

LIFTING THEOREMS AND SMOOTH PROFINITE GROUPS

CHARLES DE CLERCQ AND MATHIEU FLORENCE¹*October 2017*

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. This work is motivated by the search for an "explicit" proof of the Bloch-Kato conjecture in Galois cohomology, proved by Voevodsky in [Vo]. Our concern here is to lay the foundation for a theory that, we believe, will lead to such a proof- and to further applications.

Let p be a prime number. Let k be a perfect field of characteristic p . Let m be a positive integer. Our first goal is to provide a canonical process for "lifting" a module M , over the ring of Witt vectors $\mathbf{W}_m(k)$ (of length m), to a $\mathbf{W}_{m+1}(k)$ -module, in a way that deeply respects Pontryagin duality. These are our big, medium and small Omega powers (cf. Definitions 8.17 and 12), each of which naturally occurs as a direct factor of the previous one. In the case where M is a k -vector space, they come equipped with Verschiebung and Frobenius operations (cf. section 10). If moreover the field k is finite, Omega powers are endowed with a striking extra operation: the Transfer, to shifted Omega powers of finite-codimensional linear subspaces (cf. section 13). To show how this formalism fits into Galois theory, we first offer an axiomatized approach to Hilbert's Theorem 90 (or more precisely, to its consequence for cohomology with finite coefficients: Kummer theory). In the context of profinite group cohomology, we thus define the notions a cyclotomic G -module (Definition 14.9), and of a smooth profinite group (Definition 14.18). We bear in mind that the fundamental example is that of an absolute Galois group, together with the Tate module of roots of unity. We then define the notion of exact sequences of G -modules *of Kummer type*- see Definition 14.30.

To finish, we give applications of this formalism. The first ones are the Stable Lifting Theorems (Theorems 16.2 and 16.3), enabling the lifting to higher torsion in the cohomology of smooth profinite groups, with p -primary coefficients. To illustrate their meaning, we translate the second one in the concrete context of Galois cohomology, with values in two-dimensional Galois representations (Corollary 16.4). We finish by an application to p -adic deformations. We state and prove a (perhaps unusual) general descent statement, for the quotient map $\mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$. It is Proposition 17.9.

¹Florence was partially supported by the French National Agency (Project GeoLie ANR-15-CE40-0012).

CONTENTS

1. Introduction.	3
1.1. First idea.	3
1.2. Second idea.	5
2. Notation and basic facts.	8
2.1. Witt vectors.	9
2.2. Profinite groups and cohomology.	10
2.3. Categories of representations.	11
3. On induction from subgroups, and Shapiro's Lemma.	11
4. The Tense product.	14
5. Divided powers.	18
5.1. Polynomial laws.	19
5.2. Divided powers and duality.	21
5.3. Divided powers versus symmetric powers.	22
6. The Teichmüller representative, as a polynomial law.	23
6.1. Divided powers of torsion $\mathbf{W}(k)$ -modules.	25
6.2. An alternate description of Γ^p for vector spaces.	30
7. The Frobenius and the Verschiebung.	30
8. Divided powers and Pontryagin duality.	33
8.1. Duality.	33
8.2. Medium and big Omega powers.	36
8.3. Medium Omega powers as a direct factor of big Omega powers.	37
9. Functorial properties of Omega powers.	39
9.1. Multilinearity.	39
9.2. Omega powers of $\mathbf{W}_m(k)$ -algebras	40
9.3. Behaviour of Omega powers under field extensions.	41
10. Frobenius and Verschiebung, for Omega powers.	43
11. The Transfer.	45
11.1. Laws in one variable.	45
11.2. The Transfer, as a polynomial law.	47
12. Small Omega powers.	51
12.1. Small Omega powers as a direct factor of medium Omega powers.	51
13. The Transfer, for small Omega Powers.	54
13.1. The Transfer, as a contravariant functor.	56
13.2. The Integral Formulas for the Frobenius and the Verschiebung.	59
14. Axiomatizing Hilbert's Theorem 90.	60
14.1. The notion of n -surjectivity.	60

14.2. Cyclotomic modules and smoothness.	62
14.3. The Smoothness Conjecture.	64
14.4. Exact sequences of Kummer type.	65
15. About Hilbert's Theorem 90.	68
16. The Stable Lifting Theorems.	70
17. An application to p -adic deformation theory.	74
17.1. The case of perfect \mathbb{F}_p -algebras.	74
17.2. Descent for the arrow $\mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$.	74
Acknowledgements	79
Bibliography	79

1. INTRODUCTION.

The main goal of this paper is to define and study a very low level smoothness notion. By "low level", we mean that most of our constructions just depend on a given prime number p . In a subsequent paper, we plan to strengthen the Stable Lifting Theorems for Galois cohomology that we present here, in order to achieve an explicit proof of the Bloch-Kato conjecture. This was our starting motivation. Let us simply say that, though we did not achieve a full proof yet, we are confident that the present approach will eventually be successful- when the foundations are solid enough.

It is folklore that mod p cohomology often encodes subtle phenomena in higher p -primary torsion. For instance, section 6.2 presents a mod p Hochschild 2-cocycle, canonically attached to a mod p^2 algebraic object. The general philosophy of this paper is, whenever possible, to lift mod p algebraic data to higher p -primary torsion in a natural way. This data may be a module, an algebra, a Hopf algebra, a cohomology class, etc... We try to do so using, as a basic algebraic tool, divided powers of finite modules over the ring of Witt vectors $\mathbf{W}(k)$. It is often enlightening to think of these modules as the coefficients of some cohomology theory. Hence, in practice, the field k will often be finite- a seemingly crucial requirement to define the Transfers (see Section 11).

We now wish to share some ideas which motivated this work. In what follows, k is a perfect field of characteristic p , and F is a field of characteristic not p . Let F_{sep}/F be a separable closure of F . We put $G := \text{Gal}(F_{sep}/F)$. We denote by $d = p^s$ a power of the prime p .

1.1. FIRST IDEA. Let us start by giving a purely Galois-theoretic statement of the Norm-Residue Isomorphism Theorem, proved by Rost, Suslin and Voevodsky. Our point here is to make clear that this Theorem presents a deep connection with the general notion of smoothness.

For each integer $i \geq 0$, denote by \mathcal{H}^i the Galois cohomology group $H^i(F, \mu_p^{\otimes i})$.

Then the cup-product operation, being \mathbb{F}_p -multilinear, yields a homomorphism of graded \mathbb{F}_p -algebras

$$h : \bigoplus_{i=0}^{\infty} T^i(\mathcal{H}^1) \longrightarrow \bigoplus_{i=0}^{\infty} \mathcal{H}^i,$$

where $T^i(\mathcal{H}^1) = \bigotimes_{\mathbb{F}_p}^i \mathcal{H}^1$ is the i -th fold tensor power of \mathcal{H}^1 (note that this map actually factors through the exterior power $\Lambda_{\mathbb{F}_p}^i(\mathcal{H}^1)$, if p is odd or if $p = 2$ and (-1) is a square in F). Then the Norm-Residue Isomorphism Theorem states that h is surjective, and that its kernel is generated, in degree two, by all pure tensors

$$a \otimes b \in \mathcal{H}^1 \otimes_{\mathbb{F}_p} \mathcal{H}^1,$$

such that $a \cup b = 0 \in \mathcal{H}^2$.

Indeed, pure tensors arising from Steinberg's relation are a particular instance of these, and it is not too hard to show directly that all pure quadratic tensors in $\text{Ker}(h)$ are combinations of pure tensors arising from Steinberg's relation.

Now, let (A, M_x) be the local ring of variety X over \mathbb{F}_p , at a *smooth* rational point $x \in X(\mathbb{F}_p)$. Then the natural homomorphism of graded \mathbb{F}_p -algebras

$$\bigoplus_{i=0}^{\infty} T^i(M_x/M_x^2) \longrightarrow \bigoplus_{i=0}^{\infty} (M_x^i/M_x^{i+1}),$$

is surjective, with kernel generated by degree two tensors of the shape $a \otimes b - b \otimes a$.

It is clear that these two results present strong similarities- though the second one, of commutative nature, is much easier to prove...

What is more, it is known to expert that the hard part of the Bloch-Kato conjecture is to show that the natural map

$$H^i(F, \mu_{p^s}^{\otimes i}) \longrightarrow H^i(F, \mu_p^{\otimes i})$$

is surjective, for every i and every field F , of characteristic not p . Thinking (abusively) of

$$H^i(F, \mu_{p^s}^{\otimes i})$$

as points modulo p^s of some algebraic object defined over \mathbb{Z}_p , the surjectivity in question is, again, the definition of (formal) smoothness. Note that, for $i = 1$, surjectivity is given by usual Kummer theory. Our Smoothness Conjecture 14.25 states, in particular, that surjectivity for i arbitrary should "formally" follow from the $i = 1$ case.

Let us now briefly explain how one can hope to apply general lifting results in Galois cohomology, to prove the Bloch-Kato conjecture. For simplicity, we concentrate on surjectivity part, in the $i = 2$ case (the Merkurjev-Suslin Theorem).

Let e be a class in $H^2(F, \mu_p^{\otimes 2})$. By a general fact from group cohomology, one can find a finite discrete G -module V , which is an \mathbb{F}_p -vector space, classes

$$a \in H^1(F, V \otimes_{\mathbb{F}_p} \mu_p) \text{ and } b \in H^1(F, V^{\vee} \otimes_{\mathbb{F}_p} \mu_p),$$

such that

$$e = a \cup b,$$

where the cup-product is relative to the canonical pairing

$$(V \otimes_{\mathbb{F}_p} \mu_p) \times (V^\vee \otimes_{\mathbb{F}_p} \mu_p) \longrightarrow \mu_p^{\otimes 2}.$$

(here $V^\vee = \text{Hom}_{\mathbb{F}_p}(V, \mathbb{F}_p)$).

This may seem obscure at first. Assuming that $\mu_p = \mathbb{F}_p$ for simplicity -which is a harmless assumption- it becomes clear if we adopt the viewpoint of (Yoneda) extensions. Indeed, a 2-extension in $\text{Ext}_{(\mathbb{F}_p, G)}^2(\mathbb{F}_p, \mathbb{F}_p)$ ($= H^2(G, \mathbb{F}_p)$) can always be seen as the cup-product of two 1-extensions.

If $V = \mathbb{F}_p^N$ was equipped with the *trivial* G -action, then e would be a sum of N^2 symbols, and the job would be done. More generally, imagine we can find a surjective morphism of (\mathbb{F}_p, G) -modules

$$f : W \longrightarrow V,$$

such that the following two conditions hold.

- 1) the induced map $H^1(G, W) \rightarrow H^1(G, V)$ is onto.
- 2) the (\mathbb{F}_p, G) -module W is permutation, i.e. has an \mathbb{F}_p -basis which is permuted by G .

Using Shapiro's Lemma, we see that the (projection) formula

$$f_*(c) \cup b = c \cup (f^\vee)_*(b),$$

valid for any $c \in H^1(G, W)$, would then present e as a sum of *corestrictions* of symbols. An input from Milnor K -theory (namely, the existence of the norm, and its compatibility with the norm-residue homomorphism), shows that a corestriction of a symbol (in Galois cohomology) is a sum of symbols, and we would be done.

A map f with the properties above does, as one may guess, not exist in general. Meanwhile, our Stable Lifting Theorem 16.3 (for $k = \mathbb{F}_p$) does a very similar job. However, it applies only in higher p -primary torsion. Indeed, note that the module

$$\bigoplus_{L \in \mathbb{F}(V)} \underline{\Omega}^n(L)(s)$$

is not a fearsome beast at all: it is a honest module which is *induced from dimension one* (in the sense of Definition 2.6, with the H_i 's being the stabilizers of lines of V). For example, if $n = 0$ and G is a pro- p -group, it is a permutation (\mathbb{F}_p, G) -module in the sense of 2) above.

Note that the Stable Lifting Theorem can nonetheless apply to lift our cohomology classes a and b , but only after pushing them by a power of the Verschiebung

$$\text{Ver}^n : V \longrightarrow \underline{\Omega}^n(V).$$

In Exercise 16.1, we explain why the Stable Lifting Theorems do not hold for $n = 0$, using Manin's R -equivalence (in the context of Galois cohomology).

1.2. SECOND IDEA. The theory of Witt vectors associates, to every perfect field k of characteristic p , a discrete valuation ring $\mathbf{W}(k)$, whose basic properties we shall recall in the next section. We develop here the theory of divided powers for torsion modules over Witt vectors, whose purpose is, somehow, to categorify Witt's construction. To do so, we use the divided powers functors $\Gamma_{\mathbf{W}(k)}^{p^n}$, applied to torsion $\mathbf{W}(k)$ -modules. We view them as *representing polynomial laws* (cf. [Ro], or the nice and short paper [Fe]). Note that truncated Witt vectors themselves, through a simple recursive process, can be defined just using $\Gamma_{\mathbb{Z}}^p$, see Proposition 6.8.

We try to proceed as functorially as possible. We eventually offer three ways of lifting a $\mathbf{W}_m(k)$ -module to a $\mathbf{W}_{m+n}(k)$ -module: the big, medium and small Omega powers (respectively, $\overline{\Omega}^n$, Ω^n and $\underline{\Omega}^n$). The composition formula $\overline{\Omega}^{n+n'} = \overline{\Omega}^n \circ \overline{\Omega}^{n'}$ only holds for big Omega powers. However, we prove (cf. Propositions 8.17 and 12.10) that medium (resp. small) Omega powers canonically embed, in a duality-preserving way, in big (resp. medium) Omega powers. In the course of the proofs of these two Propositions, mysterious p -adic constants appear- see Definition 8.14 and Lemma 12.4. We do not know understand their meaning. Do they have one? Note that, in dimension one, small, medium and big Omega powers all coincide, and are indeed a "categorification" of the multiplicative Teichmüller section

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

In the recent preprints [K1] and [K2], related constructions are proposed, in a different language. It would be interesting to explore the connections.

When the field k is finite, we introduce a $\mathbf{W}(k)$ -linear map "in the wrong direction": the Transfer, notably for small Omega powers. We believe that it presents connections to the (algebraic) Steenrod algebra, as defined in [Sm]. Indeed, our formula for the hyperplane Transfer (cf. Lemma 11.15), is very close to the formula defining $P(\xi)(l)$, in Smith's paper.

In section 14, we spend some time to axiomatize Kummer theory- a consequence of Hilbert's Theorem 90 for (Galois) cohomology with values in roots of unity. In the general context of profinite group cohomology, we define the notion of a smooth profinite group G , of a cyclotomic G -module and of a Kummer-type exact sequence. We state the Smoothness Conjecture 14.25, implying the Bloch-Kato conjecture.

Combining our formalism with classical techniques from group cohomology (restriction, corestriction and Shapiro's Lemma), we are finally able to prove very general results for the cohomology of smooth profinite groups: the Stable Lifting Theorems (Theorem 16.2 and Theorem 16.3). They are not yet sufficient to prove the Smoothness Conjecture, but we strongly believe that they will- after some improvement.

The formalism we develop here presents potential for applications to other topics. We now venture to list five of these. On this matter, we deeply welcome comments, (constructive) criticism, suggestions and collaborative work.

1) The first one is p -adic deformation theory. The descent statement that we offer in Proposition 17.9 is most likely an explicit description of an abstract *non linear* (degree p) descent statement for algebraic structures mod p^n . It would be interesting to identify it.

To illustrate what we mean by "explicit", we proceed with an analogy in the classical context. This analogy is for sure well known to many experts- though the explicit computations that make it precise are hard to find in the litterature.

Grothendieck's faithfully flat descent theory for Modules (say, for simplicity, in the affine case) has many concrete incarnations. For G -Galois algebras, it specializes to Galois descent (this is Speiser's Lemma, cf. [GS], Lemma 2.3.8). In characteristic p , for purely inseparable field extensions of height one, it specializes to Cartier's descent (*loc. cit.*, Theorem 9.3.6). If $X = \text{Spec}(A)$ is an affine smooth variety over any field k of characteristic p , then the Frobenius morphism

$$\text{Frob} : A \otimes_{\text{frob}} k \longrightarrow A,$$

$$x \otimes \lambda \mapsto \lambda x^p$$

is finite and flat, and Cartier's Frobenius descent is, again, an explicit geometric description of faithfully flat descent.

