm{Aut}_{\mathbf{YExt}^1_{(G,\mathcal{O}_S)-Mod}(A,B)}(\mathcal{E}),$$

$$f \mapsto (x \in E \mapsto x + i(f(\pi(x))))$$

is an isomorphism of abelian groups.

Proof. Exercise, working for 1-extensions in any Abelian category. □

4.7. Equivalence classes of Yoneda extensions. Let us say that two n-extensions $\mathcal{E}_1$ and $\mathcal{E}_2$ are linked, if there exists an n-extension $\mathcal{E}_3$, together with morphisms

$$\begin{tikzcd} \mathcal{E}_1 \arrow[dr] & & \mathcal{E}_2 \arrow[dl] \\ & \mathcal{E}_3. & \end{tikzcd}$$

Being linked is an equivalence relation (see [24], end of Section 2), compatible with Baer sum, pullbacks, pushforwards and change of the base.

Definition 4.2. *We denote by* $\mathrm{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A,B)$ *the Abelian group of equivalence classes of linked Yoneda n-extensions, in the category* $\mathbf{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A,B)$.

Lemma 4.3. *Assume that A is a G-vector bundle on S. Then, there is a canonical isomorphism*

$$\mathrm{YExt}^n_{(G,\mathcal{O}_S)-Mod}(A,B) \xrightarrow{\sim} \mathrm{YExt}^n_{(G,\mathcal{O}_S)-Mod}(\mathcal{O}_S, \underline{\mathrm{Hom}}(A,B)).$$

Proof. Same proof as [5, Lemma 2.5]. □

4.8. G-affine spaces. In this text, we'd like to lay emphasis on the notion of an "*affine space*". We first define it as a set, equipped with barycentric operations, with coefficients in a commutative ring R. This terminology unfortunately collides with the "affine R-scheme" $\mathbb{A}^n_R$, but we try our best to avoid ambiguities. Note that an "*affine space*", whose R-module of translations is free of rank n, is isomorphic to an "*affine scheme*" $\mathbb{A}^n_R$, over R. We decided to allow the empty set to qualify as an affine space. Our motivation to do so is simple: the intersection of affine subspaces is then always an affine subspace.

Following tradition, we use the word "torsor" (under a group M) to denote a nonempty set X, equipped with a simply transitive action of M. Thus, a nonempty affine space is a torsor under the (abelian) group of its translations. Conversely, a torsor over an abelian group is canonically endowed with the structure of a (nonempty) affine space over $\mathbb{Z}$.

We now discuss details. They are routine exercises, taking into account (naive) actions of a given profinite group G, and transposing the set-theoretic notions above to algebraic geometry. We hope the interested reader will enjoy reading these lines.

Definition 4.4. *Let M be a (not necessarily abelian) G-group.*

A (G,M)-torsor is a nonempty left G-set X, equipped with a right action of M, subject to the following conditions :

i) The action of M on X is simply transitive, i.e. the arrow

$$X \times M \longrightarrow X \times X,$$

$$(x,m) \mapsto (x, x.m)$$

is bijective.

ii) We have

$$g(x.m) = g(x).g(m),$$

for all $g \in G$, $x \in X$ and $m \in M$.

Let $S = \mathrm{Spec}(A)$ be an affine G-scheme, i.e. the ring A is endowed with an action of G.

Definition 4.5. *Let $n \geq 1$ be an integer. We denote by*

$$\Delta_n(A) := \{(\alpha_1, \ldots, \alpha_n) \in A^n / \sum_{i=1}^{n} \alpha_i = 1\}$$

the usal simplex; it is a G-set.

Definition 4.6. *A G-affine space over A is the data of a G-set X, equipped with G-equivariant barycentric operations, with coefficients in A.*
Concretely, this means that X is given with G-equivariant functions, one for each $n \geq 2$,

$$B_n : \Delta_n(A) \times X^n \longrightarrow X,$$

simply denoted by

$$((\alpha_1, \ldots, \alpha_n), (x_1, \ldots, x_n)) \mapsto \sum \alpha_i x_i,$$

satisfying the usual associativity relations, together with $B_1 = \mathrm{Id}_X$.
If G is trivial, we just say "affine space over A" for "G-affine space over A".
We denote by $X^G \subset X$ the subset consisting of G-fixed points. It is an affine space over A^G.

An affine map $X \xrightarrow{f} X'$, between G-affine spaces over A, is the data of a map

$$f : X \longrightarrow X',$$

compatible with the barycentric operations of X and X'.
We write $\mathrm{Hom}(X, X')$ for the set of such morphisms. It is a G-affine space, in a natural way.
We put

$$\mathrm{Hom}_G(X, X') := H^0(G, \mathrm{Hom}(X, X')).$$

The set $\mathrm{Hom}_G(X, X')$ thus consists of G-equivariant affine maps $X \longrightarrow X'$, also called affine G-maps.
The collection of G-affine spaces over A form a category, having the G-sets $\mathrm{Hom}(\cdot, \cdot)$ as morphisms.

Example 4.7. It is clear that (G, A)-modules are G-affine spaces over A, in a natural way. The G-invariant subset $\Delta_n(A) \subset A^n$ is stable under barycentric operations in the free G-module A^n; it is thus also a G-affine space over A.

Exercise 4.8. Let X be a G-affine space over A.
1) Show that all barycentric operations on X can be recovered from the data of

$$\begin{array}{cccc} T: & X \times X \times X & \longrightarrow & X \\ & (x, y, z) & \longmapsto & x + y - z \end{array}$$

together with the operations

$$\begin{array}{cccc} t_\alpha: & X \times X & \longrightarrow & X \\ & (x, y) & \longmapsto & \alpha x + (1 - \alpha) y \end{array},$$

for all $\alpha \in A$.
2) Assume that there exists an element $\alpha_0 \in A$, such that α_0 and $1 - \alpha_0$ are both invertible. Show that T can be recovered from the t_α's, for well-chosen α's.

Definition 4.9. *Let X be a nonempty G-affine space. An affine automorphism of the shape*

$$\begin{array}{ccc} X & \longrightarrow & X \\ x & \longmapsto & x+y-z \end{array}$$

for some $y, z \in X$, will be called a translation, and simply denoted by "$y - z$". We denote by $\overrightarrow{X} \subset \mathrm{Aut}(X)$ the (abelian) subgroup of translations. It comes naturally equipped with the structure of a (G, A)-module.

Remark 4.10. We have $y - z = y' - z' \in \overrightarrow{X}$ iff $y - z + z' = y' \in X$.

Lemma 4.11. *Let X be an nonempty G-affine space over A. Then X is naturally endowed with the structure of a $(G, \overrightarrow{X})$-torsor.*
Conversely, let M be a (G, A)-module, and let X be a (G, M)-torsor. Then, X is naturally endowed with the structure of a (nonempty) G-affine space over A, having $\overrightarrow{X} = M$.

Proof. This is clear. □

The next Lemma is an adaptation of the usual construction, in classical real affine geometry, which provides a canonical embedding of an n-dimensional affine space, as an affine hyperplane inside an $(n + 1)$-dimensional vector space.

Lemma 4.12 ("Modulification" of a nonempty affine space).
Let

$$\mathcal{E} : 0 \longrightarrow M \longrightarrow N \xrightarrow{\pi} A \longrightarrow 0$$

be an exact sequence of (G, A)-modules. Then

$$X := \pi^{-1}(1)$$

is a nonempty G-affine space over A, with $\overrightarrow{X} = M$.
Conversely, given a nonempty G-affine space X over A, there exists a canonical exact sequence of (G, A)-modules

$$\mathcal{E}(X) : 0 \longrightarrow \overrightarrow{X} \longrightarrow E(X) \xrightarrow{\pi} A \longrightarrow 0,$$

together with a canonical isomorphism of G-affine spaces

$$X \simeq \pi^{-1}(1).$$

Proof. The first assertion is clear. The second one is less obvious. We put

$$E(X) := (X \times A \times \overrightarrow{X})/\sim,$$

where the equivalence relation $\sim$ is given by

$$(x, \alpha, y - z) \sim (x', \alpha', y' - z')$$

if and only if $\alpha = \alpha'$ and

$$\alpha x - \alpha x' + y = y' - z' + z \in X.$$

The (class of the) element $(x, \alpha, y - z)$ is then understood as "$\alpha x + y - z \in E(X)$". Addition is defined by

$$(x, \alpha, y - z) + (x', \alpha', y' - z') = (x, \alpha + \alpha', \alpha'(x' - x) + y + y' - z - z').$$

Muliplication by scalars is given by

$$\beta.(x, \alpha, y - z) := (x, \beta\alpha, \beta(y - z)).$$

The G-action is defined in the obvious way- as well as the extension $\mathcal{E}(X)$. □

Definition 4.13 (Restriction and Extension of scalars, for affine spaces). *Let $S' = \mathrm{Spec}(A')$ be another affine G-scheme and $F : A \longrightarrow A'$ a G-equivariant morphisms of rings.*

i) Let X' be a G-affine space over A'. We denote by $(X')_{|f}$ the G-affine space over A obtained from X', using F to restrict scalars.

ii) Let X be a non-empty G-affine space over A. We denote by

$$X \otimes_A A' := (\pi \otimes \mathrm{Id}_{A'})^{-1}(1)$$

the G-affine space over A' associated to the exact sequence

$$\mathcal{E}(X) \otimes_A A' : 0 \longrightarrow \overrightarrow{X} \otimes_A A' \longrightarrow E(X) \otimes_A A' \xrightarrow{\pi} A' \longrightarrow 0.$$

We thus have $\overrightarrow{X \otimes_A A'} = \overrightarrow{X} \otimes_A A'$. If $X = \varnothing$, we set $X \otimes_A A' = \varnothing$.

Remark 4.14. Extension of scalars is left adjoint to restriction of scalars, for affine maps.

The previous Definitions can clearly be sheafified, in the usual fashion. We briefly explain how.

Definition 4.15. *Let $S = \mathrm{Spec}(A)$ be an affine G-scheme. Let X be a G-affine space over A. We denote by $\tilde{X}$ the G-sheaf on S*

$$U \mapsto X \otimes_A \mathcal{O}_S(U).$$

For each G-invariant open $U \subset X$, $\tilde{X}(U)$ is thus a G-affine space over $\mathcal{O}_S(U)$.

Definition 4.16. *Let S be a G-scheme.*
A G-affine space over S is the data of a G-sheaf

$$\mathcal{X} : U \mapsto \mathcal{X}(U),$$

with values in the category of G-affine spaces, such that the following holds.

i) For all G-invariant open $U \subset S$, $\mathcal{X}(U)$ is a G-affine space over $\mathcal{O}_S(U)$.

ii) For all G-invariant opens $V \subset U \subset S$, the morphism

$$\mathcal{X}(\rho_{V,U}) : \mathcal{X}(U) \longrightarrow \mathcal{X}(V)$$

is a G-equivariant affine morphism, where $\mathcal{X}(V)$ is considered as a G-affine space, via change of rings through the restriction $\rho_{V,U} : \mathcal{O}_S(U) \longrightarrow \mathcal{O}_S(V)$.

iii) Each $s \in S$ has an open affine G-invariant neighborhood $U = \mathrm{Spec}(A)$, such that $\mathcal{X}_{|U}$ is isomorphic to $\tilde{X}$, for some G-affine space X over A.

The G-affine space $\mathcal{X}$ over S is said to be everywhere nonempty, if each point $s \in S$ has a G-invariant open neighborhood U, with $\mathcal{X}(U) \neq \emptyset$. In this case, there exists a unique $(G, \mathcal{O}_S)$-Module M, such that $M(U) = \overrightarrow{\mathcal{X}(U)}$, for all G-invariant open subsets $U \subset S$. We denote this M by $\overrightarrow{\mathcal{X}}$.

Definition 4.17. *Let S be a G-scheme, and let M be a $(G, \mathcal{O}_S)$-Module over S. A (G, M)-torsor (over S) is a G-affine space $\mathcal{X}$ over S, everywhere nonempty, together with an isomorphism of $(G, \mathcal{O}_S)$-Modules $\overrightarrow{\mathcal{X}} \xrightarrow{\sim} M$.*

4.9. Twisting 1-extensions. Recall that S denotes a G-scheme.

Definition 4.18. *Let E and M be $(G, \mathcal{O}_S)$-Modules. A (left) action of M on E is a G-equivariant morphism*

$$M \longrightarrow \underline{\mathrm{Aut}}_{\mathcal{O}_S}(E),$$

between G-sheaves with values in $G - \mathbf{Grp}$.

Example 4.19. Let M be a $(G, \mathcal{O}_S)$-Module over S. Then, M acts on

$$E := M \bigoplus \mathcal{O}_S,$$

by the formula (on functors of points)

$$x.(y, \lambda) = (y + \lambda x, \lambda),$$

for all $x, y \in M$, and all $\lambda \in \mathcal{O}_S$.
This example deserves to be compared to "an exponential series, truncated in degree 2", thinking of $1 + x$ as e^x.

Let $m \geq 1$ be an integer. Let E and M be $(G, \mathcal{O}_S)$-Modules over S. Assume given an action of M on E. Let P be a (G, M)-torsor over S. Then, one can form the twisted $(G, \mathcal{O}_S)$-Module E^P, through the "usual twisting process". We briefly explain how.
Assume first that $S = \mathrm{Spec}(A)$ is affine. View M and E as A-modules, equipped with a semilinear action of G. We put

$$E^P := (P \times E)/M.$$

Here, the quotient is taken with respect to the natural diagonal action of M, identifying $(x.m, e)$ and $(x, m.e)$, for all $e \in E$, $m \in M$ and $x \in P$. It is a set, equipped with an action of G, inherited from the diagonal action of G on $P \times E$. Temporarily forgetting the action of G, it is easily shown that there is a unique structure of an A-module on E^P such that, for any $b \in P$, the map

$$\begin{array}{ccc} E & \longrightarrow & E^P \\ e & \longmapsto & \overline{(b, e)} \end{array}$$

is an isomorphism of A-modules.
We then see that the natural action of G on E^P occurs through semilinear automorphisms. The case S arbitrary follows by gluing, using the fact that affine G-invariant opens of S form a basis of the G-topology of S.

Twisting is functorial. More precisely, let

$$f : E \longrightarrow E'$$

be an M-equivariant homomorphism between $(G, \mathcal{O}_S)$-Modules, equipped with an action of M.
Twisting by the (G, M)-torsor P then yields a morphism of $(G, \mathcal{O}_S)$-Modules

$$f^P : E^P \longrightarrow {E'}^P.$$

The twist E^P is canonically isomorphic to E, in each of the following cases.

i) The (G, M)-torsor P is equal to M, the trivial torsor.

ii) The action of M on E is trivial.

We can now precisely formulate an equivalence of categories, linking 1-extensions of $\mathcal{O}_S$ by M to (G, M)-torsors. It is a "sheafification" of Lemma 4.12.

