Smooth profinite groups and applications

Charles De Clercq and Mathieu Florence

August 2016

> La simplicité est la réussite absolue. Après avoir joué une grande quantité de notes, toujours plus de notes, c'est la simplicité qui émerge comme une récompense venant couronner l'art.
>
> Frédéric Chopin.

Abstract. In this paper, we introduce a notion of smoothness for profinite groups, relative to a given prime number p (cf. Definition 9.7). The fundamental example, following from Hilbert's Theorem 90 for $\mathbb{G}_m$, is that of an absolute Galois group of a field F of characteristic not p (Proposition 9.11). Using the theory of divided powers over Witt vectors, we prove Lifting Theorems for the cohomology of smooth profinite groups (see for instance Theorems 12.1 and 12.4). In section 13, we prove a general Smoothness Theorem (Theorem 13.8). We then give three applications. The first one is a new proof of the surjectivity of the norm-residue homomorphism (Corollary 14.1). The second one is a bound on the symbol length of central simple algebras (Theorem 14.2). The third one is a Lifting Theorem for Galois representations: every mod p Galois representation, over a field F of characteristic not p, can be lifted mod p^2 (Theorem 15.2).

Contents

1. Introduction.

The main goal of this paper is to define and study a smoothness notion for profinite groups, relative to a given prime number, and to prove general Lifting Theorems for their cohomology. We then give three applications.

First of all, we give a new self-contained proof of the surjectivity of the norm-residue homomorphism. Recall that, if F is a field, and n, d are positive integers with d invertible in F, the norm-residue homomorphism is a group homomorphism

$$\delta^n : K_n^M(F)/d \longrightarrow H^n(F, \mu_d^{\otimes n}),$$

from the mod d Milnor K-theory of F to its Galois cohomology. The Bloch-Kato Conjecture, also known as the norm-residue isomorphism Theorem, was proved by Rost, Suslin and Voevodsky. It states that δ^n is an isomorphism. We focus our efforts on proving surjectivity (cf. Corollary 14.1), which is, as it is well-known by experts, the hardest part of the proof. As a byproduct of our approach, we get upper bounds for the symbol length problem for central simple algebras (cf. Theorem 14.2, which the authors suspect can be improved drastically). This is our second application.

The third application is Theorem 15.2. It states that, over an arbitrary field F of characteristic not p, any mod p Galois representation can be lifted mod p^2 (note that, in dimension one, this Theorem goes back to Teichmüller). This Theorem is perhaps surprising, since most previously known results held over local or global fields, often under extra assumptions. Let us mention the works of Böckle, Hamblen, Khare, Manoharmayum, Taylor and Ramakrishna (see, e.g., [H] or [M] for more details). The methods used by these authors seem to be of arithmetic nature, whereas our work perhaps stresses a more Galois-theoretic aspect of the problem, as well as its deep connection to Hilbert's Theorem 90.

Note that the first two applications of our Lifting Theorems are rather immediate, whereas the last one requires the use of (seemingly) new material. In particular, we introduce the fundamental 2-extension associated to a (Galois) representation V over a finite field k (cf. section 15.2). It is the obstruction to the existence of a lift of V over $\mathbf{W}_2(k)$, the ring of length two Witt vectors over k.

The techniques we develop in this paper do not involve any algebraic geometry over F, but rather algebraic geometry over finite fields, through the use of divided powers of finite $\mathbb{Z}_p$-modules- the coefficients of the cohomology considered. Of all algebro-geometric information concerning the field F, we only remember the fact that its absolute Galois group, as well as all its open subgroups, satisfy Hilbert's Theorem 90 for $\mathbb{G}_m$.
We now wish to share the main ideas which are at the heart of this paper. In what follows, F is a field and d is a positive integer, invertible in F. We assume that $d = p^s$ is a prime power. Let F_{sep}/F be a separable closure of F. We put $G := \mathrm{Gal}(F_{sep}/F)$.

1.1. First idea. Imagine you want to prove the surjectivity of the norm-residue homomorphism, in the Merkurjev-Suslin case ($n = 2$). It amounts to proving the following. For every class $e \in H^2(F, \mu_d^{\otimes 2})$, there exists an integer $r \geq 1$, such that e is in the image of the cup-product map

$$H^1(F, \mu_d^r) \times H^1(F, \mu_d^r) \longrightarrow H^2(F, \mu_d^{\otimes 2}),$$

relative to the canonical diagonal pairing

$$\mu_d^r \times \mu_d^r \longrightarrow \mu_d^{\otimes 2}$$

(note that μ_d^r stands here for the direct sum of r copies of μ_d).
But it is immediate that, given a class $e \in H^2(F, \mu_d^{\otimes 2})$, one can find a finite discrete G-module M, which is a free $\mathbb{Z}/d\mathbb{Z}$-module, and such that e is in the image of the cup-product map

$$H^1(F, M \otimes_{\mathbb{Z}} \mu_d) \times H^1(F, M^* \otimes_{\mathbb{Z}} \mu_d) \longrightarrow H^2(F, \mu_d^{\otimes 2}),$$

relative to the canonical pairing

$$(M \otimes_{\mathbb{Z}} \mu_d) \times (M^* \otimes_{\mathbb{Z}} \mu_d) \longrightarrow \mu_d^{\otimes 2},$$

where

$$M^* = \mathrm{Hom}_{\mathbb{Z}/d\mathbb{Z}}(M, \mathbb{Z}/d\mathbb{Z}).$$

This is an avatar of the trivial fact that a (Yoneda) 2-extension is a cup-product of two 1-extensions! The surjectivity of the norm-residue homomorphism is then equivalent to saying that one may choose M such that G acts trivially on it. Roughly speaking, our Lifting Theorems (Theorem 12.4 in particular), will allow us to do the following. Starting from an arbitrary M, we will be able to recursively simplify the way G acts on it, until M becomes *induced*, i.e. possesses a $\mathbb{Z}/d\mathbb{Z}$-basis which is permuted by G. Of course, this is done at the expense of considerably increasing the rank of M as a $\mathbb{Z}/d\mathbb{Z}$-module. An elementary input from Milnor K-theory (namely, the existence of the norm, and its compatibility with the norm-residue homomorphism) then allows us to assume that G acts trivially on M. Note that we can in fact control the evolution of the rank of M (cf. Theorem 14.2), using the Theorem of Rosset and Tate in Milnor K-theory.

1.2. Second idea. How can we prove that a cohomology class, in Galois cohomology, vanishes? To the authors' knowledge, the only systematic way to do so is by invoking, somewhere, Hilbert's Theorem 90. It is indeed folklore that, in cohomological statements involving Galois cohomology of an arbitrary field, with values in (twists of) roots of unity, Hilbert's Theorem 90 plays an essential rôle. This paper can in fact be viewed as a machinery, drawing information on the Galois theory of a field F, by applying Hilbert's Theorem 90 to a -huge- amount of its finite field extensions. Let us be more precise.
Working with finite coefficients, this Theorem asserts that the canonical surjection

$$\mu_{p^{s+1}} \stackrel{x\mapsto x^p}{\longrightarrow} \mu_{p^s}$$

induces a surjective map

$$H^1(E, \mu_{p^{s+1}}) \longrightarrow H^1(E, \mu_{p^s}),$$

for every (finite separable) field extension E/F. We interpret this, in the spirit of the classical definition of a formally smooth morphism in algebraic geometry, as a smoothness property of the roots of unity, which we systematically study. Through our Lifting Theorems, we eventually prove the Smoothness Theorem (Theorem 13.8). it essentially states that all maps

$$H^n(E, \mu_{p^{s+1}}^{\otimes n}) \longrightarrow H^n(E, \mu_{p^s}^{\otimes n})$$

are also surjective, and that this (almost) formally follows from the $n = 1$ case, using the Third Idea below.

1.3. Third idea. The theory of Witt vectors associates, to every perfect field k of characteristic p, a ring $\mathbf{W}(k)$, whose basic properties we shall recall in the next section. We develop here the theory of divided powers over Witt vectors, whose purpose is, somehow, to 'categorify' Witt's construction. In other words, we associate to every k-vector space V, the divided power $\mathbf{W}(k)$-modules $\Gamma^i_{\mathbf{W}(k)}(V)$. This is done in such a way that, in dimension one, we recover the construction given by the Teichmüller section

$$\tau : k^\times \longrightarrow \mathbf{W}(k)^\times.$$

In the recent preprint [K], a related construction is introduced. Note that Kaledin's construction, which does not use divided powers, commutes with Pontryagin duality, whereas the formation of divided powers over Witt vectors does not. As a matter of fact, we shall use the Pontryagin dual counterpart of divided powers over Witt vectors, which we call Omega powers. We develop a Kummer-like theory, for Omega powers of arbitrary (Galois) representations over a finite field. We introduce the Transfer, of crucial importance. It is a slightly refined version of the Steenrod algebra. Combining this with classical techniques from group cohomology (dimension shifting, restriction, corestriction, cup-product and Shapiro's Lemma), we are able to prove very general Lifting Theorems for the cohomology of smooth profinite groups (e.g. Theorem 12.4).

The paper is organized as follows. We first recall some classical facts about profinite groups, representation theory, cohomology, and Yoneda extensions. We define the categories $\mathcal{M}(\mathbf{W}(k), G)$ and $\mathcal{M}(k, G)$, in which we shall be working later on. We then explain, in section 4, a categorical formulation of the induction process from open subgroups and of Shapiro's Lemma. Though elementary, it plays an important rôle in this paper, where most properties concerning a profinite group G (eg. n-surjectivity) involve all open subgroups of G at once. In

section 5, we recall (mostly well-known) facts about divided powers. We mainly concentrate on the case of modules over Witt vectors. Along the way, we give a simple presentation of truncated Witt vectors, as a quotient of a divided power module over $\mathbb{Z}$ (cf. Proposition 5.21). In section 6, we introduce the Frobenius and Verschiebung operators, for divided powers. In section 7, we introduce Omega powers, which are Pontryagin dual to divided powers, and which are much better behaved for applications to (Galois) cohomology. In section 8, we define the transfer, a fundamental gadget for Omega powers, enabling us to prove some Theorems by induction on the dimension of the (k, G)-modules under consideration (for k finite). In section 9, we introduce the notions of n-surjectivity and of n-smoothness for profinite groups. We give, as a fundamental example for 1-smoothness, that of an absolute Galois group. Section 10 sheds light on the importance of Hilbert's Theorem 90 in our approach. In Proposition 10.4, we give a general formulation of this Theorem, probably well-known to some algebraists. In section 11, we first emphasize the canonical (equivariant) aspect of all the constructions done before. We then focus on a Lifting Proposition, for the cohomology of smooth profinite groups. The proof is quite technical and proceeds by induction from the one-dimensional case, using the transfer and Shapiro's Lemma. It is the key tool to proving the Lifting Theorems of the next sections, culminating with Theorem 12.4, and with the Smoothness Theorem (Theorem 13.8). We conclude by the applications we promised: a new proof of the surjectivity of the norm-residue homomorphism, a bound on the symbol length of central simple algebras, and a Lifting Theorem for mod p Galois representations.

This paper contains numerous remarks and exercises, which goal is to help the reader getting familiar with our approach, especially for those wishing to read it 'linearly'. Note that, though we decided to treat the case of an arbitrary finite field k in our Lifting Theorems, the case $k = \mathbb{F}_p$ is the essential one.

2. Notation and basic facts.

Throughout this paper, p is a prime number. For any integer n, we denote by $v_p(n)$ the p-adic valuation of n. We denote by $\mathcal{S}_n$ the symmetric group on n letters.

If M is an Abelian group and $n \geq 1$ is an integer, we denote by $T_n(M)$ the n-torsion of M. Let A be a ring. If X is a finite set, we shall denote by $A[X]$ the free A-module with basis indexed by X. For $x \in X$, the basis vector corresponding to x will be denoted by $[x]$. If M is an A-module, we denote by

$$M^* = \mathrm{Hom}(M, A)$$

the A-dual of M. We denote by

$$\mathrm{Sym}_A(M) = \bigoplus_{i=0}^{\infty} \mathrm{Sym}_A^i(M)$$

the symmetric algebra of M. We denote by

$$\Lambda_A(M) = \bigoplus_{i=0}^{\infty} \Lambda_A^i(M)$$

the exterior algebra of M.
If M is locally free of finite rank (as an A-module), we denote by

$$\mathbb{A}_A(M) := \mathrm{Spec}(\mathrm{Sym}_A(M^*))$$

the affine space of M; it is an affine variety over $\mathrm{Spec}(A)$. On the level of the functor of points, we have

$$\mathbb{A}_A(M)(B) = M \otimes_A B,$$

for every commutative A-algebra B.

Let k be a field. Let V be finite-dimensional k-vector space. We denote by $\mathbb{P}(V)$ the projective space of V, consisting of lines $d \subset V$ (when needed, these shall be identified with hyperplanes in V^*). It can, of course, be viewed as a k-variety. However, in this work (where in most cases k and V will be finite), it will only be considered as a set. Note that, if V is a linear representation of a group G, $\mathbb{P}(V)$ is naturally endowed with an action of G.

2.1. Witt vectors. If k is a perfect field of characteristic $p > 0$, we denote by $\mathbf{W}(k)$ the ring of Witt vectors built out from k. It is, up to isomorphism, the unique complete discrete valuation ring whose maximal ideal is generated by p, and with residue field k. Its construction is functorial in k. For any positive integer n, we denote by

$$\mathbf{W}_n(k) := \mathbf{W}(k)/p^n$$

the truncated Witt vectors of size n.
A simple (and perhaps new) formula, presenting $\mathbf{W}_{n+1}(k)$ as a quotient of the p^n-th divided power of the $\mathbb{Z}$-module k, shall be given later on.
We shall put

$$K := \mathrm{Frac}(\mathbf{W}(k)).$$

For any $\mathbf{W}(k)$-module M, we put

$$M^\vee := \mathrm{Hom}_{\mathbf{W}(k)}(M, K/\mathbf{W}(k)).$$

The Frobenius morphism

$$k \longrightarrow k,$$
$$x \mapsto x^p$$

lifts to a ring homomorphism

$$\mathrm{Frob} : \mathbf{W}(k) \longrightarrow \mathbf{W}(k).$$

For any $\mathbf{W}(k)$-module V, and any integer $i \geq 0$, we put

$$V^{(i)} := V \otimes_{\mathbf{W}(k)} \mathbf{W}(k);$$

where the tensor product is taken with respect to Frob^i.

2.2. Profinite groups and cohomology. Let G be a profinite group. By definition, a G-set is a set X, equipped with a continuous action of G (i.e. such that the stabilizer of every element of X is open in G).
Let M be a discrete G-module; that is, an Abelian group M, equipped with the structure of a G-set, for which the action of G is $\mathbb{Z}$-linear. We then denote by $H^n(G, M)$ the usual cohomology groups, as defined in [Se]. At our disposal, we have the restriction maps

$$\mathrm{Res} : H^n(G, M) \longrightarrow H^n(G', M),$$

for any closed subgroup $G' \subset G$, and the corestriction maps

$$\mathrm{Cor} : H^n(G', M) \longrightarrow H^n(G, M),$$

for any (nontrivial) open subgroup $G' \subset G$.
If $G' \subset G$ is a (nontrivial) open subgroup, of index n in G, then Cor $\circ$ Res equals multiplication by n.

Remark 2.1. In most of the proofs of the main Theorems of this paper, involving a profinite group G, we shall often reduce to the case where G is pro-p-group, using the 'restriction-corestriction' argument. More precisely, imagine that the discrete G-module M is of p-primary torsion, and that we have to show that a class in $H^n(G, M)$ is zero. Then, it is enough to show that its restriction to $H^n(G_p, M)$ vanishes, where G_p is a pro-p-Sylow of G.

3. Categories of representations and Yoneda extensions

Let G be a profinite group. Let k be a finite field, of characteristic p.

Definition 3.1. *A $(\mathbf{W}(k), G)$-module is $\mathbf{W}(k)$-module M, which is finite as a set, endowed with a continuous $\mathbf{W}(k)$-linear action of G (i.e. factoring through a nontrivial open subgroup of G). A (k, G)-module is a $(\mathbf{W}(k), G)$-module which is a k-vector space.*

Remark 3.2. Let F_{sep}/F be a separable closure of a field F, of characteristic not p. Then a $(k, \mathrm{Gal}(F_{sep}/F))$-module is nothing but a Galois representation over the field k.

Remark 3.3. if G is a pro-p-group, we shall, in many places, use the following classical facts.
(i) Every one-dimensional (k, G)-module is trivial, i.e. isomorphic to k, equipped with the trivial action of G.
(ii) Let V be a nonzero (k, G)-module. Then, it admits a one-dimensional sub-(k, G)-module. Equivalently, we have $V^G \neq \{0\}$.

Definition 3.4. *We denote by $\mathcal{M}(\mathbf{W}(k), G)$ (resp. $\mathcal{M}(k, G)$ the category of $(\mathbf{W}(k), G)$-modules (resp. of (k, G)-modules), with morphisms being $\mathbf{W}(k)$-linear maps respecting the action of G. These categories are Abelian. They come equipped with a tensor product*

$$\otimes = \otimes_{\mathbf{W}(k)}.$$

They are, moreover, equipped with a perfect duality

$$M \mapsto M^\vee = \mathrm{Hom}_{\mathbf{W}(k)}(M, K/\mathbf{W}(k)).$$

Let $n \geq 1$ be an integer. Let $A, B \in \mathcal{M}(\mathbf{W}(k), G)$. As in any Abelian category, we have the notion of Yoneda n-extension of A by B, which we now briefly recall. As usual, $\mathrm{YExt}^0_{(\mathbf{W}(k),G)}(A, B)$ is defined to be $\mathrm{Hom}(A, B)$.

A n-extension of A by B is an exact sequence (in $\mathcal{M}(\mathbf{W}(k), G)$)

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

One can add two n-extensions of A by B using the Baer sum, the trivial extension being the direct sum

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

if $n = 1$, or the n-extension

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

otherwise. The Baer sum of two n-extensions $\mathcal{E}_1$ and $\mathcal{E}_2$ (of A by B) will be denoted simply by $\mathcal{E}_1 + \mathcal{E}_2$. 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 A and B. The n-extensions of A by B thus form an additive category $\mathbf{YExt}^n_{(\mathbf{W}(k),G)}(A,B)$.
Moreover, a morphism $f : B \longrightarrow B'$ (resp. $g : A' \longrightarrow A$) induces a push forward functor

$$f_* : \mathbf{YExt}^n_{(\mathbf{W}(k),G)}(A,B) \longrightarrow \mathbf{YExt}^n_{(\mathbf{W}(k),G)}(A,B')$$

(resp. a pullback functor

$$g^* : \mathbf{YExt}^n_{(\mathbf{W}(k),G)}(A,B) \longrightarrow \mathbf{YExt}^n_{(\mathbf{W}(k),G)}(A',B)).$$

Those functors commute, in the sense that f_*g^* and g^*f_* are canonically isomorphic.

Let us say that two n-extensions $\mathcal{E}_1$ and $\mathcal{E}_2$ are elementary linked if there exists a morphism $\mathcal{E}_1 \longrightarrow \mathcal{E}_2$ or $\mathcal{E}_2 \longrightarrow \mathcal{E}_1$. Now, say that $\mathcal{E}$ and $\mathcal{E}'$ are equivalent if there exists extensions $\mathcal{E} = \mathcal{E}_0, \mathcal{E}_0, \ldots, \mathcal{E}_r = \mathcal{E}'$, such that $\mathcal{E}_i$ is elementary linked to $\mathcal{E}_{i+1}$ for each i. This is an equivalence relation, compatible with the Yoneda sum.

Definition 3.5. *We denote by* $\mathrm{YExt}^n_{(\mathbf{W}(k),G)}(A,B)$ *the Abelian group of equivalence classes of Yoneda n-extensions, in the category* $\mathbf{YExt}^n_{(\mathbf{W}(k),G)}(A,B)$.

Note that the exact functor $M \mapsto M^\vee$ induces a canonical isomorphism

$$\mathrm{YExt}^n_{(\mathbf{W}(k),G)}(B,A) \xrightarrow{\sim} \mathrm{YExt}^n_{(\mathbf{W}(k),G)}(A^\vee, B^\vee).$$

Definition 3.6. *Similary, we define* $\mathbf{YExt}^n_{(k,G)}(A,B)$ *and* $\mathrm{YExt}^n_{(k,G)}(A,B)$*, for* $A, B \in \mathcal{M}(k,G)$*, by working in the smaller category* $\mathcal{M}(k,G)$.

Note that k-linear duality induces a canonical isomorphism

$$\mathrm{YExt}^n_{(k,G)}(A,B) \xrightarrow{\sim} \mathrm{YExt}^n_{(k,G)}(B^*, A^*).$$

Lemma 3.7. *Let A, B be two (k,G)-modules. Then, for any $n \geq 0$, there is a canonical isomorphism*

$$\mathrm{YExt}^n_{(k,G)}(A,B) \xrightarrow{\sim} \mathrm{YExt}^n_{(k,G)}(k, \mathrm{Hom}_k(A,B)).$$

Proof. Clearly, we have a canonical isomorphism

$$A^* \otimes B \xrightarrow{\sim} \mathrm{Hom}_k(A,B).$$

Applying the functor $A^* \otimes .$ yields a functor

$$\Phi : \mathbf{YExt}^n_{(k,G)}(A,B) \longrightarrow \mathbf{YExt}^n_{(k,G)}(A^* \otimes A, A^* \otimes B),$$

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

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

But the G-equivariant map

$$\Psi : k \longrightarrow A^* \otimes A = \mathrm{End}_k(A),$$

$$\lambda \mapsto \lambda \mathrm{Id}$$

gives a pullback functor

$$\Psi^* : \mathbf{YExt}^n_{(k,G)}(A^* \otimes A, A^* \otimes B) \longrightarrow \mathbf{YExt}^n_{(k,G)}(k, \mathrm{Hom}_k(A,B)).$$

The composite

$$\Psi^* \circ \Phi : \mathbf{YExt}^n_{(k,G)}(A,B) \longrightarrow \mathbf{YExt}^n_{(k,G)}(k, \mathrm{Hom}_k(A,B))$$

gives, by passing to isomorphism classes of objects, a group homomorphism

$$\mathrm{YExt}^n_{(k,G)}(A,B) \longrightarrow \mathrm{YExt}^n_{(k,G)}(k, \mathrm{Hom}_k(A,B)),$$

which is easily seen to be an isomorphism.

□

PROPOSITION 3.8. *Let V be a (k,G)-module. Then, for any $n \geq 0$, there is a canonical isomorphism*

$$\mathrm{YExt}^n_{(k,G)}(k,V) \simeq H^n(G,V).$$

Proof. Let us first deal with the case where G is finite.
The group $H^n(G,V)$ is the n-th derived functor of the functor

$$V \mapsto V^G = \mathrm{Hom}_{(k,G)}(k,V).$$

Thus, it is nothing but the usual Ext group $\mathrm{Ext}^n_{(k,G)}(k,V)$, computed using injective resolutions. But, for any Abelian category with enough injectives, the derived Ext's coincide with the Yoneda YExt's ([Ve], Ch. III, Par. 3).
The case G arbitrary readily follows from a classical limit argument, over the finite quotients of G. □

4. On induction from subgroups, and Shapiro's Lemma.

We now make some essential remarks, with which the reader shall tacitly be assumed to be familiar in the sequel.

DEFINITION 4.1. *Let G be a profinite group. Let X be a finite G-set. A discrete G-module over X is the data of*

$$\mathcal{M} = (M_x, \phi_{g,x}),$$

consisting of an Abelian group M_x, for each $x \in X$, and of additive maps

$$\phi_{g,x} : M_x \longrightarrow M_{gx},$$

for each $x \in X$ and $g \in G$, subject to the following conditions.
(i) For all $x \in X$, and all $m \in M_x$, the map

$$G \longrightarrow \bigsqcup_{g \in G} M_{gx},$$

$$g \mapsto \phi_{g,x}(m),$$

is continuous (=locally constant).
ii) For all $x \in X$, we have

$$\phi_{e,x} = \mathrm{Id}.$$

(iii) For all $x \in X$ and $g,h \in G$, we have

$$\phi_{g,hx} \circ \phi_{h,x} = \phi_{gh,x}.$$

Remark 4.2. In the particular case of a one-element set, it is clear that a discrete G-module over $\{*\}$ is just a discrete G-module.