2) The second one concerns the question of lifting (mod p) Galois representations to mod p^2 Galois representations- and perhaps even to higher torsion. This important topic has already been investigated by many authors, notably in the context of local or global fields. We already have some (new) results for arbitrary fields, and plan to publish them in a dedicated paper.

3) We believe that Omega powers could perhaps be used in modular representation theory- of finite groups, or of algebraic groups. For instance, if V is a finite-dimensional k -vector space, the quotient

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

is a k -linear representation of the algebraic group $\mathrm{GL}_k(V)$ (in the sense of [J]). We believe that it cannot, in general, be obtained as a subquotient of a tensor power of V . In other words, divided powers over $\mathbf{W}(k)$ are required in its construction- though, in the end, it is a mod p object.

4) It is likely that our "gentle" machinery can help to say something about resolution of singularities. A strong reason for this fact is the following. The $\mathbf{W}(k)$ -module

$$\Gamma_{\mathbf{W}(k)}^p(\mathbf{W}_m(k)) (\simeq \mathbf{W}_{m+1}(k))$$

is an elementary algebraic blowup of $\mathbf{W}_m(k)$, that lifts (the exponent of) its torsion by one. Forming Omega powers of $\mathbf{W}_m(k)$ -algebras (cf. section 9.2) is thus a way of performing a vast amount of these small blowups. This point of view is connected to the notion of Rees algebra of a module, as investigated in the recent paper [St].

5) Last, but not least, let us remark that our approach here is purely local, at a given prime p . Once polished, it could be fruitfully globalized, considering all functors $\Gamma_{\mathbb{Z}}^n$ at once...

The paper is organized as follows. We first recall some classical facts about profinite groups, representation theory and cohomology. We then explain, in section 3, a categorical formulation of the induction process from open subgroups and of Shapiro's Lemma. Though elementary, it plays an important role in this paper, where most properties concerning a profinite group G (eg. n -surjectivity) involve all open subgroups of G at once. We then emphasize the importance of Pontryagin duality (in algebra). Though invisible, it is omnipresent in all cohomological theories: the injective Abelian group \mathbb{Q}/\mathbb{Z} naturally occurs when building canonical injective resolutions of sheaves. After that, it is (unfortunately...) often disregarded or forgotten. In section 4, we begin with recalling that Pontryagin duality does not commute to the tensor product- even in the category of $(\mathbb{Z}/p^n\mathbb{Z})$ -modules, for $n \geq 2$. Note that, if it did, the topological issue of tensor completions would be much simpler. We make a short attempt to define the "Tense Product", a symmetric monoidal operation on the category of $(\mathbb{Z}/p^n\mathbb{Z})$ -modules, that commutes to Pontryagin duality. It behaves well with the Omega power functors, that we define later on.

In section 5, we recall (mostly well-known) facts about divided powers. We see them as representing homogeneous polynomial laws- as explained in [Ro]. We

mainly concentrate on the case of modules over Witt vectors. Along the way, we give a simple presentation of truncated Witt vectors themselves, as a quotient of a divided power module over \mathbb{Z} (cf. Proposition 6.8). In section 7, we introduce the Frobenius and Verschiebung operators, for divided powers. In section 8.7, we investigate the lack of commutation between Pontryagin duality and divided powers- reminiscent of Section 4. We introduce (big and medium) Omega powers, as the "correct" quotients of divided powers, commuting to duality. We show that medium Omega powers occur as a direct factor of big Omega powers. We study their first functorial properties. In section 11, we define the Transfer, a fundamental gadget to prove Lifting Theorems in cohomology, by induction on the dimension of the coefficients. In section 12, we introduce small Omega powers. We show that they are a direct factor of medium Omega powers. Small Omega powers enjoy rich functorial properties (notably through the Transfer) which we begin to investigate in Section 13. See, in particular, Proposition 13.7. We prove the Integral Formulas for the Frobenius and the Verschiebung. They are, perhaps, connected to motivic integration. In Section 14, we present a possible axiomatization of Kummer theory. We define the notions of cyclotomic module, of smooth profinite group and of Kummer-type extension. We bear in mind that the fundamental example of a smooth profinite group is that of an absolute Galois group, equipped with the Tate module of roots of unity. Section 15 is a short digression, to stress the importance of Hilbert's Theorem 90 in our approach- perhaps the purest of all descent statements. In section 16, we prove two first applications of our formalism to Galois theory: the Stable Lifting Theorems. We present a concrete corollary of the second one (Corollary 16.4). We conclude by an application of our point of view to deformations: Proposition 17.9, which is a descent statement for the quotient map $\mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$.

This paper contains numerous remarks and exercises, the goal of which 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 perfect field k of characteristic p when possible, the case $k = \mathbb{F}_p$ is the essential one.

2. NOTATION AND BASIC FACTS.

Throughout this paper, p is a prime number. For obvious historical reasons, we could have chosen to denote p by l : the prime " p " here is the " l " of l -adic cohomology. A few months ago, we thus made an attempt to replace p by l everywhere in the text. The resulting formulae were esthetically questionable (if not ugly), and we decided to go back to the previous notation...

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 $M[n]$ the n -torsion of M . Let A be a ring. If M is an A -module, we denote by

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

the A -dual of M . We denote by

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

the symmetric algebra of M . We denote by

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

the exterior algebra of M . We have pairings

$$\begin{aligned} \Lambda_A^i(M) \times \Lambda_A^i(M^*) &\longrightarrow A, \\ (x_1 \wedge \dots \wedge x_i, \phi_1 \wedge \dots \wedge \phi_i) &\mapsto \det(\phi_b(x_a))_{1 \leq a, b \leq i}, \end{aligned}$$

and

$$\begin{aligned} \Lambda_A^i(M) \times \Lambda_A^j(M) &\longrightarrow \Lambda_A^{i+j}(M), \\ (x, y) &\mapsto x \wedge y. \end{aligned}$$

These are perfect if M is a finite locally free A -module of (constant) rank d , and $i + j = d$. In that case, we put

$$\text{Det}(M) := \Lambda_A^d(M);$$

it is an invertible A -module.

If the A -module M is locally free of finite rank, we denote by

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

the affine space of M ; it is an affine variety over $\text{Spec}(A)$. 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 $\delta(V)$ the dimension of V . We denote by $\mathbb{P}_k(V)$ the projective space of V , consisting of lines $L \subset V$ (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 , $\mathbb{P}_k(V)$ 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 .

Note that a simple (and perhaps new) recursive formula, presenting $\mathbf{W}_{n+1}(k)$ as a quotient of the p -th divided power of the \mathbb{Z} -module $\mathbf{W}_n(k)$, shall be given later on (Proposition 6.8).

We put

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

We shall often use the natural arrow

$$\begin{aligned} \mathbf{W}_n(k) &\longrightarrow K/\mathbf{W}(k), \\ 1 &\mapsto \frac{1}{p^n} \end{aligned}$$

to identify the p^n -torsion in $K/\mathbf{W}(k)$ with $\mathbf{W}_n(k)$. However, one has to be careful in doing so- see for instance section 4.

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

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

it is the Pontryagin dual of M . Note that Pontryagin duality extends the linear duality of k -vector spaces to all $\mathbf{W}(k)$ -modules. More precisely, if M is seen as a $\mathbf{W}_n(k)$ -module, one has a canonical isomorphism

$$M^\vee \simeq \text{Hom}_{\mathbf{W}_n(k)}(M, \mathbf{W}_n(k)) = M^*.$$

The Frobenius morphism

$$\begin{aligned} k &\longrightarrow k, \\ x &\mapsto x^p \end{aligned}$$

lifts to a ring homomorphism

$$\text{frob} : \mathbf{W}(k) \longrightarrow \mathbf{W}(k).$$

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

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

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 cohomology groups, defined by Serre in [Se]. At our disposal, we have the restriction maps

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

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

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

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

If $G' \subset G$ is an open subgroup, of index n in G , then $\text{Cor} \circ \text{Res}$ equals multiplication by n .

Remark 2.1. In the course of proving results involving a profinite group G , we shall often reduce to the case where G is pro- p -group, using the standard "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 .

2.3. CATEGORIES OF REPRESENTATIONS. Let G be a profinite group. Let k be a perfect field of characteristic p , often finite in our applications.

DEFINITION 2.2. A $(\mathbf{W}(k), G)$ -module is a torsion $\mathbf{W}(k)$ -module M of finite-type, 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 2.3. Assume that k is finite, and that F_{sep}/F is a separable closure of a field F . Then a $(k, \text{Gal}(F_{sep}/F))$ -module is nothing but a Galois representation over the field k .

Remark 2.4. 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 2.5. 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

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

Among $(\mathbf{W}(k), G)$ -modules, the simplest are those who come from an action of G on a finite set- the permutation modules. Let us give a precise Definition.

DEFINITION 2.6. Let M be a $(\mathbf{W}(k), G)$ -module. It is said to be induced from rank one if it is isomorphic to a finite direct sum

$$\bigoplus_i \text{Ind}_{H_i}^G(L_i),$$

where $H_i \subset G$ are open subgroups, and L_i are $(\mathbf{W}(k), H_i)$ -modules, which are (free) $\mathbf{W}_{n_i}(k)$ -module of rank one, for some positive integers n_i .

If moreover all L_i 's are equipped with the trivial H_i -action, M is said to be a permutation module.

Remark 2.7. If G is a p -group, all one-dimensional (k, G) -modules are trivial. Hence, a (k, G) -module is induced from rank one if and only if it is permutation. Through the usual 'restriction-corestriction' argument, for G arbitrary, (k, G) -modules which are induced from rank one may often be assumed to be permutation.

3. ON INDUCTION FROM SUBGROUPS, AND SHAPIRO'S LEMMA.

Shapiro's Lemma is a fundamental basic tool in group cohomology. We now briefly explain how we can view it.

DEFINITION 3.1. 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

$$\begin{aligned} G &\longrightarrow \bigsqcup_{g \in G} M_{gx}, \\ g &\mapsto \phi_{g,x}(m), \end{aligned}$$

is continuous (=locally constant).

(ii) For all $x \in X$, we have

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

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

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

Remark 3.2. In the particular case of a one-element set, it is clear that a discrete G -module over $\{*\}$ is simply a discrete G -module.

Remark 3.3. 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 $h \in H = \text{Stab}(x_0)$. 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 3.4. 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 $\text{Ind}_H^G(M)$. Note that, since H has finite index in G , this induced module can be defined either by the formula

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

or by

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

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 $H^n(G, \text{Ind}_H^G(M))$ and $H^n(H, M)$ are canonically isomorphic. Putting what we just said together, we get the following statement.

PROPOSITION 3.5. *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 3.6. 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 .

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

$$\mathcal{M}_L := V/L,$$

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 be crucial in the proof the Stable Lifting Theorems.

4. THE TENSE PRODUCT.

In this section, we elaborate on the lack of commutation between the (usual) tensor product, and Pontryagin duality. This phenomenon is at the heart of our approach. We thus chose to introduce some related notions (the valuation of a module, its trace and its Chern character) that we find colorful- though they will not be used in the rest of this paper.

Let k be a perfect field of characteristic $p > 0$. We denote by $\{\mathbf{W}_n(k) - \text{Mod}\}$ the category of (arbitrary) $\mathbf{W}_n(k)$ -modules. In what follows, the symbol \otimes means $\otimes_{\mathbf{W}_n(k)}$.

Recall that, for any $\mathbf{W}_n(k)$ -module M , we have an 'equality'

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

We will now see that it strongly depends on n .

Let M and N be two $\mathbf{W}_n(k)$ -modules. Through the preceding identification, we have a pairing

$$\begin{aligned} \Phi_{n,M,N} : (M \otimes N) \times (M^\vee \otimes N^\vee) &\longrightarrow \mathbf{W}_n(k), \\ ((m \otimes n), (\phi \otimes \psi)) &\mapsto \phi(m)\psi(n). \end{aligned}$$

It is perfect if (and only if) M or N is a finite and free $\mathbf{W}_n(k)$ -module. What is more, it is somewhat badly behaved, in the sense that it strongly depends on n : if $m \geq n$ is another integer, viewing M and N as $\mathbf{W}_m(k)$ -modules yields the formula

$$\Phi_{m,M,N} = p^{m-n} \Phi_{n,M,N},$$

as pairings with values in $K/\mathbf{W}(k)$. In particular, if M and N are actually k -vector spaces, the pairing $\Phi_{2,M,N}$ is zero!

Thinking further, we see that the category of $\mathbf{W}_n(k)$ -modules is actually equipped with (at least) *two* tensor product structures: the usual one, and the one given by the formula

$$M \tilde{\otimes} N := (M^\vee \otimes N^\vee)^\vee.$$

If $n \geq 2$, there is no canonical isomorphism (of bifunctors) $M \tilde{\otimes} N \simeq M \otimes N$. This fact is a simple algebraic analogue of Grothendieck's theory of tensor products of topological vector spaces. Note that the Tense Product defined shortly will be ubiquitous later, when we mod out the kernel of Pontryagin duality for divided powers (see for instance Proposition 8.12).

DEFINITION 4.1. (*Tense Product.*) *Let M and N be two $\mathbf{W}_n(k)$ -modules. We put*

$$M \overline{\otimes}_n N := (M \otimes N) / \text{Ker}(\Phi_{n,M,N}),$$

where

$$\text{Ker}(\Phi_{n,M,N}) = \{x \in M \otimes N, \Phi_{n,M,N}(x, y) = 0, \forall y \in M^\vee \otimes N^\vee\}.$$

It is a $\mathbf{W}_n(k)$ -module, called the Tense Product of the $\mathbf{W}_n(k)$ -modules M and N . If the dependence in n is clear from the context, we shall denote it simply by $M\overline{\otimes}N$.

Remark 4.2. Assume that $M = \mathbf{W}_a(k)$ and $N = \mathbf{W}_b(k)$, with $1 \leq a, b \leq n$. We then have

$$M \otimes_{\mathbf{W}_n(k)} N = \mathbf{W}_{\min(a,b)}(k),$$

whereas

$$M\overline{\otimes}_n N = \mathbf{W}_{a+b-n}(k),$$

with the convention that $\mathbf{W}_i(k) = 0$ for negative i .

LEMMA 4.3. *The category $\{\mathbf{W}_n(k) - \text{Mod}\}$, equipped with the Tense Product, is a symmetric monoidal category, with coherence axioms inherited from those of the usual tensor product. The Tense Product commutes with Pontryagin duality of finite modules: for two finite $\mathbf{W}_n(k)$ -modules, we have a canonical isomorphism*

$$(M\overline{\otimes}N)^\vee \simeq M^\vee\overline{\otimes}N^\vee.$$

Proof. This is routine check. Let us perhaps explain why the Tense Product is (bi)functorial. Let $f : M \rightarrow N$ and $f' : M' \rightarrow N'$ be morphisms between $\mathbf{W}_n(k)$ -modules. Then, for $m \in M$, $m' \in M'$, $\phi \in N^\vee$ and $\phi' \in N'^\vee$, one has

$$\begin{aligned} \Phi_{n,N,N'}(f(m) \otimes f'(m'), \phi \otimes \phi') &= \phi(f(m))\phi'(f'(m')) \\ &= \Phi_{n,M,M'}(m \otimes m', f^\vee(\phi) \otimes f'^\vee(\phi')). \end{aligned}$$

This adjunction formula shows that

$$f \otimes f' : M \otimes M' \rightarrow N \otimes N'$$

passes to the quotient by the kernel of the duality Φ_n , yielding a linear map

$$f\overline{\otimes}f' : M\overline{\otimes}M' \rightarrow N\overline{\otimes}N'.$$

□

We can now state the following definition.

DEFINITION 4.4. *We will denote by \mathcal{W}_n the symmetric monoidal category of $\mathbf{W}_n(k)$ -modules, with monoidal structure given by the Tense Product. It is equipped with the perfect duality $M \mapsto M^\vee$, induced by Pontryagin duality.*

As one may guess, reducing mod p^n yields a (lax monoidal) functor from \mathcal{W}_{n+1} to \mathcal{W}_n .

LEMMA 4.5. *Let M and N be $\mathbf{W}_{n+1}(k)$ -modules. Then the natural map*

$$(M/p^n) \otimes_{\mathbf{W}_n(k)} (N/p^n) \rightarrow (M \otimes_{\mathbf{W}_{n+1}(k)} N)/p^n$$

induces by passing to the quotient a $\mathbf{W}_n(k)$ -linear map

$$(M/p^n)\overline{\otimes}_n(N/p^n) \rightarrow (M\overline{\otimes}_{n+1}N)/p^n.$$

Proof. To check this, one may assume that $M = \mathbf{W}_a(k)$ and $N = \mathbf{W}_b(k)$ are of rank one, and use Remark 4.2.