Proposition 4.20. *Let S be a G-scheme. Let M be a $(G,\mathcal{O}_S)$-Module over S. Let*

$$\mathcal{E} : 0 \longrightarrow M \longrightarrow E \xrightarrow{\pi} \mathcal{O}_S \longrightarrow 0$$

be an exact sequence of $(G,\mathcal{O}_S)$-Modules. Then, the assignment

$$U \mapsto \pi^{-1}(1) \subset H^0(U,E),$$

for every G-invariant open $U \subset S$, defines a (G,M)-torsor over S. We denote it by $X(\mathcal{E})$.
Conversely, let P be a (G,M)-torsor over S. Consider the trivial extension

$$\mathcal{E}_0 : 0 \longrightarrow M \xrightarrow{i} M \bigoplus \mathcal{O}_S \xrightarrow{\pi} \mathcal{O}_S \longrightarrow 0.$$

Equip M and $\mathcal{O}_S$ with the trivial action of M, and $M \bigoplus \mathcal{O}_S$ with the action of M given in Example 4.19. The arrows i and π are then M-equivariant, and we denote by $\mathcal{E}(P)$ the twisted extension

$$\mathcal{E}_0^P : 0 \longrightarrow M \xrightarrow{i^P} E(P) := (M \bigoplus \mathcal{O}_S)^P \xrightarrow{\pi^P} \mathcal{O}_S \longrightarrow 0.$$

The assignments

$$\mathcal{E} \mapsto X(\mathcal{E})$$

and

$$P \mapsto \mathcal{E}(P)$$

are mutually inverse equivalences of categories, from $\mathbf{YExt}^1_{(G,\mathcal{O}_S)-Mod}(\mathcal{O}_S, M)$ to the category of (G,M)-torsors over S.

Proof. This is done in Lemma 4.12 if S is affine. The general case follows by glueing. □

4.10. Representability of torsors under G-vector bundles.

Definition 4.21. *Let V be a vector bundle over a scheme S. We set*

$$\mathbb{A}(V) := \mathrm{Spec}(\mathrm{Sym}_{\mathcal{O}_S}(V^\vee)) \longrightarrow S.$$

It is the affine space associated to V. It represents the functor of points of V: for each morphism of schemes $T \longrightarrow S$, we have

$$\mathbb{A}(V)(T) = H^0(T, V \otimes_{\mathcal{O}_S} \mathcal{O}_T).$$

Definition 4.22. *Let*

$$\mathcal{E} : 0 \longrightarrow V \xrightarrow{i} E \xrightarrow{\pi} \mathcal{O}_S \longrightarrow 0$$

be an extension of vector bundles, over a scheme S.
We denote its dual extension by

$$\mathcal{E}^\vee : 0 \longrightarrow \mathcal{O}_S \xrightarrow{\pi^\vee} E^\vee \xrightarrow{i^\vee} V^\vee \longrightarrow 0.$$

For $n \geq 1$, we then define the n-th symmetric power of $\mathcal{E}^\vee$ as

$$\mathrm{Sym}^n(\mathcal{E}^\vee) : 0 \longrightarrow \mathrm{Sym}^{n-1}(E^\vee) \xrightarrow{\times \pi^\vee} \mathrm{Sym}^n(E^\vee) \xrightarrow{\mathrm{Sym}^n(i^\vee)} \mathrm{Sym}^n(V^\vee) \longrightarrow 0.$$

Remark 4.23. The extension $\mathrm{Sym}^n(\mathcal{E}^\vee)$ as above, is the global version of the following local construction. For a commutative ring A, denote by $A[X_0, X_1, \ldots, X_d]_n$ the space of polynomials with coefficients in A, in $d+1$ variables, homogeneous of degree n. Then, we have an exact sequence of free A-modules

$$0 \longrightarrow A[X_0, X_1, \ldots, X_d]_{n-1} \xrightarrow{\times X_0} A[X_0, X_1, \ldots, X_d]_n \xrightarrow{X_0=0} A[X_1, \ldots, X_d]_n \longrightarrow 0.$$

Indeed, this is the particular case where $S = \mathrm{Spec}(A)$, $E = \mathcal{O}_S^{d+1}$, and π is the projection on the first factor.

The next Lemma will create no big surprise, but is very important: a key tool, in the proof of Theorem B, indeed consists in performing changes of the base, to appropriate G-affine spaces– splitting schemes of extensions of G-vector bundles.

Proposition 4.24. *Let V be a G-vector bundle over a G-scheme S. Let X be a (G, V)-torsor over S. Then, X is represented by a G-scheme, affine over S. Slightly abusing notation, we still denote this G-scheme by $X \longrightarrow S$.*

If X corresponds to an extension (of G-vector bundles over S)

$$\mathcal{E} : 0 \longrightarrow V \xrightarrow{i} E \xrightarrow{\pi} \mathcal{O}_S \longrightarrow 0,$$

then this (G, S)-scheme is the scheme of sections of π.
It is an affine subspace of $\mathbb{A}(E)$, having $\mathbb{A}(V)$ as its space of translations. As such, it is the Spec *of the filtered $(G, \mathcal{O}_S)$-Algebra*

$$\varinjlim(\mathrm{Sym}^n(E^\vee)),$$

where the limit is taken with respect to the injections of the natural exact sequences

$$\mathrm{Sym}^n(\mathcal{E}^\vee) : 0 \longrightarrow \mathrm{Sym}^{n-1}(E^\vee) \xrightarrow{\times \pi^\vee} \mathrm{Sym}^n(E^\vee) \xrightarrow{\mathrm{Sym}^n(i^\vee)} \mathrm{Sym}^{n+1}(V^\vee) \longrightarrow 0.$$

Proof. This follow from the observation that

$$X \subset \mathbb{A}(E)$$

is the closed subscheme given by the single affine equation

$$\pi^\vee = 1.$$

□

5. Recollections on G-W Modules, $(G, \mathbf{W}_r)$-affine spaces and (G, S)-cohomology.

We shall need the G-equivariant version of the notions of W-Modules and, especially, of Witt vector bundles, as introduced in [8]. Teichmüller lifts of line bundles will play a decisive rôle. For the convenience of the reader, we recall these notions below. They give rise to a bunch of algebro-geometric structures, over Witt vectors $\mathbf{W}_r$. We mainly focus in finite depth $r < \infty$– actually, $r = 2$ is sufficient for our purposes. Most structures, in depth $r = \infty$ (i.e. over $\mathbf{W}_\infty = \mathbf{W}$), are simply "compatible structures over $\mathbf{W}_r$, for all $r \geq 1$", through the following general construction.

For each integer $r \geq 1$, let $\mathcal{S}_r$ be a category, consisting of algebro-geometric structures over $\mathbf{W}_r$. For intance, $\mathcal{S}_r$ may be $(G, \mathbf{W}_r)$-affine spaces over a given $(G, \mathbb{F}_p)$-scheme S, or Yoneda n-extensions of $(G, \mathbf{W}_r)$-bundles over S. Assume that there are natural reduction arrows (functors) $\rho_r : \mathcal{S}_r \longrightarrow \mathcal{S}_{r-1}$. This is the case in the previous examples. Then, we define a category

$$\mathcal{S}_\infty = \varprojlim \mathcal{S}_r$$

as follows. An object of $\mathcal{S}_\infty$ is, by definition, the data of an object $X_r \in \mathcal{S}_r$ for all $r \geq 1$, together with compatibility isomorphisms

$$\phi_r : \rho_r(X_r) \xrightarrow{\sim} X_{r-1},$$

for all $r \geq 2$. An arrow

$$(X_r, \phi_r) \longrightarrow (X'_r, \phi'_r)$$

is a collection of arrows $f_r : X_r \longrightarrow X'_r$, with the obvious commutation conditions. A concrete instance of this general construction appears in Definition 5.3, with

$$\mathcal{S}_r = \{(G, \mathbf{W}_r) - \text{bundles over S}\},$$

where S is a $(G, \mathbb{F}_p)$-scheme S.

Keeping in mind that focusing on finite depth is sufficient for our proof of the Smoothness Theorem provided in [7], we move on to the main definitions.

Definition 5.1 ($(G, \mathbf{W}_r)$-Module, $(G, \mathbf{W}_r)$-bundle, $(G, \mathbf{W}_r)$-affine space and (G, M)-torsor over S).
Let S be a $(G, \mathbb{F}_p)$-scheme. Pick $r \in \mathbb{N}_* \cup \{\infty\}$. Recall that $\mathbf{W}_r(S)$ is a G-scheme, equipped with its Frobenius

$$\mathrm{Frob} : \mathbf{W}_r(S) \longrightarrow \mathbf{W}_r(S),$$

lifting the (absolute) Frobenius of S.
A $(G, \mathbf{W}_r)$-Module $\mathcal{M}$ over S is a $\mathbf{W}_r(\mathcal{O}_S)$-module, equipped with a semi-linear action of G.
If $\mathcal{M}$ is locally free of finite rank as a $\mathbf{W}_r$-bundle, we shall say that $\mathcal{M}$ is a $(G, \mathbf{W}_r)$- bundle over S.

In case mentionning r is superfluous, a $(G, \mathbf{W}_r)$-Module over S is simply referred to as a G-Witt (or G-W) Module over S.

Similarly, a $(G, \mathbf{W}_r)$-affine space over S is, by definition, a G-affine space over $\mathbf{W}_r(S)$. If $\mathcal{M}$ is a $(G, \mathbf{W}_r)$-module over S, a $(G, \mathcal{M})$-torsor is defined as in 4.17, where $\mathcal{M}$ is viewed as a $(G, \mathcal{O}_{\mathbf{W}_r(S)})$-Module.

If $\mathcal{M}$ is a $(G, \mathbf{W}_r)$-module over S, Proposition 4.20 implies that the category of $(G, \mathcal{M})$-torsors is equivalent to the category

$$\mathbf{YExt}^1_{(G, \mathbf{W}_r(\mathcal{O}_S))-Mod}(\mathbf{W}_r(\mathcal{O}_S), \mathcal{M}).$$

Definition 5.2. *((G, S)-cohomology)*
Let S be a $(G, \mathbb{F}_p)$-scheme, and let $r \in \mathbb{N}_* \cup \{\infty\}$.
Let $\mathcal{M}$ be a $(G, \mathbf{W}_r)$-Module over S.
For $n \geq 0$, we set

$$H^n((G, S), \mathcal{M}) := \mathrm{YExt}^n_{(G, \mathbf{W}_r(\mathcal{O}_S))-Mod}(\mathbf{W}_r(\mathcal{O}_S), \mathcal{M}).$$

In particular, $H^1((G, S), \mathcal{M})$ is the abelian group formed by isomorphism classes of $(G, \mathcal{M})$-torsors over S.

Definition 5.3 (Lifting $(G,\mathbf{W}_r)$-bundles).
Let $\mathcal{M}_r$ be a $(G,\mathbf{W}_r)$-bundle over S. Pick an integer $s \geq r$.
A lifting of $\mathcal{M}_r$ to p^s-torsion, is the data of a $(G,\mathbf{W}_s)$-bundle $\mathcal{M}_s$ over S, together with an isomorphism of $(G,\mathbf{W}_r)$-bundles

$$\mathcal{M}_s \otimes_{\mathbf{W}_s} \mathbf{W}_r \xrightarrow{\sim} \mathcal{M}_r.$$

If specifying an isomorphism is not necessary, we simply say that $\mathcal{M}_r$ lifts to $\mathcal{M}_s$.
We say that $\mathcal{M}_r$ lifts completely if $\mathcal{M}_r$ admits a compatible system of liftings, i.e. for every $s > r$, a $(G,\mathbf{W}_s)$-bundle $\mathcal{M}_s$ is given, together with isomorphisms

$$\mathcal{M}_{s+1} \otimes_{\mathbf{W}_{s+1}} \mathbf{W}_s \xrightarrow{\sim} \mathcal{M}_s.$$

5.1. Scheme of sections of an extension of $(G,\mathbf{W}_r)$-bundles.

Given an $(\mathbb{F}_p, G)$-scheme S, Proposition 4.24 can be generalized to the context of $(G,\mathbf{W}_r)$-bundles over S, as follows.

Definition 5.4. *Let $r \geq 1$ be an integer, and let*

$$\mathcal{E}_r : 0 \longrightarrow V_r \xrightarrow{i_r} E_r \xrightarrow{\pi_r} \mathbf{W}_r(\mathcal{O}_S) \longrightarrow 0$$

be an extension of $(G,\mathbf{W}_r)$-bundles over S.
We consider the functor

$$\begin{array}{llll}\Phi_r(=\Phi_r(\mathcal{V}_r)): & \{(G,S)-Sch\} & \longrightarrow & \{G-Sets\} \\ & (t:T\longrightarrow S) & \longmapsto & \{\sigma_r : \mathbf{W}_r(\mathcal{O}_T) \to t^*(E_r),\ \text{s.t. } \pi_r\circ\sigma_r = \mathrm{Id}_{\mathbf{W}_r(\mathcal{O}_T)}\}.\end{array}$$

It is the functor of sections of π_r.

Proposition 5.5. *The functor Φ_r is representable, by a G-scheme*

$$\mathbb{S}_r(\mathcal{E}_r) \xrightarrow{g_r} S,$$

the scheme of sections of $\mathcal{E}_r$. It is naturally presented as a composite

$$\mathbb{S}_r(\mathcal{E}_r) = X_r \xrightarrow{h_r} X_{r-1} \xrightarrow{h_{r-1}} \dots \xrightarrow{h_2} X_1 \xrightarrow{g_1} S.$$

The morphism g_1 is the G-scheme of sections of the mod p reduction

$$\mathcal{E}_1 : 0 \longrightarrow V_1 \xrightarrow{i_1} E_1 \xrightarrow{\pi_1} \mathcal{O}_S \longrightarrow 0,$$

as constructed in Proposition 4.24.
The morphism $h_i : X_i \longrightarrow X_{i-1}$ is a $(G, V_1^{(i-1)})$-torsor.

Proof. The functor Φ_r is represented by the Greenberg transfer

$$\mathbf{R}_{\mathbf{W}_r/\mathbf{W}_1}(\mathbb{S}(\mathcal{E}_r) \longrightarrow \mathbf{W}_r(S)) \longrightarrow S.$$

Here $\mathbb{S}(\mathcal{E}_r) \longrightarrow \mathbf{W}_r(S)$ denotes the scheme of sections of $\mathcal{E}_r$, viewed as an extension of G-vector bundles over $\mathbf{W}_r(S)$ (see Proposition 4.24). The rest of the statement follows from Greenberg's structure theorem (see [1]). It can be concretely presented as follows. Over

$$X_1 := \mathbb{S}(\mathcal{E}_1) \longrightarrow S,$$

the extension $\mathcal{E}_1$ acquires a canonical section

$$\sigma_1 \in H^0(X_1, E_1).$$

We want to lift σ_1 to a section σ_2 of the mod p^2 reduction of $\mathcal{E}_r$, reading as

$$\mathcal{E}_2 : 0 \longrightarrow V_2 \xrightarrow{i_2} E_r \xrightarrow{\pi_2} \mathbf{W}_2(\mathcal{O}_S) \longrightarrow 0.$$

The space of such σ_2's is naturally a $(G, V_1^{(1)})$-torsor, which we denote by

$$h_2 : X_2 \longrightarrow X_1.$$

Over X_2, $\mathcal{E}_2$ acquires a canonical section σ_2. Then, we iterate, lifting σ_2 to σ_3, and so forth. □

5.2. Teichmüller lift of a line bundle. As shown in [8, §3], the multiplicative section for Witt vectors provides a compatible system of liftings, for G-line bundles over S. Its main properties are gathered in the next Proposition, proved in *loc. cit.*.