Remark 4.3. Discrete G-modules over X form an Abelian category in the obvious way. More precisely, a morphism

$$\mathcal{M} = (M_x, \phi_{g,x}) \longrightarrow \mathcal{M}' = (M'_x, \phi'_{g,x})$$

is the data of additive maps

$$f_x : M_x \longrightarrow M'_x,$$

one for each $x \in X$, such that

$$\phi'_{g,x} \circ f_x = f_{gx} \circ \phi_{g,x},$$

for all $x \in X$ and all $g \in G$.

If $\mathcal{M} = (M_x, \phi_{g,x})$ is a discrete G-module over X, we can form the direct sum

$$N(\mathcal{M}) := \bigoplus_{x \in X} M_x;$$

it is a G-module in an obvious way, given by applying the $\phi_{g,x}$'s. The association

$$\mathcal{M} \mapsto N(\mathcal{M})$$

is a functor, from the category of discrete G-modules over X to that of discrete G-modules. It plays the rôle of a trace map, and is a categorical formulation of the usual induction process, from open subgroups of G. We now explain why.

Assume that

$$X = G/H,$$

for $H \subset G$ a nontrivial open subgroup. Denote by $x_0 \in X$ the class of the neutral element.
Then we have a functor

$$\mathcal{M} = (M_x, \phi_{g,x}) \longrightarrow M_{x_0},$$

from the category of discrete G-modules over X to that of discrete H-modules, where M_{x_0} is considered as an H-module via the maps ϕ_{h,x_0}, for $h \in H = \mathrm{Stab}(\mathrm{x}_0)$. It is not hard to see that this functor is an equivalence of categories. The proof is left to the reader as an exercise.

Remark 4.4. What precedes is a concrete example of the following philosophical statement: if $X = G/H$, a G-equivariant structure over the base X is nothing but an H-equivariant structure.

Now, let $\mathcal{M} = (M_x, \phi_{g,x})$ be a G-module over X. Put $M := M_{x_0}$, seen as a discrete H-module. Then

$$N(\mathcal{M}) = \bigoplus_{x \in X} M_x$$

is canonically isomorphic to the induced module $\mathrm{Ind}_H^G(M)$. Note that, since H has finite index in G, this induced module can be defined either by the formula

$$\mathrm{Ind}_H^G(M) = M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G],$$

or by

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

the group of H-equivariant maps from G to M ('induction=coinduction' in this case).
Now, recall Shapiro's Lemma -which is elementary but of crucial importance in this paper- asserting that the cohomology groups $H^n(G, \mathrm{Ind}_H^G(M))$ and $H^n(H, M)$ are

canonically isomorphic. Putting what we just said together, we get the following statement.

PROPOSITION 4.5. *Put*

$$X = G/H,$$

for $H \subset G$ a nontrivial open subgroup. Denote by $x_0 \in X$ the neutral class.
Let $\mathcal{M} = (M_x, \phi_{g,x})$ be a discrete G-module over X. Then M_{x_0} is canonically a discrete H-module, and Shapiro's lemma yields canonical isomorphisms

$$H^n(G, \bigoplus_{x \in X} M_x) \xrightarrow{\sim} H^n(H, M_{x_0}),$$

for each $n \geq 0$.

Remark 4.6. If X is an arbitrary finite G-set and $\mathcal{M} = (M_x, \phi_{g,x})$ is a discrete G-module over X, we can adapt the preceding Proposition, yielding canonical isomorphisms

$$H^n(G, \bigoplus_{x \in X} M_x) \xrightarrow{\sim} \bigoplus_{i=1}^{m} H^n(G_i, M_{x_i}),$$

where the $x_i's$ form a system of representatives of G-orbits in X, and where G_i is the stabilizer of x_i.

The preceding Remark shall be used constantly in proofs later on, without further notice.
To finish this section, let us give a typical example of how this Remark will be applied.
Let k be a finite field of characteristic p. Let V be a (k, G)-module. Put

$$X := \mathbb{P}(V);$$

it is obviously a finite G-set.
There is a 'tautological' discrete G-module over X, which is $\mathcal{M}$, defined by

$$M_L := V/L,$$

for each line $L \in X$, and where the map

$$\phi_{g,L} : V/L \longrightarrow V/g(L)$$

is induced by the linear map $v \mapsto g.v$. Shapiro's Lemma then yields canonical isomorphisms

$$H^n(G, N(\mathcal{M})) = H^n(G, \bigoplus_{L \in \mathbb{P}(V)} V/L) \xrightarrow{\sim} \bigoplus_{i=1}^{m} H^n(G_i, V/L_i),$$

like we just discussed in the Remark above. This fundamental fact will mostly be used in the proof of Proposition 11.6, where, using the transfer, it allows us to proceed by induction on the dimension of the (k, G)-modules under consideration.

5. DIVIDED POWERS.

For a nice and short account on properties of divided powers, we refer the reader to [Fe]. A more comprehensive study of divided powers can be found in [Ro], which contains all the proofs of the Propositions which we state here without proof.

In this section, A is a commutative ring.

DEFINITION 5.1. *Let V be an A-module.*
We denote by $\Gamma_A(V)$ (or simply by $\Gamma(V)$ if the dependence in A is clear) the graded divided power algebra of V, defined as follows. It is generated by degree i symbols $[v]_i$, for each $i \in \mathbb{N}$ and each $v \in V$, with relations:

i) $[v]_0 = 1$,
ii)$[v + v']_n = \sum_0^n [v]_i [v']_{n-i}$,
iii)$[\lambda v]_n = \lambda^n [v]_n$,
iv) $[v]_n [v]_m = \binom{n+m}{n} [v]_{n+m}$.

We define $\Gamma^n(V)$ to be the homogeneous component of degree n of $\Gamma(V)$. We put $\Gamma^+(V) := \oplus_{n \geq 1} \Gamma^n(V)$; it is an ideal of $\Gamma(V)$.

Remarks 5.2. As it is well-known, the symbol $[v]_n$ plays the rôle of $v^n/n!$.
For each positive integer i, the ideal $\Gamma^+(V)$ is moreover equipped with an operator

$$\gamma_i : \Gamma^+(V) \longrightarrow \Gamma^+(V),$$
$$a \mapsto \gamma_i(a),$$

playing the rôle of $a \mapsto a^i/i!$, which endows $(\Gamma(V), \Gamma(V)^+)$ with the structure of an A-algebra with divided powers. We shall not use this operator.

Remark 5.3. Equality iv), applied several times, yields the formula

$$[v]_{n_1} \dots [v]_{n_r} = \binom{n_1 + \dots + n_r}{n_1, \dots, n_r} [v]_{n_1 + \dots + n_r},$$

where

$$\binom{n_1 + \dots + n_r}{n_1, \dots, n_r} = \frac{(n_1 + \dots + n_r)!}{n_1! \dots n_r!}$$

is the usual multinomial coefficient.

PROPOSITION 5.4. *Let M, N be A-modules. We have a canonical isomorphism*

$$\Gamma^n(M \oplus N) \simeq \oplus_0^n (\Gamma^i(M) \otimes_A \Gamma^{n-i}(N)).$$

Remark 5.5. The previous Proposition says that divided power functors are strictly polynomial, in the sense of [FFSS].

PROPOSITION 5.6. *Let M be an A-module, and let B/A be a commutative A-algebra. We have a canonical isomorphism of graded rings*

$$\Gamma_A(M) \otimes B \simeq \Gamma_B(M \otimes_A B).$$

5.1. POLYNOMIAL LAWS. Let A be a commutative ring.

DEFINITION 5.7. *If M is an A-module, we denote by $\underline{M}$ the functor*

$$R \mapsto M \otimes_A R,$$

from the category of commutative A-algebras to that of sets.

DEFINITION 5.8. *Let M, N be A-modules. A polynomial law from M to N is a morphism of functors*

$$F : \underline{M} \longrightarrow \underline{N}.$$

We shall say that F is homogeneous of degree $n \geq 0$ if, for every commutative A-algebra R and every $t \in R$ and $m \in M \otimes_A R$, we have

$$F(tm) = t^n F(m).$$

Remark 5.9. One can show that a degree 0 (resp. degree 1) polynomial law is obtained from a constant (resp. A-linear) map $M \longrightarrow N$.

Remark 5.10. Slightly abusing notation, we will sometimes denote a polynomial law

$$F : \underline{M} \longrightarrow \underline{N}$$

simply by

$$F : M \longrightarrow N,$$

dropping the underscore. We shall do so only if there is no chance of confusing F with a mere map.

Remark 5.11. If M and N are locally free A-modules of finite rank, then a polynomial law from M to N is nothing but a morphism of affine A-schemes

$$\mathbb{A}_A(M) \longrightarrow \mathbb{A}_A(N).$$

In this paper, we shall mainly be interested in polynomial laws between vector spaces over a finite field k, and shall thus view them as morphisms between affine spaces, defined over k.

PROPOSITION 5.12. *Let V, W be A-modules. Then $\mathrm{Hom}_A(\Gamma^n(V), W)$ is canonically isomorphic to the group of polynomial laws from V to W, which are homogeneous of degree n.*

For V an A-module, the association

$$V \longrightarrow (V^{\otimes n})^{\mathcal{S}_n},$$

$$v \mapsto v^n,$$

is obviously a polynomial law, which is homogeneous of degree n. It thus induces an A-linear morphism

$$F_n(V) : \Gamma^n_A(V) \longrightarrow (V^{\otimes n})^{\mathcal{S}_n}.$$

PROPOSITION 5.13. *If V is locally free of finite rank, the morphism $F_n(V)$ above is an isomorphism.*

Remark 5.14. If V is locally free of finite rank, the A-dual of $(V^{\otimes n})^{\mathcal{S}_n}$ is nothing but the symmetric power $\mathrm{Sym}^n_A(V^*)$. Thus, the formation of divided powers, for finite locally free modules, is dual to that of symmetric powers.

Among polynomial laws, there are fundamental ones: those, roughly speaking, given by Teichmüller representatives in truncated Witt vectors. Let us be more precise.

LEMMA 5.15. *The map*

$$A \longrightarrow A/p^{n+m}A,$$

$$x \mapsto x^{p^n},$$

factors through the quotient $A \longrightarrow A/p^m A$. Since this hold functorially for any commutative ring A, we get this way a polynomial law of $\mathbb{Z}$-modules

$$\mathbb{Z}/p^m\mathbb{Z} \longrightarrow \mathbb{Z}/p^{m+n}\mathbb{Z},$$

$$x \mapsto x^{p^n}.$$

Proof. By induction, it is enough to check the claim for $n = 1$. In this case, for any $x, y \in A$, we have the well-known congruence

$$(x + p^m y)^p \equiv x^p$$

modulo $p^{m+1}A$, whence the claim.

□

We now concentrate on the characteristic p case.

LEMMA 5.16. *Let*

$$n = a_1 + \ldots + a_r$$

be a decomposition of the positive integer n into a sum of r nonnegative integers, such that there are no carryovers in the base-p addition of $a_1, a_2, \ldots, a_r$.
Then $\binom{n}{a_1,\ldots,a_r}$ is prime-to-p.

Proof. It is easy to reduce to the case $r = 2$, using the formula

$$\binom{n}{a_1, \ldots, a_r} = \binom{n}{a_1 + a_2, a_3, \ldots, a_r}\binom{a_1 + a_2}{a_1, a_2}.$$

We then use the following well-known fact: if a and b are positive integers, then $v_p(\binom{a+b}{a,b})$ equals the number of carryovers in the base-p addition of a and b.

□

Remark 5.17. In particular, the hypothesis of the preceding Lemma is satisfied if all a_i's are powers of p, such that each power of p occurs at most $p - 1$ times among them.

LEMMA 5.18. *Let V be an A-module, such that $pV = 0$, and let n be a positive integer. Then $\Gamma^n_A(V)$ is of $p^{v_p(n)+1}$-torsion.*

Proof. Note first the following obvious fact. Let

$$n = a_1 + \ldots + a_r$$

be a decomposition of n into a sum of r nonnegative integers. For $i = 1 \ldots r$, let v_i be an element of V. Then the (additive) order of

$$[v_1]_{a_1} \ldots [v_r]_{a_r} \in \Gamma^n_A(V)$$

is at most the minimum of the orders of the elements $[v_i]_{a_i} \in \Gamma^{a_i}_A(V)$.
In view of Lemma 5.16, of Remark 5.17 and of Remark 5.3, considering the base-p expansion of n, we may thus assume that $n = p^m$ is a power of p. We have

$$\binom{p^m}{p^{m-1}, \ldots, p^{m-1}}[v]_{p^m} = [v]^p_{p^{m-1}},$$

and it is easy to see that the multinomial coefficient $\binom{p^m}{p^{m-1},\ldots,p^{m-1}}$ has p-valuation equal to one, hence

$$p[v]_{p^m} = N(m)[v]^p_{p^{m-1}},$$

with $N(m)$ prime-to-p (in fact congruent to -1 mod p). Since the symbols $[v]_1$ depend linearly on V, they are of p-torsion, and the preceding formula readily implies the result, by induction on m. □

Remark 5.19. The preceding Lemma is crucial. It outlines a fundamental difference between divided powers and symmetric powers. Indeed, let V be an A-module. If it is of p-torsion, then so will be the symmetric powers $\mathrm{Sym}^n_A(V)$, whereas the divided powers $\Gamma^n_A(V)$ will in general not be. For instance, we have

$$\Gamma^p_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p^2\mathbb{Z}.$$

We will now study this phenomenon in more detail.

From now on, k is a perfect field of characteristic p. We shall denote by

$$\tau : k \longrightarrow \mathbf{W}(k)$$

the Teichmüller representative (we set $\tau(0) = 0$). Recall that the map

$$\tau_{|k^\times} : k^\times \longrightarrow \mathbf{W}(k)^\times$$

is the unique multiplicative section of the quotient map

$$\mathbf{W}(k)^\times \longrightarrow k^\times.$$

Recall that K denotes the field of fractions of $\mathbf{W}(k)$. Note that the functor

$$M \mapsto M^\vee = \mathrm{Hom}_{\mathbf{W}(k)}(M, K/\mathbf{W}(k))$$

yields an equivalence between the category of torsion $\mathbf{W}(k)$-modules of finite type and its opposite category. This fact is nothing but a slight generalization of a usual statement when $k = \mathbb{F}_p$.

Let n be a positive integer. Take A to be $\mathbf{W}_{n+1}(k)$, the truncated Witt vectors of size $n+1$. By Lemma 5.15, the formula

$$k = A/pA \longrightarrow A/p^{n+1}A = \mathbf{W}_{n+1}(k),$$
$$x \mapsto x^{p^n},$$

defines a (multiplicative) polynomial law over $\mathbb{Z}$, homogeneous of degree p^n. It thus induces a group homomorphism

$$T'_n : \Gamma^{p^n}_{\mathbb{Z}}(k) \longrightarrow \mathbf{W}_{n+1}(k).$$

It is easy to see that $T'_n([x]_{p^n}) \in \mathbf{W}_{n+1}(k)$ is the Teichmüller representative $\tau(x^{p^n})$. Since the Teichmüller representatives generate $\mathbf{W}_{n+1}(k)$ additively, the map T'_n is surjective. But obviously, the polynomial law

$$k = A/pA \longrightarrow A/p^{n+1}A = \mathbf{W}_{n+1}(k),$$
$$x \mapsto x^{p^n},$$

might as well be considered as a polynomial law over $\mathbf{W}(k)$, hence as a $\mathbf{W}(k)$-linear homomorphism

$$T_n : \Gamma^{p^n}_{\mathbf{W}(k)}(k) \longrightarrow \mathbf{W}_{n+1}(k).$$

Lemma 5.20. *The map T_n is an isomorphism.*

Proof. It is clearly surjective. But $\Gamma^{p^n}_{\mathbf{W}(k)}(k)$ is generated by $[1]_{p^n}$, as a $\mathbf{W}(k)$-module, and is killed by p^{n+1}, by Lemma 5.18. It is thus a $\mathbf{W}_{n+1}(k)$-module, generated by one element. The claim follows. □

Thus, the map T'_n factors as

$$T'_n : \Gamma^{p^n}_{\mathbb{Z}}(k) \longrightarrow \Gamma^{p^n}_{\mathbf{W}(k)}(k) \xrightarrow{T_n} \mathbf{W}_{n+1}(k).$$

It is then easy to infer a description of the kernel of T'_n, which in turn provides a rather simple, seemingly new, functorial description of $\mathbf{W}(k)$. It will not be used in the sequel.

PROPOSITION 5.21. *Denote by $\mathcal{I}$ the homogeneous ideal of $\Gamma_{\mathbb{Z}}(k)$ generated by expressions of the form*

$$[x]_{p^{s+r}}[y]_{p^s} - [x^{p^r}y]_{p^s}[1]_{p^{r+s}},$$

with $x, y \in k$ and $r, s \geq 1$. Then the kernel of T'_n is $\mathcal{I}_{p^n}$, the homogenous component of degree p^n of $\mathcal{I}$.

Proof. First of all, let us check that $\mathcal{I}_{p^n} \subset \mathrm{Ker}(T'_n)$. To do so, it is enough to check that we have $[x]_{p^{r+s}}[y]_{p^s} = [x^{p^r}y]_{p^s}[1]_{p^{r+s}}$ in $\Gamma_{\mathbf{W}(k)}(k)$. This is obvious: both sides equal $\tau(x^{p^{r+s}}y^{p^s})[1]_{p^s}[1]_{p^{r+s}}$. The rest of the proof is left as an exercise for the reader. □

From now on, if V is a k-vector space (regarded as a $\mathbf{W}(k)$-module of p-torsion), we shall put

$$\Gamma^n(V) := \Gamma^n_{\mathbf{W}(k)}(V)$$

and

$$\mathrm{Sym}^n(V) = \mathrm{Sym}^n_{\mathbf{W}(k)}(V) = \mathrm{Sym}^n_k(V).$$

Note that Γ^n is a functor, from the category of k-vector spaces to that of $\mathbf{W}(k)$-modules. It is, of course, not additive if $n \geq 2$.

Remark 5.22. Note that the preceding discussion shows that $\Gamma^{p^r}(k)$, as a $\mathbf{W}(k)$-module, is generated by $[1]_{p^r}$ and is canonically isomorphic to $\mathbf{W}_{r+1}(k)$. We are now going to make this statement more canonical.

If L is a one-dimensional k-vector space, seen as a $\mathbf{W}(k)$-module, then we put

$$\mathbf{W}_{n+1}(L) := \Gamma^{p^n}(L);$$

it is is a free $\mathbf{W}_{n+1}(k)$-module of rank one, whose construction is functorial in L. It comes equipped with a Teichmüller-like map (which is in fact a polynomial law)

$$T_n : L \longrightarrow \mathbf{W}_{n+1}(L),$$

$$v \mapsto [v]_{p^n}.$$

Note that, if $L = k$, then $\mathbf{W}_{n+1}(L) = \mathbf{W}_{n+1}(k)$, and $T_n(x) = \tau(x^{p^n})$, as noted before.

LEMMA 5.23. *Let L be a one-dimensional k-vector space. Let $n = p^r m$ be a positive integer, with m prime to p. Then the formula*

$$L \longrightarrow \mathbf{W}_{r+1}(L^{\otimes m}),$$

$$v \mapsto [v^{\otimes m}]_{p^r},$$

defines a polynomial law, which is homogeneous, of degree n. The induced $\mathbf{W}(k)$-linear map

$$\phi : \Gamma^n(L) \longrightarrow \mathbf{W}_{r+1}(L^{\otimes m})$$

is an isomorphism.

Proof. Only the fact that ϕ is an isomorphism has, perhaps, to be checked. We may assume that $L = k$. By lemma 5.18, the $\mathbf{W}(k)$-module $\Gamma^n(k)$, which is obviously generated by $[1]_n$, is of p^{r+1}-torsion, hence a $\mathbf{W}_{r+1}(k)$-module generated by one element. The map ϕ is obviously surjective, with target a free $\mathbf{W}_{r+1}(k)$-module. It is thus an isomorphism.

□

LEMMA 5.24. *Let V be a k-vector space. For any positive integer n, and any nonzero $v \in V$, the symbol*

$$[v]_n \in \Gamma(V)$$

has order $p^{v_p(n)+1}$.

Proof. By Lemma 5.18, the symbol in question has order $\leq p^{v_p(n)+1}$. Now, pick a k-linear form

$$f : V \longrightarrow k,$$

sending v to 1. By functoriality, it induces a $\mathbf{W}(k)$-linear map

$$F : \Gamma^n(V) \longrightarrow \Gamma^n(k),$$

mapping $[v]_n$ to $[1]_n$. By Lemma 5.23, and by the fact that $1 \in \mathbf{W}_{r+1}(k)$ has order p^{r+1}, we know that $[1]_n$ has order $p^{v_p(n)+1}$. The claim follows. □

LEMMA 5.25. *Let V be a k-vector space. Let n be a positive integer, lesser or equal to the cardinality of k. Then the symbols $[v]_n$, for $v \in V$, generate $\Gamma^n(V)/p$ (as a k-vector space).*

Proof. By a straightforward induction on the dimension $d \geq 2$ of V, it is enough to show that the natural map

$$\bigoplus_{H \in \mathbb{P}(V^*)} \Gamma^n(H)/p \longrightarrow \Gamma^n(V)/p,$$

given by the sum of the inclusions $\Gamma^n(H)/p \longrightarrow \Gamma^n(V)/p$, for all hyperplanes $H \subset V$, is surjective. Dually, letting $W := V^*$, we have to show that the natural map

$$\mathrm{Sym}^n(W) \longrightarrow \oplus_{L \in \mathbb{P}(W)} \mathrm{Sym}^n(W/L),$$

given as the sum of the quotient maps, is injective. But, choosing a k-basis of W, an element of $\mathrm{Sym}^n(W)$ is just a homogeneous polynomial of degree n in d variables. The fact that it dies in $\mathrm{Sym}^n(W/L)$ is equivalent to asking that it is divisible by v, where $v \in L$ is a nonzero vector. The statement now follows, since $\mathbb{P}(W)$ has cardinality at least $|k|+1 \geq n+1$, and since a homogeneous polynomial of degree n, which is divisible by $n+1$ two by two non proportional linear factors, has to be zero.

□

LEMMA 5.26. *Let V be a k-vector space. Let n be a positive integer, lesser or equal to the cardinality of k. Then the symbols $[v]_n$, for $v \in V$, generate $\Gamma^n(V)$ (as a $\mathbf{W}(k)$-module).*

Proof. Consider the filtration

$$\Gamma^n(V) \supset p\Gamma^n(V) \supset p^2\Gamma^n(V) \supset \ldots \supset \{0\},$$

and apply induction using Lemma 5.25 to get the result.

□

We conclude this section by a concrete description of the divided power modules of a k-vector space, using a basis.

PROPOSITION 5.27. *Let V be a k-vector space, with basis $e_1, \dots, e_d$. Let $n \geq 0$ be an integer. Then there exists an isomorphism*

$$\bigoplus_{a_1+\dots+a_d=n} (\bigotimes_{i=1}^{d} \Gamma^{a_i}(k)) \xrightarrow{\sim} \Gamma^n(V),$$

$$[1]_{a_1} \otimes \dots \otimes [1]_{a_d} \mapsto [e_1]_{a_1} \dots [e_d]_{a_d},$$

and the (additive) order of $[e_1]_{a_1} \dots [e_d]_{a_d}$ is $p^{\min(v_p(a_i))+1}$.

The p^t-torsion in $\Gamma^n(V)$ is then identified with the the subgroup generated by elements of the shape

$$p^r [e_1]_{a_1} \dots [e_d]_{a_d},$$

where $\min(v_p(a_i)) - r + 1 \leq t$.

Proof. The first statement follows from Proposition 5.4 and Lemma 5.23. The determination of the order of $[e_1]_{a_1} \dots [e_d]_{a_d}$ follows directly from Lemma 5.23. The assertion concerning the torsion is then obvious. □

5.2. AN ALTERNATE DESCRIPTION OF $\Gamma^p(V)$. Here $k = \mathbb{F}_p$. Assume that $V = M \otimes_{\mathbb{Z}} \mathbb{F}_p$, for M a free $\mathbb{Z}$-module of finite rank. One readily checks that the map

$$C : M \times M \longrightarrow \mathrm{Sym}^p_{\mathbb{Z}}(M),$$

$$(x, y) \mapsto \frac{(x+y)^p - x^p - y^p}{p},$$

is a symmetric 2-cocycle, for the trivial action of M on $\mathrm{Sym}^p_{\mathbb{Z}}(M)$. Indeed, this can be checked after extending scalars to $\mathbb{Q}$, where it is obvious: c is then a trivial cocycle by definition! Reducing mod p, we obtain a symmetric cocycle

$$c : V \times V \longrightarrow \mathrm{Sym}^p_k(V),$$

in fact given by

$$c(x, y) = \sum_{1}^{p-1} \frac{(-1)^{i-1}}{i} x^i y^{p-i}.$$

This cocycle defines an Abelian extension of V by $\mathrm{Sym}^p_k(V)$. We leave it to the reader, as an instructive exercise, to check that this extension is canonically isomorphic to $\Gamma^p(V)$.