□

DEFINITION 4.6. *The functor*

$$\begin{aligned} \mathcal{W}_{n+1} &\rightarrow \mathcal{W}_n \\ M &\rightarrow M/p^n \end{aligned}$$

will be denoted by Θ . Thanks to the previous Lemma, it is a lax monoidal functor.

DEFINITION 4.7. (*Tense Algebra, Tense Symmetric Powers, Tense Exterior Powers.*)

Let M be a $\mathbf{W}_n(k)$ -module. For every nonnegative integer i , we put

$$M^{\overline{\otimes}_n^i} := \underbrace{M \overline{\otimes}_n M \overline{\otimes}_n \dots \overline{\otimes}_n M}_{i \text{ times}}.$$

We set

$$\overline{T}_n(M) := \bigoplus_{i=0}^{\infty} M^{\overline{\otimes}_n^i};$$

it is naturally a $\mathbf{W}_n(k)$ -algebra, the Tense Algebra of M . We define

$$\overline{\text{Sym}}_n(M) := \bigoplus_{i=0}^{\infty} \overline{\text{Sym}}_n^i(M)$$

to be the largest commutative quotient of $\overline{T}_n(M)$. As usual, it is obtained by modding out the ideal spanned by the elements

$$x \otimes y - y \otimes x,$$

for $x, y \in M$. It is the Tense Symmetric Algebra of M . Similarly, we define

$$\overline{\Lambda}_n(M) := \bigoplus_{i=0}^{\infty} \overline{\Lambda}_n^i(M)$$

to be the quotient of $\overline{T}_n(M)$ obtained by modding out the ideal spanned by the elements

$$x \otimes x,$$

for $x \in M$. It is the Tense Exterior Algebra of M .

DEFINITION 4.8. A tense algebra is an algebra in the category \mathcal{W}_n . In other words, it is a $\mathbf{W}_n(k)$ -algebra, such that the multiplication map

$$\mu : A \otimes_{\mathbf{W}_n(k)} A \longrightarrow A$$

factors through the natural quotient map

$$A \otimes_{\mathbf{W}_n(k)} A \longrightarrow A \overline{\otimes}_n A.$$

Example 4.9. The tense symmetric (resp. exterior) algebra of an arbitrary $\mathbf{W}_n(k)$ -module is of course a tense algebra.

If A is a usual $\mathbf{W}_n(k)$ -algebra which is flat (=free) as a $\mathbf{W}_n(k)$ -module, it is automatically tense.

Exercise 4.10. Let $A \in \mathcal{W}_n$ be a tense $\mathbf{W}_n(k)$ -algebra. Show that the unit $1 \in A$ has (additive) order p^n . In other words, it spans a free direct summand of rank one of A , as a $\mathbf{W}_n(k)$ -module.

DEFINITION 4.11. Let M be a (finite) $\mathbf{W}_n(k)$ -module. Consider the largest number

$$i \in \{-n, -n+1, \dots, -1, 0\}$$

such that M/p^{n+i} is a free $\mathbf{W}_{n+i}(k)$ -module.

We put

$$v_n(M) = i.$$

It is the valuation of M .

Remark 4.12. The $\mathbf{W}_n(k)$ -module M has valuation 0 if and only if it is free. In case it is not, its valuation is strictly negative, and can be thought of as the highest 'pole' of M .

LEMMA 4.13. *Let M and N be (finite) $\mathbf{W}_n(k)$ -modules. Then we have*

$$v_n(M \overline{\otimes}_n N) = v_n(M) + v_n(N),$$

and

$$v_n(M \oplus N) = \min(v_n(M), v_n(N))$$

with the convention that all integers $\leq -n$ are identified to $-n$.

Proof. Straightforward. \square

LEMMA 4.14. *Let M be a (finite) $\mathbf{W}_n(k)$ -module. Then $v_n(M)$ is the largest negative number i , such that the composite*

$$M \otimes_{\mathbf{W}_n(k)} (M^\vee) \xrightarrow{\text{ev}} \mathbf{W}_n(k) \longrightarrow \mathbf{W}_{n+i}$$

passes to the quotient by $\text{Ker}(\Phi_{n,M,M^\vee})$.

Proof.

Assume first that $M = \mathbf{W}_a(k)$, where a is an integer, with $1 \leq a \leq n$. Then the evaluation arrow under consideration is

$$\begin{aligned} \mathbf{W}_a(k) &\longrightarrow \mathbf{W}_n(k), \\ 1 &\mapsto p^{n-a}. \end{aligned}$$

On the other hand, $\text{Ker}(\Phi_{n,M,M^\vee})$ is generated by p^{2a-n} , or is everything if $a \leq \frac{n}{2}$. We then see that the composite under consideration factors through $\text{Ker}(\Phi_{n,M,M^\vee})$ if, and only if,

$$p^{2a-n+n-a} = p^a = 0 \in \mathbf{W}_{n+i}(k),$$

meaning that $i \leq a - n = v_n(M)$. The general case follows. \square

DEFINITION 4.15. *Let M be a (finite) $\mathbf{W}_n(k)$ -module. By the preceding Lemma, the composite*

$$M \otimes_{\mathbf{W}_n(k)} M^\vee \xrightarrow{\text{ev}} \mathbf{W}_n(k) \longrightarrow \mathbf{W}_{n+v_n(M)}(k)$$

induces an arrow

$$M \overline{\otimes}_n M^\vee \longrightarrow \mathbf{W}_{n+v_n(M)}(k),$$

which we denote by tr_M . It is the trace of M .

We conclude this section by defining the Chern character of a finite $\mathbf{W}_n(k)$ -module, and stating a first property.

DEFINITION 4.16. *Let M be a finite $\mathbf{W}_n(k)$ -module. We put*

$$\text{Ch}_n(M) := a_n + a_{n-1}X^{-1} + a_{n-2}X^{-2} + \dots + a_1X^{-n+1} \in \mathbb{Z}[X^{-1}].$$

LEMMA 4.17. *Let M and N be two finite $\mathbf{W}_n(k)$ -modules. Then*

$$v_n(M) = v_X(\text{Ch}_n(M)).$$

Modulo $X^{-n}\mathbb{Z}[X^{-n}]$, we have

$$\text{Ch}_n(M \overline{\otimes}_n N) = \text{Ch}_n(M)\text{Ch}_n(N).$$

Proof.

Follows from Remark 4.2. \square

Remark 4.18. We believe it could be interesting, in the future, to investigate the behaviour of the Chern character of Omega powers of k -vector spaces (see section 8.7). For instance, if V is a finite-dimensional k -vector space, what can we say about the map

$$n \in \mathbb{N} \mapsto Ch_{n+1}(\Omega^n(V))?$$

We should, of course, also extend these considerations to modules over global rings.

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

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

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

Remark 5.2. As it is well-known, the symbol $[x]_n$ plays the rôle of $\frac{1}{n!}x^n$. More precisely, if $n!$ is invertible in A (which typically happens if A has prime characteristic p and $n = p - 1$), the natural map

$$\begin{aligned} \text{Sym}_A^n(M) &\longrightarrow \Gamma_A^n(M), \\ x_1 \otimes \dots \otimes x_n &\mapsto [x_1]_1 \dots [x_n]_1 \end{aligned}$$

is an isomorphism, with inverse given by

$$\begin{aligned} \Gamma_A^n(M) &\longrightarrow \text{Sym}_A^n(M), \\ [x]_n &\mapsto \frac{1}{n!}x^n. \end{aligned}$$

At this point, the reader may wonder whether the last formula makes any sense. Why does it yield a well-defined A -linear map? This will become apparent in a moment, using the viewpoint of polynomial laws.

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

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

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.

For each positive integer i , the ideal $\Gamma^+(M)$ is moreover equipped with an operator

$$\begin{aligned}\gamma_i : \Gamma^+(M) &\longrightarrow \Gamma^+(M), \\ x &\mapsto \gamma_i(x),\end{aligned}$$

playing the role of $x \mapsto x^i/i!$, which endows $(\Gamma(M), \Gamma(M)^+)$ with the structure of an A -algebra with divided powers. Let us be more precise.

PROPOSITION 5.4. *Let M be an A -module. For each positive integer $i \geq 0$, the polynomial law*

$$\begin{aligned}M &\longrightarrow \Gamma^+(M), \\ x &\mapsto [x]_i,\end{aligned}$$

uniquely extends to a polynomial law

$$\gamma_i : \Gamma^+(M) \longrightarrow \Gamma^+(M),$$

which is homogeneous of degree i , such that the following conditions hold.

- 1) *The γ^i 's are functorial in A and M .*
- 2) *We have $\gamma_1 = \text{Id}$.*
- 3) *We have*

$$\gamma_i(x + y) = \sum_{a+b=i} \gamma_a(x)\gamma_b(y),$$

identically.

- 4) *We have*

$$\gamma_j \circ \gamma_i = \frac{(ij)!}{j!(i!)^j} \gamma_{ij}.$$

Moreover, the four properties above uniquely determine the γ^i 's.

PROPOSITION 5.5. *Let M, N be A -modules. We have a canonical isomorphism*

$$\Gamma^n(M \oplus N) \simeq \bigoplus_{i=0}^n (\Gamma^i(M) \otimes_A \Gamma^{n-i}(N)).$$

Remark 5.6. The previous Proposition says that divided power functors are strictly polynomial, in the sense of [FFSS].

PROPOSITION 5.7. *Let M be an A -module, and let B 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 5.8. *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 5.9. *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 5.10. 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 5.11. 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 5.12. Let M be an A -module. Let i, j be positive integers. The divided power operation

$$\gamma_i : \Gamma_A^j(M) \longrightarrow \Gamma_A^{ij}(M)$$

is a polynomial law, which is homogeneous, of degree i . It will often be considered as such in the sequel.

Remark 5.13. If V and W are locally free A -modules of finite rank, then a polynomial law from V to W is nothing but a morphism of affine A -schemes

$$\mathbb{A}_A(V) \longrightarrow \mathbb{A}_A(W).$$

The next Proposition is crucial. Its content is that the functor Γ represents the functor of polynomial laws.

PROPOSITION 5.14. *Let M, N be A -modules. Then $\text{Hom}_A(\Gamma^n(M), N)$ is canonically isomorphic to the group of polynomial laws from M to N , which are homogeneous of degree n .*

The previous Proposition admits an obvious generalization, as follows.

PROPOSITION 5.15. *Let M_1, M_2, \dots, M_r and N be A -modules. Let n_1, \dots, n_r be positive integers. Then*

$$\text{Hom}_A(\Gamma^{n_1}(M_1) \otimes_A \Gamma^{n_2}(M_2) \otimes_A \dots \otimes_A \Gamma^{n_r}(M_r), N)$$

is canonically isomorphic to the (A -module of) polynomial laws

$$\underline{M}_1 \times \underline{M}_2 \times \dots \times \underline{M}_r \longrightarrow \underline{N},$$

which are homogeneous of degree n_i in M_i (for $i = 1 \dots r$).

For M an A -module, the association

$$\begin{aligned} M &\longrightarrow (M^{\otimes n})^{\mathcal{S}_n}, \\ x &\mapsto x^{\otimes n}, \end{aligned}$$

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

$$F_n(M) : \Gamma_A^n(M) \longrightarrow (M^{\otimes n})^{\mathcal{S}_n}.$$

PROPOSITION 5.16. *If M is locally free of finite rank, the morphism $F_n(M)$ above is an isomorphism.*

Remark 5.17. If M is locally free of finite rank, the A -dual of $(M^{\otimes n})^{\mathcal{S}_n}$ is nothing but the symmetric power $\text{Sym}_A^n(M^*)$. Thus, the formation of divided powers, for finite locally free modules, is dual to that of symmetric powers.

5.2. DIVIDED POWERS AND DUALITY. Let us now mention a nice compatibility of divided powers, with respect to duality.

DEFINITION 5.18. *Let M be an A -module. Let $n \geq 1$ be an integer. The formula*

$$(v, \phi) \mapsto \phi(v)^n$$

defines a polynomial law (of A -modules)

$$\underline{M} \times \underline{M}^* \longrightarrow A,$$

which is bihomogeneous, of bidegree (n, n) . By Proposition 5.15, this law corresponds to a pairing

$$\Gamma_A^n(M) \times \Gamma_A^n(M^*) \longrightarrow A.$$

We will denote this pairing by Δ_n , or by Δ , or even by $\langle \cdot, \cdot \rangle$, if the context is clear enough. On the level of pure symbols, we have

$$\langle [\phi]_n, [v]_n \rangle = \phi(v)^n.$$

LEMMA 5.19. *Let M be an A -module. The following assertions are true.*

1) *For $x_1, \dots, x_r \in M$, $\phi \in M^*$ and i_1, \dots, i_r positive integers, we have*

$$\begin{aligned} \langle [x_1]_{i_1} \dots [x_r]_{i_r}, [\phi]_{i_1 + \dots + i_r} \rangle &= \binom{i_1 + \dots + i_r}{i_1, \dots, i_r} \phi(x_1)^{i_1} \dots \phi(x_r)^{i_r} \\ &= \binom{i_1 + \dots + i_r}{i_1, \dots, i_r} \langle [x_1]_{i_1}, [\phi]_{i_1} \rangle \dots \langle [x_r]_{i_r}, [\phi]_{i_r} \rangle. \end{aligned}$$

2) *Let m and n be positive integers. For $X \in \Gamma^n(M)$ and $\phi \in M^*$ the formula*

$$\langle \gamma_m(X), [\phi]_{mn} \rangle = \frac{(mn)!}{(n!)^m m!} \langle X, [\phi]_n \rangle^m \in A$$

holds (note that the integer coefficient appearing here is the number of partitions of a set of cardinality mn in m subsets of cardinality n).

Proof. We can assume that M is an A -module of finite type.

If $f : L \rightarrow M$ is a surjective linear map between A -modules, then the Lemma holds for M if it holds for L . Hence, we are reduced to the case where $M = A^n$ is free. Let $g : B \rightarrow A$ be a surjective homomorphism of commutative rings. Let N be a B -module, for which the Lemma holds (over the ring B , of course). Then the Lemma holds for $M = N \otimes_B A$ (use Proposition 5.7). Altogether, we can assume that M is a free module and that A is a domain of characteristic zero. But then, divided powers of M are free A -modules, and we can check everything after extending scalars to the fraction field F of A . We are thus reduced to the case where $A = F$ is an algebraically closed field of characteristic zero, in which case pure symbols additively span divided power modules. We can then identify $\Gamma_A^n(M)$ and $\text{Sym}_A^n(M)$, through the symmetrizing operator ($[x]_n$ corresponds to $\frac{x^n}{n!}$). Then the duality Δ is given by the usual (reassuring, but awkward) formula

$$\text{Sym}_A^n(M) \times \text{Sym}_A^n(M^*) \longrightarrow A,$$

$$(x_1 \otimes \dots \otimes x_n, \phi_1 \otimes \dots \otimes \phi_n) \mapsto n! \sum_{\sigma \in S_n} \phi_1(x_{\sigma(1)}) \dots \phi_n(x_{\sigma(n)}).$$

Checking point 1) is then straightforward.
For 2), write

$$X = \sum_i [x_i]_n.$$

We compute, using 1):

$$\begin{aligned} \langle \gamma_m(X), [\phi]_{mn} \rangle &= \langle \frac{X^m}{m!}, [\phi]_{mn} \rangle = \frac{1}{m!} \langle (\sum_i [x_i]_n)^m, [\phi]_{mn} \rangle \\ &= \frac{1}{m!} \langle \sum_{i_1, \dots, i_m} [x_{i_1}]_n \dots [x_{i_m}]_n, [\phi]_{mn} \rangle \\ &= \frac{1}{m!} \binom{mn}{n, n, \dots, n} \sum_{i_1, \dots, i_m} \phi(x_{i_1})^n \dots \phi(x_{i_m})^n \\ &= \frac{1}{m!} \binom{mn}{n, n, \dots, n} \sum_{i_1, \dots, i_m} \langle [x_{i_1}]_n, [\phi]_n \rangle \dots \langle [x_{i_m}]_n, [\phi]_n \rangle \\ &= \frac{1}{m!} \binom{mn}{n, n, \dots, n} (\langle [x_{i_1}]_n, [\phi]_n \rangle + \dots + \langle [x_{i_m}]_n, [\phi]_n \rangle)^m \\ &= \frac{(mn)!}{(n!)^m m!} \langle X, [\phi]_n \rangle^m \end{aligned}$$

(here we write sums over all integers i_1, \dots, i_m , repetitions allowed, to avoid multinomial coefficients). The proof is over. □

5.3. DIVIDED POWERS VERSUS SYMMETRIC POWERS. At this point, it seems legitimate to compare symmetric powers and divided powers more closely. Victory shall belong to the latter, and by far: they are much simpler, versatile and better behaved- for many reasons. We mention two of them.