Proposition 5.6. *Let S be a $(G, \mathbb{F}_p)$-scheme. Let L be a G-line bundle over S. For any $r \geq 1$, there exists a canonical lift of L to a $(G, \mathbf{W}_r)$-line bundle over S.*

It is the r-th Teichmüller lift of L, denoted by $\mathbf{W}_r(L)$. Teichmüller lifts of L are compatible, in the following sense.

1) We have $\mathbf{W}_1(L) = L$.
2) For all $s \geq r \geq 1$, we have a natural exact sequence (of G-W Modules over S)

$$0 \longrightarrow (\mathrm{Frob}^r)_*(\mathbf{W}_{s-r}(L^{\otimes p^r})) \longrightarrow \mathbf{W}_s(L) \overset{\pi_{s,r,L}}{\longrightarrow} \mathbf{W}_r(L) \longrightarrow 0.$$

Furthermore, the surjection $\pi_{s,r,L}$ admits a canonical (non-linear, sheaf-theoretic, G-equivariant) section- its Teichmüller section. We denote it by $\tau_{s,r,L}$, or simply by τ_L. It is obtained by twisting the "usual" Teichmüller section, by the $\mathbb{G}_m$-torsor associated to L.

6. Cyclotomic pairs and smooth profinite groups.

6.1. (n,e)-cyclotomic pairs. We set

$$\mathbb{Z}/p^\infty\mathbb{Z} := \mathbb{Z}_p.$$

We endow $\mathbb{Z}_p$-modules of finite-type with the p-adic topology.

Definition 6.1. *Let G be a profinite group. Let $e \in \mathbb{N}^* \cup \{\infty\}$ be a number. A $(\mathbb{Z}/p^e\mathbb{Z}, G)$-module $\mathcal{M}$ is a $\mathbb{Z}/p^e\mathbb{Z}$-module of finite type, endowed with a continuous action of G. (In case $e < \infty$, the action is thus naive.)*

For an integer $1 \leq f \leq e$ and a $(\mathbb{Z}/p^e\mathbb{Z}, G)$-module $\mathcal{M}$, we put

$$\mathcal{M}/p^f := \mathcal{M} \otimes_{\mathbb{Z}_p} (\mathbb{Z}/p^f\mathbb{Z}),$$

and we denote by

$$\pi_{e,f} : \mathcal{M} \longrightarrow \mathcal{M}/p^f$$

the quotient map.

Definition 6.2. *Let $n \geq 1$ and $e \in \mathbb{N}^* \cup \{\infty\}$. Let $\mathcal{T}$ be a $(\mathbb{Z}/p^{e+1}\mathbb{Z}, G)$-module, free of rank one as a $\mathbb{Z}/p^{e+1}\mathbb{Z}$-module. We say that the pair $(G, \mathcal{T})$ is (n,e)-cyclotomic if, for every open subgroup $H \in G$, the morphism*

$$H^n(H, \mathcal{T}^{\otimes n}) \longrightarrow H^n(H, (\mathcal{T}/p)^{\otimes n}),$$

induced by $\pi_{e+1,1}$, is surjective. The integer e is then called the depth of the cyclotomic pair.

Remark 6.3. By a limit argument, "open" may be replaced by "closed" in the preceding definition.

Remark 6.4. Let $\mathcal{T}$ be a $(\mathbb{Z}/p^{e+1}\mathbb{Z}, G)$-module, free of rank one as a $\mathbb{Z}/p^{e+1}\mathbb{Z}$-module. Let $G_1 \subset G$ be an open subgroup of prime-to-p index. Then, the pair $(G, \mathcal{T})$ is (n, e)-cyclotomic if, and only if, the pair $(G_1, \mathcal{T})$ is (n, e)-cyclotomic, by a usual restriction/corestriction argument.
In particular, we can take G_1 to be the kernel of the multiplicative character

$$\chi_1 : G \longrightarrow \mathbb{F}_p^\times,$$

giving the action of G on $\mathcal{T}/p$. By doing so, we can reduce many problems to the case where $\mathcal{T}/p \simeq \mathbb{F}_p$ is equipped with the trivial action of G.

Remark 6.5. Let $(G, \mathcal{T})$ be an (n, e)-cyclotomic pair. Then, for every integer f, $1 \leq f < e + 1$, and for every open subgroup $H \in G$, the arrow

$$H^n(H, \mathcal{T}^{\otimes n}) \longrightarrow H^n(H, (\mathcal{T}/p^f)^{\otimes n})$$

is surjective. The proof is by induction on f, using the exact sequences

$$0 \longrightarrow \mathcal{T}/p^f \xrightarrow{\times p} \mathcal{T}/p^{f+1} \longrightarrow \mathcal{T}/p \longrightarrow 0.$$

If $(G, \mathcal{T})$ is a (n, e)-cyclotomic pair, then $\mathcal{T}$ is given by a continuous character

$$\chi : G \longrightarrow (\mathbb{Z}/p^{e+1}\mathbb{Z})^\times,$$

which is the analogue of the usual cyclotomic character in number theory. Pulling this analogy further, we set, for any integer $i \geq 1$,

$$\mathbb{Z}/p^{e+1}\mathbb{Z}\,(i) := \mathcal{T}^{\otimes^i_{\mathbb{Z}_p}},$$

and for any $\mathbb{Z}/p^{e+1}\mathbb{Z}$-module $\mathcal{M}$, we put

$$\mathcal{M}(i) := \mathcal{M} \otimes_{\mathbb{Z}_p} \mathbb{Z}/p^{e+1}\mathbb{Z}\,(i).$$

This is the notation for "cyclotomic twists".

Example 6.6. Let F be a field of characteristic not p. Let $G = Gal(F_{sep}/F)$ be the Galois group associated to a separable closure F_s/F. Let

$$\mu := \varprojlim_r \mu_{p^r}$$

be the Tate module of roots of unity of p-primary order. It is a free $\mathbb{Z}_p$-module of rank one, equipped with a continuous action of G. Kummer theory implies that the pair (G, μ) is $(1, \infty)$-cyclotomic. As explained in the introduction, the statement of the Bloch-Kato conjecture is equivalent to (G, μ) being $(n, 1)$-cyclotomic, for every $n \geq 1$. Other fundamental examples of cyclotomic pairs are given in [5, §4].

We conclude this section with an instructive exercise.

Exercise 6.7. Assume that $p = 2$. The goal is to present a group-theoretic version of the famous identity

$$(x) \cup (x) = (-1) \cup (x) \in H^2(F, \mathbb{Z}/2),$$

valid for every $x \in F^\times$, with F a field of characteristic not 2.

(1) Let G be a profinite group. Let

$$\chi : G \longrightarrow \{1, -1\} (\simeq \mathbb{F}_2)$$

be a character of G. Denote by $\mathbb{Z}/4(\chi)$ the group $\mathbb{Z}/4$, on which G act via χ. Let

$$\mathcal{E}_1 : 0 \longrightarrow \mathbb{Z}/2 \longrightarrow E_1 \longrightarrow \mathbb{Z}/2 \longrightarrow 0$$

be an extension of $(\mathbb{F}_2, G)$-modules, with class $e_1 \in H^1(G, \mathbb{F}_2)$. Assume that $\mathcal{E}_1$ lifts to an extension of $(\mathbb{Z}/4, G)$-modules

$$\mathcal{E}_2 : 0 \longrightarrow \mathbb{Z}/4(\chi) \longrightarrow E_2 \longrightarrow \mathbb{Z}/4 \longrightarrow 0.$$

Show that the identity

$$e_1 \cup e_1 = \chi \cup e_1 \in H^2(G, \mathbb{F}_2)$$

holds.

(2) How does (1) generalize the famous identity above, to the context of cyclotomic pairs?

(3) State and prove the analogue of the identity above when p is odd, for a $(1,1)$-cyclotomic pair $(G, \mathbb{Z}/p^2(1))$.

6.2. (n, e)-SMOOTH PROFINITE GROUPS. We now proceed to state our *new* definition of smooth profinite groups. We provide, in sections 11 and 12, several equivalent definitions of smoothness, which will be used in the next parts of this work.

DEFINITION 6.8 (Smooth profinite group).
Let $n \geq 1$ and $e \in \mathbb{N}^* \cup \{\infty\}$. A profinite group G is said to be (n, e)-smooth if the following lifting property holds.
Let A be a perfect $\mathbb{F}_p$-algebra equipped with a (naive) action of G. Let L_1 be a locally free A-module of rank one, equipped with a semi-linear (naive) action of G. Let

$$c \in H^n(G, L_1)$$

be a cohomology class. Then, there exists a lift of L_1, to a $(\mathbf{W}_{e+1}(A), G)$-module $L_{e+1}[c]$, locally free of rank one as a $\mathbf{W}_{e+1}(A)$-module (and depending on c), such that c belongs to the image of the natural map

$$H^n(G, L_{e+1}[c]) \longrightarrow H^n(G, L_1).$$

7. THE LAURENT EXTENSION OF A CYCLOTOMIC PAIR.

Let F be a field of characteristic zero, with absolute Galois group Γ. It is then standard that the absolute Galois group of the field of Laurent power series $F((t))$ is the semi-direct product $\hat{\mathbb{Z}}(1) \rtimes \Gamma$. Extending this construction to cyclotomic pairs is natural, as residues play an important role in several reductions of the Bloch-Kato conjecture.

DEFINITION 7.1. *Let $(G, \mathbb{Z}_p(1))$ be a $(1, \infty)$-cyclotomic pair. We put*

$$G((t)) := \mathbb{Z}_p(1) \rtimes G.$$

We call $G((t))$ the Laurent extension of G, w.r.t. $\mathbb{Z}_p(1)$. We can view $\mathbb{Z}_p(1)$ as a $G((t))$-module, via the natural surjection $G((t)) \longrightarrow G$. The formula

$$\begin{array}{ccc} G((t)) & \longrightarrow & \mathbb{Z}_p(1) \\ (x,g) & \longmapsto & x \end{array}$$

defines a 1-cocycle, whose cohomology class we denote by

$$(t) \in H^1(G((t)), \mathbb{Z}_p(1)).$$

The next Proposition follows from [25, Theorem 3.11]. For completeness, we give a proof.

Proposition 7.2. *Let $(G, \mathbb{Z}_p(1))$ be a $(1,\infty)$-cyclotomic pair. Then, $(G((t)), \mathbb{Z}_p(1))$ is $(1,\infty)$-cyclotomic as well.*

Proof. Denote by $\pi : G((t)) \longrightarrow G$ the natural surjection.
Let $H \subset G((t))$ be an open subgroup, and let $c \in H^1(H, \mathbb{F}_p(1))$ be a cohomology class. We want to lift c to $H^1(H, \mathbb{Z}_p(1))$. Replacing G by $\pi(H)$, we can assume that $\pi(H) = G$.
Put

$$H_0 := H \cap \mathbb{Z}_p(1) \subset \mathbb{Z}_p(1) \subset G((t)).$$

If $H_0 = 1$, then $\pi_{|H} : H \longrightarrow G$ is an isomorphism, and the claim is obvious, using that $(G, \mathbb{Z}_p(1))$ is a $(1,\infty)$-cyclotomic pair.
Otherwise, we have $H_0 = p^f \mathbb{Z}_p(1)$ for some $f \geq 0$. Consider the factor group

$$H/H_0 \subset \mathbb{Z}/p^f(1) \rtimes G.$$

The arrow π induces an isomorphism $H/H_0 \xrightarrow{\sim} G$, giving rise to a 1-cocycle

$$c_g : G \longrightarrow \mathbb{Z}/p^f(1),$$

such that the map

$$\begin{array}{ccc} G & \longrightarrow & H/H_0 \\ g & \longmapsto & (c_g, g) \end{array}$$

is bijective. Since $(G, \mathbb{Z}_p(1))$ is $(1,\infty)$-cyclotomic, c_g lifts to a 1-cocycle

$$C_g : G \longrightarrow \mathbb{Z}_p(1),$$

giving rise to a section of $\pi_{|H} : H \longrightarrow G$. Consequently, H is isomorphic to the semi-direct product $p^f \mathbb{Z}_p(1) \rtimes G \simeq \mathbb{Z}_p(1) \rtimes G$. We are thus reduced to the case $H = G((t))$. Then, consider the class

$$c_0 := Res^{\mathbb{Z}_p(1)}_{G((t))}(c) \in H^1(\mathbb{Z}_p(1), \mathbb{F}_p(1)) = \mathbb{F}_p.$$

If $c_0 = 0$, then c is inflated from $H^1(G, \mathbb{F}_p(1))$ via π, and its liftability follows. If $c_0 \neq 0$, rescaling, we can assume $c_0 = 1 \in \mathbb{F}_p$. Replacing c by $c - (t)$, we are sent back to the case $c_0 = 0$. □

Remark 7.3. The analogue of the preceding Proposition, in finite depth $e \in \mathbb{N}$, does not hold.

Proposition 7.4. *(Residues)*
Let $(G, \mathbb{Z}_p(1))$ be a $(1,\infty)$-cyclotomic pair. Then, for a positive integer n, an $(\mathbb{F}_p, G)$-module M and an integer k, we have a natural exact sequence

$$0 \longrightarrow H^n(G, M(k)) \longrightarrow H^n(G((t)), M(k)) \longrightarrow H^{n-1}(G, M(k-1)) \longrightarrow 0.$$

It is split by $x \mapsto x \cup (t)$.

Proof. The proof is the same as for residues in Galois cohomology (see [16, Corollary 6.8.8]). □

8. Lifting $(G, \mathbf{W}_r(L)(1))$-torsors.

8.1. Why cohomology with $\mathbf{W}_r(L)$-coefficients? Let S be a $(G, \mathbb{F}_p)$-scheme, let L be a G-line bundle over S, and let $r \geq 1$ be an integer. The $(G, \mathbf{W}_r(L)(1))$-torsors on S are suitable for many applications in algebraic and arithmetic geometry, as follows.
Let X be a (smooth, geometrically integral) variety over a field F, of characteristic $\neq p$. Denote by $G = \pi_1(X)$ "the" étale fundamental group of X, and by $\mathbb{Z}_p(1)$ the usual Tate module. Then, the machinery provided by the groups

$$H^i((G,S), \mathbf{W}_r(L)(j)),$$

for various $(G, \mathbb{F}_p)$-schemes S and G-line bundles L over them, is thought of as

$$\text{“}H^i_{et}(X, \mathbf{W}_r(L)(j))''$$

with L is a system of mod p coefficients of purely multiplicative nature, broadly extending the notion of rank one $\mathbb{F}_p$-local system on X. This analogy can be made very accurate– especially if X is a $K(\pi, 1)$.
Applying our point of view to algebraic geometry amounts to performing subtle geometric operations on the level of the coefficients of the desired cohomology, instead of doing them on the variety X itself. These present similarities with Steenrod operations- except that Steenrod operations apply to cohomology groups, not to coefficients themselves. As usual, these coefficients have to be (of p-primary) torsion. This is fine, since torsion coefficients for cohomology theories are commonly accepted as the most relevant ones. The variety X then becomes almost invisible, and only subsists via its algebraic fundamental group- which is indeed, in many cases of interest, a smooth profinite group- see [5].