6. THE FROBENIUS AND THE VERSCHIEBUNG.

Recall that k is a perfect field of characteristic p.
Let A be a commutative ring of characteristic p. Denote by

$$F_A : A \longrightarrow A,$$

$$x \mapsto x^p,$$

the Frobenius endomorphism of A. For any A-module M, put

$$M^{(1)} := M \otimes_A A,$$

where the tensor product is taken with respect to F_A. This notation is obviously coherent with the one used before.
Moreover, if B/A is a commutative algebra, we have a canonical isomorphism

$$M^{(1)} \otimes_A B \xrightarrow{\sim} (M \otimes_A B)^{(1)}.$$

In other words, forming the twist by Frobenius commutes with extensions of commutative rings of characteristic p.
Now, let V be a k-vector space. By what precedes, the formula

$$V \longrightarrow V^{(1)},$$
$$v \mapsto v^{(1)} := v \otimes 1,$$

actually defines a polynomial law, homogeneous of degree p. We shall refer to this law as the Frobenius law. It can be viewed as a morphism of affine k-spaces

$$\mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(V^{(1)}).$$

The next proposition contains the definition of the Frobenius and of the Verschiebung, borrowed from the theory of commutative group schemes in characteristic p. They are, needless to say, tools of utmost importance in this paper.

PROPOSITION 6.1. *Let V be a finite-dimensional k-vector space and let $n \geq 1$ be an integer.*

Then the formula

$$V \longrightarrow \Gamma^n(V^{(1)}),$$
$$v \mapsto [v^{(1)}]_n,$$

is a polynomial law of degree np, thus defining a $\mathbf{W}(k)$-linear map

$$\mathrm{Frob} : \Gamma^{np}(V) \longrightarrow \Gamma^n(V^{(1)}),$$

the Frobenius homomorphism (for divided powers).
The polynomial law

$$V \longrightarrow \Gamma^{np}(V),$$
$$v \mapsto p[v]_{pn}$$

canonically factors through the Frobenius law $V \longrightarrow V^{(1)}$. The resulting polynomial law

$$V^{(1)} \longrightarrow \Gamma^{np}(V)$$

is homogeneous of degree n, yielding a $\mathbf{W}(k)$-linear map

$$\mathrm{Ver} : \Gamma^n(V^{(1)}) \longrightarrow \Gamma^{np}(V),$$
$$[v^{(1)}]_n \longrightarrow p[v]_{pn},$$

the Verschiebung homomorphism (for divided powers).

Proof.

The first statement (defining the Frobenius map for divided powers) follows from the definition of the Frobenius law. For the second one, pick a basis $e_1, \ldots, e_d$ of V. On the one hand, the Frobenius $V \longrightarrow V^{(1)}$ then becomes the law

$$k^d \longrightarrow k^d,$$
$$(X_1, \ldots, X_d) \mapsto (X_1^p, \ldots, X_d^p).$$

On the other hand, The polynomial law (of $\mathbf{W}(k)$-modules)

$$V \longrightarrow \Gamma^{np}(V),$$

$$v \mapsto p[v]_{pn}$$

then becomes the law

$$k^d \longrightarrow \Gamma^{np}(k^d),$$
$$(X_1, \ldots, X_d) \mapsto p[X_1 e_1 + \ldots + X_d e_d]_{pn}$$
$$= \sum_{a_1+\ldots+a_d=pn} X_1^{a_1} \ldots X_d^{a_d} p[e_1]_{a_1} \ldots [e_d]_{a_d}$$
$$= \sum_{a_1+\ldots+a_d=n} X_1^{pa_1} \ldots X_d^{pa_d} p[e_1]_{pa_1} \ldots [e_d]_{pa_d},$$

where the first (resp. second) sum is taken over all decompositions of pn (resp. of n) into the sum of d nonnegative integers. Indeed, the symbols $[e_i]_a$, for a not divisible by p, are of additive order p, hence all terms $p[e_1]_{a_1} \ldots [e_d]_{a_d}$ vanish, as soon as one of the a_i's is not divisible by p. The second part of the lemma, yielding the definition of the Verschiebung morphism for divided powers, is now obvious.

□

Lemma 6.2. *Let V be a k-vector space. Let $a_1, \ldots, a_d, n$ be nonnegative integers, satistying $a_1 + \ldots + a_d = np$. For $v_1, \ldots, v_d \in V$, the Frobenius*

$$\mathrm{Frob} : \Gamma^{np}(V) \longrightarrow \Gamma^n(V^{(1)})$$

satisfies

$$\mathrm{Frob}([v_1]_{a_1} \ldots [v_d]_{a_d}) = 0,$$

if one of the a_i's is not divisible by p. If all a_i's are divisible by p, says $a_i = pb_i$, then

$$\mathrm{Frob}([v_1]_{a_1} \ldots [v_d]_{a_d}) = [v_1^{(1)}]_{b_1} \ldots [v_d^{(1)}]_{b_d}.$$

Dually, the Verschiebung

$$\mathrm{Ver} : \Gamma^n(V^{(1)}) \longrightarrow \Gamma^{np}(V)$$

satisfies

$$\mathrm{Ver}([v_1^{(1)}]_{a_1} \ldots [v_d^{(1)}]_{a_d}) = p[v_1]_{pa_1} \ldots [v_d]_{pa_d}.$$

Proof. We work in the polynomial ring $\mathbf{W}(k)[X_1, \ldots X_d]$. The relation

$$\mathrm{Frob}([X_1 v_1 + \ldots + X_d v_d]_{np}) = [X_1^p(v_1^{(1)}) + \ldots + X_d^p(v_d^{(1)})]_n$$

holds by definition. But

$$[X_1 v_1 + \ldots + X_d v_d]_{np} = \Sigma_{a_1+\ldots+a_d=np}(X_1^{a_1} \ldots X_d^{a_d}[v_1]_{a_1} \ldots [v_d]_{a_d})$$

and

$$[X_1^p(v_1^{(1)}) + \ldots + X_d^p(v_d^{(1)})]_n = \Sigma_{b_1+\ldots+b_d=n}(X_1^{pb_1} \ldots X_d^{pb_d}[v_1^{(1)}]_{b_1} \ldots [v_d^{(1)}]_{b_d}),$$

so that the first assertion follows by identifying the coefficients of the monomials occuring in those expansions. The proof for the Verschiebung is similar.

□

Corollary 6.3. *For any $s \geq 1$, the kernel of*

$$\mathrm{Frob}^s : \Gamma^{np^s}(V) \longrightarrow \Gamma^n(V^{(s)})$$

coincides with the p^s-torsion of $\Gamma^{np^s}(V)$.

Proof. This immediately follows from the description, given in Proposition 5.27, of the torsion in $\Gamma^{np^s}(V)$, and from Lemma 6.2. □

PROPOSITION 6.4. *Let V be a k-vector space. Let $n, s \geq 1$ be integers. Then the Frobenius*

$$\mathrm{Frob}^s : \Gamma^{np^s}(V) \longrightarrow \Gamma^n(V^{(s)}),$$

$$[v]_{np^s} \longrightarrow [v^{(s)}]_n$$

is surjective. We have an exact sequence

$$0 \longrightarrow T_{p^s}(\Gamma^{np^s}(V)) \longrightarrow \Gamma^{np^s}(V) \xrightarrow{\mathrm{Frob}^s} \Gamma^n(V^{(s)}) \longrightarrow 0.$$

The Verschiebung

$$\mathrm{Ver}^s : \Gamma^n(V^{(s)}) \longrightarrow \Gamma^{np^s}(V),$$

$$[v^{(s)}]_n \longrightarrow p^s[v]_{np^s},$$

is injective. We have an exact sequence

$$0 \longrightarrow \Gamma^n(V^{(s)}) \xrightarrow{\mathrm{Ver}^s} \Gamma^{np^s}(V) \longrightarrow \Gamma^{np^s}(V)/p^s \longrightarrow 0.$$

Proof. We may assume that V is finite dimensional, with basis $e_1, \ldots, e_d$. The surjectivity of Frob^s directly follows from the description given in Lemma 6.2. That its kernel is the p^s-torsion is the content of Corollary 6.3. By Lemma 6.2, it is clear that the image of Ver^s is $p^s\Gamma^{np^s}(V)$. It follows from the same Lemma, combined with Proposition 5.27, that Ver^s is injective.

□

7. Omega powers and the Kummer-Witt exact sequence.

Recall that, for every k-vector space V, we have canonical isomorphisms

$$\Gamma^p_k(V) \simeq (V^{\otimes p})^{\mathcal{S}_p} \simeq \mathrm{Sym}^p_k(V^*)^*.$$

When working over a field of characteristic zero, it is common (though somewhat misleading) to identify $\mathrm{Sym}^p_k(V^*)^*$ and $\mathrm{Sym}^p_k(V)$, using what is called the 'symmetrizing operator'. Equivalently, in characteristic zero, the map

$$\Gamma^p_k(V) \longrightarrow \mathrm{Sym}^p_k(V),$$

$$[v]_p \mapsto v^p,$$

is an isomorphism. It is of course far to be so in our context, where the perfect field k has characteristic p. In other terms, the functor Γ^p_k does not commute with duality of vector spaces. However, it can be shown that the functor $\Gamma^p = \Gamma^p_{\mathbf{W}(k)}$ does commute with duality, in the sense that $\Gamma^p(V^*)$ and $\Gamma^p(V)^\vee$ are canonically isomorphic. This phenomenon does unfortunately not extend to higher divided powers: the functors Γ^n, in general, do not commute with duality. In the spirit of the classical duality between (split) groups of multiplicative type and Abelian groups of finite type, we are thus led to introduce new functors which are Pontryagin dual to divided powers. We then define the first and second Kummer-Witt exact sequence, which generalize the usual sequences

$$S_1(A) : 0 \longrightarrow pA \longrightarrow A \longrightarrow A/p \longrightarrow 0,$$

and

$$S_2(A) : 0 \longrightarrow T_p(A) \longrightarrow A \longrightarrow pA \longrightarrow 0,$$

for A a torsion $\mathbf{W}(k)$-module of finite type.. Note that $S_2(A)$ is Pontryagin dual to $S_1(A^\vee)$; in other words, we have a commutative diagram

$$\begin{array}{ccccccccc} S_1(A^\vee): 0 & \longrightarrow & p(A^\vee) & \longrightarrow & A^\vee & \longrightarrow & A^\vee/p & \longrightarrow & 0 \\ & & \downarrow\wr & & \| & & \downarrow\wr & & \\ S_2(A)^\vee: 0 & \longrightarrow & (pA)^\vee & \longrightarrow & A^\vee & \longrightarrow & (T_p(A))^\vee & \longrightarrow & 0, \end{array}$$

and simiarly by replacing p by q, where q is a power of p. In the sequel, we shall tacitly identify $A^\vee/q$ and $T_q(A)^\vee$.

Definition 7.1. *Let V be a finite-dimensional k-vector space. Let $n \geq 0$ be an integer. We put*

$$\Omega^n_{\mathbf{W}(k)}(V) = \Gamma^{p^n}_{\mathbf{W}(k)}(V^*)^\vee.$$

We call $\Omega^n_{\mathbf{W}(k)}(V)$ the n-th Omega power of V, and denote it simply by $\Omega^n(V)$, if the dependence in k is clear. The Frobenius map

$$\mathrm{Frob} : \Gamma^{p^{n+1}}(V^*) \longrightarrow \Gamma^{p^n}(V^*)^{(1)}$$

induces, by Pontryagin duality, a $\mathbf{W}(k)$-linear map

$$\Omega^n(V)^{(1)} \longrightarrow \Omega^{n+1}(V),$$

which we denote by Ver*, the Verschiebung for (Omega powers). The Verschiebung map*

$$\mathrm{Ver} : \Gamma^{p^n}(V^*)^{(1)} \longrightarrow \Gamma^{p^{n+1}}(V^*)$$

induces, by duality, a $\mathbf{W}(k)$-linear map

$$\Omega^{n+1}(V) \longrightarrow \Omega^n(V)^{(1)},$$

which we denote by Frob*, the Frobenius (for Omega powers).*

Remark 7.2. The n-th Omega power

$$V \mapsto \Omega^n(V)$$

is a covariant functor from the category of k-vector spaces to that of $\mathbf{W}(k)$-modules.

Exercise 7.3. Show that we have $\mathrm{Frob} \circ \mathrm{Ver} = p$ and $\mathrm{Ver} \circ \mathrm{Frob} = p$, for divided powers and for Omega powers. This relation will not be used in this paper.

Remark 7.4. Note that the Pontryagin duality $A \mapsto A^\vee$, from the category of torsion $\mathbf{W}(k)$-modules of finite type to itself, does not a priori commute with the tensor product $\otimes = \otimes_{\mathbf{W}(k)}$. Thus, the functors Ω^n are not strictly polynomial in general.

Definition 7.5. *Let V be a k-vector space. Let $r, s \geq 0$ be integers. The exact sequence*

$$0 \longrightarrow T_{p^s}(\Gamma^{p^{r+s}}(V^*)) \longrightarrow \Gamma^{p^{r+s}}(V^*) \longrightarrow p^s\Gamma^{p^{r+s}}(V^*) \overset{\mathrm{Frob}^s}{\simeq} \Gamma^{p^r}(V^{*(s)}) \longrightarrow 0$$

(cf. Proposition 6.4) gives by duality an exact sequence

$$0 \longrightarrow \Omega^r(V^{(s)}) \overset{\mathrm{Ver}^s}{\simeq} p^s\Omega^{r+s}(V) \longrightarrow \Omega^{r+s}(V) \longrightarrow \Omega^{r+s}(V)/p^s \longrightarrow 0.$$

It is called the first Kummer-Witt sequence (for V, r and s). It is denoted by $\mathcal{KW}_1(V, r, s)$.

Similarly, the exact sequence

$$0 \longrightarrow \Gamma^{p^r}(V^{*(s)}) \overset{\mathrm{Ver}^s}{\simeq} p^s\Gamma^{p^{r+s}}(V^*) \longrightarrow \Gamma^{p^{r+s}}(V^*) \longrightarrow \Gamma^{p^{r+s}}(V^*)/p^s \longrightarrow 0$$

gives by duality an exact sequence

$$0 \longrightarrow T_{p^s}(\Omega^{r+s}(V)) \longrightarrow \Omega^{r+s}(V) \longrightarrow p^s\Omega^{r+s}(V) \overset{\mathrm{Frob}^s}{\simeq} \Omega^r(V^{(s)}) \longrightarrow 0$$

It is called the second Kummer-Witt sequence (for V, r and s). It is denoted by $\mathcal{KW}_2(V, r, s)$.

The next Proposition gives, in a particular case, a concrete interpretation of the Verschiebung.

PROPOSITION 7.6. *Let V be a k-vector space. Let $s \geq 0$ be an integer. Then, we have a canonical injection*

$$j_V : \mathrm{Sym}^{p^s}(V) \longrightarrow \Omega^s(V),$$

identifying $\mathrm{Sym}^{p^s}(V)$ with $T_p(\Omega^s(V))$. Define a k-linear map

$$i_V : V^{(s)} \longrightarrow \mathrm{Sym}^{p^s}(V)$$

by the formula

$$i_V(x) = x^{p^s}.$$

Then the composite

$$V^{(s)} \xrightarrow{i_V} \mathrm{Sym}^{p^s}(V) \xrightarrow{j_V} \Omega^s(V)$$

equals Ver^s.

Proof. Let us prove the first claim. By Proposition 5.13, we have a canonical (k-linear) isomorphism

$$\Gamma^{p^s}(V^*)/p = \Gamma_k^{p^s}(V^*) \xrightarrow{\sim} ((V^*)^{\otimes p^s})^{\mathcal{S}_{p^s}},$$

$$[\phi]_{p^s} \mapsto \phi^{\otimes p^s}.$$

The arrow j_V is then given by applying Pontryagin duality to the composite

$$\Gamma^{p^s}(V^*) \longrightarrow \Gamma^{p^s}(V^*)/p \xrightarrow{\sim} ((V^*)^{\otimes p^s})^{\mathcal{S}_{p^s}},$$

using Remark 5.14.

We now prove the second claim. The dual of i_V is obviously the arrow

$$\Gamma^{p^s}(V^*)/p = \Gamma_k^{p^s}(V^*) \longrightarrow V^{*(s)},$$

$$[\phi]_{p^s} \mapsto \phi^{(s)},$$

which is the reduction mod p of the Frobenius

$$\mathrm{Frob}^s : \Gamma^{p^s}(V^*) \longrightarrow V^{*(s)}.$$

The claim follows, by definition of the Verschiebung for Omega powers. □

7.1. Divided powers versus Omega powers. In this subsection, we investigate the difference between divided powers and Omega powers. When needed, we shall identify $\mathbf{W}_n(k) = \mathbf{W}(k)/p^n\mathbf{W}(k)$ with the submodule

$$(\frac{1}{p^n}\mathbf{W}(k))/\mathbf{W}(k) \subset K/\mathbf{W}(k).$$

Definition 7.7. *Let V be a k-vector space, of finite dimension $d \geq 1$. Let $n \geq 1$ be an integer. For any $\phi \in V^*$, the formula*

$$V \longrightarrow \Gamma^{p^n}(k) = \mathbf{W}_{n+1}(k)$$
$$v \mapsto [\phi(v)]_{p^n}$$

defines a polynomial law, which is homogeneous, of degree p^n. Hence a morphism

$$\delta(\phi) : \Gamma^{p^n}(V) \longrightarrow \mathbf{W}_{n+1}(k) \subset K/\mathbf{W}(k),$$
$$[v]_{p^n} \mapsto [\phi(v)]_{p^n}.$$

The association

$$\delta : V^* \longrightarrow (\Gamma^{p^n}(V))^\vee$$

is itself a polynomial law, homogeneous of degree p^n, inducing a $\mathbf{W}(k)$-linear morphism

$$\Delta : \Gamma^{p^n}(V^*) \longrightarrow (\Gamma^{p^n}(V))^\vee.$$

Remark 7.8. The morphism Δ can of course be viewed as a pairing

$$\Delta' : \Gamma^{p^n}(V) \times \Gamma^{p^n}(V^*) \longrightarrow \mathbf{W}_{n+1}(k) \simeq \frac{1}{p^{n+1}}\mathbf{W}(k)/\mathbf{W}(k) \subset K/\mathbf{W}(k).$$

We will denote $\Delta'(x, y)$ simply by $< x, y >$.

Lemma 7.9. *Choose a basis $e_1, \ldots, e_d$ of V, with dual basis $e_1^*, \ldots, e_d^*$. We then have a commutative diagram*

$$\begin{array}{ccc} \Gamma^{p^n}(V) \times \Gamma^{p^n}(V^*) & \xrightarrow{<.,.>} & K/\mathbf{W}(k) \\ \downarrow \wr & & \| \\ \bigoplus_{a_1+\ldots+a_d=p^n}(\bigotimes_{i=1}^d \Gamma^{a_i}(ke_i)) \times \bigoplus_{b_1+\ldots+b_d=p^n}(\bigotimes_{j=1}^d \Gamma^{b_j}(ke_j^*)) & \longrightarrow & K/\mathbf{W}(k) \end{array},$$

where the vertical map on the left is the product of the isomorphism given by Lemma 5.27, and the lower horizontal map is the pairing given by

$$([e_1]_{a_1} \ldots [e_d]_{a_d}, [e_1^*]_{b_1} \ldots [e_d^*]_{b_d}) \mapsto \binom{p^n}{a_1, a_2, \ldots, a_d},$$

if $a_i = b_i$ for all i, or by

$$([e_1]_{a_1} \ldots [e_d]_{a_d}, [e_1^*]_{b_1} \ldots [e_d^*]_{b_d}) \mapsto 0$$

otherwise.

Proof. We work over the polynomial ring $\mathbf{W}_{n+1}(k)[X_i, Y_i,\ i = 1 \ldots d]$. By definition,

$$< [X_1e_1 + \ldots + X_de_d]_{p^n}, [Y_1e_1^* + \ldots + Y_de_d^*]_{p^n} >= (X_1Y_1 + \ldots + X_dY_d)^{p^n}.$$

Developping the lefthand side, we get that the coefficient of $X_1^{a_1} \ldots X_d^{a_d} Y_1^{b_1} \ldots Y_d^{b_d}$ is $< [e_1]_{a_1} \ldots [e_d]_{a_d}, [e_1^*]_{b_1} \ldots [e_d^*]_{b_d} >$, whenever a_i and b_i are positive integers such that $a_1 + \ldots + a_d = b_1 + \ldots + b_d = p^n$. Developping the righthand side, and identifying the coefficients, yields the result.

□

LEMMA 7.10. *Choose a basis $e_1, \ldots, e_d$ of V. For every decomposition $a_1 + \ldots + a_d = p^n$ of p^n into a sum of nonnegative integers, put*

$$N(a_1, \ldots, a_d) = \max(0, n + 1 - v_p(\binom{p^n}{a_1, a_2, \ldots, a_d})).$$

Then the kernel of

$$\Delta : \Gamma^{p^n}(V) \longrightarrow (\Gamma^{p^n}(V^*))^\vee$$

is generated by the elements

$$p^{N(a_1,\ldots,a_d)}[e_1]_{a_1} \ldots [e_d]_{a_d},$$

where $a_1 + \ldots + a_d = p^n$ runs through all decompositions of p^n into a sum of nonnegative integers.

Proof. Obvious from Lemma 7.9. □

PROPOSITION 7.11. *Let V be a finite-dimensional k-vector space. If $n \leq 1$, or if n is arbitrary and V has dimension less than or equal to two, the arrow*

$$\Delta : \Gamma^{p^n}(V) \longrightarrow \Omega^n(V) = (\Gamma^{p^n}(V^*))^\vee$$

is an isomorphism.

Proof. Since the source and the target of Δ are finite $\mathbf{W}(k)$-modules of the same length, it suffices to show injectivity. The case $n = 0$ is obvious. Assume that $n = 1$. We use Lemma 7.10. Take a decomposition $a_1 + \ldots + a_d = p$. Assume that none of the a_i's equals p. Then $[e_1]_{a_1} \ldots [e_d]_{a_d}$ has order p, and $N(a_1, \ldots, a_d) = 2 - 1 = 1$, hence $p^{N(a_1,\ldots,a_d)}[e_1]_{a_1} \ldots [e_d]_{a_d} = 0$. If, on the other hand, one of the $a_i's$ equals p (hence all other a_j's are zero), then $[e_1]_{a_1} \ldots [e_d]_{a_d} = [e_i]_p$ has order p^2, and $N(a_1, \ldots, a_d) = 2 - 0 = 2$. Thus $p^{N(a_1,\ldots,a_d)}[e_1]_{a_1} \ldots [e_d]_{a_d} = 0$, as well. Assume now that $d = 2$. Then,

$$N(a_1, a_2) = n + 1 - v_p(\binom{p^n}{a_1, a_2}) = 1 + \min(v_p(a_1), v_p(a_2))$$

is the base p logarithm of the order of $[e_1]_{a_1}[e_2]_{a_2}$, and the claim becomes obvious.

□

It will become clear in the sequel that Omega powers are far better behaved than divided powers, for applications to (Galois) cohomology.

Exercise 7.12. Show that Δ is, in general, not an isomorphism.

8. The Transfer.

In this section, we build an essential gadget for Omega powers *over a finite field*, the transfer. The authors believe that it is very close to Steenrod operations in algebra.

Let $q = p^r$ be a power of p, and let V be a k-vector space. In what follows, we shall play with the Frobenius -law-

$$\mathrm{Frob}^r : \mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(V^{(r)})$$

$$v \mapsto v^{(r)} := v \otimes 1.$$

Up to the choice of a basis, it is given by raising all coordinates to the q-th power. Note that the existence of this law does not rely on the fact that k is a field: it

exists for any commutative ring of characteristic p, and any k-module V.
Now, assume that k is finite, of cardinality $q = p^r$. Then the Frobenius -map-

$$\mathrm{Frob}^r : V \longrightarrow V^{(r)}$$

(given by the Frobenius law applied to k-rational points) is a k-linear isomorphism, enabling us to canonically identify the vector spaces V and $V^{(r)}$, which we shall do.