1) Let V and W be two A -modules. On the one hand, $\text{Hom}_A(\text{Sym}_A^n(V), W)$ corresponds to symmetric n -multilinear forms

$$F : V^n \longrightarrow W.$$

Such a form is defined by an expression of the shape

$$(v_1, \dots, v_n) \mapsto F(v_1, \dots, v_n).$$

It is a function of the n variables v_1, \dots, v_n .

On the other hand, $\text{Hom}_A(\Gamma^n(V), W)$ corresponds to polynomial laws from V to W , which are homogeneous of degree n . Such a law is defined by an expression of the shape

$$v \mapsto F(v).$$

Being a natural transformation between the functors \underline{V} and \underline{W} , the expression $F(v)$ has to functorially make sense for any commutative A -algebra R , and every $v \in V \otimes_A R$. However, it depends on a -single- variable v . In that sense, it is much easier to define than a symmetric n -multilinear form.

2) Let m be positive integer. Symmetric powers (or tensor powers) of a module, which is of m -torsion, will remain of m -torsion, regardless to the ring of coefficients. This is far from being so for divided powers- a major fact which is at the heart of this paper. The underlying phenomena (in prime power torsion) will be

studied extensively, starting from the next section. For instance, we shall see that, if L is a free $(\mathbb{Z}/p^n\mathbb{Z})$ -module of rank one, then $\Gamma_{\mathbb{Z}}^{p^s}(L)$ is a free $(\mathbb{Z}/p^{n+s}\mathbb{Z})$ -module of rank one.

6. THE TEICHMÜLLER REPRESENTATIVE, AS A POLYNOMIAL LAW.

Among polynomial laws, there are fundamental ones, given by Teichmüller representatives in truncated Witt vectors. Let us be more precise. We begin with a standard but extremely important Lemma, at the heart of p -adic theory.

LEMMA 6.1. *Let A be a commutative ring.
The map*

$$\begin{aligned} A &\longrightarrow A/p^{n+m}A, \\ x &\mapsto x^{p^n}, \end{aligned}$$

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

$$\begin{aligned} \mathbb{Z}/p^m\mathbb{Z} &\longrightarrow \mathbb{Z}/p^{m+n}\mathbb{Z}, \\ x &\mapsto x^{p^n}. \end{aligned}$$

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. □

DEFINITION 6.2. *The polynomial law (of $\mathbb{Z}/p^{m+n}\mathbb{Z}$ -modules)*

$$\begin{aligned} \mathbb{Z}/p^m\mathbb{Z} &\longrightarrow \mathbb{Z}/p^{m+n}\mathbb{Z}, \\ x &\mapsto x^{p^n} \end{aligned}$$

will be denoted by $\bar{\tau}_n$.

Remark 6.3. Note that, for any $x \in k$, we have

$$\bar{\tau}_n(x) = \tau(x^{p^n}) \in \mathbf{W}_{n+1}(k),$$

where τ is the usual Teichmüller representative. Looking closely at this equality reveals the following.

In the theory of Witt vectors over perfect fields of characteristic p , the expression $\tau(x) \in \mathbf{W}_{n+1}(k)$ is well-defined because we can extract a (unique) p^n -th root of x in our base ring k . The expression $\bar{\tau}_n(x) \in A$, in contrast, makes sense for any base ring A of characteristic p^{n+m} , and any $x \in A/p^m$.

We need a simple arithmetic Lemma.

LEMMA 6.4. *Let a_1, \dots, a_r be r nonnegative integers. Put $n = a_1 + \dots + a_r$.
The following assertions are true.*

i) The number of carryovers in the base- p addition

$$n = (\dots (a_1 + a_2) + a_3) + \dots) + a_r$$

does not depend on the order of the a_i 's. It is equal to the p -adic valuation of the multinomial coefficient $\binom{n}{a_1, \dots, a_r}$.

ii) We have

$$v_p\left(\binom{pn}{pa_1, \dots, pa_r}\right) = v_p\left(\binom{n}{a_1, \dots, a_r}\right)$$

and

$$v_p\left(\binom{n}{a_1, \dots, a_r}\right) \geq \max_i \{v_p(n) - v_p(a_i)\}.$$

iii) In the particular case where $r = 2$ and $a_1 + a_2 = \iota p^m$, with $m \geq 0$ and $1 \leq \iota \leq p - 1$, the inequality in ii) is an equality. In other words, we have

$$v_p\left(\binom{\iota p^m}{a_1, a_2}\right) = m - v_p(a_1) = m - v_p(a_2).$$

Proof.

For i), we can reduce to the case $r = 2$ using the formula

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

The claim to prove is then a classical fact, which is also a nice elementary exercise left to the reader.

Assertion ii) is an easy consequence of i).

Let us now prove iii). The case $m = 0$ is obvious; we thus assume that $m \geq 1$. By ii), we then note that

$$v_p\left(\binom{\iota p^{m+1}}{pa_1, pa_2}\right) = v_p\left(\binom{\iota p^m}{a_1, a_2}\right),$$

allowing us to reduce to the case where a_1 and a_2 are prime-to- p . Write

$$a_i = b_i + c_i p^m$$

for $i = 1, 2$, with b_i prime-to- p , and $b_i \leq p^m - 1$. The number $b_1 + b_2$ is divisible by p^m , hence equals p^m . We thus have

$$1 + c_1 + c_2 = \iota \leq p - 1,$$

from which we infer that the number of carryovers in the base- p addition of a_1 and a_2 equals that of b_1 and b_2 , which is obviously m . The claim is proved. \square

Remark 6.5. The formula

$$v_p\left(\binom{pa_1 + \dots + pa_r}{pa_1, \dots, pa_r}\right) = v_p\left(\binom{a_1 + \dots + a_r}{a_1, \dots, a_r}\right)$$

suggests that the function

$$(a_1, \dots, a_r) \mapsto v_p\left(\binom{a_1 + \dots + a_r}{a_1, \dots, a_r}\right)$$

behaves like a height on the projective space \mathbb{P}^{r-1} , locally at p . This is perhaps worth investigating.

LEMMA 6.6. *Let V be an A -module, such that $p^m V = 0$, for some $m \geq 0$. Let n be a positive integer. Then $\Gamma_A^n(V)$ is of $p^{m+v_p(n)}$ -torsion.*

Proof. Note first the following two obvious facts.

i) Since V is annihilated by p^m , $\Gamma_A^n(V)$ is annihilated by p^{mn} . In particular, it is a \mathbb{Z}_p -module.

ii) Let

$$n = a_1 + \dots + a_r$$

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

$$[v_1]_{a_1} \dots [v_r]_{a_r} \in \Gamma_A^n(V)$$

is at most the minimum of the orders of the elements $[v_i]_{a_i} \in \Gamma_A^{a_i}(V)$.

We now show that

$$p^{m+v_p(n)}[v]_n = 0 \in \Gamma_A^n(V),$$

for each $v \in V$. Let

$$n = a_0 + a_1p + \dots + a_rp^r$$

be the base- p expansion of n . In the equality

$$[v]_{a_0}[v]_{a_1p} \dots [v]_{a_rp^r} = \binom{n}{a_0, a_1p, \dots, a_rp^r} [v]_n \in \Gamma_A^n(V),$$

the multinomial coefficient is prime-to- p , by Lemma 6.4. We can thus assume that $n = ip^r$, with $1 \leq i \leq p-1$. In the formula

$$[v]_{ip^r}^i = \binom{ip^r}{p^r, \dots, p^r} [v]_n,$$

the multinomial coefficient is prime-to- p , by Lemma 6.4 again. We thus reduce to the case $i = 1$, i.e. $n = p^r$.

We then see that

$$[v]_{p^{r-1}}^p = \binom{p^r}{p^{r-1}, \dots, p^{r-1}} [v]_n,$$

and that the multinomial coefficient occurring in this formula has p -valuation one. Induction on r yields the result, since $V = \Gamma_A^1(V)$ is of p^m -torsion by assumption.

□

6.1. DIVIDED POWERS OF TORSION $\mathbf{W}(k)$ -MODULES. From now on, k is a perfect field of characteristic p .

We will explain the first steps towards a canonical process for lifting torsion $\mathbf{W}(k)$ -modules to modules of higher torsion. To do so, we use divided powers, which are arguably the most efficient "elementary" algebraic tool at disposal.

Before beginning, let us mention here the work of Kaledin- notably in the recent papers [K1] and [K2]. His constructions are very close to what we produce here, though expressed in a different language. We did not have time to explore the connections so far and it would be interesting to do so in the future.

Recall that we denote by

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

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

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

is the unique multiplicative section of the quotient map

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

Let n, m be positive integers. Take A to be $\mathbf{W}_{n+m}(k)$, the truncated Witt vectors of size $n + m$. By Lemma 6.1, the formula

$$\begin{aligned} \bar{\tau}_n : A/p^m A &\longrightarrow A/p^{n+m} A = \mathbf{W}_{n+m}(k), \\ x &\mapsto x^{p^n}, \end{aligned}$$

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

$$\Gamma_{\mathbb{Z}}^{p^n}(\mathbf{W}_m(k)) \longrightarrow \mathbf{W}_{n+m}(k),$$

which we denote by T'_n . Since the Teichmüller representatives generate $\mathbf{W}_{n+m}(k)$ additively, the map T'_n is surjective. But obviously, the polynomial law $\bar{\tau}_n$ might as well be considered as a polynomial law over $\mathbf{W}(k)$, hence giving rise to a $\mathbf{W}(k)$ -linear homomorphism

$$T_n : \Gamma_{\mathbf{W}(k)}^{p^n}(\mathbf{W}_m(k)) \longrightarrow \mathbf{W}_{n+m}(k).$$

LEMMA 6.7. *The map T_n is an isomorphism.*

Proof. It is clearly surjective. But $\Gamma_{\mathbf{W}(k)}^{p^n}(\mathbf{W}_m(k))$ is generated by $[1]_{p^n}$, as a $\mathbf{W}(k)$ -module, and is killed by p^{n+m} , by Lemma 6.6. It is thus a $\mathbf{W}_{n+m}(k)$ -module, generated by one element. The claim follows. \square

Thus, the map T'_n factors as

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

One can then infer a description of the kernel of T'_n , which in turn provides a rather simple, seemingly new, natural recursive definition of $\mathbf{W}_m(k)$ by generators and relations. It does not involve any intricate computation- assuming, of course, some familiarity with the spirit of divided powers.

PROPOSITION 6.8. *Assume that $n = 1$ in what precedes. Then the kernel of the natural surjection*

$$T'_1 : \Gamma_{\mathbb{Z}}^p(\mathbf{W}_m(k)) \longrightarrow \mathbf{W}_{m+1}(k)$$

is generated, as an Abelian group, by elements of the form

$$[x]_1[y]_{p-1} - [xy^{p-1}]_1[1]_{p-1},$$

with $x, y \in \mathbf{W}_m(k)$.

Proof. We try to offer an algorithmic proof. The reader who is not familiar with divided powers is advised to assume $p = 2$, to begin with.

First of all, it is not hard to see that these elements are in the kernel, since, on 'impure' symbols, we have

$$T'_1([x]_1[y]_{p-1}) = p!X^iY^j \in \mathbf{W}_{m+1}(k),$$

for all $x, y \in \mathbf{W}_m(k)$, where $X, Y \in \mathbf{W}_{m+1}(k)$ are arbitrary lifts of x and y , respectively. Denote by $I \subset \Gamma_{\mathbb{Z}}^p(\mathbf{W}_m(k))$ the Abelian group spanned the elements

$$[x]_1[y]_{p-1} - [xy^{p-1}]_1[1]_{p-1}.$$

Pick an element $X \in \text{Ker}(T'_1)$. A little computation shows that, modulo I , every element of $\Gamma_{\mathbb{Z}}^p(\mathbf{W}_m(k))$ is congruent to an element of the shape

$$[a]_p + [b]_1[1]_{p-1},$$

with $a, b \in \mathbf{W}_m(k)$. We can thus assume that

$$X = [a]_p + [b]_1[1]_{p-1}.$$

Denote by $A \in \mathbf{W}_{m+1}(k)$ and $B \in \mathbf{W}_{m+1}(k)$ arbitrary lifts of A and B , respectively. The relation $T'_1(X) = 0$ translates as

$$A^p + p!B = 0 \in \mathbf{W}_{m+1}(k),$$

which implies that a is divisible by p , say $a = pa'$, for $a' \in \mathbf{W}_m(k)$. From the fact that, modulo I , we have

$$[a]_p = p^p[a']_p = \frac{p^{p-1}}{(p-1)!}[a']_1[a']_{p-1} \equiv \frac{p^{p-1}}{(p-1)!}[a'^p]_1[1]_{p-1} \in \Gamma_{\mathbb{Z}}^p(\mathbf{W}_m(k)),$$

we are thus reduced to case $a = 0$. But then $pB = 0 \in \mathbf{W}_{m+1}(k)$, implying $b = 0 \in \mathbf{W}_m(k)$. Hence, I indeed equals $\text{Ker}(T'_1)$. \square

From now on, if M is a torsion $\mathbf{W}(k)$ -module, we shall put

$$\Gamma^n(M) := \Gamma_{\mathbf{W}(k)}^n(M)$$

and

$$\text{Sym}^n(M) = \text{Sym}_{\mathbf{W}(k)}^n(M).$$

Note that these are polynomial functors, in the category of torsion $\mathbf{W}(k)$ -modules.

Remark 6.9. The preceding discussion shows that $\Gamma^{p^n}(\mathbf{W}_m(k))$, as a $\mathbf{W}(k)$ -module, is generated by $[1]_{p^n}$ and is canonically isomorphic to $\mathbf{W}_{m+n}(k)$. We are now going to make this statement (a bit) more precise.

Let n, m be positive integers.

Let L be a $\mathbf{W}_m(k)$ -module which is free of rank one. Seeing it as a $\mathbf{W}(k)$ -module, we put

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

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

$$\begin{aligned} \bar{\tau}_n : L &\longrightarrow \mathbf{W}_{n+m}(L), \\ v &\mapsto [v]_{p^n}. \end{aligned}$$

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

LEMMA 6.10. *Let $i = p^n j$ be a positive integer, with j prime to p . Then the formula*

$$\begin{aligned} L &\longrightarrow \mathbf{W}_{n+m}(L^{\otimes j}), \\ v &\mapsto [v^{\otimes j}]_{p^n}, \end{aligned}$$

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

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

is an isomorphism.

Proof. Only the fact that ϕ is an isomorphism has, perhaps, to be checked. We may assume that $L = \mathbf{W}_m(k)$. By lemma 6.6, the $\mathbf{W}(k)$ -module $\Gamma^n(\mathbf{W}_m(k))$, which is obviously generated by $[1]_n$, is of p^{m+n} -torsion, hence a $\mathbf{W}_{m+n}(k)$ -module generated by one element. The map ϕ is obviously surjective, with target a free $\mathbf{W}_{m+n}(k)$ -module. It is thus an isomorphism. \square

LEMMA 6.11. *Let n, m be positive integers. Let M be a $\mathbf{W}_m(k)$ -module. Pick an element x , of order p^m . Then the symbol*

$$[x]_n \in \Gamma^n(M)$$

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

Proof. By Lemma 6.6, the symbol in question has order $\leq p^{v_p(n)+m}$. Now, pick a $\mathbf{W}_m(k)$ -linear map

$$f : M \longrightarrow \mathbf{W}_m(k),$$

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

$$F : \Gamma^n(M) \longrightarrow \Gamma^n(\mathbf{W}_m(k)),$$

mapping $[v]_n$ to $[1]_n$. By Lemma 6.10, and by the fact that $1 \in \mathbf{W}_{m+n}(k)$ has order p^{m+n} , we know that $[1]_n$ has order $p^{v_p(n)+m}$. The claim follows. \square

LEMMA 6.12. *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. We can assume that V is finite-dimensional. 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

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

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. \square

LEMMA 6.13. *Let M be a torsion $\mathbf{W}(k)$ -module. Let n be a positive integer, lesser or equal to the cardinality of k . Then the symbols $[x]_n$, for $x \in M$, generate $\Gamma^n(M)$ (as a $\mathbf{W}(k)$ -module).*

Proof. We can assume that M is of finite type. Consider the filtration

$$\Gamma^n(M) \supset p\Gamma^n(M) \supset p^2\Gamma^n(M) \supset \dots \supset \{0\},$$

and note that the successive quotients are all quotients of $\Gamma^n(M)/p \simeq \Gamma_k^n(M/p)$. Apply induction, using Lemma 6.12, to get the result.