8.2. Lifting geometrically split extensions. In this section, n is a positive integer, $e \in \mathbb{N}^* \cup \{\infty\}$ and S denotes a $(G, \mathbb{F}_p)$-scheme. We assume that

$$(G, \mathbb{Z}/p^{1+e}(1))$$

is a (n, e)-cyclotomic pair.

Recall the notation for cyclotomic twists: if M is a $(G, \mathbf{W}_{1+e})$-Module on S, we denote by $M(n)$ the sheaf

$$U \longmapsto M(U)(n).$$

It is a $(G, \mathbf{W}_{e+1})$-module, called the n-th cyclotomic twist of M.

The next Definitions are a prerequisite for stating the main Theorems of this section. They are especially meaningful, when $n = 1$.

Definition 8.1 (Lifting cohomology). *Let S be a $(G, \mathbb{F}_p)$-scheme and L be a G-linearized line bundle over S.*
Let $1 \leq r \leq e$ be an integer and

$$c_r \in H^n((G,S), \mathbf{W}_r(L)(n))$$

be a cohomology class.

If $s \in \{r+1, ..., e+1\}$ is an integer and

$$c_s \in H^n((G,S), \mathbf{W}_s(L)(n))$$

is a cohomology class, we say that c_s lifts c_r, if c_s is sent to c_r by the map

$$H^n((G,S), \mathbf{W}_s(L)(n)) \longrightarrow H^n((G,S), \mathbf{W}_r(L)(n))$$

induced by the natural reduction arrow

$$\mathbf{W}_s(L)(n) \longrightarrow \mathbf{W}_r(L)(n),$$

between G-W Modules on S.

Accordingly, we say that a $(G, \mathbf{W}_r(L)(1))$-torsor lifts, if its cohomology class does.

Definition 8.2 (Strongly geometrically trivial classes). *Let S be a $(G, \mathbb{F}_p)$-scheme, and let*

$$\mathcal{E} : 0 \longrightarrow M_0 \longrightarrow M_1 \xrightarrow{\pi} M_2 \longrightarrow 0$$

be a short exact sequence of $(G, \mathbf{W}_r)$-modules on S.
We say that $\mathcal{E}$ is geometrically trivial (or geometrically split), if π admits an $\mathcal{O}_S$-linear (non-necessarily G-equivariant) section.

More generally, an n-extension of $(G, \mathbf{W}_r)$-modules over S

$$0 \longrightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} ... \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \longrightarrow 0$$

is strongly geometrically trivial if the following holds. Split off the extension, as a cup product of short exact sequences

$$\mathcal{E}_i : 0 \longrightarrow A_{i-1} \longrightarrow M_i \longrightarrow A_i \longrightarrow 0,$$

$i = 1, \dots, n$, given by the kernels and cokernels of the f_i's. Then, all the $\mathcal{E}_i$'s are geometrically trivial.

Accordingly, for a $(G, \mathbf{W}_r)$-module M, we say that a (G, M)-torsor, or more generally a cohomology class $c \in H^n((G,S), M)$, is strongly geometrically trivial if it can be represented by a strongly geometrically trivial n-extension of $(G, \mathbf{W}_r)$-modules

$$0 \longrightarrow M = M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} ... \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} \mathbf{W}_r(\mathcal{O}_S) \longrightarrow 0.$$

Strongly geometrically trivial classes form a subgroup

$$H^n_{sgt}((G,S), M) \subset H^n((G,S), M).$$

Remark 8.3. For $n = 1$, we have

$$H^1_{sgt}((G,S), M) = \mathrm{Ker}(H^1((G,S), M) \longrightarrow H^1(S, M)).$$

For $n \geq 2$, we have an inclusion

$$H^n_{sgt}((G,S), M) \subset \mathrm{Ker}(H^n((G,S), M) \longrightarrow H^n(S, M)),$$

which is, in general, far from being an equality.

Lemma 8.4. *Let S be an affine $(G, \mathbb{F}_p)$-scheme. Let M be a $(G, \mathbf{W}_r)$-module on S. Then, all cohomology classes are strongly geometrically trivial: we have*

$$H^n_{sgt}((G,S), M) = H^n((G,S), M).$$

Proof. Adapting the process of [9, Lemma 5.1], we can represent a given cohomology class $c \in H^n((G,S), M)$ by an n-extension of $(G, \mathbf{W}_r)$-modules on S

$$\mathcal{C} : 0 \longrightarrow M \longrightarrow M_1 \xrightarrow{f_1} ... \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} \mathbf{W}_r(\mathcal{O}_S) \longrightarrow 0,$$

where $M_2, \dots, M_n$ are $G\mathbf{W}_r$-bundles. Such an extension is strongly geometrically split. Indeed, over an affine base, short exact sequences of quasi-coherent modules, having a vector bundle as cokernel, are split. □

Proposition 8.5. *Let S be a $(G,\mathbb{F}_p)$-scheme. Let M be a $(G,\mathbf{W}_r)$-bundle on S. For all $n \geq 1$, there is a natural isomorphism*

$$\gamma : H^n(G, H^0(S,M)) \xrightarrow{\sim} H^n_{sgt}((G,S),M),$$

built through a natural algorithm given below.

Proof. Start with a class $c \in H^n(G, H^0(S,M))$. Using [9, Lemma 5.1], represent it by an n-extension of $(\mathbb{Z}/p^r, G)$-modules

$$\mathcal{C} : 0 \longrightarrow H^0(S,M) \longrightarrow E_1 \xrightarrow{g_1} ... \xrightarrow{g_{n-1}} E_n \xrightarrow{g_n} \mathbb{Z}/p^r \longrightarrow 0,$$

where $E_2, E_3, \ldots, E_n$ are free as $\mathbb{Z}/p^r$-modules. It is then straighforward to check, by descending induction on i, that $\mathrm{Ker}(g_i)$ is also free as a $\mathbb{Z}/p^r$-module, for $i = 2, \ldots, n$.

Applying $\cdot \otimes_{\mathbb{Z}/p^r} \mathbf{W}_r(\mathcal{O}_S)$ to $\mathcal{C}$ thus preserves its exactness, yielding an n-extension of $G\mathbf{W}_r$-modules on S

$$\mathcal{C}_S : 0 \longrightarrow H^0(S,M) \otimes \mathbf{W}_r(\mathcal{O}_S) \longrightarrow M_1 \xrightarrow{f_1} ... \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} \mathbf{W}_r(\mathcal{O}_S) \longrightarrow 0,$$

where $M_i := E_i \otimes \mathbf{W}_r(\mathcal{O}_S)$. Note that $M_2, \ldots, M_n$ are $G\mathbf{W}_r$-bundles. Denote by

$$\alpha : H^0(S,M) \otimes \mathbf{W}_r(\mathcal{O}_S) \longrightarrow M$$

the canonical arrow, given by restricting global sections. Form the pushforward

$$\mathcal{E} := \alpha_*(\mathcal{C}_S) : 0 \longrightarrow M \longrightarrow M_1' \xrightarrow{f_1} M_2 \xrightarrow{f_2} ... \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} \mathbf{W}_r(\mathcal{O}_S) \longrightarrow 0;$$

it is an n-extension of $G\mathbf{W}_r$-modules on S. Set $\gamma(c)$ to be the class of $\mathcal{E}$ in $H^n_{sgt}((G,S),M)$.
To get an arrow in the reverse direction, start with $e \in H^n_{sgt}((G,S),M)$, represented by a strongly geometrically trivial n-extension of $G\mathbf{W}_r$-modules on S

$$\mathcal{E} : 0 \longrightarrow M \longrightarrow M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} ... \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} \mathbf{W}_r(\mathcal{O}_S) \longrightarrow 0.$$

Taking global sections yields an n-extension of $(\mathbb{Z}/p^r, G)$-modules

$$H^0(S,\mathcal{E}) : 0 \longrightarrow H^0(S,M) \longrightarrow H^0(S,M_1) \xrightarrow{g_1} ... \xrightarrow{g_{n-1}} H^0(S,M_n) \xrightarrow{g_n} H^0(S,\mathbf{W}_r(\mathcal{O}_S)) \longrightarrow 0,$$

which we pullback by the arrow

$$\begin{array}{ccc} \mathbb{Z}/p^r & \longrightarrow & H^0(S,\mathbf{W}_r(\mathcal{O}_S)) \\ 1 & \longmapsto & 1 \end{array}$$

to get an n-extension of $(\mathbb{Z}/p^r, G)$-modules

$$\mathcal{C} : 0 \longrightarrow H^0(S,M) \longrightarrow \cdots \longrightarrow \mathbb{Z}/p^r \longrightarrow 0.$$

Set $\gamma'(e)$ to be the class of $\mathcal{C}$ in $H^n(G, H^0(S,M))$. One then checks that the arrow

$$\gamma' : H^n_{sgt}((G,S),M) \longrightarrow H^n(G, H^0(S,M))$$

is the inverse of γ.

□

Remark 8.6. In Definition 8.2, assume that M is a $(G,\mathbf{W}_r)$-bundle. Using (the proof of) Proposition 8.5, every element of $H^n_{sgt}((G,S),M)$ can be represented by a strongly geometrically trivial n-extension of $(G,\mathbf{W}_r)$-bundles

$$0 \longrightarrow M = M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} ... \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} \mathbf{W}_r(\mathcal{O}_S) \longrightarrow 0.$$

9. Lifting (G, M)-torsors.

In this section, we state and prove the first lifting theorem of this article, to be thought of as a generalization of classical Kummer theory, for $H^1(\mathrm{Gal}(F_{sep}/F), \mu_{p^r})$, to the broader context of torsors for $(G, \mathbf{W}_r)$-line bundles, over a $(G, \mathbb{F}_p)$-scheme S. It applies to arbitrary depth e.

Theorem A. *Let $(G, \mathbb{Z}/p^{1+e}(1))$ be a (n, e)-cyclotomic pair, relatively to some integer $n \in \mathbb{N}^*$ and $e \in \mathbb{N}^* \cup \{\infty\}$.*

Pick an integer $1 \leq r \leq e$. Let S be a $(G, \mathbb{F}_p)$-scheme and L be a G-linearized line bundle over S. Consider a strongly geometrically trivial class

$$c_r \in H^n_{sgt}((G, S), \mathbf{W}_r(L)(n)).$$

Then, there is an integer $m \geq 0$ such that the Frobenius pullback $c_r^{(m)}$ of c_r lifts to a strongly geometrically trivial class, via

$$H^n_{sgt}((G, S), \mathbf{W}_{1+e}(L^{(m)})(n)) \longrightarrow H^n_{sgt}((G, S), \mathbf{W}_r(L^{(m)})(n)).$$

In particular, if S is a perfect affine scheme, the natural arrow

$$H^n((G, S), \mathbf{W}_{1+e}(L)(n)) \longrightarrow H^n((G, S), \mathbf{W}_r(L)(n))$$

is onto. Therefore, G is (n, e)-smooth.

Remark 9.1. By the very definition of a cyclotomic pair, Theorem A also clearly holds if we replace G by an open (or even closed) subgroup $H \subset G$. Its proof actually invokes a tremendous amount of such subgroups.

Remark 9.2. For proving Theorem A, without loss of generality, we can assume that $\mathbb{F}_p(1) \simeq \mathbb{F}_p$ has the trivial G-action. Indeed, the action of G on $\mathbb{F}_p(1)$ occurs through a multiplicative character

$$\xi : G \longrightarrow \mathbb{F}_p^\times$$

whose kernel G_0 has index dividing $p - 1$, hence prime-to-p. Invoking the usual restriction-corestriction argument, it is then free to replace G by G_0.

9.1. Permutation modules and factorizing Frobenius.

In this section, and only in this section, we will encounter infinite dimensional $\mathbb{F}_p$-vector spaces, endowed with a naive action of G– for instance, $(\mathbb{F}_p, G)$-algebras, which are of finite-type as $\mathbb{F}_p$-algebras. We thus state the following definition.

Definition 9.3.
If G is a profinite group, an $[\mathbb{F}_p, G]$-module is an $\mathbb{F}_p$-vector space, equipped with a naive $\mathbb{F}_p$-linear action of G.

Remark 9.4. For G finite, an $[\mathbb{F}_p, G]$-module is simply a module over the group algebra $\mathbb{F}_p[G]$.

The goal of this section is to provide Theorem 9.7, a remarkable algebraic device and the key ingredient in the proof of Theorem A.

Lemma 9.5. *Let A be an $(\mathbb{F}_p, G)$-algebra, reduced and of finite-type as an $\mathbb{F}_p$-algebra. Set $B =: A^G$.*

Then, the following assertions hold.

i) The $\mathbb{F}_p$-algebra B is of finite-type, and A is finite, as a B-module.

ii) There exists a finite G-set X, and an element $f \in B$, which is not a zero divisor in A, with the following properties:

a) The algebra A_f/B_f is finite étale.

b) There exists G-equivariant homomorphisms of B-modules

$$\phi : A \longrightarrow B^X, \qquad \textit{and} \qquad \psi : B^X \longrightarrow A,$$

such that

$$\psi \circ \phi = f\mathrm{Id}.$$

iii) The extension of $[\mathbb{F}_p, G]$-modules

$$(\mathcal{E}_1) : 0 \longrightarrow A \xrightarrow{\times f} A \xrightarrow{\pi} A/f \longrightarrow 0$$

is split by pullback by the natural quotient map $q : A/f^2 \longrightarrow A/f$.

Proof. Point i) is classical. Let us prove ii). Denote by $H \subset G$ the kernel of the action of G on A; it is an open subgroup.

Assume first that A is a domain. Denote by L (resp. K) the field of fractions of A (resp. of B). By Artin's Lemma, the extension L/K is Galois, with Galois group G/H. Put $X := G/H$. Then, by the normal basis theorem, there exists a G-equivariant isomorphism of K-vector spaces $L \xrightarrow{\sim} K^X$. The existence of $f \in B$, enjoying the properties required in a) and b), readily follows. This argument instantly extends to the case where A is a finite product of domains, after noting that the group G naturally permutes the factors of the finite product in question (which correspond to the primitive idempotents of A).

Let us deal now with the general case: denote by $P_1, \ldots, P_s$ the generic points of $\mathrm{Spec}(A)$. Put

$$K_i := A_{P_i};$$

it is a reduced Artinian ring, hence a field. The canonical map

$$\iota : A \longrightarrow \prod_{i=1}^{s} K_i$$

is injective.
For each index $i = 1, \ldots, s$, there exists an element

$$a_i \in (\cap_{j \neq i} P_j) - P_i.$$

Equivalently, the element a_i is nonzero in K_i, but vanishes in all K_j's, for $j \neq i$. Put

$$a := a_1 + \ldots + a_s.$$

We then have

$$a_i^2 - aa_i = 0 \in A$$

for all i; indeed, these elements vanish in all K_j's. The element $a \in A$ is not a zero divisor, hence so is

$$b := N_{G/H}(a) \left(= \prod_{g \in G/H} g \cdot a \right) \in B.$$

Furthermore, the elements

$$e_i := \frac{a_i}{a} \in A_b$$

are primitive idempotents, decomposing A_b into a finite product of domains. We are thus reduced to the previous case.