DEFINITION 8.1. *If k is a finite field, of cardinality $q = p^r$, and if V is a k-vector space, the Frobenius law*

$$\mathrm{Frob}^r : \mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(V)$$

shall simply be denoted by F_V (or even by F if the dependence in V is clear) in the sequel.

Let $H \subset V$ be a hyperplane. Let $\pi \in V^*$ be a linear form with kernel H. The formula

$$T_{V,\pi} : \mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(V),$$
$$v \mapsto F(v) - \pi(v)^{q-1} v$$

defines a polynomial law, homogeneous of degree q. Since $\lambda^{q-1} = 1$, for all $\lambda \in k^\times$, it is clear that $T_{V,\pi}$ depends on H only . Moreover, we have

$$\pi(T_{V,\pi}(v)) = \pi(F(v)) - \pi(v)^q = \pi(v)^q - \pi(v)^q = 0,$$

hence $T_{V,\pi}$ actually takes its values in $\mathbb{A}_k(H) \subset \mathbb{A}_k(V)$.

It is thus legitimate to state the following important Definition.

DEFINITION 8.2. *Let $H \subset V$ be a hyperplane. Let $\pi \in V^*$ be a linear form with kernel H. The formula*

$$\mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(H),$$
$$v \mapsto F(v) - \pi(v)^{q-1} v$$

defines a polynomial law, independent of the choice of π. We denote it by $T_{V,H}$. It is homogeneous, of degree q. We shall refer to it as the transfer, from V to H.

Remark 8.3. There is a fancy algebro-geometric way of seeing the transfer, as follows. The k-variety $X := \mathbb{P}_k(V^*)$ (of hyperplanes in V) is equipped with the tautological bundle $\mathcal{T}$, whose fiber at H is H itself.
Then, the transfer might be view as a single polynomial law of degree q

$$\mathbb{A}_X(V \otimes O_X) \longrightarrow \mathbb{A}_X(\mathcal{T}),$$

between affine spaces associated to locally free sheaves of $\mathcal{O}_X$-modules.

Remark 8.4. Note that the transfer, on k-rational points, is just the extension by zero of the inclusion $H \longrightarrow V$ to all of V. Let us make this statement more precise

LEMMA 8.5. *Let V be a finite-dimensional k-vector space. Let H_1, H_2 be distinct hyperplanes of V. Put $K := H_1 \cap H_2$; it has codimension two in V. Then we have commutative diagrams*

$$\begin{array}{ccc} \mathbb{A}_k(H_2) & \xrightarrow{T_{H_2,K}} & \mathbb{A}_k(K) \\ \downarrow can & & \downarrow can \\ \mathbb{A}_k(V) & \xrightarrow{T_{V,H_1}} & \mathbb{A}_k(H_1) \end{array}$$

and

$$\begin{array}{ccc} \mathbb{A}_k(H_1) & \xrightarrow{\mathrm{Frob}^r} & \mathbb{A}_k(H_1) \\ \downarrow{\scriptstyle can} & & \| \\ \mathbb{A}_k(V) & \xrightarrow{T_{V,H_1}} & \mathbb{A}_k(H_1). \end{array}$$

Proof. This is rather obvious, by definition of the transfer. □

Definition 8.6. *Let $X \subset \mathbb{P}(V^*)$ be a subset.*
We define

$$T_X : \mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(\bigoplus_{H \in X} H),$$

$$v \mapsto (T_{V,H}(v))_H$$

to be the (finite!) sum of the transfers $T_{V,H}$, for all hyperplanes H belonging to X.

The next Proposition is a key tool in this paper.

Proposition 8.7. *Let $W \subset V$ be a linear subspace, of codimension at least two. Take $X \subset \mathbb{P}(V^*)$ to be the set of hyperplanes containing W (that is, $X = \mathbb{P}((V/W)^*)$).*
Then the composite

$$\mathbb{A}_k(V) \xrightarrow{T_X} \mathbb{A}_k(\bigoplus_{H \in X} H) \longrightarrow \mathbb{A}_k(V),$$

where the second map is given by the sum of the inclusions $H \longrightarrow V$, equals Frob^r.

Proof. We argue on the level of the functor of points of the k-variety $\mathbb{A}_k(V)$.
Let k'/k be a commutative k-algebra. Pick $v \in V \otimes_k k'$.
Since each hyperplane in X is the kernel of $q-1$ linear forms vanishing on W (a number which equals -1 modulo p), the composite under consideration sends v to

$$-\sum_{\pi \in (V/W)^*, \pi \neq 0} (F(v) - \pi(v)^{q-1} v).$$

The Proposition then follows from the fact that

$$\sum_{\pi \in (V/W)^*} \pi(v)^{q-1} = 0.$$

Indeed, put $n = \dim_k(V/W) \geq 2$. Then the sum above is of the shape

$$\sum_{x \in k^n} P(x),$$

where $P \in k'[X_1, \ldots, X_n]$ is a homogeneous polynomial, of degree $q-1$. It is a classical fact (used in the proof of the Chevalley-Warning Theorem) that the only monomials which can contribute to this sum are those of the form $X_1^{a_1} \ldots X_n^{a_n}$, with all a_i's nonzero and divisible by $q-1$. Since $n \geq 2$, these do not occur, and the claim is proved. □

We now define the transfer for divided powers, and for Omega powers.

DEFINITION 8.8. *Let $X \subset \mathbb{P}(V^*)$ be a subset. For any integer $s \geq 0$, we set*

$$t_X : \Gamma^{p^{s+r}}(V) \longrightarrow \Gamma^{p^s}(\bigoplus_{H \in X} H),$$

$$[v]_{p^{s+r}} \mapsto [T_X(v)]_{p^s};$$

it is a $\mathbf{W}(k)$-linear map. It is the transfer with respect to X, for divided powers.

DEFINITION 8.9. *Let $X \subset \mathbb{P}(V)$ be a subset. Let $s \geq 0$ be an integer. The Pontryagin dual of the $\mathbf{W}(k)$-linear map*

$$t_X : \Gamma^{p^{s+r}}(V^*) \longrightarrow \Gamma^{p^s}(\bigoplus_{L \in X} (V/L)^*)$$

is a $\mathbf{W}(k)$-linear map

$$t_X : \Omega^s(\bigoplus_{L \in X} V/L) \longrightarrow \Omega^{s+r}(V).$$

It is the transfer relative to X, for Omega powers.

By Pontryagin duality, proposition 8.7 immediately yields the following.

PROPOSITION 8.10. *Let $W \subset V$ be a linear subspace, of dimension at least two. Put $X := \mathbb{P}(W) \subset \mathbb{P}(V)$. Let $s \geq 0$ be an integer. Then the composite*

$$\Omega^s(V) \xrightarrow{can} \Omega^s(\bigoplus_{L \in X} V/L) \xrightarrow{t_X} \Omega^{s+r}(V)$$

equals Ver^r.

Remark 8.11. Informally speaking, the preceding Proposition says that Omega powers, through the transfer, 'eat' quotients, converting them into torsion.

Remark 8.12. The transfer

$$t_{V,L} : V/L \longrightarrow \Omega^r(V)$$

takes its values in the p-torsion of $\Omega^r(V)$, which is $\mathrm{Sym}^{p^r}(V)$ by Proposition 7.6.

For $s = 0$, Proposition 8.10 may then by rephrased by saying that the k-linear map

$$\mathrm{Ver}^r : V \longrightarrow \mathrm{Sym}^{p^r}(V) \subset \Omega^r(V),$$

$$x \mapsto x^{p^r},$$

canonically factors through the k-linear map

$$V \longrightarrow \bigoplus_{L \in X} V/L.$$

Exercise 8.13. Show that the transfer

$$t_{V,L} : V/L \longrightarrow \mathrm{Sym}^q(V) \subset \Omega^r(V)$$

is given by the formula

$$x \mapsto x^q - x v_L^{q-1},$$

where v_L is any nonzero element of L.

9. The notions of n-surjectivity and of n-smoothness.

In this section, k is a finite field of cardinality $q = p^r$, and G is a profinite group.

Definition 9.1. *A cyclotomic G-module (relative to k) is a free $\mathbf{W}(k)$-module of rank one, endowed with a continuous $\mathbf{W}(k)$-linear action of G. Such a module will often be denoted by $\mathbf{W}(k)(1)$.*

Remark 9.2. A cyclotomic G-module is thus given by a continuous character

$$\chi : G \longrightarrow \mathbf{W}(k)^\times,$$

which shall, in our theory, play the rôle of the cyclotomic character in Galois theory.

Let $\mathbf{W}(k)(1)$ be a cyclotomic G-module. For i a non negative integer, we put

$$\mathbf{W}(k)(i) = \otimes^i_{\mathbf{W}(k)} \mathbf{W}(k)(1).$$

For negative i, put

$$\mathbf{W}(k)(i) = \mathrm{Hom}_{\mathbf{W}(k)}(\mathbf{W}(k)(-i), \mathbf{W}(k)).$$

For any $\mathbf{W}(k)$-module M, we put

$$M(i) = \mathbf{W}(k)(i) \otimes_{\mathbf{W}(k)} M.$$

Remark 9.3. Let M be a $(\mathbf{W}(k), G)$-module. It is clear that all twists $M(i)$ are $(\mathbf{W}(k), G)$-modules, whereas $\mathbf{W}(k)(1)$ itself is not.

Definition 9.4. *Let k be a finite field. Let G be a profinite group. Let $n \geq 1$ be an integer. Let*

$$f : M \longrightarrow N$$

be a morphism of $(\mathbf{W}(k), G)$-modules. We say that f is n-surjective (resp. n-injective) if the following holds. For every open subgroup $G' \subset G$, the map

$$f_* : H^n(G', M) \longrightarrow H^n(G', N)$$

is surjective (resp. injective).

Remark 9.5. Let $n \geq 0$ be an integer. Let

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

be an exact sequence of $(\mathbf{W}(k), G)$-modules.
Then π is n-surjective if and only if i is $(n+1)$-injective. Indeed, using the associated long exact sequences in cohomology, both conditions are equivalent to the vanishing of the connecting homomorphism (Bockstein)

$$H^n(G', C) \longrightarrow H^{n+1}(G', A),$$

for every open subgroup $G' \subset G$.

The next Lemma states that n-surjectivity is preserved by pullback and pushforward of exact sequences.

LEMMA 9.6. *Let $n \geq 0$ be an integer. Let*

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

be an exact sequence of $(\mathbf{W}(k), G)$-modules. Let

$$f : A \longrightarrow A'$$

and

$$g : C' \longrightarrow C$$

be morphisms of $(\mathbf{W}(k), G)$-modules. Denote by

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

the exact sequence $f_*(g^*(\mathcal{E}))$. If π is n-surjective, then so is π'.

Proof. Easy diagram chase, using the associated long exact sequences in cohomology. □

DEFINITION 9.7. *Let k be a finite field. Let G be a profinite group. Let $n \geq 0$ be an integer. Let $\mathbf{W}(k)(1)$ be a cyclotomic G-module. It is said to be n-smooth if, for every integer $s \geq 1$, the quotient map*

$$\mathbf{W}(k)(n)/p^{s+1} \longrightarrow \mathbf{W}(k)(n)/p^s$$

is n-surjective. A smooth cyclotomic module is one which is n-smooth, for every $n \geq 1$.

Remark 9.8. Let G be an arbitrary profinite group. Put $\mathbf{W}(k)(1) := \mathbf{W}(k)$, with trivial G-action. Then it is clear that $\mathbf{W}(k)(1)$ is 0-smooth.

DEFINITION 9.9. *Let k be a finite field. Let G be a profinite group. Let $n \geq 0$ be an integer. The group G is said to be n-smooth (resp. smooth), relative to k, if there exists an n-smooth (resp. smooth) cyclotomic G-module (relative to k).*

One of the main results of this paper, the Smoothness Theorem (Theorem 13.8), states that 1-smoothness implies smoothness.

Remark 9.10. It follows from Remark 9.8 that every profinite group G is 0-smooth. Note, however, that a smooth cyclotomic G-module needs not be 0-smooth. In the following, we shall mainly investigate the notions of n-smoothness, for $n \geq 1$.

The fundamental example of 1-smoothness is given by absolute Galois groups.

PROPOSITION 9.11. *Let k be an arbitrary finite field of characteristic p. Let F be a field, of characteristic not p, and let F_{sep}/F be a separable closure. Put*

$$G := \mathrm{Gal}(F_{sep}/F).$$

Put

$$\mu = \varprojlim_n \mu_{p^n}(F_{sep})$$

and

$$\mathbf{W}(k)(1) := \mu \otimes_{\mathbb{Z}_p} \mathbf{W}(k);$$

it is a cyclotomic G-module. It is 1-smooth.

Proof. Since $\mathbf{W}(k)$ is a free $\mathbb{Z}_p$-module of finite rank, we are immediately reduced to the case $k = \mathbb{F}_p$. We then have a diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_p & \longrightarrow & \mu_{p^{s+1}} & \xrightarrow{x\mapsto x^p} & \mu_{p^s} & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mu_p & \longrightarrow & \mathbb{G}_m & \xrightarrow{x\mapsto x^p} & \mathbb{G}_m & \longrightarrow & 1, \end{array}$$

given by classical Kummer theory. An easy diagram chase, combined with Hilbert's Theorem 90 for $\mathbb{G}_m$, yields the result. □

We conclude this section with an amusing exercise.

Exercise 9.12. Let G be a finite p-group, which is 1-smooth (relative, say, to $\mathbb{F}_p$). Show that G is either trivial, or $p = 2$ and G is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

10. About Hilbert's Theorem 90.

The authors now want to stress the importance of Hilbert's Theorem 90. It is, by the way, the favorite Theorem of the second author of this paper. The theory developped here shows that this Theorem, perhaps contrary to what one could expect, is -the- key ingredient to a 'short' proof of the Bloch-Kato conjecture, over a field F of characteristic not p. Indeed, the Lifting Theorems in the next section, in practise, are a machinery that applies Hilbert's Theorem 90 for $\mathbb{G}_m$ ceaselessly, not only to the base field F itself, but also to a vast amount of finite extensions of F. Furthermore, we are tempted to make the following analogy. Adopting the point of view of Grothendieck's descent theory, the main content of (the classical version of) Hilbert's Theorem 90 for GL_n is to convert into cohomological information ($H^1(F, \mathrm{GL}_n) = 1$) the highly non canonical fact that, over a field, every vector space possesses a basis. This is perfectly in the spirit of this paper: studying intrinsic properties of divided powers over Witt vectors, the proof of which may involve choosing a basis.

In the sequel, we shall need the following generalization of Hilbert's Theorem 90. It is probably folklore for some algebraists. It makes precise the following philosophical statement: two finite linear data over a local ring A, which become isomorphic after a faithfully flat extension of A, are already isomorphic over A. Lacking a suitable reference, we include a proof.

We begin by an elementary correspondence, which is the set-theoretic version of the equivalence between line bundles and $\mathbb{G}_m$-torsors.

Lemma 10.1. *Let S be a (not necessarily commutative, unital) ring. Then there is an equivalence between (left) S-modules L which are free of rank one, and sets X equipped with a (left) simply transitive action of the multiplicative group $S^\times$. In one direction, it is given by associating to L its set of generators:*

$$L \mapsto X := \{x \in L, L = Sx\}.$$

In the other direction, it is given by

$$X \mapsto (S \times X)/S^\times,$$

where we mod out the free action of $S^\times$ given by

$$\lambda.(s, x) = (s\lambda^{-1}, \lambda.x).$$

Proof. This is clear. □

LEMMA 10.2. *Let A be a Noetherian local ring. Let A'/A be a faitfully flat extension of commutative rings, and let S be a A-algebra, which is finite as an A-module. Let M be an S-module. Put $S' := S \otimes_A A'$ and $M' := M \otimes_A A'$. If M' is a free S'-module of rank one, then M is a free S-module of rank one.*

Proof. Let κ be the residue field of A. Put $\overline{M} := M \otimes_A \kappa$, $\overline{S} := S \otimes_A \kappa$. Assume that $\overline{M}$ is a free $\overline{S}$-module of rank one. Then, by Nakayama's Lemma, the lift of a generator of $\overline{M}$ (as an $\overline{S}$-module) to M will be a generator of M (as an S-module). Hence, we are reduced to the case where A is a field. Another similar application of Nakayama's Lemma shows that we may mod out the Jacobson radical of S, and assume that S is a semi-simple algebra. Hence, S is isomorphic direct product of matrix rings of the form $M_{n_i}(D_i)$, where D_i are division A-algebras. We may thus assume thatt $S = M_n(D)$ for D a division A-algebra. But then, by Morita equivalence, M is isomorphic to a sum of r copies of the simple module D^n. Since $M \otimes_A A'$ is free of rank one as an S'-module, we must have $r = n$ by dimension count, and M is free of rank one.

□

Remark 10.3. Assume, in what precedes, that S is finite and locally free as an A-module. Then, the group of invertible elements in S is representable by the affine A-group scheme $GL_1(S)$ (which is an open subscheme of $\mathbb{A}_A(S)$), and Grothendieck's descent theory asserts that $GL_1(S)$-torsors over $\mathrm{Spec}(A)$, for the fppf topology, correspond to S-modules M as in the previous Lemma. We thus get

$$H^1(\mathrm{Spec}(A), GL_1(S)) = \{*\},$$

where cohomology is taken with respect to the fppf topology. This statement is known as Grothendieck-Hilbert's Theorem 90.

PROPOSITION 10.4. *Let A be a Noetherian local ring. Let A'/A be a faitfully flat extension of commutative rings, and let R be an A-algebra. Let N be an R-module, which is finite as an A-module. Let M_1, M_2 be two R-submodules of N. Put $R' = R \otimes_A A'$, $N' = N \otimes_A A'$, $M_1' = M_1 \otimes_A A'$ and $M_2' = M_2 \otimes_A A'$. Assume there exists $f' \in GL_{R'}(N')$ such that $f'(M_1') = M_2'$. Then there exists $f \in GL_R(N)$ such that $f(M_1) = M_2$.*

Proof.

Put

$$S := \{f \in \mathrm{End}_R(N), f(M_1) \subset M_1\};$$

it is an A-algebra. It is a subalgebra of $\mathrm{End}_A(N)$. Writing N as a quotient of a free module A^n, $\mathrm{End}_A(N)$ then occurs as a sub-A-module of N^n, which is finite by assumption. Hence, S itself is a finite A-module. Put $S' := S \otimes_A A'$. By faithful flatness, we get that the canonical morphism

$$S' \longrightarrow \{f' \in \mathrm{End}_{R'}(N'), f'(M_1') \subset M_1'\}$$

is an isomorphism. The set

$$X := \{f' \in \mathrm{GL}_{R'}(N'), f'(M_1') = M_2'\}$$

is endowed with a simply transitive action of the multiplicative group $S'^{\times}$. As such (see Lemma 10.1), it canonically corresponds to a free S'-module of rank one M', given by the set-theoretical formula

$$M' = (X \times S')/S'^{\times}.$$

But the S'-module M', viewed as an A'-module, is endowed with a canonical descent data for the faithfully flat morphism A'/A. By descent, we get an A-module M, which is in fact a locally free S-module of rank one. To prove the Proposition is equivalent to proving that M is actually a free S-module of rank one (to give a generator of the S-module M is equivalent to giving $f \in GL_R(N)$ such that $f(M_1) = M_2$). We conclude by applying Lemma 10.2.

□

Corollary 10.5. *Let A be a Noetherian local ring. Let A'/A be a faitfully flat extension of commutative rings, and let R be an A-algebra. Put $R' := R \otimes_A A'$. Let N, M be two R-modules, one of which is finite as an A-module. Assume that $M \otimes_A A'$ and $N \otimes_A A'$ are isomorphic as R'-modules. Then M and N are isomorphic as R-modules.*

Proof. To see this, just apply the Proposition to M and N, viewed as R-submodules of $M \bigoplus N$. □

Remark 10.6. Specializing to linear representations, we get the following statement. Two finite-dimensional linear representations of an abstract group G over a field F, which become isomorphic over an extension E/F, are already isomorphic over F. Note that this holds, in particular, in the modular case (i.e. where F has characteristic p and G is a finite p-group).

We finish this section by stating a stronger corollary, which will be used in the sequel.

Corollary 10.7. *Let A be a Noetherian local ring. Let A'/A be a faitfully flat extension of commutative rings, and let R be an A-algebra. Put $R' := R \otimes_A A'$. Let*

$$\mathcal{E} : 0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

and

$$\mathcal{E}' : 0 \longrightarrow M_1' \longrightarrow M_2' \longrightarrow M_3' \longrightarrow 0$$

be two short exact sequences of R-modules, where the M_i's and the M_j''s are finite as A-modules. If $\mathcal{E} \otimes_A A'$ and $\mathcal{E}' \otimes_A A'$ are isomorphic, as exact sequences of R'-modules, then $\mathcal{E}$ and $\mathcal{E}'$ are isomorphic, as exact sequences of R-modules.

Proof. Left as an exercise for the reader. □

Remark 10.8. In all what precedes, the Noetherian assumptions may probably be dropped. They are here to simplify the proofs.

11. The Lifting Proposition.

In this section, k is a finite field, of cardinality $q = p^r$, and G is a profinite group. All tensor products are taken over $\mathbf{W}(k)$.

The theory of divided powers (and Omega powers), equipped with the Frobenius, Verschiebung and transfer morphisms, is perfectly canonical. Hence, divided powers and Omega powers shall, from now on, be viewed as functors from $\mathcal{M}(k,G)$ to $\mathcal{M}(\mathbf{W}(k),G)$. Moreover, the Frobenius, Verschiebung and transfer morphisms are G-equivariant. Let us give an example. Let V be a (k,G)-module, of finite dimension $d \geq 2$. Let $X \subset \mathbb{P}(V)$ be a G-invariant subset. Then the transfer

$$t_X : \Omega^s(\bigoplus_{L \in X} V/L) \longrightarrow \Omega^{r+s}(V)$$

is a morphism of $(\mathbf{W}(k),G)$-modules. Recall that, as explained in section 4, the source of t_X is naturally a $(\mathbf{W}(k),G)$-module, induced from dimension $d-1$.

Definition 11.1. *Let*

$$f : A \longrightarrow B$$

be a morphism of (k,G)-modules. We denote by $K^s(f)$ the kernel of the map

$$\Omega^s(A) \stackrel{\Omega^s(f)}{\longrightarrow} \Omega^s(B).$$

If f is the quotient of A by a (k,G)-submodule A', we put

$$K^s(A,A') := K^s(f).$$

Remark 11.2. Let

$$f : A \longrightarrow B$$

be a surjective linear map between (k,G)-modules. Then f admits a (non canonical) k-linear splitting

$$g : B \longrightarrow A.$$

By functoriality of Omega powers, $\Omega^s(g)$ is then a $\mathbf{W}(k)$-linear splitting of $\Omega^s(f)$. Hence, the sequence

$$0 \longrightarrow K^s(f) \longrightarrow \Omega^s(A) \stackrel{\Omega^s(f)}{\longrightarrow} \Omega^s(B) \longrightarrow 0,$$

is not only an exact sequence of $\mathbf{W}(k)$-modules, but is also split. It is, of course, not split in general as an exact sequence of $(\mathbf{W}(k),G)$-modules.
We infer that, for every $r \geq 0$, the sequence

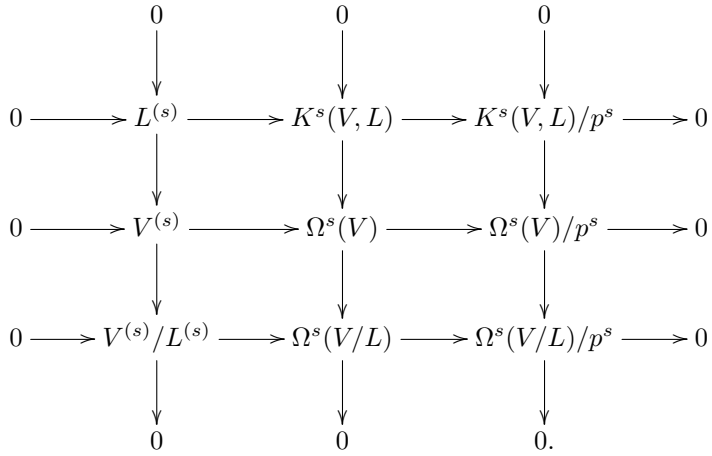
$$0 \longrightarrow K^s(f)/p^r \longrightarrow \Omega^s(A)/p^r \stackrel{\Omega^s(f)}{\longrightarrow} \Omega^s(B)/p^r \longrightarrow 0$$

is also exact; a fact which shall constantly be used in the sequel.