□

We conclude this section by a concrete description of divided power modules, using a basis. We first fix some useful notation.

DEFINITION 6.14. (*Weighted partitions.*) Let n be a positive integer. A partition of n is a decomposition

$$A : (a_1 + \dots + a_d = n)$$

of n into a sum of d nonnegative integers. The partition A is said to be weighted, if we are given the extra data of a d -tuple

$$w := (w_1, \dots, w_d)$$

of nonnegative integers, such that, for all $i = 1 \dots, d$, w_i is zero if a_i is zero. The (weighted) partition (A, w) is said to be proper if all a_i 's are $\leq n - 1$, or Dirac otherwise.

DEFINITION 6.15. Let M be a finite $\mathbf{W}_m(k)$ -module. Choose a decomposition

$$M = \bigoplus_{i=1}^d \mathbf{W}_{m-w_i}(k)e_i,$$

where $e_i \in M$ has order p^{m-w_i} (the w_i 's are $\leq m$, and uniquely determined by M). Put

$$w = (w_1, \dots, w_d).$$

Denote by

$$M^\vee = \bigoplus_{i=1}^d \mathbf{W}_{m-w_i}(k)e_i^\vee$$

the dual decomposition, with

$$\langle e_i, e_j^\vee \rangle = p^{w_i} \delta_{i,j}.$$

Let n be a positive integer. For each partition

$$A : (a_1 + \dots + a_d = n),$$

put

$$\tilde{W}(A, w) := \max\{v_p(n) - v_p(a_i) + w_i, i = 1 \dots d\}$$

and

$$[e]_A := [e_1]_{a_1} \dots [e_d]_{a_d} \in \Gamma^n(M).$$

PROPOSITION 6.16. Let M be a finite $\mathbf{W}_m(k)$ -module. Let $n \geq 0$ be an integer. We use the notation of Definition 6.15.

Then the order of $[e]_A$ in the $\mathbf{W}_{m+v_p(n)}(k)$ -module $\Gamma^n(M)$ is $p^{m+v_p(n)-\tilde{W}(A,w)}$, and there exists a natural isomorphism of $\mathbf{W}_{m+v_p(n)}(k)$ -modules

$$\bigoplus_A \mathbf{W}_{m+v_p(n)-\tilde{W}(A,w)}(k) \xrightarrow{\sim} \Gamma^n(M),$$

$$1_A \mapsto [e]_A,$$

where the sum is taken over all partitions A of n , of size d .

Proof. The first statement follows from Proposition 5.5 and Lemma 6.10, which implies that

$$\bigotimes_{i=1}^d \Gamma^{a_i}(\mathbf{W}_{m-w_i}(k))$$

is canonically isomorphic to $\mathbf{W}_{m+v_p(n)-\tilde{v}(A,w)}(k)$.

□

6.2. AN ALTERNATE DESCRIPTION OF Γ^p FOR VECTOR SPACES. 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

$$\begin{aligned} C : M \times M &\longrightarrow \mathrm{Sym}_{\mathbb{Z}}^p(M), \\ (x, y) &\mapsto \frac{(x+y)^p - x^p - y^p}{p}, \end{aligned}$$

is a symmetric 2-cocycle, for the trivial action of M on $\mathrm{Sym}_{\mathbb{Z}}^p(M)$. 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

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

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 $\mathrm{Sym}_k^p(V)$. We leave it to the reader, as an instructive exercise, to check that this extension is canonically isomorphic to $\Gamma^p(V)$.

7. 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

$$\begin{aligned} \mathrm{frob}_A : A &\longrightarrow A, \\ x &\mapsto x^p, \end{aligned}$$

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 frob_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

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

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

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

Note that the Frobenius law exists only for k -vector spaces. For $n \geq 2$, an arbitrary (say, finite free) $\mathbf{W}_n(k)$ -module does not come naturally equipped with such a law. The next proposition contains the definition of the Frobenius and of the Verschiebung, borrowed from the theory of commutative group schemes in characteristic p .

PROPOSITION 7.1. *Let V be a finite-dimensional k -vector space and let $n \geq 1$ be an integer.*

Then the formula

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

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

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

the Frobenius homomorphism (for divided powers).

The polynomial law

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

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

$$\begin{aligned} \text{Ver} : \Gamma^n(V^{(1)}) &\longrightarrow \Gamma^{np}(V), \\ [v^{(1)}]_n &\longrightarrow p[v]_{pn}, \end{aligned}$$

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, \dots, e_d of V . On the one hand, the Frobenius $V \longrightarrow V^{(1)}$ then becomes the law

$$\begin{aligned} k^d &\longrightarrow k^d, \\ (X_1, \dots, X_d) &\mapsto (X_1^p, \dots, X_d^p). \end{aligned}$$

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

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

then becomes the law

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

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 $p[e_1]_{a_1} \dots [e_d]_{a_d}$ 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. \square

LEMMA 7.2. *Let V be a k -vector space. Let a_1, \dots, a_d, n be nonnegative integers, satisfying $a_1 + \dots + a_d = np$. For $v_1, \dots, v_d \in V$, the Frobenius*

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

satisfies

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

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

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

Dually, the Verschiebung

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

satisfies

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

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

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

holds by definition. But

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

and

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

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

COROLLARY 7.3. *For any $s \geq 1$, the kernel of*

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

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

Proof. This follows from Proposition 6.16 and Lemma 7.2. \square

PROPOSITION 7.4. *Let V be a k -vector space. Let $n, s \geq 1$ be integers. Then the Frobenius*

$$\begin{aligned} \text{Frob}^s : \Gamma^{np^s}(V) &\longrightarrow \Gamma^n(V^{(s)}), \\ [v]_{np^s} &\longrightarrow [v^{(s)}]_n \end{aligned}$$

is surjective. We have an exact sequence

$$0 \longrightarrow \Gamma^{np^s}(V)[p^s] \longrightarrow \Gamma^{np^s}(V) \xrightarrow{\text{Frob}^s} \Gamma^n(V^{(s)}) \longrightarrow 0.$$

The Verschiebung

$$\begin{aligned} \text{Ver}^s : \Gamma^n(V^{(s)}) &\longrightarrow \Gamma^{np^s}(V), \\ [v^{(s)}]_n &\longrightarrow p^s[v]_{np^s}, \end{aligned}$$

is injective. We have an exact sequence

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

Proof. We may assume that V is finite-dimensional, with basis e_1, \dots, e_d . Let k'/k be an extension of perfect fields, with k' infinite. Since the formation of divided powers commutes to the (faithfully flat!) base-change $\mathbf{W}(k')/\mathbf{W}(k)$, we can assume that k is infinite. In this case, Lemma 6.13 ensures that pure symbols are additive generators of divided powers. The surjectivity of Frob^s then directly follows from the description given in Lemma 7.2. That its kernel is the p^s -torsion is the content of Corollary 7.3. By Lemma 7.2, 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 6.16, that Ver^s is injective. □

COROLLARY 7.5. *The Frobenius*

$$\text{Frob} : \Gamma(V) \longrightarrow \Gamma(V^{(1)})$$

is a surjective homomorphism of $\mathbf{W}(k)$ -algebras, with kernel $\Gamma^+(V)[p]$.

Proof. This is now obvious. □

8. DIVIDED POWERS AND PONTRYAGIN DUALITY.

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

$$\Gamma_k^p(V) \simeq (V^{\otimes p})^{S_p} \simeq \text{Sym}_k^p(V^*)^*.$$

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

$$\begin{aligned} \Gamma_k^p(V) &\longrightarrow \text{Sym}_k^p(V), \\ [v]_p &\mapsto v^p, \end{aligned}$$

is an isomorphism. It is of course far from being so in our context, where the perfect field k has characteristic p . In other terms, the functor Γ_k^p does not commute with duality of vector spaces. However, we will see that, for any $m \geq 1$, the functor $\Gamma^p = \Gamma_{\mathbf{W}_{m+1}(k)}^p$ does commute with duality for a free $\mathbf{W}_m(k)$ -module M , in the sense that $\Gamma^p(M^\vee)$ and $\Gamma^p(M)^\vee$ are canonically isomorphic, as $\mathbf{W}_{m+1}(k)$ -modules.

This phenomenon does unfortunately not extend to higher divided powers: the functors Γ^{p^n} , for $n \geq 2$, behave very badly with duality- except in dimension two. This is a rather subtle fact, linked to intricate computations of p -adic valuations of scary multinomial coefficients. To bypass this difficulty, we can choose to apply Γ^p n times in a row, instead of applying the functor Γ^{p^n} just once. In doing so, we lift the (p -adic valuation of the) torsion of the modules by one at each step. In some sense, this choice is justified by the basic computational fact that, for an ideal in a \mathbb{Z}_p -algebra, a divided power structure is uniquely determined by the operation γ_p . Note that, for non free $\mathbf{W}_m(k)$ -modules, we will have to take a *quotient* of the functor Γ^p anyway, in order to respect duality.

In what follows, we explore these two points of view: applying Γ^{p^n} , or applying Γ^p n times in a row. Forming their 'correct' quotients (which commutes to Pontryagin duality) will give rise to medium and big Omega powers, respectively. Medium Omega powers will turn out to be a *direct factor* of big Omega powers.

From now on, m fixed positive integer. The Pontryagin dual of a $\mathbf{W}_m(k)$ -module M shall be viewed as

$$M^\vee = \text{Hom}_{\mathbf{W}_m(k)}(M, \mathbf{W}_m(k)).$$

Let M be a $\mathbf{W}_m(k)$ -module. Then the duality law

$$\Delta : \overline{M} \times \overline{M}^\vee \longrightarrow \mathbf{W}_m(k)$$

of Definition 5.18 canonically factors through the projection

$$\pi : \mathbf{W}_{m+1}(k) \longrightarrow \mathbf{W}_m(k).$$

Explicitly, the pairing

$$\begin{aligned} \tilde{\Delta}_p : \overline{M} \times \overline{M}^\vee &\longrightarrow \mathbf{W}_{m+1}(k) \\ (m, \phi) &\mapsto \overline{\tau}_1(\phi(m)) \end{aligned}$$

is a polynomial law, bihomogeneous of bidegree (p, p) , satisfying

$$\Delta_p = \pi \circ \tilde{\Delta}_p.$$

It strongly depends on m . The integer m being fixed in this section, we shall abusively write Δ , or even $\langle \cdot, \cdot \rangle$ for $\tilde{\Delta}_p$. By the universal property of divided powers, it corresponds to a pairing of $\mathbf{W}_{m+1}(k)$ -modules

$$\Gamma_{\mathbf{W}_{m+1}(k)}^p(M) \times \Gamma_{\mathbf{W}_{m+1}(k)}^p(M^\vee) \longrightarrow \mathbf{W}_{m+1}(k),$$

given, on the level of pure symbols, by the formula

$$\langle [\phi]_p, [v]_p \rangle = \overline{\tau}_1(\phi(v)) \in \mathbf{W}_{m+1}(k).$$

Similarly, for any nonnegative integer $n \geq 2$, we get a pairing of $\mathbf{W}_{m+n}(k)$ -modules

$$\begin{aligned} \Gamma_{\mathbf{W}_{m+n}(k)}^{p^n}(M) \times \Gamma_{\mathbf{W}_{m+n}(k)}^{p^n}(M^\vee) &\longrightarrow \mathbf{W}_{m+n}(k), \\ \langle [\phi]_{p^n}, [v]_{p^n} \rangle &= \overline{\tau}_n(\phi(v)) \in \mathbf{W}_{m+n}(k). \end{aligned}$$

We shall denote this pairing by $\tilde{\Delta}_{p^n}$, or again simply by Δ if the context is clear.

LEMMA 8.1. *Let n be a nonnegative integer.*

Let M be a finite $\mathbf{W}_m(k)$ -module. Using the notation of Definition 6.15, we have a commutative diagram

$$\begin{array}{ccc} \Gamma^{p^n}(M) \times \Gamma^{p^n}(M^\vee) & \xrightarrow{\langle \dots \rangle} & \mathbf{W}_{m+n}(k) \\ \downarrow \wr & & \parallel \\ (\bigoplus_A \mathbf{W}_{N(A)}(k)[e]_A) \times (\bigoplus_B \mathbf{W}_{N(B)}(k)[e^\vee]_B) & \longrightarrow & \mathbf{W}_{m+n}(k), \end{array}$$

where the vertical map on the left is the product of the isomorphisms given by Lemma 6.16, and the lower horizontal map is the pairing given by

$$([e]_A, [e^\vee]_B) \mapsto p^{(\sum_1^d w_i a_i)} \binom{p^n}{a_1, a_2, \dots, a_d} \in \mathbf{W}_{m+n}(k),$$

if $A = B = (a_1, \dots, a_d)$, or by

$$([e]_A, [e^\vee]_B) \mapsto 0$$

if $A \neq B$.

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

$$\langle [X_1 e_1 + \dots + X_d e_d]_{p^n}, [Y_1 e_1^* + \dots + Y_d e_d^*]_{p^n} \rangle = (p^{w_1} X_1 Y_1 + \dots + p^{w_d} X_d Y_d)^{p^n}.$$

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

DEFINITION 8.2. *let d be a positive integer. Pick a weighted partition (A, w) of p^n , of size d . Put*

$$W((A, w)) := \min\{m + n, v_p\left(\binom{p^n}{A}\right) + \sum_1^d w_i a_i\}.$$

Remark 8.3. Note that

$$W((A, w)) \geq \tilde{W}((A, w)).$$

If $n = 1$, then equality holds if, and only if, either $w = 0$, or w_i is nonzero for a single index i , for which $a_i = 1$.

If $d = 2$ and $w = 0$, equality holds for any n . This holds because, in this case, $v_p\left(\binom{p^n}{a_1, a_2}\right)$ is precisely $n - v_p(a_1) = n - v_p(a_2)$.

In the context of Lemma 6.16, we know that the order of $[e]_A \in \Gamma^{p^n}(M)$ is $p^{m+n-\tilde{W}((A, w))}$. We will now show that the order of (the class of) $[e]_A$ in $\Gamma^{p^n}(M)/\text{Ker}(\Delta)$ is $p^{m+n-W((A, w))}$.

LEMMA 8.4. *Let M be a finite $\mathbf{W}_m(k)$ -module. Let n be a nonnegative integer. We use the notation of Definition 6.15.*

We have a canonical isomorphism

$$\begin{aligned} \Gamma^{p^n}(M)/\text{Ker}(\Delta) &\xrightarrow{\sim} \bigoplus_A \mathbf{W}_{m+n-W(A, w)}(k), \\ [e]_A &\mapsto 1_A, \end{aligned}$$

where the direct sum is taken over all partitions A of p^n , of size d .

It fits into a commutative diagram

$$\begin{array}{ccc} \Gamma^{p^n}(M) & \longrightarrow & \bigoplus_A \mathbf{W}_{m+n-\tilde{W}(A, w)}(k) \\ \downarrow & & \downarrow \\ \Gamma^{p^n}(M)/\text{Ker}(\Delta) & \longrightarrow & \bigoplus_A \mathbf{W}_{m+n-W(A, w)}(k) \end{array}$$

Proof. Obvious from Lemma 8.1. \square

It is natural to ask whether the pairing Δ is non-degenerate; in other words, to ask whether

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

is an isomorphism of $\mathbf{W}_{m+n}(k)$ -modules. We can now answer this question.