To prove *iii*), consider first the commutative diagram of $[\mathbb{F}_p, G]$-modules

$$\begin{tikzcd}
(\mathcal{E}_2) : 0 \arrow[r] & A \arrow[r, "\times f^2"] \arrow[d, "\phi"] & A \arrow[r] \arrow[d, "\phi"] & A/f^2 \arrow[r] \arrow[d, "\phi/f^2"] & 0 \\
(\mathcal{F}_2) : 0 \arrow[r] & B^X \arrow[r, "\times f^2"] \arrow[d, "\psi"] & B^X \arrow[r] \arrow[d, "\psi"] & (B/f^2)^X \arrow[r] \arrow[d, "\psi/f^2"] & 0 \\
(\mathcal{E}_2) : 0 \arrow[r] & A \arrow[r, "\times f^2"] & A \arrow[r] & A/f^2 \arrow[r] & 0.
\end{tikzcd}$$

The middle exact sequence $\mathcal{F}_2$ is split, since $B \longrightarrow B/f^2$ splits as an $\mathbb{F}_p$-linear map. Since $\psi \circ \phi = f\mathrm{Id}$, it follows that

$$f\mathcal{E}_2 = 0 \in \mathrm{Ext}^1_{[\mathbb{F}_p,G]}(A/f^2, A).$$

The diagram

$$\begin{tikzcd}
(\mathcal{E}_1) : 0 \arrow[r] & A \arrow[r, "\times f"] \arrow[d, equal] & A \arrow[r] \arrow[d, "\times f"] & A/f \arrow[r] \arrow[d, "\times f"] & 0 \\
(\mathcal{E}_2) : 0 \arrow[r] & A \arrow[r, "\times f^2"] & A \arrow[r] & A/f^2 \arrow[r] & 0
\end{tikzcd}$$

shows that $q^*(\mathcal{E}_1) = f\mathcal{E}_2$. This completes the proof. □

Definition 9.6 (Permutation modules). *An $[\mathbb{F}_p, G]$-module is said to be a permutation module if it has an $\mathbb{F}_p$-basis (possibly infinite) which is permuted by G.*
In other words, P is permutation, if it is isomorphic to an $[\mathbb{F}_p, G]$-module of the shape

$$\mathbb{F}_p^{(X)},$$

where X is a G-set (the action of G being naive).

We say that a morphism of $[\mathbb{F}_p, G]$-modules

$$f : M \longrightarrow N$$

factors through a permutation module if there is a permutation module P and a factorization

$$\begin{tikzcd}
& P \arrow[dr, "g_2"] & \\
M \arrow[ur, "g_1"] \arrow[rr, "f"'] & & N
\end{tikzcd}$$

Such morphisms form a subgroup of $\mathrm{Hom}_{[\mathbb{F}_p,G]}(M, N)$.

Arguably, the next theorem maximizes the product (simplicity × depth), among all results of this article.

Theorem 9.7. *Let A be an $(\mathbb{F}_p, G)$-algebra, of finite-type as an $\mathbb{F}_p$-algebra. Then, there exists an integer $m \geq 0$ such that, as a morphism of $[\mathbb{F}_p, G]$-modules,*

$$\mathrm{Frob}_A^m : A \longrightarrow A$$

factors through a permutation module.

Proof. Let $i \geq 0$ be such that the nilradical $\mathcal{N}$ of A satisfies $\mathcal{N}^{p^i} = 0$. Then Frob_A^i canonically factors through $A \longrightarrow A_{red}$. We can thus assume that A is reduced, and proceed by induction on the (Krull) dimension of A. We use the notation and the results of Lemma 9.5. By induction, there exists an integer $m' \geq 0$, working for A/f. By point *iii*) of Lemma 9.5, there exist a morphism of $[\mathbb{F}_p, G]$-modules $s : A/f^2 \longrightarrow A$, such that $\pi \circ s = q$. Denote by $\phi : A/f \longrightarrow A/f^2$ the canonical map, sending $a \pmod f$ to $a^p \pmod{f^2}$. Put

$$F_1 := s \circ \phi \circ \mathrm{Frob}_{A/f}^{m'} \circ \pi : A \longrightarrow A;$$

it is a morphism of $[\mathbb{F}_p, G]$-modules, factoring through a permutation module (because $\mathrm{Frob}_{A/f}^{m'}$ does). Then, the difference $\mathrm{Frob}^{m'+1} - F_1$ takes values in the ideal $fA \subset A$. Hence, there exists a morphism of $[\mathbb{F}_p, G]$-modules

$$F_2 : A \longrightarrow A,$$

such that

$$\mathrm{Frob}_A^{m'+1} = F_1 + fF_2.$$

By point *ii*) of Lemma 9.5, the morphism " multiplication by f ": $A \longrightarrow A$ factors through a permutation module- hence so does fF_2. Finally, we thus see that $m := m' + 1$ does the job. □

Exercise 9.8. Adapt the proof of Theorem 9.7, to show the following more precise statement, under the same assumptions. Consider the product

$$\mathbf{P}(A) := \prod_{x \in \mathrm{Max}(A)} k(x),$$

taken over all closed points $x \in \mathit{Spec}(A)$, with residue field the finite field $k(x)$. Show that it is a permutation $[\mathbb{F}_p, G]$-module, and that there exists an integer $m \geq 0$, such that

$$\begin{array}{rccc} \mathrm{Frob}_A^m : & A & \longrightarrow & A \\ & a & \longmapsto & a^{p^m} \end{array}$$

factors through the natural map $A \longrightarrow \mathbf{P}(A)$, as a morphism of $[\mathbb{F}_p, G]$-modules.

Question 9.9. (Does Theorem 9.7 hold for modules?)
Let M be an $A[G]$-module, which is finite locally free an an A-module. Is there an integer $m \geq 0$ such that

$$\begin{array}{rccc} \mathrm{Frob}_M^m : & M & \longrightarrow & M^{(m)} \\ & x & \longmapsto & 1 \otimes x \end{array}$$

factors through the natural map $M \longrightarrow \mathbf{P}(A) \otimes_A M$, as a morphism of $[\mathbb{F}_p, G]$-modules? In general, the answer is most likely "no".

9.2. Proof of Theorem A, for S affine and $L = \mathcal{O}_S$.

In order to lighten notations, we write the proof of Theorem A for $n = 1$, the general case being the same.

We first assume that $S = \mathrm{Spec}(A)$ and $L = \mathcal{O}_S$. Note that in this case, any $(G, \mathbf{W}_r(L)(1))$-torsor is strongly geometrically trivial by Lemma 8.4. By Proposition 8.5, $(G, \mathbf{W}_r(L)(1))$-torsors are then classified by $H^1(G, \mathbf{W}_r(A)(1))$- in the usual setting of the cohomology of a profinite group G, with values in a discrete G-module. We are then concerned with showing that after some suitable Frobenius pullback, all such classes admit a compatible system of liftings.

To prove the Theorem, it is straightforward to reduce to the case where A is an $\mathbb{F}_p$-algebra of finite-type. To understand why, consider a cohomology class c, represented by a cocycle

$$z_g \in Z^1(G, \mathbf{W}_r(A)(1)),$$

which factors through an open subgroup of G. It thus only takes finitely many values, each of which can be represented as a finite sum of Teichmüller representatives of elements of A. The G-orbit of each of these elements is also finite. We may then indeed replace A by the $(G, \mathbb{F}_p)$-algebra generated by this finite G-invariant collection of elements of A.

In the current setting, Theorem A is then a consequence of the following Proposition. Note that its content is more precise: the growth of the power of Frobenius needed to lift classes in $H^1(G, \mathbf{W}_r(A)(1))$ is actually linear in r.

Proposition 9.10. *Let $(G, \mathbb{Z}/p^{1+e}(1))$ be a $(1,e)$-cyclotomic pair with $e \in \mathbb{N}^* \cup \{\infty\}$. Let A be a $(G, \mathbb{F}_p)$-algebra, of finite-type over $\mathbb{F}_p$. Then there is a non-negative integer $m(A)$ with the following property.*

Let $r \in \{1, \dots, e\}$ be an integer and $c \in H^1(G, \mathbf{W}_r(A)(1))$ be a cohomology class. Then $(\mathrm{Frob}^{m(A)r})^*(c)$ lifts to $H^1(G, \mathbf{W}_{e+1}(A)(1))$.

Proof. By Theorem 9.7 there exists $m = m(A) \geq 0$ and a factorization

$$\mathrm{Frob}^m : A \xrightarrow{f} \mathbb{F}_p^{(X)} \xrightarrow{g} A,$$

for some G-set X. We are going to show that this m satisfies the conclusion of the Proposition. We first deal with the case $r = 1$, showing that classes in the image of (the map induced on $H^1(G, \cdot)$ by the cyclotomic twist of) g lift to $H^1(G, \mathbf{W}_{e+1}(A)(1))$. The G-set X is a disjoint union of cosets G/H_i, where the H_i's are open subgroups of G. It suffices to treat the case of a single orbit G/H. Using Shapiro's Lemma, we can then replace G by H, reducing to the case $X = \{*\}$. Put

$$a := g([*]) \in A.$$

For all $i \geq 1$, denote by

$$a_{i+1} := \tau_{i+1}(a) \in \mathbf{W}_{i+1}(A)$$

the Teichmüller representative of a.

Let $0 \leq i \leq e$ be an integer. We have a commutative diagram

$$\begin{tikzcd}
\mathbb{Z}/p^{i+1}\mathbb{Z} \arrow[r] \arrow[d] & \dots \arrow[r] & \mathbb{Z}/p^2\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/p\mathbb{Z} \arrow[d] \\
\mathbf{W}_{i+1}(A) \arrow[r] & \dots \arrow[r] & \mathbf{W}_2(A) \arrow[r] & A,
\end{tikzcd}$$

where the horizontal maps are the natural surjections, and the i-th vertical map sends $1 \in \mathbb{Z}/p^{i+1}\mathbb{Z}$ to a_{i+1}. After twisting this diagram by $\mathbb{Z}/p^{1+e}(1)$, by definition of $(1,e)$-smoothness, all arrows in the upper line induce surjections on $H^1(K, \cdot)$, for any open subgroup K of G. Thus, $\mathrm{Im}(g_*) \subset H^1(G, A(1))$ indeed consists of classes, that lift as required.

The proof of the general case is by induction on r. Assuming the result known for r, let

$$c \in H^1(G, \mathbf{W}_{r+1}(A)(1))$$

be a cohomology class. Denote by b its reduction to a class in $H^1(G, \mathbf{W}_r(A)(1))$. By induction, we know that $b_r := (\mathrm{Frob}^{rm})^*(b)$ admits a lifting

$$(b_{1+e}) \in H^1(G, \mathbf{W}_{1+e}(A)(1)).$$

Denote by $(b_{r+1}) \in H^1(G, \mathbf{W}_{1+r}(A)(1))$ the reduction of b_{1+e}. Set

$$c' := (\mathrm{Frob}^{rm})^*(c) - b_{r+1}.$$

Via the maps induced in cohomology from the exact sequence

$$0 \longrightarrow A(1) \xrightarrow{i_r} \mathbf{W}_{r+1}(A)(1) \longrightarrow \mathbf{W}_r(A)(1) \longrightarrow 0,$$

c' reduces to 0 in $H^1(G, \mathbf{W}_r(A)(1))$, hence comes from a class $b' \in H^1(G, A(1))$. By the $n = 1$ case, we get that $(\mathrm{Frob}^m)^*(b')$ lifts to $H^1(G, \mathbf{W}_{1+e}(A)(1))$. Hence, $(\mathrm{Frob}^m)^*(c')$ lifts as well. Finally, we see that

$$(\mathrm{Frob}^{(r+1)m})^*(c) = (\mathrm{Frob}^m)^*(b_{r+1}) + (\mathrm{Frob}^m)^*(c')$$

lifts as stated- as a sum of classes sharing this property. □

9.3. The general case. We now prove Theorem A, for S and L arbitrary. By assumption, there exists a (not necessarily G-equivariant) trivialization

$$F : P \xrightarrow{\sim} \mathbf{W}_r(L)(1)$$

of the $\mathbf{W}_r(L)(1)$-torsor P over S. Remembering that the automorphism group of the trivial $\mathbf{W}_r(L)(1)$-torsor is $H^0(S, \mathbf{W}_r(L)(1))$, we see that the assignment

$$\begin{array}{rccc} z: & G & \longrightarrow & H^0(S, \mathbf{W}_r(L)(1)) \\ & g & \longmapsto & z_g := F^{-1} \circ g \circ F \circ g^{-1} \end{array}$$

is a 1-cocycle. The $(G, \mathbf{W}_r(L)(1))$-torsor P can be recovered as the twist of the trivial $(G, \mathbf{W}_r(L)(1))$-torsor by this cocycle. Denote by

$$c \in H^1(G, H^0(S, \mathbf{W}_r(L)(1)))$$

the cohomology class of z.
Lifting P as required is then equivalent to lifting c to

$$c_{1+e} \in H^1(G, H^0(S, \mathbf{W}_{1+e}(L)(1))).$$

Theorem 9 thus boils down to the following Proposition.

Proposition 9.11. *Let $e \in \mathbb{N}_* \cup \{\infty\}$. Let $(G, \mathbb{Z}/p^{1+e}(1))$ be a $(1, e)$-cyclotomic pair. Let S be a $(G, \mathbb{F}_p)$-scheme. Pick an integer $1 \leq r \leq e$.*

Let

$$c \in H^1(G, H^0(S, \mathbf{W}_r(L))(1))$$

be a cohomology class. Then, there exists an integer $m \geq 0$, such that the class

$$(\mathrm{Frob}^m)^*(c) \in H^1(G, H^0(S, \mathbf{W}_r(L^{\otimes p^m}))(1))$$

lifts to

$$c_{1+e} \in H^1(G, H^0(S, \mathbf{W}_{1+e}(L^{\otimes p^m}))(1)).$$

Proof. By Proposition 5.6, we have a commutative diagram, with exact rows

$$\begin{tikzcd}
0 \arrow[r] & H^0(S,\mathbf{W}_{2+i}(L^{\otimes p^r})) \arrow[r] \arrow[d] & H^0(S,\mathbf{W}_{r+2+i}(L)) \arrow[r] \arrow[d] & H^0(S,\mathbf{W}_{r+1+i}(L)) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H^0(S,\mathbf{W}_{1+i}(L^{\otimes p^r})) \arrow[r] \arrow[d] & H^0(S,\mathbf{W}_{r+1+i}(L)) \arrow[r] \arrow[d] & H^0(S,\mathbf{W}_{r+i}(L)) \arrow[r] \arrow[d] & 0 \\
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & H^0(S,L^{\otimes p^r}) \arrow[r, "i"] & H^0(S,\mathbf{W}_{r+1}(L)) \arrow[r, "\pi"] & H^0(S,\mathbf{W}_r(L)) \arrow[r] & 0,
\end{tikzcd}$$

where Frobenius pushforwards are dismissed for clarity.