Let V be a (k,G)-module, and let $L \subset V$ be a G-invariant linear subspace. Then we have an exact sequence

$$0 \longrightarrow L^{(s)} \longrightarrow K^s(V,L) \longrightarrow K^s(V,L)/p^s \longrightarrow 0,$$

fitting into the commutative diagram



Our goal here is Proposition 11.6. It is the key step towards the main Lifting Theorems of this paper.
We start by introducing a slightly abusive notation, whose goal is to increase the readability of the proofs.

DEFINITION 11.3. *Let $\mathcal{T}$ be a free $\mathbf{W}(k)$-module of finite rank, endowed with a continuous $\mathbf{W}(k)$-linear action of G. For every $(W(k), G)$-module M, we shall put*

$$M(*) := M \otimes_{\mathbf{W}(k)} \mathcal{T},$$

the dependence in $\mathcal{T}$ being implicit. It is obviously a $(W(k), G)$-module.

Remark 11.4. The module $\mathcal{T}$ will only be used through the 'twisting' (exact) functor

$$M \mapsto M(*)$$

it induces. Note that, although it will later often be the case, we do not assume here that $\mathcal{T}$ has rank one over $\mathbf{W}(k)$.

Remark 11.5. The module $\mathcal{T}$ is of course not a $(W(k), G)$-module, unless it is trivial. However, all finite quotients $\mathcal{T}/p^s$ are $(W(k), G)$-modules.

PROPOSITION 11.6. *Let $\mathcal{T}$ be a free $\mathbf{W}(k)$-module of finite rank, endowed with a continuous $\mathbf{W}(k)$-linear action of G. Let $n \geq 0$ be an integer. Assume that, for every integer $s \geq 0$, the quotient map*

$$\mathcal{T}/p^{s+1} \longrightarrow \mathcal{T}/p^s$$

is n-surjective. Let V be a (k, G)-module. Let $L_0 \subset V$ be a G-invariant line. Then, for every integer $s \geq 0$, the quotient map

$$K^s(V, L_0)(*) \longrightarrow K^s(V, L_0)(*)/p^s$$

is n-surjective.

11.1. PROOF OF PROPOSITION 11.6. It is by induction on the dimension d of V, though the case $d = 2$ is dealt with separately. Note that n does not play an important rôle in the proof. For instance, assuming that $n = 0$ does not make it any simpler.
We may assume that G is a pro-p-group, by the usual restriction-corestriction argument.

11.1.1. *A Reduction step.* The following will be used in the sequel. It says that making a finite field extension does not affect the conclusion of the Proposition.

LEMMA 11.7. *Let k'/k be a finite field extension.*
Put $V' := V \otimes_k k', L_0' := L_0 \otimes_k k'$ and $K'^s(V', L_0') := K^s(V, L_0) \otimes_{\mathbf{W}(k)} \mathbf{W}(k')$.
If the quotient map

$$K'^s(V', L_0')(*) \longrightarrow K'^s(V', L_0')(*)/p^s$$

is n-surjective, then so is the map

$$K^s(V, L_0)(*) \longrightarrow K^s(V, L_0)(*)/p^s.$$

Proof. This follows rather formally from the fact that the canonical inclusion

$$\mathbf{W}(k) \longrightarrow \mathbf{W}(k'),$$

as a $\mathbf{W}(k)$-linear map, admits a retraction. More precisely, there exists an isomorphism of $\mathbf{W}(k)$-modules

$$\mathbf{W}(k') \xrightarrow{\sim} \mathbf{W}(k) \oplus C,$$

with C a free $\mathbf{W}(k)$-module. The choice of such an isomorphism induces, for every $(\mathbf{W}(k), G)$-module M, a functorial G-equivariant retraction of natural injection

$$M \longrightarrow M \otimes_{\mathbf{W}(k)} \mathbf{W}(k'),$$
$$m \mapsto m \otimes 1,$$

whence the claim. □

11.1.2. *The one-dimensional case.* If $d = 1$, then $V = L_0$ is isomorphic to the trivial one-dimensional representation k (recall that G is a pro-p-group!), and $K^s(V, L_0)$ is thus isomorphic to $\mathbf{W}_{s+1}(k)$. Thus, there is nothing to prove in this case.

11.1.3. *The two-dimensional case.* We now want to prove the $d = 2$ case, where we know that $\Omega^s(V)$ is canonically isomorphic to $\Gamma^{p^s}(V)$ (cf. Proposition 7.11). Thus, we may replace Omega powers by divided powers.

We have a commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K^{s-1}(V^{(1)}, L_0^{(1)})/p^{s-1} & \longrightarrow & K^s(V, L_0)/p^s & \longrightarrow & K^s(V, L_0)/p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Gamma^{p^{s-1}}(V^{(1)})/p^{s-1} & \xrightarrow{\mathrm{Ver}} & \Gamma^{p^s}(V)/p^s & \longrightarrow & \Gamma^{p^s}(V)/p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \Gamma^{p^{s-1}}(V^{(1)}/L_0^{(1)})/p^{s-1} & \xrightarrow{\mathrm{Ver}} & \Gamma^{p^s}(V/L_0)/p^s & \longrightarrow & \Gamma^{p^s}(V/L_0)/p & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0. & &
\end{array}$$

A straightforward induction on s, using the (twist by $\mathcal{T}$ of the) top row of this diagram, then shows that it is enough to prove that the quotient map

$$K^s(V, L_0)(*) \longrightarrow K^s(V, L_0)(*)/p$$

is n-surjective, which we now do. We first deal with the $k = \mathbb{F}_p$ case, and then deduce the result for k arbitrary.

11.1.4. *The case $d = 2$ and $k = \mathbb{F}_p$.* Assume first that $k = \mathbb{F}_p$. The group G, being a pro-p-group, then acts on V via an additive character

$$\chi : G \longrightarrow C \subset \mathrm{GL}_k(V),$$

where C is a cyclic group of order p, sitting as a p-Sylow subgroup in $\mathrm{GL}_k(V) \simeq \mathrm{GL}_2(\mathbb{F}_p)$. We can assume that χ is non trivial. Indeed, if the action of G on V is trivial, then V is isomorphic to $k \oplus k$ as a (k, G)-module, and the statement is an immediate consequence of the one-dimensional case, using the strict polynomiality of divided powers.

Denote by k' a field with p^s elements. Put

$$\Gamma' := \Gamma_{\mathbf{W}(k')}, V' = V \otimes_k k', L'_0 = L_0 \otimes_k k'.$$

We denote by $\mathbb{P}(V')$ the G-set of one-dimensional k'-subspaces $L' \subset V'$; it has cardinality $p^s + 1$.
Note that any k'-vector space W' is canonically isomorphic to $W'^{(s)}$. Moreover, the Frobenius map

$$\mathrm{Frob}^s : \Gamma'^{p^s}(W') \longrightarrow W'^{(s)} = W'$$

induces a k'-linear map

$$\mathrm{Frob}^s : \Gamma'^{p^s}(W')/p \longrightarrow W',$$

which is an isomorphism if W' is one-dimensional.
For a k'-rational line $L' \in \mathbb{P}(V')$ (not necessarily defined over k), recall that we have the transfer (for divided powers)

$$t_{V',L'} : \Gamma'^{p^s}(V') \longrightarrow L'.$$

It induces a k'-linear map

$$\Gamma'^{p^s}(V')/p \longrightarrow L',$$

which we also denote by $t_{V',L'}$.

The following Lemma was the starting point of this paper.

Lemma 11.8. *The k'- linear morphism*

$$\Gamma'^{p^s}(V')/p \longrightarrow \bigoplus_{L' \in \mathbb{P}(V')} L',$$

which is the sum of the transfers for all k'-rational lines $L' \subset V'$ (including L'_0), is an isomorphism of (k', G)-modules.

Proof. For $L' \in \mathbb{P}(V')$ and $v \in V'$, the transfer $t_{V',L'}$ sends a symbol $[v]_{p^s}$ to v if $v \in L'$, or to zero otherwise (cf. Remark 8.4). Thus, the map of the Lemma is surjective (a nonzero vector belongs to a unique line!). It is then bijective, since both source and target are k'-vector spaces of dimension $p^s + 1$ (recall that V' is a two-dimensional k'-vector space!). □

Note that the previous isomorphism holds over k', and has, a priori, no canonical analogue over k. However, by Lemma 11.7, base-changing from $\mathbf{W}(k)$ to $\mathbf{W}(k')$, which we now do, has no effect on what has to be proven (namely, Proposition 11.6, in the particular case of a two-dimensional $(\mathbb{F}_p, G)$-module V).

Any $L' \in \mathbb{P}(V')$, distinct from L'_0, will be a complement of L'_0, whence a canonical isomorphism

$$L' \longrightarrow V'/L'_0,$$

which we use to identify those two k'-rational lines. The isomorphism of Lemma 11.8 then gives rise to a commutative diagram (of $(W(k'), G)$-modules)

$$\begin{array}{ccccccc}
\tilde{N} \bigoplus \Gamma'^{p^s}(L'_0) & \longrightarrow & K^s(V', L'_0) & \longrightarrow & K^s(V', L'_0)/p & \xrightarrow{\sim} & N \bigoplus L'_0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
(\bigoplus_{L' \neq L'_0} \Gamma'^{p^s}(L')) \bigoplus \Gamma'^{p^s}(L'_0) & \longrightarrow & \Gamma'^{p^s}(V') & \longrightarrow & \Gamma'^{p^s}(V')/p & \xrightarrow{\sim} & (\bigoplus_{L' \neq L'_0} L') \bigoplus L'_0 \\
\downarrow \tilde{\pi} & & \downarrow & & \downarrow & & \downarrow \pi \\
\Gamma'^{p^s}(V'/L'_0) & = & \Gamma'^{p^s}(V'/L'_0) & \longrightarrow & \Gamma'^{p^s}(V'/L'_0)/p & \xrightarrow{\sim} & V'/L'_0,
\end{array}$$

where $\tilde{\pi}$ is zero on $\Gamma'^{p^s}(L'_0)$, and is induced by the isomorphism $L' \xrightarrow{\sim} V'/L'_0$ if $L' \neq L'_0$, and where $\tilde{N}$ is the kernel of $\tilde{\pi}$ restricted to $\bigoplus_{L' \neq L'_0} \Gamma'^{p^s}(L')$ (and similarly for π and N). Note that $N = \tilde{N}/p$. By an immediate diagram chase, it is then enough to show that the map

$$\tilde{N}(*) \bigoplus \Gamma'^{p^s}(L'_0)(*) \longrightarrow N(*) \bigoplus L'_0(*),$$

which is the composite of the arrows of the top row, is n-surjective. But the map

$$\Gamma'^{p^s}(L'_0)(*) \longrightarrow L'_0(*)$$

is obviously n-surjective, by the one-dimensional case.
Hence, it remains to show that the quotient map

$$\tilde{N}(*) \longrightarrow N(*) = \tilde{N}(*)/p$$

is n-surjective. But recall that we started from a two-dimension vector space V over $k = \mathbb{F}_p$, on which the pro-p-group G acts through the nontrivial additive character $\chi : G \longrightarrow C$, where C is a cyclic group of order p. The G-set $\mathbb{P}(V')$, of cardinality $p^s + 1$, is thus the disjoint union of the orbits $\{L'_0\}$, and of p^{s-1} orbits of size p. The $(\mathbf{W}(k'), G)$-module $\bigoplus_{L' \neq L'_0} \Gamma'^{p^s}(L')$ is thus isomorphic to $\mathbf{W}_{s+1}(k')[C]^{p^{s-1}}$, and N fits into an exact sequence

$$0 \longrightarrow N \longrightarrow \mathbf{W}_{s+1}(k')[C]^{p^{s-1}} \longrightarrow \mathbf{W}_{s+1}(k') \longrightarrow 0,$$

where the surjection is the augmentation map, sending each element of the canonical permutation basis to 1. Note that everything is actually defined over $\mathbb{Z}$ here. In other words, the surjection in the exact sequence above is obtained from the surjection (augmentation)

$$\mathbb{Z}[C]^{p^{s-1}} \longrightarrow \mathbb{Z} \longrightarrow 0,$$

by extending scalars from $\mathbb{Z}$ to $\mathbf{W}_{s+1}(k')$.
Consider the usual exact sequence

$$0 \longrightarrow I \longrightarrow \mathbb{Z}[C] \longrightarrow \mathbb{Z} \longrightarrow 0,$$

where I is the augmentation ideal of $\mathbb{Z}[C]$.

LEMMA 11.9. *Let $m \geq 1$ be an integer. Denote by J_m the kernel of the G-equivariant surjection*

$$\mathbb{Z}[C]^m \longrightarrow \mathbb{Z},$$

sending each element of the canonical basis to 1. *Then there exists a G-equivariant isomorphism*

$$\mathbb{Z}[C]^{m-1} \oplus I \xrightarrow{\sim} J_m.$$

Proof. Consider the map

$$\mathbb{Z}[C]^{m-1} \oplus I \longrightarrow \mathbb{Z}[C]^m,$$

$$(x_1, \ldots, x_{m-1}, y) \mapsto (y + x_1, x_2 - x_1, x_3 - x_2, \ldots, x_{m-1} - x_{m-2}, -x_{m-1}).$$

It is straightforward to check that this map takes values in J_m, and induces an isomorphism $\mathbb{Z}[C]^{m-1} \oplus I \xrightarrow{\sim} J_m$.
□

Put

$$I_{k'} := I \otimes_{\mathbb{Z}} \mathbf{W}(k').$$

By the previous Lemma, we see that N is isomorphic to

$$\mathbf{W}_{s+1}(k')[C]^{p^{s-1}-1} \bigoplus I_{k'}/p^{s+1}.$$

By Shapiro's Lemma, and by the one-dimensional case, the map

$$\mathbf{W}_{s+1}(k')[C]^{p^{s-1}-1}(*) \longrightarrow \mathbf{W}_{s+1}(k')[C]^{p^{s-1}-1}(*)/p$$

is n-surjective.

Hence, we are reduced to showing that the map

$$I_{k'}(*)/p^{s+1} \longrightarrow I_{k'}(*)/p$$

is n-surjective. We will do this by showing that the sequence

$$0 \longrightarrow (pI_{k'}/p^{s+1}I_{k'})(*) \longrightarrow (I_{k'}/p^{s+1})(*) \longrightarrow (I_{k'}/p)(*) \longrightarrow 0$$

is obtained by pullback and pushforward from the sequence

$$0 \longrightarrow (\mathcal{T}/p^s)[C] \xrightarrow{*p} (\mathcal{T}/p^{s+1})[C] \longrightarrow (\mathcal{T}/p)[C] \longrightarrow 0,$$

in which the quotient map is n-surjective by assumption on $\mathcal{T}$, using Shapiro's Lemma. We then use Lemma 9.6.
Working over $\mathbb{Z}$, it is of course enough to show that the exact sequence (of $\mathbb{Z}[G]$-modules)

$$\mathcal{F} : 0 \longrightarrow I/p^s \xrightarrow{*p} I/p^{s+1} \longrightarrow I/p \longrightarrow 0$$

is obtained by pullback and pushforward from the sequence

$$\mathcal{E} : 0 \longrightarrow (p\mathbb{Z}/p^{s+1}\mathbb{Z})[C] \longrightarrow (\mathbb{Z}/p^{s+1}\mathbb{Z})[C] \xrightarrow{\pi} \mathbb{F}_p[C] \longrightarrow 0,$$

which we now do.

Choose a generator σ of C, which we identify with the corresponding basis element of $\mathbb{Z}[C]$. We then have the usual exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[C] \xrightarrow{\tau} I \longrightarrow 0,$$

where

$$\tau(1) = 1 - \sigma.$$

Put

$$N := 1 + \sigma + \ldots + \sigma^{p-1} \in \mathbb{Z}[C].$$

We have an injective map

$$j : I/p \longrightarrow \mathbb{F}_p[C],$$

realizing I/p as the kernel of the augmentation map. We also have a map

$$i : (p\mathbb{Z}/p^{s+1}\mathbb{Z})[C] \longrightarrow I/p^s,$$

$$p \mapsto 1 - \sigma.$$

Then $j^* i_*(\mathcal{E})$ is an extension

$$0 \longrightarrow I/p^s \longrightarrow E \longrightarrow I/p \longrightarrow 0.$$

I claim it is canonically isomorphic to the extension $\mathcal{F}$. Indeed, the element

$$f := (1 - \sigma) \in (\mathbb{Z}/p^{s+1}\mathbb{Z})[C]$$

maps to $\mathrm{Im}(j)$ via π. It thus defines an element $e \in E$. Since $Nf = 0$, we get $Ne = 0$ in E. We thus have a $\mathbb{Z}[C]$-equivariant map

$$I/p^{s+1} = (\mathbb{Z}[C]/N)/p^{s+1} \longrightarrow E,$$

$$1 \mapsto e.$$

I claim it is an isomorphism. Since E and I/p^{s+1} have the same cardinality, it suffices to show injectivity. Assume that $xe = 0$, with $x \in \mathbb{Z}[C]$.

Lemma 11.10. *One can write*

$$x = py + uN,$$

with $u \in \mathbb{Z}$, and $y \in \mathbb{Z}[C]$, not involving σ^{p-1} (in other words,

$$y = \sum_{i=0}^{p-2} y_i \sigma^i,$$

with $y_i \in \mathbb{Z}$).

Proof. For sure, we can write

$$x = z + uN,$$

with $u \in \mathbb{Z}$ and $z \in \mathbb{Z}[C]$, not involving σ^{p-1} (in other words, $z = \sum_{i=0}^{p-2} z_i \sigma^i$, with $z_i \in \mathbb{Z}$). From the equality $xe = 0$, we deduce that $x(1 - \sigma)$ has to lie in $p\mathbb{Z}[C]$, hence that $z(1 - \sigma)$ also lies in $p\mathbb{Z}[C]$. This readily implies that z itself belongs to $p\mathbb{Z}[C]$, i.e. that we can write $z = py$, for $y \in \mathbb{Z}[C]$, qed. □

We then write

$$x = py + uN,$$

as in the previous Lemma. We get $pye = 0$, hence

$$i(py(1 - \sigma)) = 0,$$

which is possible only if $y \in p^s\mathbb{Z}[C]$. Thus, x reduces to zero in $(\mathbb{Z}[C]/N)/p^{s+1}$, and the claim is proved.

11.1.5. *The case $d = 2$ and k arbitrary.* Let us now deal with the case where k is an arbitrary finite field, equipped with a G-invariant line $L_0 \subset V$. We can assume that $V = k^2$ as a vector space, that the action of G on V occurs through an additive character

$$\chi : G \longrightarrow k,$$

by the formula

$$g.(x, y) = (x, \chi(g)x + y),$$

and that L_0 is the second axis, i.e. $L_0 = 0 \oplus k$.
Choose an $\mathbb{F}_p$-basis $(x_1, \ldots, x_r)$ of k, yielding an isomorphism $k \longrightarrow \mathbb{F}_p^r$. The character χ breaks down into r characters

$$\chi_i : G \longrightarrow \mathbb{F}_p,$$

for $i = 1, \ldots, r$, each of which defines a two-dimensional $(\mathbb{F}_p, G)$-module

$$V_i := \mathbb{F}_p^2,$$

on which G acts by the same formula as above. Call L_i the second axis; it is a G-invariant line of the $(\mathbb{F}_p, G)$-module V_i.

Definition 11.11. *We denote by $\mathcal{E}$ the exact exact sequence of $(\mathbb{Z}_p, G)$-modules which is the direct sum of the exact sequences*

$$\mathcal{E}_i : 0 \longrightarrow K^s(V_i, L_i) \longrightarrow \Omega^s_{\mathbb{Z}_p}(V_i) \longrightarrow \Omega^s_{\mathbb{Z}_p}(V_i/L_i) \longrightarrow 0,$$

for $i = 1, \ldots, r$.

Lemma 11.12. *The exact sequence $\mathcal{E}$, up to isomorphism of exact sequence of $(\mathbb{Z}_p, G)$-modules, is independent of the choice of the $\mathbb{F}_p$-basis $(x_1, \ldots, x_r)$.*

Proof. Pick another basis $(x'_1, \ldots, x'_r)$. Denote by χ'_i, V'_i, L'_i, $\mathcal{E}'_i$ the constructions explained before, but relative to this new basis. Clearly, we have a natural G-invariant isomorphism

$$\bigoplus_{i=1}^{r} V_i \longrightarrow \bigoplus_{i=1}^{r} V'_i$$

(both sides are canonically isomorphic to V!). It is given by G-equivariant maps

$$f_{i,j} : V_i \longrightarrow V'_j,$$

sending L_i to L'_j. They induce, by functoriality, maps

$$g_{i,j} : \Omega^s_{\mathbb{Z}_p}(V_i) \longrightarrow \Omega^s_{\mathbb{Z}_p}(V'_j).$$

Taking the direct sum of these, we get a commutative diagram

$$\begin{array}{ccc} \bigoplus_{i=1}^r \Omega^s_{\mathbb{Z}_p}(V_i) & \longrightarrow & \bigoplus_{i=1}^r \Omega^s_{\mathbb{Z}_p}(V_i/L_i) \\ \downarrow & & \downarrow \\ \bigoplus_{j=1}^r \Omega^s_{\mathbb{Z}_p}(V'_j) & \longrightarrow & \bigoplus_{j=1}^r \Omega^s_{\mathbb{Z}_p}(V'_j/L'_j) \end{array},$$

yielding the result. □

LEMMA 11.13. *The exact sequence*

$$\mathcal{F} : 0 \longrightarrow K^s(V, L_0) \longrightarrow \Omega^s_{W(k)}(V) \longrightarrow \Omega^s_{W(k)}(V/L_0) \longrightarrow 0,$$

seen as an exact sequence of $(\mathbb{Z}_p, G)$-modules, is isomorphic to $\mathcal{E}$.

Proof. Put $A' = \mathbf{W}(k)$, and $A = \mathbb{Z}_p$. The extension A'/A is an étale algebra (even cyclic Galois, of course). If it was trivial (i.e. if A' was isomorphic to A^r as an A-algebra), then the claim would be obvious, using Lemma 11.12, and picking as a basis the basis of primitive idempotents. But the situation becomes so after extending scalars to A': the étale algebra $A' \otimes_A A'/A'$ is trivial. Hence, the two exact sequences in question become isomorphic after extending scalars to A'. By Corollary 10.7, they are already isomorphic over A. The Lemma is proved.

□

We thus have an isomorphism (of $(\mathbb{Z}_p, G)$-modules)

$$K^s(V, L_0) \xrightarrow{\sim} \bigoplus_{i=1}^{r} K^s(V_i, L_i).$$

We may view $\mathcal{T}$ as a $\mathbb{Z}_p$-module of finite rank (which is r times its rank as a $\mathbf{W}(k)$-module), endowed with a continuous $\mathbb{Z}_p$-linear action of G. By the case of planes over $\mathbb{F}_p$, which was dealt with in the previous subsection, we know that the r arrows

$$K^s(V_i, L_i) \otimes_{\mathbb{Z}_p} \mathcal{T} \longrightarrow K^s(V_i, L_i) \otimes_{\mathbb{Z}_p} \mathcal{T}/p^s$$

are n-surjective. Hence, the map

$$K^s(V, L_0) \otimes_{\mathbb{Z}_p} \mathcal{T} \longrightarrow K^s(V, L_0) \otimes_{\mathbb{Z}_p} \mathcal{T}/p^s$$

is n-surjective. Considering the commutative diagram

$$\begin{array}{ccc} K^s(V, L_0) \otimes_{\mathbb{Z}_p} \mathcal{T} & \longrightarrow & K^s(V, L_0) \otimes_{\mathbb{Z}_p} \mathcal{T}/p^s \\ \downarrow & & \downarrow \\ K^s(V, L_0)(*) & \longrightarrow & K^s(V, L_0)(*)/p^s \end{array},$$

we see that it is enough to show that the canonical map

$$K^s(V, L_0) \otimes_{\mathbb{Z}_p} \mathcal{T} \longrightarrow K^s(V, L_0)(*) = K^s(V, L_0) \otimes_{\mathbf{W}(k)} \mathcal{T}$$

is n-surjective. We are going to show more: it admits a canonical G-equivariant section. We are even going to show this in a slightly more general setting. Taking $A = \mathbb{Z}_p$, $B = \mathbf{W}(k)$, $M = K^s(V, L_0)$ and $N = \mathcal{T}$ in what follows yields the result.