PROPOSITION 8.5. *Let M be a finite $\mathbf{W}_m(k)$ -module. The pairing*

$$\Delta : \Gamma^p(M) \times \Gamma^p(M^\vee) \longrightarrow \mathbf{W}_{m+1}(k)$$

is perfect if and only if M is a free $\mathbf{W}_m(k)$ -module.

If M is a free $\mathbf{W}_m(k)$ -module of rank at most two, then we have more: the pairing

$$\Delta : \Gamma^{p^n}(M) \times \Gamma^{p^n}(M^\vee) \longrightarrow \mathbf{W}_{m+n}(k)$$

is perfect, for any $n \geq 1$.

Proof. We use Lemma 8.4. In the first case, we have to see that $\tilde{W}(A, w) = W(A, w)$ for all A , if and only if $w = 0$. In the second case, we have to see that $\tilde{W}(A, 0) = W(A, 0)$ if $d = 2$. This is clear, at the light of Remark 8.3. \square

8.2. MEDIUM AND BIG OMEGA POWERS. We now present a construction of crucial importance in this paper: the so-called (big and medium) Omega powers. The choice of the name "Omega" is naturally inspired from topology: it is close to an algebraic loop space.

DEFINITION 8.6. *Let M be a $\mathbf{W}_m(k)$ -module. Let n be a nonnegative integer. We define a $\mathbf{W}_{m+n}(k)$ -module $\Gamma^{(n)}(M)$ by $\Gamma^{(0)}(M) = M$, and by the recursive formula*

$$\Gamma^{(n)}(M) := \Gamma^p(\Gamma^{(n-1)}(M)).$$

By Proposition 8.5, we now that $\Gamma^{(1)}$ commutes to Pontryagin duality, for free $\mathbf{W}_m(k)$ -modules only. Note that, if M is a free $\mathbf{W}_m(k)$ -module, $\Gamma^{(1)}(M)$ is a free $\mathbf{W}_{m+1}(k)$ -module if and only if M has rank one. The functor $\Gamma^{(2)}$ will thus never commute with duality, except for free modules of rank lesser than one. To define our Omega functor (medium and big), we are thus naturally led to mod out the kernel of Pontryagin duality.

DEFINITION 8.7. *(medium and big Omega functors.) Let M be a (non necessarily finite) $\mathbf{W}_m(k)$ -module. Let n be a positive integer. We put*

$$\Omega_m^n(M) := \Gamma_{\mathbf{W}_{m+n}(k)}^{p^n}(M) / \text{Ker}(\Delta).$$

It is the n -th medium Omega power of the $\mathbf{W}_m(k)$ -module M . It is a $\mathbf{W}_{m+n}(k)$ -module. We put $\overline{\Omega}_m^0(M) = \Omega_m^0(M) = M$.

We recursively define

$$\overline{\Omega}_m^n(M) := \Omega_{m+n-1}(\overline{\Omega}_m^{n-1}(M));$$

it is a $\mathbf{W}_{m+n}(k)$ -module as well. It is the n -th big Omega power of the $\mathbf{W}_m(k)$ -module M .

We shall denote $\Omega_m^n(M)$ (resp. $\overline{\Omega}_m^n(M)$) simply by $\Omega^n(M)$ (resp. $\overline{\Omega}^n(M)$), if the dependence in m is clear.

For $x \in M$, if this creates no confusion, we denote by

$$(x)_n \in \Omega^n(M)$$

the class of the pure symbol $[x]_{p^n} \in \Gamma_{\mathbf{W}_{m+n}(k)}^{p^n}(M)$.

Remark 8.8. We clearly have $\overline{\Omega}^1 = \Omega^1$. For $n \geq 2$, we will see in a moment that Ω^n appears canonically as a direct factor of $\overline{\Omega}^n$, in a duality-preserving way.

Remark 8.9. Let M be a $\mathbf{W}_m(k)$ -module. Let n be a nonnegative integer. We have a canonical surjection

$$\Gamma^{(n)}(M) \longrightarrow \overline{\Omega}^n(M).$$

Remark 8.10. If $M = \mathbf{W}_m(k)$ is a free $\mathbf{W}_m(k)$ -module of rank one, then $\overline{\Omega}^n(M) = \Omega^n(M) = \Gamma_{\mathbf{W}(k)}^{p^n}(M)$ is a free $\mathbf{W}_{m+n}(k)$ -module of rank one.

Remark 8.11. The associations

$$M \mapsto \overline{\Omega}^n(M)$$

and

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

are functors, from the category of $\mathbf{W}_m(k)$ -modules to that of $\mathbf{W}_{m+n}(k)$ -modules. For $n = 1$, they behave slightly like the p -th symmetric power functor Sym^p . However, this analogy is quite bad, as we have seen in Section 5.3.

The functor Ω^1 is polynomial, with respect to the Tense Product.

PROPOSITION 8.12. *Let M, N be $\mathbf{W}_m(k)$ -modules. Then, we have a canonical isomorphism of $\mathbf{W}_{m+1}(k)$ -modules*

$$\overline{\Omega}^1(M \oplus N) \simeq \overline{\Omega}^1(M) \oplus \overline{\Omega}^1(N) \oplus \bigoplus_{i,j} \left(\overline{\text{Sym}}_m^i(M) \overline{\otimes}_m \overline{\text{Sym}}_m^j(M) \right),$$

where the direct sum is taken over all proper partitions $i + j = p$.

Proof. By Proposition 6.16, we have a natural isomorphism

$$\Gamma^p(M \oplus N) \simeq \Gamma^p(M) \oplus \Gamma^p(N) \oplus \bigoplus_{i,j} \left(\Gamma^i(M) \otimes \Gamma^j(N) \right),$$

where the direct sum is taken over all proper partitions $i + j = p$. Let us write the dual decomposition

$$\Gamma^p(M^\vee \oplus N^\vee) \simeq \Gamma^p(M^\vee) \oplus \Gamma^p(N^\vee) \oplus \bigoplus_{i,j} \left(\Gamma^i(M^\vee) \otimes \Gamma^j(N^\vee) \right).$$

These are compatible with the duality pairing (with values in $\mathbf{W}_{m+1}(k)$). Notably, for $x \in M$, $y \in N$, $\phi \in M^\vee$ and $\psi \in N^\vee$, we have

$$\langle [x]_i \otimes [y]_j, [\phi]_i \otimes [\psi]_j \rangle = \binom{p}{i,j} \phi(x)^i \psi(y)^j \in \mathbf{W}_{m+1}(k).$$

Since i and j are $\leq p - 1$, the binomial coefficient in this formula has p -adic valuation one, and the claim follows. \square

8.3. MEDIUM OMEGA POWERS AS A DIRECT FACTOR OF BIG OMEGA POWERS. We now investigate the previously evoked link between medium and big Omega powers.

Let M be a $\mathbf{W}_m(k)$ -module. Recall that, for each nonnegative integer n , we have, at our disposal, the p -th divided power operation

$$\gamma_p : \Gamma^{p^n}(M) \longrightarrow \Gamma^{p^{n+1}}(M).$$

It is a polynomial law, homogeneous of degree p . It can thus be viewed as a $\mathbf{W}(k)$ -linear map

$$\begin{aligned} \Gamma^p(\Gamma^{p^n}(M)) &\longrightarrow \Gamma^{p^{n+1}}(M), \\ [X]_p &\mapsto \gamma_p(X), \end{aligned}$$

which we denote by $\tilde{\gamma}_p$. In the reverse direction, the association

$$\begin{aligned} M &\longrightarrow \Gamma^p(\Gamma^{p^n}(M)) \\ x &\mapsto [[x]_{p^n}]_p \end{aligned}$$

defines a polynomial law, homogeneous of degree p^{n+1} . It thus yields a natural $\mathbf{W}(k)$ -linear map

$$\begin{aligned}\Gamma^{p^{n+1}}(M) &\longrightarrow \Gamma^p(\Gamma^{p^n}(M)), \\ [x]_{p^{n+1}} &\longrightarrow [[x]_{p^n}]_p.\end{aligned}$$

We denote it by α_p .

DEFINITION 8.13. *Let M be a $\mathbf{W}_m(k)$ -module. Let n be a positive integer. We recursively define $\mathbf{W}(k)$ -linear maps*

$$F_n : \Gamma^{(n)}(M) \longrightarrow \Gamma^{p^n}(M)$$

and

$$G_n : \Gamma^{p^n}(M) \longrightarrow \Gamma^{(n)}(M)$$

by setting

$$\begin{aligned}F_1 &= G_1 = \text{Id}, \\ F_{n+1} &= \tilde{\gamma}_p \circ \Gamma^p(F_n)\end{aligned}$$

and

$$G_{n+1} = \Gamma^p(G_n) \circ \alpha_p.$$

DEFINITION 8.14. *We put $c_1 = 1$ and, for each integer $i \geq 2$, we put*

$$c_i = \frac{1}{p!} \binom{p^i}{p^{i-1}, p^{i-1}, \dots, p^{i-1}} \in \mathbb{N}.$$

It is an integer, which is a p -adic unit. For $n \geq 1$, we put

$$\mathcal{C}_n := c_n c_{n-1}^p \dots c_2^{p^{n-2}}.$$

It is an integer, which is a p -adic unit.

LEMMA 8.15. *We have*

$$F_n \circ G_n = \mathcal{C}_n \text{Id}.$$

Proof. The case $n = 1$ is obvious. The general case is by induction on n , using the relation

$$\gamma_p \circ \gamma_{p^n} = c_{n+1} \gamma_{p^{n+1}}$$

(cf. Proposition 5.4). □

Hence, F_n and G_n present $\Gamma^{p^n}(M)$ as a direct factor of $\Gamma^{(n)}(M)$, which is probably well-known. What is perhaps less standard, is that F_n and G_n are adjoint, for Pontryagin duality.

LEMMA 8.16. *Let M be a $\mathbf{W}_m(k)$ -module. Let n be a positive integer. For every $X \in \Gamma^{p^n}(M)$ and every $\Phi \in \Gamma^{(n)}(M^\vee)$, we have the formula*

$$\langle X, F_n(\Phi) \rangle = \mathcal{C}_n \langle G_n(X), \Phi \rangle \in \mathbf{W}_{m+n}(k).$$

Proof. Induction on n . The case $n = 1$ is obvious. For the induction step, pick $x \in M$ and $\Phi \in \Gamma^{(n)}(M^\vee)$. We compute:

$$\begin{aligned}\langle [x]_{p^{n+1}}, F_{n+1}([\Phi]_p) \rangle &= \langle [x]_{p^{n+1}}, \tilde{\gamma}_p(\Gamma^p(F_n)([\Phi]_p)) \rangle \\ &= \langle [x]_{p^{n+1}}, \gamma_p(F_n(\Phi)) \rangle = c_{n+1} \bar{\tau}_1(\langle [x]_{p^n}, F_n(\Phi) \rangle),\end{aligned}$$

where the last equality follows from point 2) of Lemma 5.19. On the other hand, we have

$$\langle G_{n+1}([x]_{p^{n+1}}), [\Phi]_p \rangle = \langle \Gamma^p(G_n)([[x]_{p^n}]_p), [\Phi]_p \rangle$$

$$= \langle [G_n([x]_{p^n})]_p, [\Phi]_p \rangle = \bar{\tau}_1(\langle G_n([x]_{p^n}), \Phi \rangle).$$

Comparing the two expressions yields the result (plugging in the formula at the previous step).

□

PROPOSITION 8.17. *Let M be a $\mathbf{W}_m(k)$ -module. The linear map G_n induces, by passing to the quotient, a canonical linear map*

$$\Psi_M^n : \Omega^n(M) \longrightarrow \bar{\Omega}^n(M),$$

compatible with the dualities on both sides. More precisely, we have

$$\langle \Psi_M^n(X), \Psi_{M^\vee}^n(\Phi) \rangle = \langle X, \Phi \rangle,$$

for all $X \in \Omega^n(M)$ and all $\Phi \in \Omega^n(M^\vee)$.

In particular, we have a canonical decomposition

$$\bar{\Omega}^n(M) = \Omega^n(M) \bigoplus \Omega^n(M^\vee)^\perp.$$

Proof. The existence of Ψ_M^n is a straightforward consequence of the adjunction formula of Lemma 8.17. The second formula is easily checked on pure symbols. The last assertion is a general fact. □

9. FUNCTORIAL PROPERTIES OF OMEGA POWERS.

Let m be a fixed positive integer.

9.1. MULTILINEARITY. Let M and N and L be three $\mathbf{W}_m(k)$ -modules. Let

$$B(., .) : M \times N \longrightarrow L$$

be a $\mathbf{W}_m(k)$ -bilinear pairing. Let n be a positive integer.

The pairing B induces a pairing

$$\begin{aligned} B_1 : L^\vee \times M &\longrightarrow N^\vee, \\ (\phi, x) &\mapsto \phi(B(x, .)), \end{aligned}$$

which gives rise to a $\mathbf{W}_{m+n}(k)$ -bilinear pairing

$$\begin{aligned} \Gamma^{p^n}(B_1) : \Gamma^{p^n}(L^\vee) \times \Gamma^{p^n}(M) &\longrightarrow \Gamma^{p^n}(N^\vee), \\ ([\phi]_{p^n}, [x]_{p^n}) &\mapsto [B_1(\phi, x)]_{p^n}. \end{aligned}$$

In a similar way, the pairing

$$\begin{aligned} B_2 : L^\vee \times N &\longrightarrow M^\vee, \\ (\phi, y) &\mapsto \phi(B(., y)), \end{aligned}$$

produces a $\mathbf{W}_{m+n}(k)$ -bilinear pairing

$$\begin{aligned} \Gamma^{p^n}(B_2) : \Gamma^{p^n}(L^\vee) \times \Gamma^{p^n}(N) &\longrightarrow \Gamma^{p^n}(M^\vee), \\ ([\phi]_{p^n}, [y]_{p^n}) &\mapsto [B_2(\phi, y)]_{p^n}. \end{aligned}$$

For $x \in M$, $y \in N$ and $\phi \in L^\vee$, it is straightforward to check that

$$\begin{aligned} \langle \Gamma^{p^n}(B_1)([\phi]_{p^n}, [x]_{p^n}), [y]_{p^n} \rangle &= \langle [B_1(\phi, x)]_{p^n}, [y]_{p^n} \rangle = \bar{\tau}_n(\phi(B(x, y))) \\ &= \langle [B(x, y)]_{p^n}, [\phi]_{p^n} \rangle = \langle \Gamma^{p^n}(B)([x]_{p^n}, [y]_{p^n}), [\phi]_{p^n} \rangle \\ &= \langle \Gamma^{p^n}(B_2)([\phi]_{p^n}, [y]_{p^n}), [x]_{p^n} \rangle. \end{aligned}$$

This shows that we actually have

$$\begin{aligned} \langle \Gamma^{p^n}(B_1)(\Phi, X), Y \rangle &= \langle \Gamma^{p^n}(B)(X, Y), \Phi \rangle \\ &= \langle \Gamma^{p^n}(B_2)(\Phi, Y), X \rangle \in \mathbf{W}_{m+n}(k), \end{aligned}$$

for all $X \in \Gamma^{p^n}(M)$, $Y \in \Gamma^{p^n}(N)$ and $\Phi \in \Gamma^{p^n}(L^\vee)$. Indeed, this can be checked after extending scalars from k to any perfect field extension of k (by Proposition 5.7, for the base change $\mathbf{W}(k')/\mathbf{W}(k)$). We can hence assume that k is infinite, in which case pure symbols generate divided power modules by Proposition 6.13. This adjunction formula show that the pairing $\Gamma^{p^n}(B)$ is compatible with the duality. Consequently, it passes to the quotient by its kernel, yielding a pairing of $\mathbf{W}_{m+n}(k)$ -modules

$$\Omega^n(B) : \Omega^n(M) \times \Omega^n(N) \longrightarrow \Omega^n(L).$$

Note that the association

$$B \longrightarrow \Omega^n(B)$$

does unfortunately not send "tense" pairings to tense pairings (in the sense of Section 4).

9.2. OMEGA POWERS OF $\mathbf{W}_m(k)$ -ALGEBRAS. Let m, n be positive integers.

Let A be a (not necessarily finite-dimensional) $\mathbf{W}_m(k)$ -algebra. We would like to canonically turn $\Omega^n(A)$ into a $\mathbf{W}_{m+n}(k)$ -algebra, with unit $(1)_n$, and multiplication given by

$$(x)_n(y)_n = (xy)_n$$

on pure symbols. This is indeed possible: denoting by $\mu : A \times A \longrightarrow A$ the multiplication of A (viewed as a $\mathbf{W}_m(k)$ -bilinear pairing), the bilinear map $\Omega^n(\mu)$ of the preceding paragraph does the job.