We work in the cyclotomic twist of this diagram, to which we apply $H^1(G,.)$, and mimic the proof of Proposition 9.10. By induction on r, we assume the result known for a given $r \geq 1$, and for all L. Let

$$c \in H^1(G, H^0(S,\mathbf{W}_{r+1}(L))(1))$$

be a cohomology class. Then, there exists $m_1 \geq 1$ such that

$$\pi_*((\mathrm{Frob}^{m_1})^*(c)) \in H^1(G, H^0(S,\mathbf{W}_r(L^{\otimes p^{m_1}}))(1))$$

admits a compatible system of liftings $(b_i)_{r \leq i \leq e+1}$. Replacing L by $L^{\otimes p^{m_1}}$, we can assume that $m_1 = 1$. Replacing c by $c - b_{r+1}$, we then reduce to the case where $\pi_*(c) = 0$. Hence, there exists

$$a \in H^1(G, H^0(S, L^{\otimes p^r}(1)))$$

such that $i_*(a) = c$. If we can show that (a high enough Frobenius twist of) a lifts to

$$H^1(G, H^0(S, \mathbf{W}_{e+1-r}(L^{\otimes p^r})))$$

(with respect to the line bundle $L^{\otimes p^r}$), then we are done, by commutativity of the diagram above.

Thus, only the case $r = 1$ remains to be considered. Put

$$A := \bigoplus_{i \in \mathbb{Z}} H^0(S, L^{\otimes i});$$

the $(\mathbb{F}_p, G)$-algebra of regular functions on the $\mathbb{G}_m$-torsor associated to L. As usual, the class $c \in H^1(G, H^0(S,L)(1))$ is defined by a cocycle taking only finitely many values. Let $A' \subset A$ be the sub-$(\mathbb{F}_p, G)$-algebra generated by these values; it is an $\mathbb{F}_p$-algebra of finite-type. Casting Theorem 9.7 again, we get an integer $m \geq 0$ and a factorization

$$\mathrm{Frob}^m : A' \xrightarrow{f} \mathbb{F}_p^{(X)} \xrightarrow{g} A',$$

where X is a G-set. Consider the composite

$$\phi : \mathbb{F}_p^{(X)} \xrightarrow{g} A' \xrightarrow{\subset} A \xrightarrow{\mathrm{pr}_m} H^0(S, L^{\otimes p^m}),$$

where pr_m is the natural projection. We are now reduced to showing that classes in the image of

$$\phi(1)_* : H^1(G, \mathbb{F}_p^{(X)}(1)) \longrightarrow H^1(G, H^0(S, L^{\otimes p^m}(1)))$$

lift to $H^1(G, H^0(S, \mathbf{W}_{1+e}(L)^{\otimes p^m}(1)))$.
Note that the stabilizers of elements of X are open subgroups of G. By definition of a cyclotomic pair, and using Shapiro's Lemma, we can thus replace G by each of these stabilizers. In short, we can assume that $X = \{*\}$ is a one-element set.
Put

$$a := \mathrm{pr}_m(g([*])) \in H^0(S, L^{\otimes p^m}).$$

For all $s \geq 1$, denote by

$$a_s := \tau_s(a) \in H^0(S, \mathbf{W}_r(L^{\otimes p^m}))$$

the Teichmüller lift of $a = a_1$. We conclude by a chase in the diagram

$$\begin{tikzcd}
(\mathbb{Z}/p^{e+1}\mathbb{Z})(1) \arrow[r] \arrow[d, "1 \mapsto a_{1+e}"] & (\mathbb{Z}/p\mathbb{Z})(1) \arrow[d, "1 \mapsto a"] \\
H^0(S, \mathbf{W}_{e+1}(L^{\otimes p^m})(1)) \arrow[r] & H^0(S, L^{\otimes p^m}(1)),
\end{tikzcd}$$

to which we apply the functor $H^1(G, \cdot)$– remembering the definition of a cyclotomic pair. □

10. A variation for Theorem A, in infinite depth.

In this section, we develop a refinement of Theorem A. It is not used in the next two papers of this series. Readers willing to go straight to the proofs of our Theorems B, C, and D are thus advised to skip it.
Looking at Theorem A, one may wonder whether the "strongly geometrically trivial" assumption could be removed, to get a broader lifting result. For $n = 1$, the following Theorem goes towards this direction, in an optimal way. It asserts that, if $(G, \mathbb{Z}_p(1))$ is a $(1, \infty)$-cyclotomic pair and P_r is a $(G, \mathbf{W}_r(L)(1))$-torsor, a (necessary and) sufficient condition for P_r to lift to a $(G, \mathbf{W}(L)(1))$-torsor, is to admit a G-invariant lift (dismissing the action of G, see Remark 2.12). Note that we don't have a similar statement in finite depth e.

Theorem 10.1. *Let $(G, \mathbb{Z}_p(1))$ be a $(1, \infty)$-cyclotomic pair. Let S be a perfect $(G, \mathbb{F}_p)$-scheme and let L be a G-linearized line bundle over S.*
Pick an integer $r \geq 1$ and consider a $(G, \mathbf{W}_r(L)(1))$-torsor P_r over S.
Denote by $\overline{P}_r$ the $\mathbf{W}_r(L)(1)$-torsor given by P_r, forgetting the action of G.

Assume that $\overline{P}_r$ lifts to a $\mathbf{W}(L)(1)$-torsor $\overline{P}$, whose class in $H^1(S, \mathbf{W}(L)(1))$ is G-invariant.

Then, $\overline{P}$ can be equipped with the structure of a $(G, \mathbf{W}(L)(1))$-torsor, lifting the $(G, \mathbf{W}_r(L)(1))$-torsor P_r.

Proof. Denote by $G_S \subset G$ the kernel of the action of G on S and put

$$s := v_p(|G/G_S|).$$

Recall the natural exact sequence

$$0 \longrightarrow \mathrm{Frob}_*^r(\mathbf{W}(L^{\otimes p^r})) \longrightarrow \mathbf{W}(L) \longrightarrow \mathbf{W}_r(L) \longrightarrow 0.$$

It has a natural non-linear section- its Teichmüller section. We thus get an exact sequence of G-modules

$$0 \longrightarrow H^0(S, \mathrm{Frob}_*^r(\mathbf{W}(L^{\otimes p^r})(1))) \longrightarrow H^0(S, \mathbf{W}(L)(1)) \xrightarrow{\pi_r} H^0(S, \mathbf{W}_r(L)(1)) \longrightarrow 0.$$

There exists a natural obstruction

$$\mathrm{Obs} \in H^2(G, H^0(S, \mathbf{W}(L^{\otimes p^r})(1))),$$

whose vanishing is equivalent to endowing $\overline{P}$ with the structure of a $(G, \mathbf{W}(L)(1))$-torsor P, lifting P_r. To build Obs, pick isomorphisms of $\mathbf{W}(L)(1)$-torsors over S,

$$\phi_g : \overline{P} \xrightarrow{\sim} g.\overline{P},$$

one for each $g \in G$. Consider their reduction, to isomorphisms of $\mathbf{W}_r(L)(1)$-torsors over S,

$$\phi_{g,r} : \overline{P}_r \xrightarrow{\sim} g.\overline{P}_r.$$

Denote by

$$can_{g,r} : \overline{P}_r \xrightarrow{\sim} g.\overline{P}_r$$

the canonical isomorphisms, giving the semi-linear action of G on P_r. Then,

$$\delta_{g,r} := \phi_{g,r}^{-1} \circ can_{g,r}$$

belongs to the automorphism group of $\overline{P}_r$, which is $H^0(S, \mathbf{W}_r(L)(1))$. We can lift $\delta_{g,r}$ through π_r, to

$$\delta_g \in H^0(S, \mathbf{W}(L)(1)) = \mathrm{Aut}_S(\overline{P}).$$

Replacing ϕ_g by $\phi_g \circ \delta_g$, we are reduced to $\phi_{g,r} = can_{g,r}$. Then, set

$$c_{g,h} := \phi_g^{-1} \circ (g.\phi_h^{-1}) \circ \phi_{gh} \in H^0(S, \mathbf{W}(L)(1)) = \mathrm{Aut}_S(\overline{P}).$$

By what precedes, $\pi_r(c_{g,h}) = 0$, so that $c_{g,h}$ is a 2-cocycle, living in

$$Z^2(G, H^0(S, \mathbf{W}(L^{\otimes p^r})(1))).$$

Set Obs to be its cohomology class.

If S is affine, then Obs is simply the obstruction to lifting the geometrically trivial torsor P_r. It thus vanishes by Theorem 9.

Suppose now that G acts trivially on S. Let (U_i) be a finite cover of S, by affine open subschemes. The preceding discussion, the image of Obs by the (arrow induced by the) injection

$$0 \longrightarrow H^0(S, \mathbf{W}(L^{\otimes p^r})(1)) \longrightarrow \bigoplus H^0(U_i, \mathbf{W}(L^{\otimes p^r})(1))$$

vanishes. Using Lemma 10.2, we see that Obs vanishes.

We no longer assume that G acts trivially on S. By restriction-corestriction (from G to G_S), we get that $p^s\mathrm{Obs}$ vanishes. Indeed, G_S acts trivially on S.
Assume first $r \geq s$, so that $p^r\mathrm{Obs} = 0$.
Consider the (twist by (1) of the) natural commutative diagram of G-W Modules on S with exact rows

$$\begin{tikzcd}
\mathcal{D} : 0 \arrow[r] & \mathrm{Frob}_*^r(\mathbf{W}(L^{\otimes p^r})) \arrow[r] \arrow[d, "{f:=\mathrm{Frob}_*^r(ad(\mathrm{Id}_{\mathbf{W}(L^{\otimes p^{r+s}})}))}"] & \mathbf{W}(L) \arrow[r] \arrow[d, "{ad(\mathrm{Id}_{\mathbf{W}(L^{\otimes p^r})})}"] & \mathbf{W}_r(L) \arrow[r] \arrow[d, "{ad(\mathrm{Id}_{\mathbf{W}_r(L^{\otimes p^r})})}"] & 0 \\
0 \arrow[r] & \mathrm{Frob}_*^{2r}(\mathbf{W}(L^{\otimes p^{2r}})) \arrow[r, "i"] & \mathrm{Frob}_*^r(\mathbf{W}(L^{\otimes p^r})) \arrow[r] & \mathrm{Frob}_*^r(\mathbf{W}_r(L^{\otimes p^r})) \arrow[r] & 0,
\end{tikzcd}$$

where we write ad for adjunction, between Frob_* and Frob^*. We have

$$i \circ f = \times p^r.$$

Twisting it by (1) and taking global sections, we get an analoguous diagram $\mathcal{C} := H^0(S, \mathcal{D}(1))$, where each G-W Module M is replaced by $H^0(S, M(1))$. By Theorem A, the arrow

$$H^1(G, H^0(S, \mathbf{W}(L^{\otimes p^r})(1))) \longrightarrow H^1(G, H^0(S, \mathbf{W}_r(L^{\otimes p^r})(1)))$$

is surjective. Chasing in the diagram induced in cohomology by $\mathcal{C}$, we get

$$f_*(\mathrm{Obs}) = 0 \in H^2(G, H^0(S, \mathbf{W}(L^{\otimes p^{2r}})(1))).$$

Since S is perfect, Obs itself vanishes, and we are done.
Assume now $r < s$. Put $t := s - r$.
Consider the natural commutative diagram of G-W Modules on S, with exact rows,

$$\begin{tikzcd}
\mathcal{D}' : 0 \arrow[r] & \mathrm{Frob}_*^{r+t}(\mathbf{W}(L^{\otimes p^{r+t}})) \arrow[r] \arrow[d, equal] & \mathrm{Frob}_*^{t}(\mathbf{W}(L^{\otimes p^{t}})) \arrow[r] \arrow[d] & \mathrm{Frob}_*^{t}(\mathbf{W}_r(L^{\otimes p^{t}})) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Frob}_*^{s}(\mathbf{W}(L^{\otimes p^{s}})) \arrow[r] & \mathbf{W}(L) \arrow[r] & \mathbf{W}_s(L) \arrow[r] & 0.
\end{tikzcd}$$

Twisting by (1) and taking global sections yields a similar diagram, denoted by $\mathcal{C}' := H^0(S, \mathcal{D}'(1))$. Since S is perfect, it suffices to show that $(\mathrm{Frob}^t)^*(\overline{P})$ can be equipped with the structure of a $(G, \mathbf{W}(L^{\otimes p^t})(1))$-torsor, lifting $(\mathrm{Frob}^t)^*(P_r)$. By chasing in the diagram induced in cohomology by $\mathcal{C}'$, we are reduced to the case $r = s$ (cohomology of the lower line), which was dealt with above. □

LEMMA 10.2. *Let S be a $\mathbb{F}_p$-scheme, endowed with the trivial action of G, and let L be a G-line bundle over S. Denote by G_L the kernel of the action of G on L.*

Let $(U_i)_{i=1,\dots,N}$ be a finite cover of S, by affine open subschemes. Let $r \geq 1$ be an integer. Consider the exact sequence

$$\mathcal{R} : 0 \longrightarrow H^0(S, \mathbf{W}_r(L)) \xrightarrow{\rho} \bigoplus_{i=1}^{N} H^0(U_i, \mathbf{W}_r(L)) \longrightarrow B_r \longrightarrow 0,$$

where B_r is defined as the cokernel of ρ. The following holds.

1. *If the index of G_L in G is prime-to-p (which holds for instance if S is reduced), then the pushforward of $\mathcal{R}$ by the natural injection*

   $$\mathrm{Frob}^{r-1} : H^0(S, \mathbf{W}_r(L)) \longrightarrow H^0(S, \mathrm{Frob}_*^{r-1}(\mathbf{W}_r(L^{\otimes p^{r-1}})))$$

   splits, as an extension of $(\mathbb{Z}/p^r\mathbb{Z})[G]$-modules.
2. *In general, denote by p^{r_L} the exponent of the p-primary component of the finite abelian group $G/G_L \subset \mathbb{G}_m(S)$.*
   Then, $(\mathrm{Frob}^{r+r_L-1})_*(\mathcal{R})$ splits, as an extension of $(\mathbb{Z}/p^r\mathbb{Z})[G]$-modules.
3. *Assume now that S is perfect. Then, the natural exact sequence of $\mathbb{Z}_p[G]$-modules*

   $$0 \longrightarrow H^0(S, \mathbf{W}(L)(1)) \xrightarrow{\rho} \bigoplus_{i=1}^{N} H^0(U_i, \mathbf{W}(L)(1)) \longrightarrow B(1) \longrightarrow 0$$

   splits.

Proof. Note that, if items (1) and (2) hold true, then so do the similar properties, replacing $\mathcal{R}$ by the cyclotomic twist $\mathcal{R}(1)$.
Item (3) follows from (1), by passing to the limit. We thus content ourselves with proving (1) and (2).