Let B/A be a finite étale extension of commutative rings. Then, as it is well-known, the multiplication map

$$\mu : B \otimes_A B \longrightarrow B$$

corresponds, geometrically, to an open-closed immersion. In other words, there exists a finite étale algebra C/A, and a canonical isomorphism

$$B \otimes_A B \xrightarrow{(\mu, \phi)} B \times C.$$

Now, let M and N be two B-modules. Then $M \otimes_A N$ is a $B \otimes_A B$-module, and

$$M \otimes_B N = (M \otimes_A N) \otimes_\mu B,$$

so that, by what precedes, the natural surjection

$$M \otimes_A N \longrightarrow M \otimes_B N$$

has a canonical section.

11.1.6. *The case $d \geq 3$.* Here k is arbitrary, of cardinality $q = p^r$. We thus have canonical isomorphisms

$$W \simeq W^{(r)},$$

for every (k, G)-module W. We will use them tacitly in what follows.
Recall that we are given a (k, G)-module V, of dimension $d \geq 3$, together with a G-invariant line $L_0 \subset V$. We have to show that the map

$$K^s(V, L_0)(*) \longrightarrow K^s(V, L_0)(*)/p^s$$

is n-surjective. We assume the result known in dimension $d - 1$.

We have a commutative diagram

$$\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
K^s(V, L_0)/p^s & \xrightarrow{\mathrm{Ver}^r} & K^{s+r}(V, L_0)/p^{s+r} \\
\downarrow & & \downarrow \\
\Omega^s(V)/p^s & \xrightarrow{\mathrm{Ver}^r} & \Omega^{s+r}(V)/p^{s+r} \\
\downarrow & & \downarrow \\
\Omega^s(V/L_0)/p^s & \xrightarrow{\mathrm{Ver}^r} & \Omega^{s+r}(V/L_0)/p^{s+r} \\
\downarrow & & \downarrow \\
0 & & 0,
\end{array}$$

where the horizontal maps are induced by the Verschiebung homomorphism.
The lifting property we have to show is stable, in the sense of the Lemma below.

Lemma 11.14. *Let $G' \subset G$ be an open subgroup of finite index. Pick a class*

$$a \in H^n(G', K^s(V, L_0)(*)/p^s).$$

Assume that the class

$$\mathrm{Ver}^r_*(a) \in H^n(G', K^{s+r}(V, L_0)(*)/p^{s+r})$$

lifts to a class in $H^n(G', K^{s+r}(V, L_0)(*))$.
Then a itself lifts to a class in $H^n(G', K^s(V, L_0)(*))$.

Proof. This is an easy chase in the (twist by $\mathcal{T}$ of the) diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L_0^{(s)} & \longrightarrow & K^s(V, L_0) & \longrightarrow & K^s(V, L_0)/p^s & \longrightarrow & 0 \\
 & & \| & & \downarrow{\scriptstyle \mathrm{Ver}^r} & & \downarrow{\scriptstyle \mathrm{Ver}^r} & & \\
0 & \longrightarrow & L_0^{(s+r)} & \longrightarrow & K^{s+r}(V, L_0) & \longrightarrow & K^{s+r}(V, L_0)/p^{s+r} & \longrightarrow & 0.
\end{array}$$

To understand this diagram, and why it commutes, recall the 9-term commutative diagram following Remark 11.2, making it clear that the top (resp. bottom) injection is induced by Ver^s (resp. by Ver^{r+s}). □

Now, choose a G-invariant two-dimensional k-subspace

$$W \subset V,$$

containing L_0. Such a W exists, since G is a pro-p-group.
For $L \in \mathbb{P}(W), L \neq L_0$, put

$$W_L := W,$$

and put

$$W_{L_0} = L_0.$$

Denote by

$$f : \bigoplus_{L \in \mathbb{P}(W)} V/L \longrightarrow \bigoplus_{L \in \mathbb{P}(W)} V/W_L$$

the sum of the quotient maps $V/L \longrightarrow V/W_L$.

We have a canonical map

$$\Phi : K^s(V, L_0) \longrightarrow K^s(f),$$

fitting into the commutative diagram

$$\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
K^s(V, L_0) & \xrightarrow{\Phi} & K^s(f) \\
\downarrow & & \downarrow \\
\Omega^s(V) & \longrightarrow & \Omega^s(\bigoplus_{L \in \mathbb{P}(W)} V/L) \\
\downarrow & & \downarrow \\
\Omega^s(V/L_0) & \longrightarrow & \Omega^s(\bigoplus_{L \in \mathbb{P}(W)} V/W_L) \\
\downarrow & & \downarrow \\
0 & & 0.
\end{array}$$

We have another commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \bigoplus_{L \in \mathbb{P}(W)} W_L^{(s)}/L^{(s)} & \longrightarrow & K^s(f) & \longrightarrow & K^s(f)/p^s & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \bigoplus_{L \in \mathbb{P}(W)} V^{(s)}/L^{(s)} & \longrightarrow & \Omega^s(\bigoplus_{L \in \mathbb{P}(W)} V/L) & \longrightarrow & \Omega^s(\bigoplus_{L \in \mathbb{P}(W)} V/L)/p^s & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \bigoplus_{L \in \mathbb{P}(W)} V^{(s)}/W_L^{(s)} & \longrightarrow & \Omega^s(\bigoplus_{L \in \mathbb{P}(W)} V/W_L) & \longrightarrow & \Omega^s(\bigoplus_{L \in \mathbb{P}(W)} V/W_L)/p^s & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Put

$$\mathbb{P}'(W) := \mathbb{P}(W) - \{L_0\};$$

it is a one-dimensional affine space over k, endowed with a continuous action of G. Note that, for each $L' \in \mathbb{P}'(W)$, we have a canonical homomorphism

$$K^s(f) \longrightarrow K^s(V/L', W/L'),$$

fitting into the commutative diagram

$$\begin{array}{ccc}
0 & & 0 \\
\downarrow & & \downarrow \\
K^s(f) & \longrightarrow & K^s(V/L', W/L') \\
\downarrow & & \downarrow \\
\Omega^s(\bigoplus_{L\in\mathbb{P}(W)} V/L) & \longrightarrow & \Omega^s(V/L') \\
\downarrow & & \downarrow \\
\Omega^s(\bigoplus_{L\in\mathbb{P}(W)} V/W_L) & \longrightarrow & \Omega^s(V/W) \\
\downarrow & & \downarrow \\
0 & & 0,
\end{array}$$

where the horizontal arrows are induced by the projections

$$\bigoplus_{L\in\mathbb{P}(W)} V/L \longrightarrow V/L'$$

and

$$\bigoplus_{L\in\mathbb{P}(W)} V/W_L \longrightarrow V/W_{L'} = V/W.$$

Lemma 11.15. *The quotient map*

$$K^s(f)(*) \longrightarrow K^s(f)(*)/p^s$$

is n-surjective.

Proof.

The claim follows from a straightforward chase in the twist by $\mathcal{T}$ of (the long exact sequence in cohomology induced by) the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \bigoplus_{L\in\mathbb{P}(W)} W_L^{(s)}/L^{(s)} & \longrightarrow & K^s(f) & \longrightarrow & K^s(f)/p^s & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \bigoplus_{L\in\mathbb{P}'(W)} W^{(s)}/L^{(s)} & \longrightarrow & \bigoplus_{L\in\mathbb{P}'(W)} K^s(V/L, W/L) & \longrightarrow & \bigoplus_{L\in\mathbb{P}'(W)} K^s(V/L, W/L)/p^s & \longrightarrow & 0
\end{array}$$

in which the lower line is n-surjective, Shapiro's Lemma and by the induction hypothesis (dimension $d-1$). □

Now, recall that we have, at our disposal, the transfer

$$t_{\mathbb{P}(W)} : \Omega^s(\bigoplus_{L\in\mathbb{P}(W)} V/L) \longrightarrow \Omega^{s+r}(V).$$

LEMMA 11.16. *We have a canonical commutative diagram (of $(W(k), G)$-modules)*

$$\begin{array}{ccc} \Omega^s(\bigoplus_{L\in\mathbb{P}(W)} V/L) & \longrightarrow & \Omega^{s+r}(V) \\ \downarrow & & \downarrow can \\ \Omega^s(V/L_0 \bigoplus V/W) & \longrightarrow & \Omega^{s+r}(V/L_0), \end{array}$$

where the vertical map on the left is obtained as follows. It is induced, by functoriality, from the linear map

$$\bigoplus_{L\in\mathbb{P}(W)} V/L \longrightarrow V/L_0 \bigoplus V/W$$

which is the direct sum of the identity map $V/L_0 \longrightarrow V/L_0$, and of the projections $V/L \longrightarrow V/W$, for $L \neq L_0$.

Proof.

Let us explain how to build the Pontryagin dual diagram, which occurs in the following setting.
Put

$$H_0 := L_0^{\perp} \simeq (V/L_0)^*$$

and

$$K := W^{\perp} \simeq (V/W)^*,$$

where $Z^{\perp}$ denotes the subspace of V^* consisting of linear forms vanishing on Z. These are linear subspaces of V^*. Put $X := \mathbb{P}(W)$, seen as the set of hyperplanes of V^*, containing K. The formula

$$\mathbb{A}_k(H_0) \longrightarrow \Gamma^{p^s}(H_0 \oplus K),$$

$$x \mapsto [(\mathrm{Frob}^r(x), T_{H_0,K}(x))]_{p^s},$$

is a polynomial law, of degree p^{s+r}. It thus defines a $\mathbf{W}(k)$-linear map

$$\Theta : \Gamma^{p^{s+r}}(H_0) \longrightarrow \Gamma^{p^s}(H_0 \oplus K).$$

Then, we have a commutative diagram

$$\begin{array}{ccc} \Gamma^{p^{s+r}}(H_0) & \xrightarrow{\Theta} & \Gamma^{p^s}(H_0 \bigoplus K) \\ \downarrow can & & \downarrow can \\ \Gamma^{p^{s+r}}(V^*) & \xrightarrow{t_X} & \Gamma^{p^s}(\bigoplus_{H\in X} H), \end{array}$$

where the vertical map on the right is induced, by functoriality, from the linear map which is the sum of the identity map $H_0 \longrightarrow H_0$, and of the inclusions $K \longrightarrow H$, for $H \neq H_0$. The diagram of the Lemma is its Pontryagin dual.
The fact that the diagram above commutes follows directly from the commutative diagrams

$$\begin{array}{ccc} \mathbb{A}_k(H_0) & \xrightarrow{T_{H_0,K}} & \mathbb{A}_k(K) \\ \downarrow can & & \downarrow can \\ \mathbb{A}_k(V^*) & \xrightarrow{T_{V^*,H}} & \mathbb{A}_k(H), \end{array}$$

for each $H \neq H_0$, containing K, and from the commutative diagram

$$\begin{array}{ccc} \mathbb{A}_k(H_0) & \xrightarrow{\mathrm{Frob}^r} & \mathbb{A}_k(H_0) \\ \downarrow{\scriptstyle can} & & \| \\ \mathbb{A}_k(V^*) & \xrightarrow{T_{V^*,H_0}} & \mathbb{A}_k(H_0) \end{array}$$

(cf. Lemma 8.5). □

From the preceding Lemma, we get a morphism Ψ, fitting into a commutative diagram

$$\begin{array}{ccc} 0 & & 0 \\ \downarrow & & \downarrow \\ K^s(f) & \xrightarrow{\Psi} & K^{s+r}(V, L_0) \\ \downarrow & & \downarrow \\ \Omega^s(\bigoplus_{L\in\mathbb{P}(W)} V/L) & \xrightarrow{t_{\mathbb{P}(W)}} & \Omega^{s+r}(V) \\ \downarrow & & \downarrow \\ \Omega^s(\bigoplus_{L\in\mathbb{P}(W)} V/W_L) & \longrightarrow & \Omega^{s+r}(V/L_0) \\ \downarrow & & \downarrow \\ 0 & & 0 \end{array}$$

Lemma 11.17. *The composite*

$$K^s(V, L_0) \xrightarrow{\Phi} K^s(f) \xrightarrow{\Psi} K^{s+r}(V, L_0)$$

equals Ver^r.

Proof. This is an immediate consequence of Lemma 8.10.

□

Remark 11.18. Note that Lemma 11.16 is just used to ensure that the map

$$t_{\mathbb{P}(W)} : \Omega^s(\bigoplus_{L\in\mathbb{P}(W)} V/L) \longrightarrow \Omega^{s+r}(V)$$

sends $K^s(f)$ to $K^{s+r}(V, L_0)$.

Lemma 11.19. *The map*

$$\Psi : K^s(f) \longrightarrow K^{s+r}(V, L_0)$$

maps

$$p^s K^s(f) = \bigoplus_{L\in\mathbb{P}(W)} W_L^{(s)}/L^{(s)}$$

to $K^{s+r}(W, L_0) \subset K^{s+r}(V, L_0)$.

Proof. Bearing in mind that Ψ is induced by the transfer $t_{\mathbb{P}(W)}$, this follows from the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \bigoplus_{L\in\mathbb{P}(W)} W_L^{(s)}/L^{(s)} & \xrightarrow{\mathrm{Ver}^s} & \Omega^s(\bigoplus_{L\in\mathbb{P}(W)} W/L) & \xrightarrow{t_{\mathbb{P}(W)}} & \Omega^{s+r}(W) \\ & & \| & & \downarrow & & \downarrow can \\ 0 & \longrightarrow & \bigoplus_{L\in\mathbb{P}(W)} W_L^{(s)}/L^{(s)} & \longrightarrow & K^s(f) & \xrightarrow{t_{\mathbb{P}(W)}} & \Omega^{s+r}(V). \end{array}$$

That this diagram commutes is a consequence of the fact that the diagram

$$\begin{array}{ccc} \Omega^s(\bigoplus_{L\in\mathbb{P}(W)} W/L) & \xrightarrow{t_{\mathbb{P}(W)}} & \Omega^{s+r}(W) \\ \downarrow can & & \downarrow can \\ \Omega^s(\bigoplus_{L\in\mathbb{P}(W)} V/L) & \xrightarrow{t_{\mathbb{P}(W)}} & \Omega^{s+r}(V) \end{array}$$

commutes. This can be seen, for instance, by writing down its Pontryagin dual diagram. □

By the preceding Lemma, Ψ induces a morphism

$$\overline{\Psi} : K^s(f)/p^s \longrightarrow K^{s+r}(V, L_0)/K^{s+r}(W, L_0).$$

We also have a morphism

$$\overline{\Phi} : K^s(V/L_0)/p^s \longrightarrow K^s(f)/p^s,$$

induced by Φ.

We now have the tools to prove the induction step, which is the only part that remains in order to prove Proposition 11.6. It is a chase in the (twist by $\mathcal{T}$ of the) commutative diagram

$$\begin{array}{ccccc} K^s(V,L_0) & \xrightarrow{\phi} & K^s(f) & \xrightarrow{\psi} & K^{s+r}(V,L_0) \\ \downarrow & & \downarrow & & \downarrow Q \\ K^s(V,L_0)/p^s & \xrightarrow{\overline{\phi}} & K^s(f)/p^s & & K^{s+r}(V,L_0)/p^{s+r} \\ \| & & \| & & \downarrow \pi \\ K^s(V,L_0)/p^s & \xrightarrow{\overline{\phi}} & K^s(f)/p^s & \xrightarrow{\overline{\psi}} & K^{s+r}(V,L_0)/K^{s+r}(W,L_0), \end{array}$$

where the vertical arrows are the canonical projections. Remember that the composite of the top arrows is Ver^r.
Let $G' \subset G$ be an open subgroup of finite index. Pick a class

$$a \in H^n(G', K^s(V, L_0)(*)/p^s).$$

We want to show that it lifts to a class in $H^n(G', K^s(V, L_0)(*))$. By Lemma 11.14, it is enough to show that

$$a' := \mathrm{Ver}^r_*(a) \in H^n(G', K^{s+r}(V, L_0)(*)/p^{s+r})$$

lifts, via Q_*, to a class in $H^n(G', K^{s+r}(V, L_0)(*))$. By Lemma 11.15, the class

$$\overline{\phi}_*(a) \in H^n(G', K^s(f)(*)/p^s)$$

lifts to a class $b \in H^n(G', K^s(f)(*))$. Put

$$A := \psi_*(b) \in H^n(G', K^{s+r}(V, L_0)(*)).$$

Modifying a' by $Q_*(A)$, we can assume that $\pi_*(a') = 0$. We now use the (twist by $\mathcal{T}$ of the) diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^{s+r}(W, L_0) & \longrightarrow & K^{s+r}(V, L_0) & \longrightarrow & K^{s+r}(V, L_0)/K^{s+r}(W, L_0) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle Q'} & & \downarrow{\scriptstyle Q} & & \| & & \\ 0 & \longrightarrow & K^{s+r}(W, L_0)/p^{s+r} & \xrightarrow{i} & K^{s+r}(V, L_0)/p^{s+r} & \xrightarrow{\pi} & K^{s+r}(V, L_0)/K^{s+r}(W, L_0) & \longrightarrow & 0. \end{array}$$

We get a class

$$a'' \in H^n(G', K^{s+r}(W, L_0)(*)/p^{s+r}),$$

such that $i_*(a'') = a'$. But the map

$$Q'(*) : K^{s+r}(W, L_0)(*) \longrightarrow K^{s+r}(W, L_0)(*)/p^{s+r}$$

is n-surjective, by the two-dimensional case which has been treated independently before. This shows that a'' lifts via Q'_*, hence that a' lifts via Q_*. This finishes the proof.

12. The Lifting Theorems.

We now deduce, from Proposition 11.6, some lifting Theorems in profinite group cohomology.

Theorem 12.1. *Let k be a finite field, of cardinality $q = p^r$. Let G be a profinite group. Let $n \geq 0$ be an integer. Let $\mathbf{W}(k)(1)$ be an n-smooth cyclotomic G-module. Let V be a (k, G)-module. Then, for every integer $s \geq 1$, the quotient map*

$$\Omega^s(V)(n) \longrightarrow \Omega^s(V)(n)/p^s$$

is n-surjective.

Proof. We can assume that G is a pro-p-group. We proceed by induction on the dimension d of V; there is nothing to prove if $d = 0$. There exists a G-invariant line $L \subset V$. Recall the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^s(V, L) & \longrightarrow & \Omega^s(V) & \longrightarrow & \Omega^s(V/L) & \longrightarrow & 0\ . \\ & & \downarrow & & \downarrow{\scriptstyle Q'} & & \downarrow{\scriptstyle Q} & & \\ 0 & \longrightarrow & K^s(V, L)/p^s & \longrightarrow & \Omega^s(V)/p^s & \xrightarrow{\theta} & \Omega^s(V/L)/p^s & \longrightarrow & 0 \end{array}$$

We know that the map $Q(n)$ is n-surjective, by the induction hypothesis.

Let $G' \subset G$ be an open subgroup of finite index. Pick a class

$$a \in H^n(G', \Omega^s(V)(n)/p^s).$$

We want to show that a lifts via Q'_*. But we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V^{(p^s)} & \xrightarrow{\mathrm{Ver}^s} & \Omega^{p^s}(V) & \xrightarrow{Q'} & \Omega^{p^s}(V)/p^s & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \mathrm{Ver}^r} & & \downarrow{\scriptstyle \mathrm{Ver}^r} & & \\ 0 & \longrightarrow & V^{(p^{s+r})} & \xrightarrow{\mathrm{Ver}^{r+s}} & \Omega^{p^{r+s}}(V) & \xrightarrow{Q''} & \Omega^{p^{r+s}}(V)/p^{r+s} & \longrightarrow & 0 \end{array}$$

(recall k has cardinality p^r, hence $M^{(r)} \simeq M$, for every $\mathbf{W}(k)$-module M). By an easy diagram chase, we see that it is enough to show that

$$a' := \mathrm{Ver}_*^r(a)$$

lifts via Q''_*, which we now prove.
We have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^{r+s}(V,L) & \xrightarrow{i} & \Omega^{r+s}(V) & \xrightarrow{\pi} & \Omega^{r+s}(V/L) & \longrightarrow & 0\ , \\ & & \downarrow & & \downarrow{\scriptstyle Q''} & & \downarrow & & \\ 0 & \longrightarrow & K^{r+s}(V,L)/p^{r+s} & \xrightarrow{\bar{i}} & \Omega^{r+s}(V)/p^{r+s} & \xrightarrow{\overline{\pi}} & \Omega^{r+s}(V/L)/p^{r+s} & \longrightarrow & 0 \end{array}$$

analoguous to the one at the beginning of this proof, but in degree $s+r$ instead of s.

There exists a class $b \in H^n(G', \Omega^s(V/L)(n))$, such that

$$Q_*(b) = \theta_*(a).$$

But we have the transfer

$$t = t_{V,L} : \Omega^s(V/L) \longrightarrow \Omega^{s+r}(V),$$

which is such that the composite

$$\Omega^s(V/L) \xrightarrow{t} \Omega^{s+r}(V) \xrightarrow{\pi} \Omega^{s+r}(V/L)$$

equals Ver^r. Hence, we may replace a' by $a' - Q''_*(t_*(b))$, and reduce to the case where

$$\overline{\pi}_*(a') = 0.$$

Hence, there exists a class

$$a'' \in H^n(G', K^{r+s}(V,L)(n)/p^{r+s}),$$

such that $\bar{i}_*(a'') = a'$. But he quotient map

$$K^{r+s}(V,L)(n) \longrightarrow K^{r+s}(V,L)(n)/p^{r+s}$$

is n-surjective, by Proposition 11.6. Thus, a' lifts by Q''_*, and the proof is complete.

□

THEOREM 12.2. *Let k be a finite field, of cardinality $q = p^r$. Let G be a profinite group. Let $n \geq 0$ be such that G is n-smooth. Let V be a (k,G)-module. Let $s \geq 1$ be an integer. Then the natural injection*

$$i_V : V^{(s)} \longrightarrow \mathrm{Sym}^{p^s}(V),$$

$$x \mapsto x^{p^s},$$

is $(n+1)$-injective.

Proof. We can assume that G is a pro-p-group. By definition of smoothness for profinite groups, there exists an n-smooth cyclotomic G-module $\mathbf{W}(k)(1)$. Since G is a pro-p-group, $k(n)$ is isomorphic to the trivial representation k. Fixing such an isomorphism $k(n) \simeq k$ yields, for every (k,G)-module W, a functorial isomorphism $W(n) \simeq W$. It is thus equivalent to show that the map

$$i_V(n) : V^{(s)}(n) \longrightarrow \mathrm{Sym}^{p^s}(V)(n)$$

is $(n+1)$-injective.
But the map

$$\mathrm{Ver}^s : V^{(s)} \longrightarrow \Omega^s(V)$$

factors through i_V, by Proposition 7.6 . It is thus enough to prove the result with $\mathrm{Ver}^s(n)$ instead of $i_V(n)$. But, in the exact sequence

$$0 \longrightarrow V^{(s)}(n) \stackrel{\mathrm{Ver}^s(n)}{\longrightarrow} \Omega^s(V)(n) \longrightarrow \Omega^s(V)(n)/p^s \longrightarrow 0,$$

the surjection on the right is n-surjective, by Theorem 12.1. Hence, the injection $\mathrm{Ver}^s(n)$ is $(n+1)$-injective, qed. □

LEMMA 12.3. *Let k be a finite field, of cardinality $q = p^r$.*
Let G be a profinite group. Let $n \geq 0$ be such that G is n-smooth. Let V be a (k, G)-module. Let $P \subset V$ be a two-dimensional G-invariant k-linear subspace. Then the natural injection (of (k, G)-modules)

$$V \longrightarrow \bigoplus_{L \in \mathbb{P}(P)} (V/L)$$

is $(n+1)$-injective.

Proof. Apply the preceding Theorem (for $r = s$), together with Remark 8.12. □

The next Theorem can be considered as the Hauptpunkt of this paper. It uses everything that that been done before. It is, surprisingly, very easy to state.

THEOREM 12.4. *Let k be a finite field, of cardinality $q = p^r$.*
Let G be a profinite group. Let $n \geq 0$ be such that G is n-smooth. Let V be a (k, G)-module. Then the natural injection

$$V \stackrel{ev}{\longrightarrow} k[V^*],$$

$$v \mapsto (f \mapsto f(v)),$$

given by evaluation of linear forms, is $(n+1)$-injective.