PROPOSITION 9.1. *Let A be a $\mathbf{W}_m(k)$ -algebra (in the usual sense), with multiplication $\mu : A \times A \longrightarrow A$. Then the $\mathbf{W}_{m+n}(k)$ -module $\Omega^n(A)$ can be canonically turned, via $\Omega^n(\mu)$, into a $\mathbf{W}_{m+n}(k)$ -algebra, with unit $(1)_n$, and multiplication given by*

$$(x)_n(y)_n = (xy)_n$$

on pure symbols.

Proof. This is clear. □

Remark 9.2. If A is a Hopf algebra over $\mathbf{W}_m(k)$, we can wonder whether $\Omega^n(A)$ is naturally a Hopf algebra over $\mathbf{W}_{m+n}(k)$. With our current definition of Ω^n , this is not the case.

To begin with, we treat the instructive case of an étale algebra. Remember that the category of étale k -algebras is equivalent to that of étale $\mathbf{W}_m(k)$ -algebras.

LEMMA 9.3. *Let E be an étale k -algebra, of degree d . Denote by l/k "the" Galois splitting field of E . Then the finite $\mathbf{W}_{n+m}(k)$ -algebra $\Omega^n(\mathbf{W}_m(E))$ is isomorphic to a finite product of local $\mathbf{W}_{n+m}(k)$ -algebras of the form $\mathbf{W}_{n_i}(k_i)$, where $1 \leq n_i \leq n+m$ is an integer, and $l/k_i/k$ is an intermediate field extension.*

Proof. We first make the following elementary observation. Let R be a finite local $\mathbf{W}_i(k)$ -algebra R , such that its maximal ideal is pR , and i minimal (i.e. $p^{i-1} \neq 0$ in R). Then R is canonically isomorphic to $\mathbf{W}_i(l)$, where $l = R/p$ is its residue field. Using Lemma 9.9, we then see that the statement of the Lemma is invariant under separable field extensions: we may thus assume that $k = \bar{k}$ is algebraically

closed. But then E is isomorphic to the trivial étale algebra k^d , and the statement is straightforward (choose the basis of primitive idempotents). \square

Now, the formula

$$\begin{aligned} \mathbf{W}_m(E) &\longrightarrow \mathbf{W}_{n+m}(E), \\ x &\mapsto \bar{\tau}_n(x) \end{aligned}$$

clearly defines a polynomial law of $\mathbf{W}_{n+m}(k)$ -modules, which is homogeneous, of degree p^n . Since it is multiplicative, the resulting $\mathbf{W}_{n+m}(k)$ -linear map

$$\rho = \rho_{E,n} : \Gamma_{\mathbf{W}_{n+m}(k)}^{p^n}(\mathbf{W}_m(E)) \longrightarrow \mathbf{W}_{n+m}(E)$$

is actually a ring homomorphism.

LEMMA 9.4. *The homomorphism ρ vanishes on $\text{Ker}(\Delta)$.*

Proof. Base-changing to an algebraic closure of k , we can assume that k itself is algebraically closed. Then, $E \simeq k^s$, and $\mathbf{W}_{n+m}(E) \simeq \mathbf{W}_{n+m}(k)^s$, as $\mathbf{W}(k)$ -algebras. The map ρ is then just given by functoriality from the s canonical projections $\pi_i : E \longrightarrow k$, and the claim becomes obvious. \square

DEFINITION 9.5. *The homomorphism $\rho_{E,n}$ above induces, by passing to the quotient, a homomorphism (of $\mathbf{W}_{n+m}(k)$ -algebras)*

$$\begin{aligned} \Omega^n(\mathbf{W}_m(E)) &\longrightarrow \mathbf{W}_{n+m}(E), \\ (x)_n &\mapsto \bar{\tau}_n(x) \end{aligned}$$

which we still denote by $\rho_{E,n}$, or simply by ρ .

Remark 9.6. In the previous definition, $\bar{\tau}_n(\tau(x))$ is nothing but $\tau(x^{p^n})$, where $\tau : E \longrightarrow \mathbf{W}(E)$ is the usual Teichmüller representative.

Remark 9.7. Note that $\mathbf{W}_{n+m}(E)$ is a free $\mathbf{W}_{n+m}(k)$ -module. Hence, by Lemma 9.3, the homomorphism ρ can be identified with the projection onto a direct factor of the $\mathbf{W}_{n+m}(k)$ -algebra $\Omega^n(\mathbf{W}_m(E))$. In other words, $\text{Spec}(\rho)$ is an open-closed immersion.

9.3. BEHAVIOUR OF OMEGA POWERS UNDER FIELD EXTENSIONS. Let k'/k be an extension of perfect fields of characteristic p .

Denote by τ (resp. τ') the Teichmüller representative for k (resp. k') and by K' the field of fractions of $\mathbf{W}(k')$. Pontryagin duality $\text{Hom}_{\mathbf{W}(k)}(\cdot, K/\mathbf{W}(k))$ (resp. $\text{Hom}_{\mathbf{W}(k')}(\cdot, K'/\mathbf{W}(k'))$) will be denoted by $(\cdot)^\vee$ (resp. $(\cdot)^{\vee'}$).

Omega powers of $\mathbf{W}_m(k)$ -modules (resp of $\mathbf{W}_m(k')$ -modules) will be denoted by Ω^n (resp. Ω'^n).

9.3.1. *Extension of scalars.* Let us first recall two properties of scalars extension, on the level of Witt vectors.

LEMMA 9.8. *Pontryagin duality commutes with scalars extension, from $\mathbf{W}(k)$ to $\mathbf{W}(k')$.*

More precisely, let M be a $\mathbf{W}(k)$ -module. Put $M' := M \otimes_{\mathbf{W}(k)} \mathbf{W}(k')$.

Then the canonical map

$$\begin{aligned} \text{Hom}_{\mathbf{W}(k)}(M, K/\mathbf{W}(k)) \otimes_{\mathbf{W}(k)} \mathbf{W}(k') &\longrightarrow \text{Hom}_{\mathbf{W}(k')} (M', K'/\mathbf{W}(k')), \\ f \otimes x &\mapsto (m \otimes y \mapsto xyf(m)), \end{aligned}$$

is an isomorphism.

Proof. This is clear. \square

Omega powers behave very nicely with respect to the extension k'/k .

LEMMA 9.9. *The formation of (medium and big) Omega powers commutes to extending scalars from k to k' . In other words, let M be a (finite) $\mathbf{W}_m(k)$ -module. Put*

$$M' := M \otimes_{\mathbf{W}_m(k)} \mathbf{W}_m(k').$$

We then have canonical isomorphisms of $\mathbf{W}_{m+n}(k)$ -modules

$$\Omega^n(M) \otimes_{\mathbf{W}_{m+n}(k)} \mathbf{W}_{m+n}(k') \simeq \Omega^n(M')$$

and

$$\overline{\Omega}^n(M) \otimes_{\mathbf{W}_{m+n}(k)} \mathbf{W}_{m+n}(k') \simeq \overline{\Omega}^n(M').$$

Proof. We know that the formation of divided powers commutes to extension of the base ring. Using Lemma 9.8, we see that the duality arrow

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

thus also commutes to extending scalars from k to k' , in the sense that $\Delta \otimes_{\mathbf{W}(k)} \mathbf{W}(k')$ is canonically isomorphic to Δ' . The claim follows. \square

9.3.2. *Restriction of scalars.* Assume now that k'/k is finite, of degree s .

Let M be a $\mathbf{W}_m(k')$ -module. We can also view it as a $\mathbf{W}_m(k)$ -module. Applying the process of Section 9.1 to the $\mathbf{W}_m(k)$ -bilinear pairing

$$\begin{aligned} \mathbf{W}_m(k') \times M' &\longrightarrow M' \\ (\lambda, v') &\mapsto \lambda v', \end{aligned}$$

we can endow $\Omega^n(M')$ with a canonical structure of a $\Omega^n(\mathbf{W}_m(k'))$ -module. On pure symbols, we have the formula

$$(\lambda)_n (v')_n = (\lambda v')'_n.$$

Now, recall the homomorphism

$$\rho : \Omega^n(\mathbf{W}_m(k')) \longrightarrow \mathbf{W}_{n+m}(k')$$

of Definition 9.5.

The natural quotient map

$$\begin{aligned} \pi : \Omega^n(M') &\longrightarrow \Omega^n(M'), \\ (v')_n &\mapsto (v')'_n \end{aligned}$$

is compatible with ρ : we have

$$\pi(a.x) = \rho(a)\pi(x),$$

for all $a \in \Omega^n(\mathbf{W}_m(k'))$ and all $x \in \Omega^n(M')$.

We thus have a canonical $\mathbf{W}_{n+m}(k')$ -linear map

$$\Psi : \Omega^n(M') \otimes_{\rho} \mathbf{W}_{n+m}(k') \longrightarrow \Omega^n(M').$$

PROPOSITION 9.10. *The map Ψ above is an isomorphism.*

Proof.

Extending scalars to an algebraic closure of k , we can replace k'/k by the trivial étale algebra k^s/k . The data of M is now the data of s $\mathbf{W}_m(k)$ -modules M_1, \dots, M_s , and both sides equal the direct sum of the s modules $\Omega^n(M_i)$. \square

10. FROBENIUS AND VERSCHIEBUNG, FOR OMEGA POWERS.

In the case $m = 1$, Omega powers naturally inherit Frobenius and Verschiebung maps, from divided powers. We now explain how.

Let V be a k -vector space. Let $n \geq 1$ be an integer. Note that the (surjective) linear maps

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

and

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

satisfy the formula

$$\begin{aligned} \langle \text{Frob}_{V^*}([\phi]_{p^{n+1}}), \text{Frob}_V([v]_{p^{n+1}}) \rangle &= \langle [\phi^{(1)}]_{p^n}, [v^{(1)}]_{p^n} \rangle \\ &= \bar{\tau}_n(\phi^{(1)}(v^{(1)})) = \bar{\tau}_n(\phi(v))^p = \langle [\phi]_{p^{n+1}}, [v]_{p^{n+1}} \rangle, \end{aligned}$$

modulo p^{n+m} . Hence, they respect the duality Δ , and the following definition makes sense.

DEFINITION 10.1. *The Frobenius map*

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

yields, by passing to the quotient, a $\mathbf{W}(k)$ -linear map

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

It is the Frobenius, for (medium) Omega powers. By perfect duality, the dual of the Frobenius for V^* is a $\mathbf{W}(k)$ -linear map

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

It is the Verschiebung, for (medium) Omega powers.

As one can expect, we can define Frobenius and Verschiebung for big Omega powers, in a way compatible with the natural embedding. Here is how.

Applying $\Gamma^{(n-1)}$ to the Frobenius map

$$\begin{aligned} \Gamma^{(1)}(V) &\longrightarrow V^{(1)}, \\ [v]_p &\mapsto v^{(1)}, \end{aligned}$$

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

$$\text{Frob}_V^{(n)} : \Gamma^{(n)}(V) \longrightarrow \Gamma^{(n-1)}(V^{(1)})$$

as Γ^p commutes to Frobenius twist.

Dually, we get a $\mathbf{W}(k)$ -linear map

$$\text{Frob}_{V^*}^{(n)} : \Gamma^{(n)}(V^*) \longrightarrow \Gamma^{(n-1)}(V^{*(1)}).$$

For $X \in \Gamma^{(n)}(V)$ and $\Phi \in \Gamma^{(n)}(V^*)$, we check by induction on n that

$$p \langle X, \Phi \rangle = \langle \text{Frob}_V^{(n)}(X), \text{Frob}_{V^*}^{(n)}(\Phi) \rangle \in \mathbf{W}_{n+1}(k).$$

Here the righthand side, a priori belonging to $\mathbf{W}_n(k)$, is viewed as an element of $\mathbf{W}_{n+1}(k)$ via the inclusion (Verschiebung)

$$\mathbf{W}_n(k) \xrightarrow{1 \mapsto p} \mathbf{W}_{n+1}(k).$$

We can also choose to write this equality as

$$\langle X, \Phi \rangle = \langle \text{Frob}_V^{(n)}(X), \text{Frob}_{V^*}^{(n)}(\Phi) \rangle \in \mathbf{W}_n(k),$$

where the lefthand side is taken modulo $p^n \dots$

Hence, $\text{Frob}^{(n)}$ yields by passing to the quotient a $\mathbf{W}(k)$ -linear map

$$\overline{\Omega}^n(V) \longrightarrow \overline{\Omega}^{n-1}(V^{(1)}).$$

DEFINITION 10.2. *The $\mathbf{W}_{n+1}(k)$ -linear map*

$$\overline{\Omega}^n(V) \longrightarrow \overline{\Omega}^{n-1}(V^{(1)})$$

that we have just defined is the Frobenius homomorphism, for big Omega powers. It will simply be denoted by Frob_V , or even by Frob , if the context is clear.

Using the duality between $\overline{\Omega}^n(V)$ and $\overline{\Omega}^n(V^)$, we define the Verschiebung homomorphism*

$$\text{Ver}_V : \overline{\Omega}^{n-1}(V^{(1)}) \longrightarrow \overline{\Omega}^n(V)$$

to be dual to Frob_V .

Remark 10.3. To be more precise, we can define the Verschiebung for big Omega powers for a finite-dimensional V first, and then define it for V arbitrary using a direct limit argument.

LEMMA 10.4. *The Frobenius and the Verschiebung for (medium or big) Omega powers are adjoint operators, satisfying*

$$\text{Ver} \circ \text{Frob} = p$$

and

$$\text{Frob} \circ \text{Ver} = p.$$

They are compatible with the natural inclusion $\Omega^n \subset \overline{\Omega}^n$.

Proof. We check the first part, for big Omega powers. That these operators are adjoint is clear from the definition of the Verschiebung. For $X \in \Gamma^{(n)}(V)$ and $\Phi \in \Gamma^{(n)}(V^*)$, the computation

$$\langle \text{Ver}(\text{Frob}(X)), \Phi \rangle = \langle \text{Frob}(X), \text{Frob}(\Phi) \rangle = p \langle X, \Phi \rangle \in \mathbf{W}_{n+1}(k)$$

ensures that $\text{Ver} \circ \text{Frob} = p$. Since Frob is surjective, the other equality follows. \square

PROPOSITION 10.5. *Let V be a k -vector space, and let n be a positive integer. We have exact sequences*

$$\overline{\mathcal{KW}}_1(V) = \overline{\mathcal{KW}}_1(V, n) : 0 \longrightarrow \overline{\Omega}^{n-1}(V^{(1)}) \xrightarrow{\text{Ver}} \overline{\Omega}^n(V) \longrightarrow \overline{\Omega}^n(V)/p \longrightarrow 0$$

and

$$\overline{\mathcal{KW}}_2(V) = \overline{\mathcal{KW}}_2(V, n) : 0 \longrightarrow \overline{\Omega}^{n-1}(V)[p] \longrightarrow \overline{\Omega}^n(V) \xrightarrow{\text{Frob}} \overline{\Omega}^{n-1}(V^{(1)}) \longrightarrow 0.$$

We shall refer to them as the first and second Kummer-Witt exact sequences for (big) Omega powers, respectively. They are dual constructions, in the sense that, if V is finite-dimensional, $\overline{\mathcal{KW}}_1(V^)$ is canonically isomorphic to $\overline{\mathcal{KW}}_2(V)^\vee$.*

We define $\mathcal{KW}_2(V, n)$ and $\mathcal{KW}_2(V, n)$, for medium Omega powers, in the same way.

Proof. Only the exactness of the sequences in question has perhaps to be checked. Note that $\overline{\mathcal{KW}}_1(V)$ is clearly exact on the right and in the middle. The injectivity of Ver follows by duality from the surjectivity of Frob . \square

11. THE TRANSFER.

In this section, k is a finite field, of cardinality $q = p^r$. The goal of this section is to define the Transfer, which is a polynomial law "in the wrong direction". More precisely, if $W \rightarrow V$ is an inclusion of k -vector spaces, of finite codimension c , we shall build a canonical polynomial law

$$T_{W,V} : \mathbb{A}_k(V) \rightarrow \mathbb{A}_k(W),$$

the Transfer, enjoying nice properties.