Since the group of automorphisms of the line bundle L is $\mathbb{G}_m(S)$, and since Frobenius additively kills p-nilpotent elements (and hence multiplicatively kills p-th roots of unity), we see that $G_{L^{\otimes p^{r_L}}}$ has index prime-to-p in G. Replacing L by $L^{\otimes p^{r_L}}$, we see that (2) follows from (1), which we now prove.
By the usual "restriction-corestriction" argument, we can assume that $G = G_L$ acts trivially on L. We then have to show that $(\mathrm{Frob}^{r-1})_*(\mathcal{R})$ splits, as a morphism of $(\mathbb{Z}/p^r\mathbb{Z})$-modules. To do so, it suffices to check the following property. For every $s \in H^0(S, \mathbf{W}_r(L))$, and every integer $1 \leq j \leq r-1$, if $(s_i) := \rho(s)$ is also divisible by p^j, in the group $\bigoplus_{i=1}^N H^0(U_i, \mathbf{W}_r(L))$, then $\mathrm{Frob}^{r-1}(s)$ is divisible by p^j in the group $H^0(S, \mathrm{Frob}_*^{r-1}(\mathbf{W}_r(L^{\otimes p^{r-1}})))$.
We now prove this. Write $s_i = p^j t_i$, for $t_i \in H^0(U_i, \mathbf{W}_r(L))$. Note that multiplication by p^j

$$\begin{array}{ccc} \mathbf{W}_r(L) & \longrightarrow & \mathbf{W}_r(L) \\ x & \longmapsto & p^j x \end{array}$$

factors as the composite of the two natural morphisms (of W-Modules over S)

$$\mathbf{W}_r(L) \xrightarrow{a_j} (\mathrm{Frob}_*)^j(\mathbf{W}_{r-j}(L^{\otimes p^j})) \xrightarrow{i_{r-j,r}} \mathbf{W}_r(L),$$

where a_j is adjoint to the reduction

$$(\mathrm{Frob}^j)^*(\mathbf{W}_r(L)) = \mathbf{W}_r(L^{\otimes p^j}) \longrightarrow \mathbf{W}_{r-j}(L^{\otimes p^j}),$$

and where $i_{r-j,r}$ is the natural injection.

Put $u_i := (a_j)_{U_i}(t_i)$, viewed as elements of $H^0(U_i, \mathbf{W}_{r-j}(L^{\otimes p^j}))$. Since $i_{r-j,r}$ is injective, the u_i glue, to a global section $u \in H^0(S, \mathbf{W}_{r-j}(L^{\otimes p^j}))$. Through the Teichmüller section [8, Section 3.1], u possesses a natural lift to an element $\tilde{u} \in H^0(S, \mathbf{W}_r(L^{\otimes p^j}))$. Observing that the composite

$$(\mathrm{Frob}_*)^j(\mathbf{W}_r(L^{\otimes p^j})) \longrightarrow (\mathrm{Frob}_*)^j(\mathbf{W}_{r-j}(L^{\otimes p^j})) \xrightarrow{i_{r-j,r}} \mathbf{W}_r(L) \longrightarrow (\mathrm{Frob}_*)^j(\mathbf{W}_r(L^{\otimes p^j}))$$

is multiplication by p^j, we see that the elements $\mathrm{Frob}^j(s)$ and $p^j\tilde{u}$ coincide when restricted to each U_i. They hence coincide.
A fortiori, we get $\mathrm{Frob}^{r-1}(s) = p^j \mathrm{Frob}^{r-1-j}(\tilde{u})$– as was to be shown. □

11. $(n,1)$-smoothness: an equivalent definition.

Theorems B, C, and D deal with $(n,1)$-smoothness. This flexible notion, involving algebraic geometry in characteristic p, is less elementary than $(n,1)$-cyclotomic pairs. Nonetheless, it turns out to be equivalent to a much simpler notion, thought of as "a profinite group G, with a moving cyclotomic character". We call these *cyclothymic* profinite groups. We warn the reader, not to take this denomination too seriously. Indeed, in the sequel, we will stick to the name "$(n,1)$-smooth", and use the property below in proofs only, especially for the second statement of Theorem D.

Definition 11.1. *(Cyclothymic profinite group.)*
Let $n \geq 1$, $e \in \mathbb{N}^* \cup \{\infty\}$ and let G be a profinite group.
We say that G is (n,e)-cyclothymic if the following holds.
Let L be an $(\mathbb{F}_p, G)$-module, of dimension one as an $\mathbb{F}_p$-vector space.
Consider a finite collection

$$H_1, \ldots, H_N \subset G$$

of open subgroups of G.
For each $i = 1, \dots, N$, let

$$c_i \in H^n(H_i, L)$$

be a cohomology class. Write $C := (c_1, \dots, c_N)$.
Then, there exists a lift of L, to a $(\mathbb{Z}/p^{1+e}, G)$-module $L_{1+e}[C]$, free of rank one as a $\mathbb{Z}/p^{1+e}$-module, such that, for each $i = 1, \dots, N$, the class c_i lifts through

$$H^n(H_i, L_{1+e}[C]) \longrightarrow H^n(H_i, L).$$

The integer e is called the depth of the cyclothymic group G.

Remark 11.2. The point, in this definition, is that $L_{1+e}[C]$ *depends* on C.

Remark 11.3. In this definition, we can assume without loss of generality that $L = \mathbb{F}_p$ has the trivial action of G. Indeed, let $G_L \subset G$ be the kernel of the action on L. Its index divides $p-1$, which is prime-to-p. We are then free to replace H_i by $H_i \cap G_L$– using a restriction-corestriction argument. As a consequence, if $(G, \mathbb{Z}/p^{1+e}(1))$ is an (n,e)-cyclotomic pair, then the profinite group G is (n,e)-cyclothymic. Indeed, as explained above, we can assume w.l.o.g. that $L = \mathbb{F}_p(1) = \mathbb{F}_p$, and set

$$L_{1+e}[C] := \mathbb{Z}/p^{1+e}(n).$$

Before investigating relations between cyclotomic pairs, cyclothymic groups and smooth groups, we state the following variant of Theorem A.

Theorem 11.4 (Cyclothymic version of Theorem A).
Pick $n \in \mathbb{N}$ and $e \in \mathbb{N}^* \cup \{\infty\}$. Let G be a (n,e)-cyclothymic profinite group.
Let S be a $(G, \mathbb{F}_p)$-scheme, and L be a G-linearized line bundle over S. Consider a strongly geometrically trivial class

$$c \in H^n((G,S), L).$$

Then, there exists $m \geq 0$, and a lift of $L^{(m)} = L^{\otimes p^m}$ to a $(G, \mathbf{W}_{1+e})$-line bundle over S, which we denote by $L_{1+e}^{[m]}[c]$, such that $c^{(m)}$ lifts, to a strongly geometrically trivial class, via the natural arrow

$$H^n_{sgt}((G,S), L_{1+e}^{[m]}[c]) \longrightarrow H^n_{sgt}((G,S), L^{\otimes p^m}).$$

In particular, taking S to be a perfect affine scheme, we get that G is (n,e)-smooth.

Proof. The proof is the same as for Theorem A. To understand why, the key is that, in the proof of Theorem A for $r = 1$, it suffices to lift a *finite* number N of classes $c_i \in H^1(H_i, \mathbb{F}_p)$, where $H_i \subset G$ are open subgroups. These H_i's occur as the stabilizers of elements of the G-set X, given by Theorem 9.7. The coefficients module used to lift the c_i's is of little importance–provided it is a $(\mathbb{Z}/p^{1+e}, G)$-module, free of rank one as a $\mathbb{Z}/p^{1+e}$-module. For this purpose, setting $C := (c_1, \dots, c_N)$, the module $L_{1+e}[C]$ of Definition 11.1 does the job– instead of $\mathbb{Z}/p^{1+e}(n)$ in the cyclotomic case.

□

We now can get to an essential point of our work, allowing us, in the sequel, to take on Definition 11.1 as an alternative way to tackle $(1,1)$-smoothness.

Theorem 11.5. *Pick $n \geq 1$ and $e \in \mathbb{N}^* \cup \{\infty\}$. Let G be a profinite group.*
If G is (n,e)-cyclothymic, then it is (n,e)-smooth.
The group G is $(n,1)$-smooth if and only if it is $(n,1)$-cyclothymic.

Proof. The first implication is contained in Theorem 11.4.
We prove the converse implication, when $e = 1$. We deal with the case $n = 1$, the general case being identical. Let $H_1, \ldots, H_k \subset G$ be open subgroups, and let

$$\chi = (\chi_1, ..., \chi_k) \in \prod_{i=1}^{k} H^1(H_i, \mathbb{F}_p)$$

be cohomology classes (characters). Introduce

$$A := \mathbb{F}_p[X_{i,c}],$$

the polynomial algebra on $d = \sum_{i=1}^{k} |G/H_i|$ variables, indexed by $i = 1, \ldots, k$ and $c \in G/H_i$. For each fixed i, the group G naturally permutes the variables $X_{i,c}$, $c \in G/H_i$, allowing to view A as an $(\mathbb{F}_p, G)$-algebra.

Using Shapiro's Lemma, the χ_i's give rise to 1-cocycles

$$\xi_i : G \longrightarrow \bigoplus_{c \in G/H_i} \mathbb{F}_p X_{i,c}$$

depending, up to a coboundary, on the choice of a system of representatives of the factor set G/H_i. We then form the 1-cocycle

$$\xi := \sum_{i=1}^{k} \xi_i : G \longrightarrow A.$$

As G is $(1,1)$-smooth, there is an integer m and a lift of the (A,G)-module A, to a $(\mathbf{W}_2(A), G)$-module

$$\mathbf{W}_2(A)(\xi^{(m)}),$$

free of rank one as a $\mathbf{W}_2(A)$-module, such that $\xi^{(m)}$ lifts to $H^1(G, \mathbf{W}_2(A)(\xi^{(m)}))$. Consider the extension of $(\mathbf{W}_2(A), G)$-modules

$$\mathcal{E} : 0 \longrightarrow A \longrightarrow \mathbf{W}_2(A)(\xi^{(m)}) \xrightarrow{\pi} A \longrightarrow 0.$$

Let $i = 1, \ldots k$ be an integer. Let $X^\alpha \in A$ be a pure monomial, in the variables $X_{i,c}$. The inclusion

$$\iota_\alpha : \mathbb{F}_p X^\alpha \longrightarrow A,$$

is then naturally split by the projection

$$\epsilon_\alpha : A \longrightarrow \mathbb{F}_p X^\alpha.$$

Setting $H_\alpha \subset G$ to be the stabilizer of α, it is clear that these arrows are H_α-equivariant.
If $X^\beta \in A$ is another pure monomial, we can form the extension of $\mathbb{Z}/p^2$-modules

$$\mathcal{F}_{\alpha,\beta} := (\epsilon_\beta)_*(\iota_\alpha^*(\mathcal{E})) : 0 \longrightarrow \mathbb{F}_p X^\beta \longrightarrow F_{\alpha,\beta} \longrightarrow \mathbb{F}_p X^\alpha \longrightarrow 0.$$

We are going to describe its middle term $F_{\alpha,\beta}$. To do so, consider the commutative diagram of $\mathbb{Z}/p^2$-modules

$$\begin{tikzcd}
\iota_0^*(\mathcal{E}) : 0 \arrow[r] & A \arrow[r] \arrow[d, "X^{p\alpha}."] & E_0 \arrow[r] \arrow[d, "\tau_2(X^\alpha)."] & \mathbb{F}_p \arrow[r] \arrow[d, "X^\alpha."] & 0 \\
\iota_\alpha^*(\mathcal{E}) : 0 \arrow[r] & A \arrow[r] & E_\alpha \arrow[r] & \mathbb{F}_p X^\alpha \arrow[r] & 0,
\end{tikzcd}$$

where $\tau_2(.) \in \mathbf{W}_2(A)$ denotes the multiplicative representative. We infer a natural isomorphism of extensions $\mathbb{Z}/p^2$-modules

$$\mathcal{F}_{\alpha,\beta} \simeq (\epsilon_\beta(X^{p\alpha}.))_*(\iota_0^*(\mathcal{E})).$$

The arrow $\epsilon_\beta(X^{p\alpha}.)$ vanishes if $p\alpha$ does not divide β. In that case, we deduce that $\mathcal{F}_{\alpha,\beta}$ has a canonical splitting. In particular, it is a trivial extension of $(\mathbb{F}_p, H_\alpha \cap H_\beta)$-modules.
If $\beta = p\alpha$, the arrow $\epsilon_\beta(X^{p\alpha}.)$ factors through ϵ_0, yielding a canonical isomorphism

$$\mathcal{F}_{\alpha,p\alpha} \simeq \mathcal{F}_{0,0}.$$

As a $\mathbb{Z}/p^2$-module, $F_{0,0}$ is free of rank one. We put

$$\mathbb{Z}/p^2[\xi] := F_{0,0}.$$

If $\beta \neq p\alpha$ and $p\alpha$ divides β, the extension $\mathcal{F}_{\alpha,\beta}$ is an extension of $(\mathbb{F}_p, H_\alpha \cap H_\beta)$-modules, which may be non-trivial.
For $i = 1, \dots, k$, denote by

$$\epsilon_i : A \longrightarrow \bigoplus_{c \in G/H_i} \mathbb{F}_p X_{i,c}^{p^{m+1}}$$

the projection, i.e. the sum of all arrows $\epsilon_{X_{i,c}^{p^{m+1}}}$. Similarly, consider

$$\iota_i : \bigoplus_{c \in G/H_i} \mathbb{F}_p X_{i,c}^{p^m} \longrightarrow A.$$

The arrows ϵ_i and α_i are G-equivariant. Form the extension of $(\mathbb{Z}/p^2, G)$-modules

$$\mathcal{E}_{i,j} := (\epsilon_j)_*(\iota_i^*(\mathcal{E})) : 0 \longrightarrow \bigoplus_{c \in G/H_j} \mathbb{F}_p X_{j,c}^{p^{m+1}} \longrightarrow E_{i,j} \longrightarrow \bigoplus_{c \in G/H_i} \mathbb{F}_p X_{i,c}^{p^m} \longrightarrow 0.$$

If $i \neq j$, from what precedes, we get that $\mathcal{E}_{i,j}$ has a (canonical, hence G-equivariant) splitting. Indeed, no $X_{i,c}^{p^m}$ divides a $X_{j,c'}^{p^{m+1}}$. Similarly, $\mathcal{E}_{i,i}$ is canonically isomorphic to

$$\mathcal{F}_{0,0}^{G/H_i} : 0 \longrightarrow \mathbb{F}_p^{G/H_i} \longrightarrow \mathbb{Z}/p^2[\xi]^{G/H_i} \longrightarrow \mathbb{F}_p^{G/H_i} \longrightarrow 0.$$

Since $\xi^{(m)}$ lifts via (the map induced on $H^1(G,.)$ by) the surjection π of $\mathcal{E}$, we deduce that it also lifts via the surjection of the extension of $(\mathbb{Z}/p^2, G)$-modules

$$\mathcal{E}' := \bigoplus_{i,j} \mathcal{E}_{i,j},$$

reading as

$$\mathcal{E}' : 0 \longrightarrow \bigoplus_{j=1,\dots,k;\, c \in G/H_j} \mathbb{F}_p X_{j,c}^{p^{m+1}} \longrightarrow E' \longrightarrow \bigoplus_{i=1,\dots,k;\, c \in G/H_i} \mathbb{F}_p X_{i,c}^{p^m} \longrightarrow 0.$$

We have shown before that

$$\mathcal{E}' = \bigoplus_i \mathcal{E}_{i,i}$$

is "diagonal". We thus get that each $\xi_i^{(m)}$ lifts via (the surjection of)

$$\mathcal{E}_{i,i} = \mathcal{F}_{0,0}^{G/H_i}.$$

Equivalently, using Shapiro's Lemma, we conclude that each χ_i lifts to $H^1(H_i, \mathbb{Z}/p^2[\xi])$. $\square$

Here is a recap of some connections made in this paper.

$$\begin{tikzcd}
& (G,\mathbb{Z}/p^{1+e}(1)) \text{ is a } (n,e)\text{-cyclotomic pair} \arrow[dl, Rightarrow, "\text{(Remark 11.3)}"'] \arrow[dr, Rightarrow, "\text{(Theorem A)}"] & \\
G \text{ is } (n,e)\text{-cyclothymic} \arrow[rr, Rightarrow, shift left, "\text{(Theorem 11.4)}"] & & G \text{ is } (n,e)\text{-smooth} \arrow[ll, Rightarrow, shift left, "\text{if e=1 (Theorem 11.5)}"]
\end{tikzcd}$$

Appendix: variations on $(n,1)$-smoothness

In this appendix, we provide some equivalent definitions of smoothness, which will be used in the next two articles of this series. First, we observe that the perfectness assumption on A, appearing in the definition of (n,e)-smoothness (Definition 6.8), can be removed if $e < \infty$, at the cost of introducing Frobenius twists. This formally follows from the existence of the perfection

$$A^{perf} := \varinjlim_n A_n,$$

where $A_n = A$ for all n, and the transition morphisms are Frob, for any $\mathbb{F}_p$-algebra A, from the isomorphisms

$$\varinjlim_n \mathbf{W}_{1+e}(A_n) \xrightarrow{\sim} \mathbf{W}_{1+e}(A^{perf})$$

for $e < \infty$, and from the commutation between cohomology and direct limits. We thus get another equivalent definition, for smooth profinite groups of finite depth.