Proof. By induction on the dimension of V, Lemma 12.3 implies that the morphism of (k, G)-modules

$$\Theta : V \longrightarrow \bigoplus_{H \in \mathbb{P}(V^*)} (V/H)$$

is $(n+1)$-injective (the sum is taken over all hyperplanes $H \subset V$). We can then, as usual, assume that G is a pro-p-group. Then, for every open subgroup $G' \subset G$, one-dimensional (k, G')-modules are trivial. Hence, there exists a G-invariant map (of G-sets)

$$\Phi : V^* - \{0\} \longrightarrow \bigsqcup_{H \in \mathbb{P}(V^*)} (V/H - \{0\}),$$

such that

$$\Phi(f) \in V/\mathrm{Ker}(f),$$

for each $f \in V^* - \{0\}$. Note that this amounts to choosing, for each hyperplane $H \subset V$, a generator of V/H, in a G-equivariant way. It is then easy to see that there exists a G-equivariant function

$$S : V^* - \{0\} \longrightarrow k^\times,$$

where G acts trivially on $k^\times$, such that

$$f(v)\Phi(f) = S(f)\overline{v} \in V/H,$$

for each $v \in V$, and for each non zero $f \in V^*$, with kernel H. Replacing Φ by $S^{-1}\Phi$, we can assume that $S = 1$, i.e. that

$$f(v)\Phi(f) = \overline{v} \in V/H.$$

Then, we can form the composite

$$\Theta' : V \xrightarrow{ev} k[V^*] \xrightarrow{\Psi} \bigoplus_{H \in \mathbb{P}(V^*)} (V/H),$$

where

$$\Psi([f]) = \Phi(f),$$

for all $f \in V^*$, and

$$\Psi([0]) = 0.$$

It is straightforward to check that $\Theta' = -\Theta$ (modulo p, there are -1 nonzero vectors on each line!). Since Θ is $(n+1)$-injective, so is ev, qed.

□

Remark 12.5. Let G be an arbitrary profinite group.
Since we know that G is 0-smooth, Theorem 12.4 implies the following. Let k be a finite field. Let V be a (k, G)-module. Then the natural injection

$$V \xrightarrow{ev} k[V^*],$$
$$v \mapsto (f \mapsto f(v)),$$

is 1-injective.

Remark 12.6. Using Shapiro's Lemma, the conclusion of Theorem 12.4 can be reformulated as follows. Pick $c \in H^{n+1}(G, V)$. Assume that, for each (nontrivial) open subgroup $G' \subset G$, and for each linear form $f \in \mathrm{Hom}_{(k,G')}(V, k)$, we have

$$f_*(\mathrm{Res}(c)) = 0 \in H^{n+1}(G', k),$$

where

$$\mathrm{Res} : H^{n+1}(G, V) \longrightarrow H^{n+1}(G', V)$$

is the restriction map. Then $c = 0$.

Remark 12.7. Note the difference, for instance, between Theorem 12.1 and Theorem 12.4. The first one concerns, in its very statement, $(\mathbf{W}(k), G)$-modules that are of p^{s+1}-torsion, where s is an arbitrary large integer. In the second one, the statements only imply (k, G)-modules! However, its proof (through the use of Theorem 12.1), uses cohomological computations modulo very large powers of p.

We conclude this section with a nice exercise.

Exercise 12.8. Let F be a global field, of characteristic not p. For each place v of F, denote by F_v the completion of F at v.

Choose a separable closure F_{sep} (resp. $F_{v,sep}$) of F (resp. of F_v).
Put $G := \mathrm{Gal}(F_{sep}/F)$ (resp. $G_v := \mathrm{Gal}(F_{v,sep}/F_v)$).
Up to conjugacy, each G_v might be viewed as a closed subgroup of G.
Let $n \geq 1$ be an integer. Let V be an $(\mathbb{F}_p, G)$-module, i.e. a mod p Galois representation over F. From what precedes, there are well-defined restriction maps

$$\mathrm{Res}_v : H^n(G, V) \longrightarrow H^n(G_v, V),$$

for each place v of F. Put

$$Ш^n(V) := \bigcap_v \mathrm{Ker}(\mathrm{Res}_v),$$

where the intersection is taken over all places v of F. It is the usual Tate-Shafarevich group of V. We know that $Ш^1(\mathbb{F}_p) = 0$ (Grunwald-Wang).
Use Remark 12.5 to show that

$$Ш^1(V) = 0,$$

for every $(\mathbb{F}_p, G)$-module V.

13. The Smoothness Theorem.

In this section, k is a finite field of cardinality $q = p^r$, and G is a profinite group.

Definition 13.1. *Let $\mathbf{W}(k)(1)$ be a cyclotomic G-module . Let $s, n \geq 1$ be integers. Cohomology classes in the image of the natural cup-product map*

$$H^1(G, \mathbf{W}(k)(1)/p^s)^n \longrightarrow H^n(G, \mathbf{W}(k)(n)/p^s)$$

are called symbols. If $H \subset G$ is a nontrivial open subgroup , the image of a symbol of $H^n(H, \mathbf{W}(k)(n)/p^s)$ by the corestriction (norm)

$$\mathrm{Cor} : H^n(H, \mathbf{W}(k)(n)/p^s) \longrightarrow H^n(G, \mathbf{W}(k)(n)/p^s)$$

is called an H-quasi-symbol. A class which can be written as a sum $a_1 + \ldots + a_N$, where a_i is an H_i-quasi-symbol, will be called a quasi-symbol.

Definition 13.2. *Let G be a profinite group. Let $\mathbf{W}(k)(1)$ be a cyclotomic G-module . We say that $\mathbf{W}(k)(1)$ has the weak Bloch-Kato property if the following holds. For every integers $s, n \geq 1$, every class in $H^n(G, \mathbf{W}(k)(n)/p^s)$ is a quasi-symbol.*

Lemma 13.3. *Let $\mathbf{W}(k)(1)$ be a cyclotomic G-module, which is 1-smooth. Let $n \geq 1$ be an integer. Assume that every class in $H^n(G, \mathbf{W}(k)(n)/p)$ is a quasi-symbol. Then, for every $s \geq 1$, every class in $H^n(G, \mathbf{W}(k)(n)/p^s)$ is a quasi-symbol, and $\mathbf{W}(k)(1)$ is n-smooth.*

Proof. First of all, notice that, by definition of 1-smoothness and of the cup-product, the natural map

$$H^n(G, \mathbf{W}(k)(n)/p^{s+1}) \longrightarrow H^n(G, \mathbf{W}(k)(n)/p)$$

is surjective on H-quasi-symbols (for every open subgroup $H \subset G$), hence on quasi-symbols. Thus, we only have to show the assertion about quasi-symbols. We now proceed by induction on s. Assume that the result holds for s; let us prove it for $s+1$. The (twisted) Kummer sequence

$$0 \longrightarrow \mathbf{W}(k)(n)/p^s \xrightarrow{*p} \mathbf{W}(k)(n)/p^{s+1} \xrightarrow{\pi} \mathbf{W}(k)(n)/p \longrightarrow 0$$

induces an exact sequence

$$H^n(H, \mathbf{W}(k)(n)/p^s) \longrightarrow H^n(H, \mathbf{W}(k)(n)/p^{s+1}) \xrightarrow{\pi_*} H^n(H, \mathbf{W}(k)(n)/p),$$

for every open subgroup $H \subset G$. An easy diagram chase, combined with the remark we just made, then yields the result.

□

DEFINITION 13.4. *Let G be a profinite group. Let k be a finite field. Pick an element*

$$e \in H^n(G,k) = \mathrm{YExt}^n_{(k,G)}(k,k).$$

The depth of e is, by definition, the lowest integer d, such that there exists an n-extension (of (k,G)-modules)

$$\mathcal{E} : 0 \longrightarrow k \longrightarrow A_0 \longrightarrow \ldots \longrightarrow A_{n-1} \longrightarrow k \longrightarrow 0,$$

whose class is e, and such that

$$\dim_k A_0 = d+1.$$

The depth of e shall be denoted by $\delta(e)$.

Remark 13.5. It is not hard to see that the depth of e may also be defined as follows. Consider all injections of (k,G)-modules

$$i : k \longrightarrow V,$$

such that $i_*(e) = 0$.
As an example of such i (using Shapiro's Lemma), one may take

$$k \longrightarrow k[G/H],$$

$$1 \mapsto \sum_{x \in G/H} [x],$$

where $H \subset G$ is a nontrivial open sugroup, such that the restriction of e vanishes in $H^n(H,k)$.
Then $\delta(e)$ is one less that the minimal possible dimension of V, where i ranges through all such injections.

LEMMA 13.6. *Let G be a pro-p-group. Let k be a finite field. Pick an element*

$$e \in \mathrm{YExt}^n_{(k,G)}(k,k) (= H^n(G,k)).$$

Then $\delta(e) = 0$ if and only if $e = 0$, and $\delta(e) = 1$ if and only if e can be written as $a \cup b$, with $a \in H^1(G,k)$ and $b \in H^n(G,k)$.

Proof. This is obvious, since all one-dimensional (k,G)-modules are trivial. □

THEOREM 13.7. *Let G be a pro-p-group, which is n-smooth, for a positive integer n. Let k be a finite field, of cardinality $q = p^r$. Pick a class*

$$e \in \mathrm{YExt}^{n+1}_{(k,G)}(k,k) (= H^{n+1}(G,k)),$$

with $\delta(e) \geq 2$.
Then there exists a class $x \in H^{n+1}(G,k)$, an open sugroup $H \subsetneq G$, of index at most p^r, and a class $y \in H^{n+1}(H,k)$, such that

$$x + \mathrm{Cor}(y) = e,$$

where $\mathrm{Cor} : H^{n+1}(H,k) \longrightarrow H^{n+1}(G,k)$ is the corestriction map, with moreover

$$\delta(x) \leq 1$$

and

$$\delta(y) < \delta(e).$$

Proof.

Pick an $(n+1)$-extension (of (k,G)-modules)

$$\mathcal{E} : 0 \longrightarrow k \longrightarrow A_0 \longrightarrow \ldots \longrightarrow A_n \longrightarrow k \longrightarrow 0,$$

whose class is e, and with $\dim_k A_0 = \delta(e)+1$. For sure, we can write $\mathcal{E}$ as the cup product of an 1-extension

$$\mathcal{E}_1 : 0 \longrightarrow k \stackrel{1\mapsto a_0}{\longrightarrow} A_0 \longrightarrow B \longrightarrow 0$$

by an n-extension

$$\mathcal{E}'_n : 0 \longrightarrow B \longrightarrow A_1 \longrightarrow \ldots \longrightarrow A_n \longrightarrow k \longrightarrow 0.$$

We have $\dim_k B = \delta(e) \geq 2$. In what follows, the class of the extension $\mathcal{E}_1$ (resp. $\mathcal{E}'_n$) shall be denoted by e_1 (resp. e'_n). Pick a nonzero G-invariant line $< kb_0 >= L \subset B$ (this is possible, since G is a pro-p-group). Form the pullback diagram

$$\begin{array}{ccccccccc}
\mathcal{P} : 0 & \longrightarrow & k & \longrightarrow & P & \stackrel{\pi}{\longrightarrow} & L & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow{\scriptstyle i} & & \\
\mathcal{E}_1 : 0 & \longrightarrow & k & \longrightarrow & A_0 & \stackrel{s}{\longrightarrow} & B & \longrightarrow & 0.
\end{array}$$

If G acts trivially on P, then the 1-extension $\mathcal{P}$ is trivial, which means the following. Denoting by

$$j : B \longrightarrow B/L$$

the quotient map, there exists an 1-extension $a \in \mathrm{YExt}^1_{(k,G)}(B/L, k)$ such that $j^*(a) = e_1$. But then,

$$e = e_1 \cup e'_n = j^*(a) \cup e'_n = a \cup j_*(e'_n),$$

and we would get $\delta(e) \leq \dim_k B - 1$, a contradiction.
Thus, G acts non trivially on P (through a nontrivial additive character, with values in k). Denote by H the kernel of this action; it is a normal subgroup of G of index at most p^r. In what follows, we denote by Res (resp. Cor) the restriction (resp. corestriction) maps from the cohomology of G to that of H (resp. from the cohomology of H to that of G). We put $X := G/H$. We are now at the main step of the proof, which essentially uses all the theory developped before.
We have the (G-equivariant) trace map

$$B[X] \stackrel{T}{\longrightarrow} B,$$

$$b[x] \mapsto b.$$

Denote by N the kernel of the surjective k-linear map

$$A_0 \bigoplus B[X] \bigoplus L \stackrel{\sigma}{\longrightarrow} B,$$

which is the direct sum of s, of T, and of i. Consider the $(n+1)$-extension

$$\mathcal{F} : 0 \longrightarrow N \longrightarrow A_0 \bigoplus B[X] \bigoplus L \longrightarrow A_1 \longrightarrow \ldots \longrightarrow A_n \longrightarrow k \longrightarrow 0,$$

which is the cup product of

$$0 \longrightarrow N \longrightarrow A_0 \bigoplus B[X] \bigoplus L \stackrel{\sigma}{\longrightarrow} B \longrightarrow 0$$

and $\mathcal{E}'_n$. Denote its class by f. We obviously have a morphism of complexes

$$\begin{array}{ccccccccccccc}
\mathcal{E}: 0 & \longrightarrow & k & \longrightarrow & A_0 & \longrightarrow & A_1 & \longrightarrow \ldots \longrightarrow & A_n & \longrightarrow & k & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle 1\mapsto(a_0,0,0)} & & \downarrow & & \| & & \| & & \| & & \\
\mathcal{F}: 0 & \longrightarrow & N & \longrightarrow & A_0 \bigoplus B[X] \bigoplus L & \longrightarrow & A_1 & \longrightarrow \ldots \longrightarrow & A_n & \longrightarrow & k & \longrightarrow & 0,
\end{array}$$

showing that
(a) The pushforward of f by the quotient map

$$N \mapsto N/ka_0$$

is zero in $H^{n+1}(G, N/ka_0)$.

But the trace map T obviously has an H-equivariant section. Thus, the 1-extension

$$0 \longrightarrow N \longrightarrow A_0 \bigoplus B[X] \bigoplus L \xrightarrow{\sigma} B \longrightarrow 0$$

is killed by restriction to H. A fortiori, we have that

(b) $\mathrm{Res}(f) = 0 \in H^{n+1}(H, N)$.

But we have a canonical injection

$$P \longrightarrow A_0 \bigoplus B[X] \bigoplus L,$$

$$x \mapsto (-x, 0, \pi(x)),$$

which obviously takes its values in N, yielding a G-equivariant injection

$$\phi : P \longrightarrow N.$$

It is clear that, for every $x \in P - \mathrm{Ker}(\pi)$, the stabilizer of $\phi(x)$ is H. From (a) and (b) (using Shapiro's Lemma), it follows that f is killed by Φ_*, where

$$\Phi : N \longrightarrow \bigoplus_{d \in \mathbb{P}(\phi(P))} (N/d)$$

is the canonical map. Hence

$$f = 0 \in H^{n+1}(G, N) = \mathrm{YExt}^{n+1}_{(k,G)}(k, N),$$

by Lemma 12.3. This implies that there exists a class

$$z = (z_1, z_2, z_3) \in H^n(G, A_0 \bigoplus B[X] \bigoplus L)$$

$$= H^n(G, A_0) \bigoplus H^n(G, B[X]) \bigoplus H^n(G, L),$$

whose pushforward by σ equals e'_n. But, trivially, we have

$$e_1 \cup s_*(z_1) = 0,$$

hence

$$e = e_1 \cup \sigma(z) = e_1 \cup (T_*(z_2) + i_*(z_3)).$$

By Shapiro's Lemma, z_2 can be viewed as a class in $H^n(H, B)$, and the preceding formula means that

$$e = i^*(e_1) \cup z_3 + e_1 \cup \mathrm{Cor}(z_2) = i^*(e_1) \cup z_3 + \mathrm{Cor}(\mathrm{Res}(e_1) \cup z_2).$$

Set $x := i^*(e_1) \cup z_3 \in H^{n+1}(G, k)$ and $y := \mathrm{Res}(e_1) \cup z_2 \in H^{n+1}(H, k)$. We obviously have $\delta(x) \leq 1$. The action of H on P is trivial, so that we can conclude, by the same argument already used at the beginning of this proof, that $\delta(y) < \delta(e)$.

□

We can now prove the main result of this paper, the Smoothness Theorem.

THEOREM 13.8. *Let G be a profinite group. Let k be a finite field. Then every 1-smooth cyclotomic G-module is smooth, and has the weak Bloch-Kato property.*

Proof.

We proceed by induction on $n \geq 1$. Thanks to Lemma 13.3, it is enough to show that, if for every $i \leq n$, we have that $W(k)(1)$ is i-smooth and that every class in $H^i(G, \mathbf{W}(k)(i)/p)$ is a quasi-symbol, then every class in $H^{n+1}(G, \mathbf{W}(k)(n+1)/p)$ is a quasi-symbol. We can assume that G is a pro-p-group. Then $\mathbf{W}(k)(n+1)/p \simeq k$, as (k, G)-modules. We are thus reduced to showing, under our assumptions, that every class in $H^{n+1}(G, k)$ is a quasi-symbol. This follows, by immediate induction on the depth of such a class, from Theorem 13.7.

□

14. Two applications of the Smoothness Theorem to Galois cohomology.

14.1. THE BLOCH-KATO GLITCH. The Smoothness Theorem yields, as a corollary, the usual Bloch-Kato conjecture, proved by Rost, Suslin and Voevodsky. As it is well-known to experts, the main part of this conjecture is the surjectivity of the norm-residue homomorphism, which we now prove.

COROLLARY 14.1. *Let F be a field of characteristic not p. Let $d \geq 1$ be an integer, which is nonzero in F. Then, for every $n \geq 1$, the cup product map*

$$\otimes^n_{\mathbb{Z}} H^1(F, \mu_d) \longrightarrow H^n(F, \mu_d^{\otimes n})$$

is surjective.

Proof. Denote by F_{sep}/F a separable closure of F, and by G its Galois group. We immediately reduce to the case where d is a power of the prime p. By Proposition 9.11, we know that the Tate module

$$\mu = \varprojlim_n \mu_{p^n}(F_{sep})$$

is 1-smooth (for $k = \mathbb{F}_p$). By Theorem 13.8, we obtain that every class in $H^n(F, \mu_d^{\otimes n})$ is a quasi-symbol, i.e. a sum of corestrictions of symbols. But, by the fact that the norm-residue homomorphism is compatible with the norm in Milnor K-theory ([GS], Proposition 7.5.5), such a class is a sum of symbols as well, qed. □

14.2. A BOUND ON SYMBOL LENGTH. A careful examination of the recursive processes used in this paper would yield bounds for the symbol length of cohomology classes. For example, here is what we can (easily) get in the Merkurjev-Suslin case, i.e. when $n = 2$, for prime exponent, and for a p-special field.

THEOREM 14.2. *Let F be a p-special field of characteristic not p. Take a central simple algebra A/F, of exponent p and of index p^d. Then A is Brauer-equivalent to the tensor product of at most $\frac{p^{p^d-1}-1}{p-1}$ cyclic algebras of degree p.*

Proof. Put $G := \mathrm{Gal}(F_{sep}/F)$; it is a pro-$p$-group. It is 1-smooth by Proposition 9.11. Under our assumptions, it is legitimate to identify μ_p and $k = \mathbb{F}_p$. Let E/F be a splitting field for A, of degree p^d. Then the exact sequence (of finite F-groups of multiplicative type)

$$1 \longrightarrow \mu_p \longrightarrow \mathrm{R}_{E/F}(\mu_p) \longrightarrow \mathrm{R}_{E/F}(\mu_p)/\mu_p \longrightarrow 1$$

is, in the langage of Galois representations, nothing but

$$0 \longrightarrow \mathbb{F}_p \xrightarrow{i} \mathbb{F}_p[X] \longrightarrow \mathbb{F}_p[X]/\mathbb{F}_p \longrightarrow 0,$$

where X is the finite G-set, of cardinality p^d, associated to the extension E/F. Denote by $x \in H^2(G, \mathbb{F}_p) \simeq T_p(\mathrm{Br}(F))$ the class of A. Then

$$i_*(x) = 0 \in H^2(G, \mathbb{F}_p[X]) \simeq T_p(\mathrm{Br}(E)).$$

Hence, x is represented by a 2-extension of the shape

$$0 \longrightarrow \mathbb{F}_p \longrightarrow \mathbb{F}_p[X] \longrightarrow A \longrightarrow \mathbb{F}_p \longrightarrow 0,$$

with A an $(\mathbb{F}_p, G)$-module, showing that $\delta(x) \leq p^d - 1$. Recall the theorem of Rosset and Tate in Milnor K-theory ([GS], Corollary 7.4.11). It implies the following. Let $H \subset G$ be an open subgroup, of index p^n. Then the image by the corestriction

$$\mathrm{Cor} : H^2(H, \mathbb{F}_p) \longrightarrow H^2(G, \mathbb{F}_p)$$

of a symbol is a sum of p^n symbols. It then readily follows, by induction on the depth using Theorem 13.7, that x is a sum of

$$p^{\delta(x)-1} + p^{\delta(x)-2} + \ldots + p + 1$$

symbols, whence the result. □

15. An application of the Smoothness Theorem to Galois representations.

In this section, we apply our lifting Theorems to the problem of lifting mod p Galois representations.

Definition 15.1. *Let G be a profinite group. Let k be a finite field. Let V be a (k, G)-module. If there exists a a $(\mathbf{W}(k), G)$-module $\mathcal{V}$, which is a free $\mathbf{W}_2(k)$-module, and such that*

$$V \simeq \mathcal{V}/p$$

as (k, G)-modules, we say that V has a lift modulo p^2, and that $\mathcal{V}$ is a lift of V modulo p^2.

Theorem 15.2. *Let G be a profinite group, which is 1-smooth (e.g. the absolute Galois group of a field F, of characteristic not p). Let k be a finite field. Then every (k, G)-module has a lift modulo p^2.*

The rest of this section is devoted to the proof of this Theorem.
Let us first discuss facts about n-extensions.

15.1. Comparing $\mathrm{YExt}^n_{(k,G)}$ and $\mathrm{YExt}^n_{(\mathbf{W}(k),G)}$. Let k be a perfect field of characteristic p. Let G be an arbitrary profinite group.

Definition 15.3. *Let A, B be (k,G)-modules. The canonical map*

$$\mathrm{YExt}^n_{(k,G)}(A,B) \longrightarrow \mathrm{YExt}^n_{(\mathbf{W}(k),G)}(A,B)$$

will be denoted by $\Theta^n_{A,B}$.

Lemma 15.4. *Let A, B be (k,G)-modules. Then the map $\Theta^1_{A,B}$ is injective.*

Proof. This is obvious, for an extension $\mathcal{E} \in \mathbf{YExt}^1_{(k,G)}(A,B)$ is trivial (in $\mathrm{YExt}^1_{(k,G)}(A,B)$, or in $\mathrm{YExt}^1_{(\mathbf{W}(k),G)}(A,B)$) if and only if it is split. □

Pick an extension

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

of $(\mathbf{W}(k),G)$-modules. Assume that A and C are (k,G)-modules.
Then B is obviously a $\mathbf{W}_2(k)$-module.

Definition 15.5. *With the preceding notation, the map*

$$B \longrightarrow B,$$

$$x \mapsto px,$$

takes values in A and contains A in its kernel. Hence, we have a well-defined map

$$C \longrightarrow A,$$

$$\pi(x) \mapsto px.$$

We denote this map by $\kappa(E)$.

The map $\kappa(E)$ enjoys a few elementary properties, which we now list. Proving them is an easy exercise, left to the reader.

The map $\kappa(E)$ is k-linear and G-equivariant.
It depends only on the isomorphism class $e \in \mathrm{YExt}^1_{(\mathbf{W}(k),G)}(C,A)$ of $\mathcal{E}$, and will thus often be denoted by $\kappa(e)$.
It vanishes identically if and only if B is a k-vector space, i.e. if $\mathcal{E}$ belongs to $\mathbf{YExt}^1_{(k,G)}(C,A)$.
If $f : A \longrightarrow A'$ and $g : C' \longrightarrow C$ are morphisms of (k,G)-modules, then we have

$$\kappa(f_* g^*(E)) = f \circ \kappa \circ g.$$

If F is another object of $\mathbf{YExt}^1_{(\mathbf{W}(k),G)}(C,A)$, we have $\kappa(\mathcal{E}+\mathcal{F}) = \kappa(\mathcal{E}) + \kappa(\mathcal{F})$.