Definition 11.6. *Let $n \geq 1$ and $e \in \mathbb{N}$. A profinite group G is (n,e)-smooth iff the following holds.*

Let A be an $(\mathbb{F}_p, G)$-algebra and let L_1 be a locally free A-module of rank one, equipped with a (naive) semi-linear action of G. Let

$$c \in H^n(G, L_1)$$

be a cohomology class. Then, there exists an integer $m \geq 0$ with the following property.

There exists a lift of $L_1^{(m)}$, to a $(\mathbf{W}_{e+1}(A), G)$-module $L_{e+1}^{[m]}[c]$, invertible as a $\mathbf{W}_{e+1}(A)$-module (and depending on c), such that $\mathrm{Frob}^m(c)$ *belongs to the image of the natural map*

$$H^n(G, L_{e+1}^{[m]}[c]) \longrightarrow H^n(G, L_1^{(m)}).$$

Note that for torsors, there is a very simple reformulation of the definition of smoothness in finite depth, in terms of liftability of one-dimensional G-affine spaces (see section 4).

Definition 11.7 ($(1,e)$-smooth profinite group, another equivalent definition). *Let $e \geq 1$ be an integer. A smooth profinite group G is $(1,e)$-smooth iff the following lifting property holds.*
Let A be a perfect $(\mathbb{F}_p, G)$-algebra and let X_1 be a G-affine space over A, such that $\overrightarrow{X_1}$ is an invertible A-module.
Then, X_1 admits a lift to a G-affine space X_{1+e} over $\mathbf{W}_{1+e}(A)$, such that $\overrightarrow{X_{1+e}}$ is an invertible $\mathbf{W}_{1+e}(A)$-module.

We move on to useful precisions for our main concern: smooth profinite groups of depth 1.

Proposition 11.8. *If $n = e = 1$, we can add in Definition 6.8 the extra requirement that $L_1 = A$ is trivial, as a (G,A)-module. Thus, $L_2[c]$ is automatically isomorphic to $\mathbf{W}_2(A)$ as a $\mathbf{W}_2(A)$-module- in a way that need not respect the action of G.*

Proof. The proof is, verbatim, the same as the second part of the proof of Proposition 11.13: reduction to the case of the trivial line bundle L_1, by extending scalars to its associated $\mathbb{G}_m$-torsor, and invoking a splitting argument for the appropriate cohomological obstruction. □

Remark 11.9. Though we shall not need it, let us mention that the previous Proposition also holds true for $e = 1$ and $n \geq 2$ arbitrary. Actually, this is part of what is proved in [7], when deducing Theorem 4.5 from Proposition 4.4.
Alternatively, Proposition 11.13 follows from combining Theorems 11.5 and 11.4.

We can now provide an equivalent Definition of $(1,1)$-smoothness, in the classical tongue of embedding problems.

Definition 11.10. *($(1,1)$-smooth profinite group, equivalent Definition)*
Denote by $\mathbf{S} \subset \mathbf{GL}_2$ one of the following two algebraic subgroups: the Borel subgroup $\mathbf{B}_2$, consisting of invertible matrices

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix},$$

or its subgroup $\mathrm{Aut}_{\mathrm{Aff}}(\mathbb{A}^1) = \mathbb{G}_a \rtimes \mathbb{G}_m \subset \mathbf{B}_2$, consisting of invertible matrices

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}.$$

A profinite group G is $(1,1)$-smooth iff the following lifting property holds.
Let A be a perfect $(\mathbb{F}_p, G)$-algebra. Then, the natural map

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

is onto.

A word is perhaps needed to explain why this definition is equivalent to Definition 6.8- where we can assume that the A-module L_1 is free of rank one by Proposition 11.8. We do this for $\mathbf{S} = \mathbf{B}_2$- the less obvious case. Notice that the datum of a cohomology class $b \in H^1(G, \mathbf{B}_2(A))$ is equivalent to an (isomorphy class of) extension of (G,A)-modules

$$\mathcal{E}_1 : 0 \longrightarrow D_1 \longrightarrow E_1 \longrightarrow D_1' \longrightarrow 0,$$

where D_1 and D'_1 are free of rank one as A-modules. The class of the extension

$$\mathcal{F}_1 := \mathcal{E}_1 \otimes_A (D'_1)^{-1} : 0 \longrightarrow D_1 \otimes_A (D'_1)^{-1} \longrightarrow F_1 := E_1 \otimes_A (D'_1)^{-1} \longrightarrow A \longrightarrow 0$$

is an element of $H^1(G, L_1)$, where

$$L_1 := D_1 \otimes_A (D'_1)^{-1}.$$

Lifting b as requested, amounts to lifting $\mathcal{E}_1$ to an extension of $(G, \mathbf{W}_2(A))$-modules

$$\mathcal{E}_2 : 0 \longrightarrow D_2 \longrightarrow E_2 \longrightarrow D'_2 \longrightarrow 0,$$

where D_2 and D'_2 are free of rank one as $\mathbf{W}_2(A)$-modules. This is equivalent to lifting $\mathcal{F}_1$ to an extension

$$\mathcal{F}_2 : 0 \longrightarrow L_2 \longrightarrow F_2 \longrightarrow \mathbf{W}_2(A) \longrightarrow 0,$$

where the $(G, \mathbf{W}_2(A))$-module $L_2 (= D_2 \otimes_{\mathbf{W}_2(A)} (D'_2)^{-1})$, free of rank one as a $\mathbf{W}_2(A)$-module, of course depends on b. This liftability is equivalent to that of Definition 6.8.

Remark 11.11. A profinite group is $(1,1)$-smooth if and only if its pro-p-Sylow subgroups are $(1,1)$-smooth.

In the definition of a (n,e)-cyclotomic profinite group, the lifting property is required for all open subgroups $H \subset G$. This is no longer needed in the definition of a $(1,1)$-smooth profinite group, as we now show.

LEMMA 11.12. *Let G be a $(1,1)$-smooth profinite group. Then, every closed subgroup $H \subset G$ is $(1,1)$-smooth as well.*

Proof. By a standard limit argument, we can assume that H is open in G. We use Definition 11.10. Let A be an $(\mathbb{F}_p, H)$-algebra. Consider the induced $(\mathbb{F}_p, G)$-algebra

$$\mathrm{Ind}_H^G(A) := \mathrm{Maps}_H(G, A),$$

consisting of (left) H-equivariant maps $G \longrightarrow A$, with ring structure induced by that of the target A. It is endowed with the natural G-action, given by the formula $(g.f)(x) := f(xg)$. We have

$$\mathbf{W}_r(\mathrm{Ind}_H^G(A)) = \mathrm{Ind}_H^G(\mathbf{W}_r(A)),$$

since the formation of Witt vectors commutes to finite products. Thus, we have

$$\mathbf{B}_2(\mathbf{W}_2(\mathrm{Ind}_H^G(A))) = \mathrm{Ind}_H^G(\mathbf{B}_2(\mathbf{W}_2(A))).$$

Shapiro's Lemma thus yields a natural bijection

$$H^1(G, \mathbf{B}_2(\mathbf{W}_2(\mathrm{Ind}_H^G(A)))) \simeq H^1(H, \mathbf{B}_2(\mathbf{W}_2(A))),$$

which we use to conclude that the arrow of Definition 11.10 is surjective for the pair (H, A) iff it is for the pair $(G, \mathrm{Ind}_H^G(A))$. □

11.1. LIFTING GEOMETRICALLY SPLIT TORSORS, IN THE $(1,1)$-SMOOTH CASE. The following proposition extends the lifting property defining $(1,1)$-smoothness, to geometrically split extensions over an arbitrary G-scheme S. This result will be handy in [12].

Proposition 11.13. *Assume that G is $(1,1)$-smooth.*
Let S be a perfect $(G,\mathbb{F}_p)$-scheme. Consider a geometrically split extension of G-linearized vector bundles over S,

$$\mathcal{E}_1 : 0 \longrightarrow L_1 \longrightarrow E_1 \xrightarrow{q} \mathcal{O}_S \longrightarrow 0,$$

where L_1 is a line bundle. Then, there exists a lift of L_1, to a $(G,\mathbf{W}_2)$-line bundle L_2 over S, such that $\mathcal{E}_1$ lifts to a geometrically split extension of $(G,\mathbf{W}_2)$-vector bundles over S,

$$\mathcal{E}_2 : 0 \longrightarrow L_2 \longrightarrow E_2 \longrightarrow \mathbf{W}_2(\mathcal{O}_S) \longrightarrow 0.$$

Proof.

We first deal with the case $L_1 = \mathcal{O}_S$. Since $\mathcal{E}_1$ is geometrically trivial, it is given by a class

$$e_1 \in H^1(G, H^0(S,\mathcal{O}_S)).$$

Using the definition of $(1,1)$-smoothness, for the $(\mathbb{F}_p,G)$-algebra

$$A := H^0(S,\mathcal{O}_S),$$

we get a lift of the trivial (G,A)-module A, to a $(G,\mathbf{W}_2(A))$-module $L_2[e_1]$, free of rank one as a $\mathbf{W}_2(A)$-module, such that e_1 lifts to

$$e_2 \in H^1(G, L_2[e_1]).$$

This e_2 is the class of an extension of $(G,\mathbf{W}_2(A))$-bundles

$$0 \longrightarrow L_2[e_1] \longrightarrow E_2[e_1] \longrightarrow \mathbf{W}_2(A) \longrightarrow 0.$$

Using

$$\mathbf{W}_2(A) = \mathbf{W}_2(H^0(S,\mathcal{O}_S)) = H^0(S,\mathbf{W}_2(\mathcal{O}_S)),$$

this extension can been seen as the sought-for geometrically split extension of $(G,\mathbf{W}_2)$-vector bundles over S

$$\mathcal{E}_2 : 0 \longrightarrow L_2 \longrightarrow E_2 \longrightarrow \mathbf{W}_2(\mathcal{O}_S) \longrightarrow 0,$$

lifting $\mathcal{E}_1$.
We now deal with an arbitrary L_1. Consider the extension of linear algebraic groups, defined over $\mathbb{F}_p$,

$$0 \longrightarrow \mathrm{Lie}(\mathbb{G}_a \rtimes \mathbb{G}_m)^{(1)} \longrightarrow \mathbf{W}_2 \rtimes \mathbf{W}_2^\times \longrightarrow \mathbb{G}_a \rtimes \mathbb{G}_m \longrightarrow 1.$$

Here the semi-direct products are taken w.r.t. the natural actions. It is good to think of these, as the automorphism group of the affine line $\mathbb{A}^1$. Our extension $\mathcal{E}_1$ corresponds to (G,S)-torsor $\mathcal{P}_1$ (i.e. a G-linearized torsor over S), under $\mathbb{G}_a \rtimes \mathbb{G}_m$. Lifting $\mathcal{E}_1$ to an $\mathcal{E}_2$, amounts to lifting $\mathcal{P}_1$ to a (G,S)-torsor, under $\mathbf{W}_2 \rtimes \mathbf{W}_2^\times$. The obstruction to do so is a class

$$Obs \in H^2((G,S), (\mathrm{Lie}(\mathbb{G}_a \rtimes \mathbb{G}_m)^{(1)})^{\mathcal{P}_1}).$$

The twisted Lie algebra, as a G-linearized vector bundle over S, is identified to $E_1^{(1)}$. Thus, Obs lives in $H^2((G,S), E_1^{(1)})$.

Denote by

$$f : T := \mathrm{Spec}(\bigoplus_{n\in\mathbb{Z}} L_1^{\otimes n}) \longrightarrow S$$

the $\mathbb{G}_m$-torsor associated to Ł$_1$. Over T, L_1 acquires a canonical trivialization, so that our lifting problem can be solved over T- after applying a Frobenius twist, since T is not perfect. Thus, there exists $m \geq 0$, with

$$f^*(Obs^{(m)}) = 0 \in H^2((G,T), E_1^{(m+1)} \otimes_{\mathcal{O}_S} \mathcal{O}_T) = H^2((G,S), E_1^{(m+1)} \otimes_{\mathcal{O}_S} f_*(\mathcal{O}_T)).$$

It remains to notice that the arrow of (G, S)-modules

$$\mathcal{O}_S \longrightarrow f_*(\mathcal{O}_T)$$

has a natural splitting, given by projecting on the factor $(n = 0)$ of $\bigoplus_{n \in \mathbb{Z}} L_1^{\otimes n}$. Thus, the arrow of (G, S)-modules

$$E_1^{(m+1)} \longrightarrow E_1^{(m+1)} \otimes_{\mathcal{O}_S} f_*(\mathcal{O}_T)$$

has a natural retraction as well, from which we get $Obs^{(m)} = 0$. Since S is perfect, $Obs = 0$, and we are done. □

Acknowledgements

Thanks to Peter Scholze, for a number of comments which helped improve the exposition.

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.

Charles De Clercq, Equipe Topologie Algébrique, Laboratoire Analyse, Géométrie et Applications, Sorbonne Paris Nord, 93430 Villetaneuse.

Mathieu Florence, Equipe de Topologie et Géométrie Algébriques, Institut de Mathématiques de Jussieu, Université Pierre et Marie Curie, 4, place Jussieu, 75005 Paris.