Remark 15.6. Let M be a $\mathbf{W}(k,G)$- module, which is a free $\mathbf{W}_2(k)$-module. We then have an exact sequence

$$\mathcal{S} : 0 \longrightarrow pM \longrightarrow M \longrightarrow M/p \longrightarrow 0,$$

where $\kappa(\mathcal{S})$ is an isomorphism. It is then clear that the following holds.
For a (k,G)-module V, to say that V has a lift modulo p^2 is equivalent to requiring the existence of an exact sequence of $\mathbf{W}(k,G)$-modules

$$\mathcal{E} : 0 \longrightarrow V \longrightarrow \mathcal{V} \longrightarrow V \longrightarrow 0,$$

with $\kappa(\mathcal{E}) = \mathrm{Id}$.

LEMMA 15.7. *Let V be a (k,G)-module. Assume that V admits a lift $\mathcal{V}$, modulo p^2. Pick an exact sequence of $\mathbf{W}(k,G)$- modules*

$$\mathcal{E} : 0 \longrightarrow V \longrightarrow \mathcal{V} \longrightarrow V \longrightarrow 0,$$

with $\kappa(\mathcal{E}) = \mathrm{Id}$.

Then, for every (k,G)-module W, the map

$$\Psi : \mathrm{YExt}^1_{(k,G)}(V,W) \bigoplus \mathrm{Hom}(V,W) \longrightarrow \mathrm{YExt}^1_{(\mathbf{W}(k),G)}(V,W),$$

$$(x,\phi) \mapsto \Theta^1_{V,W}(x) + \phi_*(\mathcal{E}),$$

is an isomorphism.

Proof. Pick an object $\mathcal{F}$ in $\mathbf{YExt}^1_{(\mathbf{W}(k),G)}(V,W)$. Then, a straightforward computation yields

$$\kappa(\kappa(\mathcal{F})_*(\mathcal{E}) - \mathcal{F}) = \kappa(F) - \kappa(F) = 0.$$

Hence, the extension $\kappa(\mathcal{F})_*(\mathcal{E}) - \mathcal{F}$ actually belongs to $\mathrm{YExt}^1_{(k,G)}(V,W)$. Passing to isomorphism classes yields the formula

$$\mathrm{YExt}^1_{(\mathbf{W}(k),G)}(V,W) \longrightarrow \mathrm{YExt}^1_{(k,G)}(V,W) \bigoplus \mathrm{Hom}(V,W),$$

$$f \mapsto (f - \kappa(f)_*(e), \kappa(f)),$$

giving the inverse of Ψ. □

PROPOSITION 15.8. *Let V be a (k,G)-module, which has a lift modulo p^2. Then, for every (k,G)-module W, the map*

$$\Theta^2_{V,W} : \mathrm{YExt}^2_{(k,G)}(V,W) \longrightarrow \mathrm{YExt}^2_{(\mathbf{W}(k),G)}(V,W)$$

is injective.

Proof.

This is a straightforward consequence of Lemma 15.7, by dimension shifting. Indeed, pick $w \in \mathrm{Ker}(\Theta^2_{V,W})$. Pick an exact sequence of (k,G)-modules

$$0 \longrightarrow W \xrightarrow{i} X \xrightarrow{\pi} Y \longrightarrow 0,$$

such that $i_*(w) = 0$. Then there exists a class $y \in \mathrm{YExt}^1_{(k,G)}(V,Y)$ such that $\delta(y) = w$, where

$$\delta : \mathrm{YExt}^1_{(k,G)}(V,Y) \longrightarrow \mathrm{YExt}^2_{(k,G)}(V,W)$$

is the connecting homomorphism. Since $w \in \mathrm{Ker}(\Theta^2_{V,W})$, there exists $x' \in \mathrm{YExt}^1_{(\mathbf{W}(k),G)}(V,X)$ such that $\pi_*(x') = \Theta^1(y)$. By Lemma 15.7, we can write $x' = \Theta^1(x) + \phi_*(e)$, for unique $x \in \mathrm{YExt}^1_{(k,G)}(V,X)$ and $\phi \in \mathrm{Hom}(V,X)$. We can assume that $x = 0$. Then $\pi \circ \phi = 0$, hence $\phi = i \circ \psi$, for $\psi \in \mathrm{Hom}(V,W)$. But then

$$x' = i_*(\psi_*(e)),$$

hence $\Theta^1(y)$=0. By injectivity of Θ^1, we get y=0. Thus $w = 0$ as well. □

15.2. The fundamental 2-extension. In this subsection, V is a (k,G)-module.

Definition 15.9. *We put*

$$\gamma^p(V) := \Gamma^p(V)/p = \Gamma^p_k(V).$$

We define $\gamma^p_0(V)$ *to be the kernel of* $\mathrm{Frob} : \gamma^p(V) \longrightarrow V^{(1)}$.

Recall that we have an exact sequence (of $\mathbf{W}_2(k)$-modules)

$$\mathcal{E}_1 = \mathcal{E}_{1,V} : 0 \longrightarrow T_p(\Gamma^p(V)) = \mathrm{Sym}^p(V) \longrightarrow \Gamma^p(V) \xrightarrow{\mathrm{Frob}} V^{(1)} \longrightarrow 0.$$

One easily checks that $\kappa_{\mathcal{E}_1}$ is induced by $\mathrm{Ver} : V^{(1)} \longrightarrow \mathrm{Sym}^p(V) \subset \Gamma^p(V)$.
Dually, we have the exact sequence

$$\mathcal{E}_2 = \mathcal{E}_{2,V} : 0 \longrightarrow V^{(1)} \xrightarrow{\mathrm{Ver}} \Gamma^p(V) \longrightarrow \gamma^p(V) \longrightarrow 0.$$

One checks that $\kappa_{\mathcal{E}_2}$ is induced by $\mathrm{Frob} : \gamma^p(V) \longrightarrow V^{(1)}$.

The composite

$$\mathrm{Sym}^p(V) \longrightarrow \Gamma^p(V) \longrightarrow \gamma^p(V)$$

has image equal to $\gamma^p_0(V)$, and has kernel equal to $V^{(1)}$. It thus yields a canonical isomorphism

$$\mathrm{Sym}^p(V)/V^{(1)} \longrightarrow \gamma^p_0(V),$$

which we use to identify these two spaces.

Exercise 15.10. Show that $\gamma^p_0(V^*)$ and $\gamma^p_0(V)^*$ are canonically isomorphic, as (k,G)-modules.

The pushforward of $\mathcal{E}_1$ by the surjection $\mathrm{Sym}^p(V) \longrightarrow \gamma^p_0(V)$ is nothing but the exact sequence

$$\mathcal{E}'_1 = \mathcal{E}'_{1,V} : 0 \longrightarrow \gamma^p_0(V) \xrightarrow{j_V} \gamma^p(V) \xrightarrow{\mathrm{Frob}} V^{(1)} \longrightarrow 0.$$

Dually, the pullback of $\mathcal{E}_2$ by the injection $\gamma^p_0(V) \longrightarrow \gamma^p(V)$ is the exact sequence

$$\mathcal{E}'_2 = \mathcal{E}'_{2,V} : 0 \longrightarrow V^{(1)} \longrightarrow \mathrm{Sym}^p(V) \longrightarrow \gamma^p_0(V) \longrightarrow 0.$$

Definition 15.11. *The cup product of* $\mathcal{E}'_1$ *and* $\mathcal{E}'_2$ *is a* 2*-extension (in* $\mathbf{YExt}^2_{(k,G)}(V^{(1)}, V^{(1)})$*)*

$$\mathcal{E}^2(V) : 0 \longrightarrow V^{(1)} \xrightarrow{i_V} \mathrm{Sym}^p(V) \longrightarrow \gamma^p(V) \longrightarrow V^{(1)} \longrightarrow 0,$$

which we call the fundamental 2*-extension associated to* V*. Its class in* $\mathrm{YExt}^2_{(k,G)}(V^{(1)}, V^{(1)})$ *will be denoted by* $e^2(V)$*.*

Remark 15.12. Here is another way of defining $\mathcal{E}^2(V)$.
Consider the extension (of $(\mathbf{W}(k), G)$-modules)

$$0 \longrightarrow \mathrm{Sym}^p(V) \longrightarrow \Gamma^p(V) \xrightarrow{\mathrm{Frob}} V^{(1)} \longrightarrow 0.$$

Applying the functor $. \otimes_{\mathbf{W}(k)} k$ to this extension yields a 2-extension

$$0 \longrightarrow \mathrm{Tor}_1^{\mathbf{W}(k)}(V^{(1)}, k) \longrightarrow \mathrm{Sym}^p(V) \longrightarrow \gamma^p(V) \xrightarrow{\mathrm{Frob}} V^{(1)} \longrightarrow 0.$$

But we have a canonical isomorphism

$$\mathrm{Tor}_1^{\mathbf{W}(k)}(V^{(1)}, k) \simeq V^{(1)}.$$

The 2-extension above is then nothing but $\mathcal{E}^2(V)$.

Remark 15.13. The arrow

$$\mathrm{Sym}^p(V) \longrightarrow \gamma^p(V),$$

in $\mathcal{E}^2(V)$, is the map

$$x_1 \otimes \ldots \otimes x_p \mapsto [x_1]_1 \ldots [x_p]_1.$$

If we identify $\gamma^p(V)$ with $(V^{\otimes p})^{\mathcal{S}_p}$, this arrow is the so-called 'symmetrizing operator'.

LEMMA 15.14. *Let V be a (k,G)-module. Then $e^2(V)$ belongs to* $\mathrm{Ker}(\Theta^2)$.

Proof. As an extension of $(\mathbf{W}(k),G)$-modules, $\mathcal{E}_2'$ is the pullback of

$$\mathcal{E}_2 = \mathcal{E}_{2,V} : 0 \longrightarrow V^{(1)} \xrightarrow{\mathrm{Ver}} \Gamma^p(V) \longrightarrow \gamma^p(V) \longrightarrow 0$$

by j_V. Hence the cup product of $\mathcal{E}_1'$ and $\mathcal{E}_2'$, in $\mathbf{YExt}^2_{(\mathbf{W}(k),G)}(V^{(1)},V^{(1)})$, is trivial, qed. □

PROPOSITION 15.15. *Let V be a (k,G)-module. The following are equivalent.*

(a) the (k,G)-module V has a lift modulo p^2,
(b) The class $e^2(V) \in \mathrm{YExt}^2_{(k,G)}(V^{(1)},V^{(1)})$ vanishes.

Proof. We have $e^2(V) \in \mathrm{Ker}(\Theta^2)$, by Lemma 15.14. It then follows from Proposition 15.8 that (a) implies (b).

Let us now prove that (b) implies (a). Assume that

$$e^2(V) = 0 \in \mathrm{YExt}^2_{(k,G)}(V^{(1)},V^{(1)}).$$

Then there exists an extension

$$\mathcal{F} : 0 \longrightarrow V^{(1)} \longrightarrow F \longrightarrow \gamma^p(V) \longrightarrow 0,$$

in $\mathbf{YExt}^1_{(k,G)}(\gamma^p(V),V^{(1)})$, such that $j_V^*(\mathcal{F})$ is isomorphic to $\mathcal{E}_1$. In the category $\mathbf{YExt}^1_{(\mathbf{W}(k),G)}(\gamma^p(V),V^{(1)})$, put

$$\mathcal{G} = \mathcal{E}_2 - \mathcal{F}.$$

Clearly, we have

$$\kappa(\mathcal{G}) = \kappa(\mathcal{E}_2) - \kappa(\mathcal{F}) = \mathrm{Frob} - 0 = \mathrm{Frob},$$

and $j_V^*(\mathcal{G})$ is trivial. Hence, there exists an extension

$$\mathcal{H} : 0 \longrightarrow V^{(1)} \longrightarrow H \longrightarrow V^{(1)} \longrightarrow 0,$$

in $\mathbf{YExt}^1_{(\mathbf{W}(k),G)}(V^{(1)},V^{(1)})$, such that $\mathrm{Frob}^*(\mathcal{H})$ is isomorphic to $\mathcal{G}$. We compute

$$\mathrm{Frob} = \kappa(\mathcal{G}) = \kappa(\mathrm{Frob}^*(\mathcal{H})) = \kappa(\mathcal{H}) \circ \mathrm{Frob}.$$

Since Frob is surjective, we infer that $\kappa(\mathcal{H}) = \mathrm{Id}$. Hence $\mathcal{H}$ is a lift of $V^{(1)}$ modulo p^2. Since k is perfect, V also possesses a lift modulo p^2, qed.

□

Combining the previous Proposition and Proposition 15.8, we immediately get the following.

PROPOSITION 15.16. *Let V be a (k,G)-module. The following are equivalent.*

(a) The (k,G)-module V has a lift modulo p^2.
(b) For every (k,G)-module W, the map

$$\Theta^2_{V,W} : \mathrm{YExt}^2_{(k,G)}(V,W) \longrightarrow \mathrm{YExt}^2_{(\mathbf{W}(k),G)}(V,W)$$

is injective.
(c) The class $e^2(V) \in \mathrm{YExt}^2_{(k,G)}(V^{(1)},V^{(1)})$ vanishes.

Remark 15.17. Let V be a (k,G)-module. It is given by a group homomorphism

$$\rho : G \longrightarrow \mathrm{GL}_k(V).$$

The 2-extension

$$\mathcal{E}^2(V) : 0 \longrightarrow V^{(1)} \longrightarrow \mathrm{Sym}^p(V) \longrightarrow \gamma^p(V) \longrightarrow V^{(1)} \longrightarrow 0$$

is actually a 2-extension of $(k,\mathrm{GL}_k(V))$-modules. Hence, the class $e^2(V)$ is in the image of

$$\rho^* : \mathrm{YExt}^2_{(k,\mathrm{GL}_k(V))}(V^{(1)},V^{(1)}) \longrightarrow \mathrm{YExt}^2_{(k,G)}(V^{(1)},V^{(1)}).$$

15.3. PROOF OF THEOREM 15.2. We proceed by induction on the dimension d of V. There is nothing to prove if $d = 0$, and the result is standard if $d = 1$ (Teichmüller). We may thus assume that $d \geq 2$, and that the conclusion of the Theorem holds for all finite fields k, and all (k,G)-modules of dimension $\leq d-1$. By Proposition 15.16, we see that it suffices to show that $e^2(V) = 0$. By Lemma 3.7, we can view $e^2(V)$ as a class

$$h^2(V) \in \mathrm{YExt}^2_{(k,G)}(k,\mathrm{Hom}_k(V^{(1)},V^{(1)})) = \mathrm{YExt}^2_{(k,G)}(k,V^{(1)}\otimes V^{*(1)}).$$

Let us briefly recall how. By definition, $e_2(V) \in \mathrm{YExt}^2_{(k,G)}(V^{(1)},V^{(1)})$ is the class of

$$\mathcal{E}^2(V) : 0 \longrightarrow V^{(1)} \xrightarrow{i_V} \mathrm{Sym}^p(V) \xrightarrow{s_p} \gamma^p(V) \xrightarrow{\mathrm{Frob}} V^{(1)} \longrightarrow 0,$$

where s_p is the symmetrizing operator. Tensoring by $V^{*(1)}$, we get a 2-extension (of (k,G)-modules)

$$0 \longrightarrow V^{(1)}\otimes V^{*(1)} \xrightarrow{I} \mathrm{Sym}^p(V)\otimes V^{*(1)} \xrightarrow{S} \gamma^p(V)\otimes V^{*(1)} \xrightarrow{F} V^{(1)}\otimes V^{*(1)} \longrightarrow 0,$$

whose class we denote by $e'^2(V) \in \mathrm{YExt}^2_{(k,G)}(V^{(1)}\otimes V^{*(1)},V^{(1)}\otimes V^{*(1)})$. Define

$$\Psi : k \longrightarrow V^{(1)}\otimes V^{*(1)}$$

by the formula

$$\lambda \mapsto \lambda\mathrm{Id}.$$

Then $h^2(V) = \Psi^*(e'^2(V))$. We now have to show that $h^2(V) = 0$.

By Theorem 12.4, or more precisely by Remark 12.6, it is enough to prove the following. Let $G' \subset G$ be a (nontrivial) open subgroup, and let

$$f \in \mathrm{Hom}_{(k,G')}(V^{(1)}\otimes V^{*(1)},k).$$

Then, we have

$$f_*(\mathrm{Res}(h^2(V))) = 0 \in H^2(G',k),$$

where Res is the restriction map, from the cohomology of G to that of G'. Without loss of generality, we can assume that $G' = G$. There exists

$$g \in \mathrm{Hom}_{(k,G)}(V,V)$$

such that

$$f(x^{(1)} \otimes \phi^{(1)}) = \phi(g(x))^p$$

(this is a fancy reformulation of the standard fact that any linear form on the space of $n \times n$ matrices is of the shape $X \mapsto \mathrm{Tr}(XY)$, for a unique matrix Y).
Let k'/k be a finite field extension. The the natural map

$$H^2(G, k) \longrightarrow H^2(G, k')$$

is obviously injective. Hence, enlarging k if necessary, we may assume that g possesses an eigenvalue $\lambda \in k$. From the decomposition

$$g = (g - \lambda \mathrm{Id}) + \lambda \mathrm{Id},$$

it follows that it is enough to show that $f_*(h^2(V)) = 0$ in one of the following two cases.

(a) The endomorphism g is not injective.
(b) We have $g = \mathrm{Id}$.

In case (a), The endomorphism g factors as

$$V \longrightarrow V/W \xrightarrow{\sim} Z \longrightarrow V,$$

with $W = \mathrm{Ker}(g)$ and $Z = \mathrm{Im}(g)$; these are k-subspaces of dimension $\leq d - 1$.
Denote by $\pi : V^{(1)} \longrightarrow (V/W)^{(1)}$ (resp $j : Z^{(1)} \longrightarrow V^{(1)}$) the natural map.
The map f hence factors through the quotient map

$$V^{(1)} \otimes V^{*(1)} \xrightarrow{\pi \otimes j^*} (V/W)^{(1)} \otimes Z^{*(1)}.$$

It is thus clear that $f_*(h^2(V))$ depends only on

$$j^*(\pi_*(e^2(V))) \in \mathrm{YExt}^2_{(k,G)}(Z^{(1)}, (V/W)^{(1)}).$$

But this class belongs to $\mathrm{Ker}(\Theta^2_{Z^{(1)},(V/W)^{(1)}})$, which is trivial by Proposition 15.16, since $Z^{(1)}$ admits a lift modulo p^2 by induction.
Hence, in case (a), we can indeed conclude that $f_*(h^2(V)) = 0$.

To finish the proof, it remains to show that $f_*(h^2(V)) = 0$ in case (b), i.e. when f is the trace map

$$\mathrm{Tr} : V^{(1)} \otimes V^{*(1)} \longrightarrow k,$$

$$x^{(1)} \otimes \phi^{(1)} \mapsto \phi(x)^p.$$

Let

$$\rho : G \longrightarrow \mathrm{GL}_k(V)$$

be the group homomorphism giving the action of G on V. By Remark 15.17, and since Tr is $\mathrm{GL}_k(V)$-equivariant, it is clear that $\mathrm{Tr}_*(h^2(V))$ is in the image of the map

$$\rho^* : H^2(\mathrm{GL}_k(V), k) \longrightarrow H^2(G, k).$$

But, by [Q], Theorem 6, the source of ρ^* is trivial if $r(p-1) > 2$, where $q = p^r$ is the cardinality of k (i.e. for all finite fields, except possibly for those of cardinality $2, 3$ and 4). But replacing k by a finite field extension does not affect what has to

be proven. To see this, take a finite field extension k'/k, put $V' := V \otimes_k k'$, and have a look at the commutative diagram

$$\begin{array}{ccc} H^2(\mathrm{GL}_{k'}(V'), k') & \xrightarrow{\rho'^*} & H^2(G, k') \\ \downarrow & & \| \\ H^2(\mathrm{GL}_k(V), k') & \xrightarrow{\rho^*} & H^2(G, k') \\ \uparrow & & \uparrow \\ H^2(\mathrm{GL}_k(V), k) & \xrightarrow{\rho^*} & H^2(G, k) \end{array}$$

where the two vertical arrows going up are injective. If k' is large enough, we have $H^2(\mathrm{GL}_{k'}(V'), k') = 0$ by *loc. cit.*
Hence, by an easy diagram chase, $\mathrm{Tr}_*(h^2(V)) = 0$, and the proof is complete.

In the course of the preceding proof, the crucial fact that $\mathrm{Tr}_*(h^2(V)) = 0$ was shown using a result of Quillen. The next exercise provides a self-contained proof of this fact.

Exercise 15.18. Let k be a finite field. Let $d \geq 1$ be an integer. Let M_2 be a free $\mathbf{W}_2(k)$-module of rank d. Put $M_1 := M_2/p$.

(1) Show that we have an commutative diagram (with exact rows and columns)

$$\begin{array}{ccccccccc} & & 1 & & 1 & & 1 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{End}_k(M_1^{(1)})_0 & \longrightarrow & \mathrm{SL}_{\mathbf{W}_2(k)}(M_2) & \longrightarrow & \mathrm{SL}_k(M_1) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{End}_k(M_1^{(1)}) & \longrightarrow & \mathrm{GL}_{\mathbf{W}_2(k)}(M_2) & \xrightarrow{\pi} & \mathrm{GL}_k(M_1) & \longrightarrow & 1 \\ & & \downarrow \mathrm{Tr} & & \downarrow \det & & \downarrow \det & & \\ 1 & \longrightarrow & k & \longrightarrow & \mathbf{W}_2(k)^\times & \longrightarrow & k^\times & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 1 & & 1 & & 1 & & \end{array},$$

where $\mathrm{End}_k(M_1^{(1)})_0$ denotes the kernel of the trace map Tr, and where the horizontal surjections are given by reduction mod p.

(2) Show that the action of $\mathrm{GL}_k(M_1)$ on $\mathrm{End}_k(M_1^{(1)})$ induced by the middle row of the preceding diagram is the natural conjugation action (twisted by Frobenius).

Now, let G be a profinite group, acting trivially on the groups in the diagram above. Let V be a (k, G)-module.

(3) Show that V corresponds to a $\mathrm{GL}_k(M_1)$-torsor X, whose class in $H^1(G, \mathrm{GL}_k(M_1))$ we denote by x. Show that V can be lifted mod p^2 if and

only if x in in the image of

$$\pi_* : H^1(G, \mathrm{GL}_{\mathbf{W}_2(k)}(M_2)) \longrightarrow H^1(G, \mathrm{GL}_k(M_1)).$$

(3) Show that the twist of $\mathrm{End}_k(M_1^{(1)})$ by X is canonically isomorphic (as a (k, G)-module) to $\mathrm{End}_k(V^{(1)})$, and that the obstruction to lifting x via π_* is a class $h'^2(V) \in H^2(G, \mathrm{End}_k(V^{(1)}))$.

(4) Use the diagram above to show that $\mathrm{Tr}_*(h'^2(V)) = 0 \in H^2(G, k)$.

(5) Show that $h'^2(V) = h^2(V)$.

Bibliography

[Fe] D. Ferrand.— *Un foncteur norme*, Bull. Soc. Math. France 126 (1998), no. 1, 1-49.

[FFSS] V. Franjou, E. Friedlander, A. Scorichenko, A. Suslin.— *General linear and functor cohomology over finite fields*, Ann. of Math. 150 (1999), no. 2, 663-728.

[GS] P. Gille, T. Szamuely.— *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics 101 (2006), Cambridge University Press.

[H] S. Hamblen.— *Lifting n-dimensional Galois representations*, Canad. J. Math. 60 (2008), 1028-1049.

[K] D. Kaledin.— *Witt vectors as a polynomial functor*, preprint, available on the arXiv server.

[M] J. Manoharmayum.— *Lifting n-dimensional Galois representations to characteristic zero*, preprint (2013), available on the arXiv server.

[Q] D. Quillen.— *On the Cohomology and K-Theory of the General Linear Group Over a Finite Field*, Ann. of Math. 96, No. 3 (1972), 552-586.

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

[Ve] J.-L. Verdier.— *Des catégories dérivées des catégories abéliennes*, Astérisque 239 (1996).

[Se] J.-P. Serre.— *Galois cohomology*, Springer-Verlag, 2002.

Charles De Clercq, Laboratoire Analyse, Géométrie et Applications, Université Paris 13, 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.