As always, the letter n denotes any positive integer. For every k -vector space V , we have a canonical k -linear isomorphism

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

which we shall tacitly use to identify these two k -vector spaces.

The r -th Frobenius *polynomial law*

$$\begin{aligned} V &\rightarrow V^{(r)} = V, \\ v &\mapsto v^{(r)} \end{aligned}$$

will be denoted by F_V , or simply by F if no confusion arises. It is homogeneous, of degree p^r .

DEFINITION 11.1. *Let V be a finite-dimensional k -vector space, of dimension d . We put*

$$\text{Det}^n(V) := \Omega^n(\text{Det}(V));$$

it is a free $\mathbf{W}_{n+1}(k)$ -module of rank one.

11.1. LAWS IN ONE VARIABLE.

DEFINITION 11.2. *Let V be a finite-dimensional k -vector space, of dimension d . Let*

$$S = \{s_0 < s_1 < \dots < s_{m-1}\} \subset \{0, \dots, d\}$$

be any subset, of cardinality m . The formula

$$\begin{aligned} \mathbb{A}_k(V) &\rightarrow \mathbb{A}_k(\Lambda^m(V)) \\ v &\mapsto F^{s_0}(v) \wedge F^{s_1}(v) \wedge \dots \wedge F^{s_{m-1}}(v) \end{aligned}$$

defines a polynomial law, which is homogenous, of degree

$$q^{s_0} + q^{s_1} + \dots + q^{s_{m-1}}.$$

It is the exterior power in one variable, with respect to V and S . We denote it by $\overline{\lambda}_V^S$, or simply by $\overline{\lambda}^S$, if the dependence in V is clear.

If $S = \{0, \dots, m-1\}$, we denote $\overline{\lambda}^S$ by $\overline{\lambda}^m$.

The law $\overline{\lambda}_V^d$ will be denoted by \det_V^1 . It is the determinant in one variable.

REMARK 11.3. The locus where the law $\overline{\lambda}^m$ vanishes is exactly the (finite) union of all linear subvarieties of $\mathbb{A}_k(V)$, which are of dimension strictly less than m .

The determinant in one variable \det_V^1 is, in fact, the product of all nonzero k -linear forms on V (up to scalar multiplication). Let us make this statement more precise. We thank Ofer Gabber for an interesting discussion, which helped us clarify the exposition.

DEFINITION 11.4. Let V be a finite-dimensional k -vector space, of dimension $d \geq 2$. For each k -rational hyperplane $H \subset V$, denote by

$$\pi_H : V \longrightarrow V/H$$

the k -linear projection. Put

$$\overline{\text{Det}}(V) := \bigotimes_{H \subset V} (V/H),$$

where the tensor product is taken over all hyperplanes $H \subset V$. It is a one-dimensional k -vector space.

Denote by $\overline{\det}^1$ the polynomial law

$$\begin{aligned} \mathbb{A}_k(V) &\longrightarrow \mathbb{A}_k(\overline{\text{Det}}V), \\ v &\mapsto \bigotimes_{H \subset V} (\pi_H(v)). \end{aligned}$$

It is homogeneous, of degree $1 + q + \dots + q^{d-1} = |\mathbb{P}_k(V)|$.

PROPOSITION 11.5. Let V be a finite-dimensional k -vector space, of dimension $d \geq 2$. There exists a canonical isomorphism

$$\theta : \overline{\text{Det}}(V) \longrightarrow \text{Det}(V)$$

of one-dimensional k -vector spaces, such that

$$\theta \circ \overline{\det}^1 = \det^1.$$

Proof. Choose coordinates $V \simeq k^d$. Then \det^1 is given by a polynomial

$$P \in k[X_1, \dots, X_d],$$

which is homogeneous, of degree $1 + q + \dots + q^{d-1} = |\mathbb{P}_k(V)|$. For each hyperplane $H \subset V$, let

$$L_H \in k[X_1, \dots, X_d]$$

be a linear polynomial, with kernel H .

Let $H \subset V$ be a k -rational hyperplane. It is clear that the composite

$$\mathbb{A}_k(H) \xrightarrow{\text{can}} \mathbb{A}_k(V) \xrightarrow{\overline{\det}^1} \mathbb{A}_k(\text{Det}(V))$$

identically vanishes (indeed, $\Lambda_k^d(H) = 0$). Thus, the polynomial P has to be divisible by L_H . Since these linear polynomials, for various H , are two by two coprime, P has to be divisible by their product

$$Q := \prod_{H \subset V} L_H,$$

which is a homogeneous polynomial of the same degree as P . Hence, $P = Q$ up to a nonzero scalar. The statement of the proposition is, obviously, the canonical translation of this fact. \square

Exercise 11.6. Let k'/k be a finite field extension, of degree n . Let V be a d -dimensional k -vector space. Show that \det_V^1 identically vanishes on k' -rational points if and only if $n < d$.

Exercise 11.7. Let V be a finite-dimensional k -vector space, of dimension d . For $i = 1 \dots d$, denote by

$$F_i : \mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(\text{Det}(V))$$

the polynomial law $\lambda_{\{0,1,\dots,\hat{i},\dots,d\}}^d$, where the symbol \hat{i} means that i is omitted. Then the morphism of affine k -varieties

$$F : \mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(\text{Det}(V))^d$$

$$v \mapsto (F_1(v), \dots, F_d(v))$$

is étale exactly outside the (finite) union of all k -rational hyperplanes of V .

11.2. THE TRANSFER, AS A POLYNOMIAL LAW. We now proceed one step further towards the definition of the Transfer. In the exterior algebra, it is easy to define such an operation, in a k -linear way. We apologize for the choice of the terminology "exterior transfer" in what follows- it is a bit pompous...

DEFINITION 11.8. *Let V be a finite-dimensional k -vector space, of dimension d . Let $W \subset V$ be a k -linear subspace, of codimension c . Consider the exact sequence*

$$0 \longrightarrow W \longrightarrow V \longrightarrow V/W \longrightarrow 0$$

and its k -dual sequence

$$0 \longrightarrow (V/W)^* = W^\perp \longrightarrow V^* \longrightarrow W^* \longrightarrow 0.$$

Pick an integer $m \geq c$. Then the wedge product

$$\begin{aligned} \Lambda^c(W^\perp) \otimes_k \Lambda^{m-c}(V^*) &\longrightarrow \Lambda^m(V^*), \\ (x, y) &\mapsto x \wedge y \end{aligned}$$

passes to the quotient by the arrow $V^* \longrightarrow W^*$, yielding an injective k -linear map

$$\text{Det}(W^\perp) \otimes_k \Lambda^{m-c}(W^*) \longrightarrow \Lambda^m(V^*).$$

Its k -dual is a surjective map

$$\Lambda^m(V) \longrightarrow \text{Det}(V/W) \otimes \Lambda^{m-c}(W),$$

which we denote by $\lambda T_{W,V}^m$.

It is the exterior transfer, from V to W .

Remark 11.9. The linear map $\lambda T_{W,V}^m$ is explicitly given by the formula

$$v_1 \wedge \dots \wedge v_m \mapsto \sum_{I=\{i_1 < \dots < i_c\}} \epsilon(I) (\pi(v_{i_1}) \wedge \dots \wedge \pi(v_{i_c})) \otimes (\rho(v_{j_1}) \wedge \dots \wedge \rho(v_{j_{m-c}})),$$

where $\pi : V \longrightarrow V/W$ is the quotient map, $\rho : V \longrightarrow W$ is any- k -linear retraction of the inclusion $W \longrightarrow V$, and the sum ranges over all subsets

$$I = \{i_1 < \dots < i_c\} \subset \{1, \dots, m\},$$

with complement $I^c = \{j_1 < \dots < j_{m-c}\}$.

The number $\epsilon(I) \in \{1, -1\}$ is a sign, which is not hard to compute.

LEMMA 11.10. *Let*

$$Z \subset W \subset V$$

be three finite-dimensional k -vector spaces. Denote by c (resp c') the codimension of W in V (resp. of Z in W). Let $m \geq c + c'$ be an integer. Through the canonical isomorphism

$$\text{Det}(V/Z) \simeq \text{Det}(V/W) \otimes_k \text{Det}(W/Z),$$

the exterior transfers satisfy the 'cocycle' condition

$$\lambda T_{Z,W}^{m-c} \circ \lambda T_{W,V}^m = \lambda T_{Z,V}^m,$$

as linear maps

$$\Lambda^m(V) \longrightarrow \text{Det}(V/Z) \otimes \Lambda^{m-c-c'}(Z).$$

Proof. Looking at the definition of the exterior transfer, the k -dual statement of this Lemma boils down to the associativity of the wedge product. \square

We can now define the Transfer, as a polynomial law.

PROPOSITION 11.11. *Let V be a (finite-dimensional) k -vector space. Let $W \subset V$ be a k -linear subspace, of codimension c . Denote by*

$$\pi : V \longrightarrow V/W$$

the projection .

Then, there exists a unique polynomial law

$$T_{W,V} : \mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(W),$$

such that

$$\lambda T_{W,V}^{c+1} \circ \bar{\lambda}_V^{c+1} = (\det^1_{V/W} \circ \pi) \otimes T_{W,V},$$

as polynomial laws

$$\mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(\Lambda_k^{c+1}(V)) \longrightarrow \mathbb{A}_k(\text{Det}(V/W) \otimes_k W).$$

It is homogeneous, of degree q^c .

Proof. Uniqueness is clear: we simply have to see that $(\det^1_{V/W} \circ \pi)$ divides $\lambda T_{W,V}^{c+1} \circ \bar{\lambda}_V^{c+1}$ (as polynomial laws). At the light of Proposition 11.5, it suffices to show that the law $\lambda T_{W,V}^{c+1} \circ \bar{\lambda}_V^{c+1}$ identically vanishes on all k -rational hyperplanes of V , which contain W . Let $H \subset V$ be such a hyperplane. Then the composite

$$\mathbb{A}_k(H) \longrightarrow \mathbb{A}_k(V) \xrightarrow{\bar{\lambda}_V^{c+1}} \mathbb{A}_k(\Lambda^{c+1}(V))$$

takes values in $\mathbb{A}_k(\Lambda^{c+1}(H))$. But $\lambda_{W,V}^{c+1}$ vanishes on $\mathbb{A}_k(\Lambda^{c+1}(H))$. To see this, first use Lemma 11.10 to reduce to the case $W = H$. It then becomes obvious, by definition of $\lambda_{W,V}^{c+1}$. \square

DEFINITION 11.12. *Let V be a (finite-dimensional) k -vector space. Let $W \subset V$ be a k -linear subspace, of codimension c . The polynomial law*

$$T_{W,V} : \mathbb{A}_k(V) \longrightarrow \mathbb{A}_k(W)$$

constructed in the previous Proposition is the Transfer, from V to W . It is homogeneous, of degree q^c .

Remark 11.13. Naively speaking, the $T_{W,V}$ can be interpreted as 'the extension by zero' of the inclusion $W \longrightarrow V$, to the whole V . Proposition 11.17 makes this statement precise.

LEMMA 11.14. *Let*

$$Z \subset W \subset V$$

be three finite-dimensional k -vector spaces. Then the Transfers satisfy the 'cocycle' condition

$$T_{Z,W} \circ T_{W,V} = T_{Z,V},$$

as polynomial laws

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

Proof. This is clear, from the definition of the Transfer, together with Lemma 11.10 and Proposition 11.5. \square

In codimension one, the Transfer is given by a very simple formula.

LEMMA 11.15. *Let $H \subset V$ be a hyperplane inclusion, with V a finite-dimensional k -vector space. Let $\pi : V \rightarrow k$ be a nonzero linear form with kernel H . Then the Transfer*

$$T_{H,V} : \mathbb{A}_k(V) \rightarrow \mathbb{A}_k(H)$$

is given by the formula

$$v \mapsto F(v) - \pi(v)^{q-1}v.$$

Proof. We identify V/H and k , through π .

The composite of the exterior power in one variable

$$\begin{aligned} \lambda^2 : \mathbb{A}_k(V) &\rightarrow \mathbb{A}_k(\Lambda_k^2(V)) \\ v &\mapsto v \wedge F(v) \end{aligned}$$

with the exterior transfer

$$\begin{aligned} \mathbb{A}_k(\Lambda_k^2(V)) &\rightarrow \mathbb{A}_k(H), \\ v \wedge w &\mapsto \pi(v)w - \pi(w)v \end{aligned}$$

is easily computed to be

$$v \mapsto \pi(v)F(v) - \pi(v)^q v.$$

Indeed, π is defined over k , hence commutes with $F = \text{Frob}^r$. By definition of the Transfer, dividing by $\pi(v)$ yields the result. \square

DEFINITION 11.16. *Let V be a (finite-dimensional) k -vector space, of dimension d . Let c be a positive integer, with $c \leq d - 1$. The law*

$$\begin{aligned} T^c = T_V^c : \mathbb{A}_k(V) &\rightarrow \mathbb{A}_k\left(\bigoplus_{W \subset V} W\right) \\ v &\mapsto (T_{W,V}(v))_{W \subset V}, \end{aligned}$$

where the direct sum is taken over all c -codimensional k -linear subspaces $W \subset V$, will be call the Total Transfer for V , in codimension c .

PROPOSITION 11.17. *Let V be a (finite-dimensional) k -vector space. Let $W \subset V$ be a k -linear subspace, of codimension $c \geq 1$.*

Then the composite

$$\mathbb{A}_k(W) \xrightarrow{\text{can}} \mathbb{A}_k(V) \xrightarrow{T_{W,V}} \mathbb{A}_k(W)$$

equals $F^c = \text{Frob}^{rc}$.

Proof. From Lemma 11.14, we can assume $c = 1$ by induction. The formula then clearly follows from the formula given in Lemma 11.15. \square

The next Proposition is much more remarkable.

PROPOSITION 11.18. *(Frobenius Integral Formula.)*

Let V be a finite-dimensional k -vector space, of dimension $d \geq 2$. Let c be an integer, with $1 \leq c \leq d - 1$.

Then the composite

$$\Phi := \mathbb{A}_k(V) \xrightarrow{T_V^c} \mathbb{A}_k\left(\bigoplus_W W\right) \rightarrow \mathbb{A}_k(V)$$

equals $F^c = \text{Frob}^{rc}$, where the second map is given by the (finite!) sum of the inclusions $W \rightarrow V$.

Proof. Induction on c . Let us first deal with the case $c = 1$. For a k -rational hyperplane $H \subset V$, the Transfer $T_{H,V}$ is a polynomial law of degree q . By the universal property of divided powers, together with Lemma 11.15, it is given by the k -linear map

$$\begin{aligned} \Gamma_k^q(V) &\longrightarrow H, \\ [v]_q &\mapsto F(v) - \pi_H(v)^{q-1}v. \end{aligned}$$

Pick a (k -rational) $v \in V$. Then $F(v) = v$, and $T_{H,V}(v)$ equals 0 if $v \notin H$ (in which case $\pi_H(v)^{q-1} = 1$), or equals v if $v \in H$ (in which case $\pi_H(v)^{q-1} = 0$). Since the number of hyperplanes H containing v is congruent to 1 modulo p , summing over all H shows that $\Phi(v) = v = F(v)$. Now, $F = \text{Frob}^r$ and Φ are both polynomial laws of the same degree q . Since we know, by Lemma 6.13, that k -rational symbols $[v]_q$ generate $\Gamma_k^q(V)$, we can indeed conclude that $\Phi = F$.

For the induction step, look at the composite

$$\mathbb{A}_k(V) \xrightarrow{T_V^1} \mathbb{A}_k\left(\bigoplus_{H \subset V} H\right) \xrightarrow{\sum T_{W,H}} \mathbb{A}_k\left(\bigoplus_{W \subset H \subset V} W\right) \longrightarrow \mathbb{A}_k\left(\bigoplus_{H \subset V} H\right) \longrightarrow \mathbb{A}_k(V),$$

where the direct sums are taken over all hyperplanes $H \subset V$, and all inclusions $W \subset H \subset V$ of a c -codimensional W into an hyperplane H , respectively (and where the last two arrows on the right are the canonical linear surjections).

On the one hand, using Lemma 11.14, together with the fact that the cardinality of a projective space over a finite field is congruent to 1 modulo p , we see that this composite equals Φ . On the other hand, the composite of the two middle arrows equal F^{c-1} by induction, so that, using the case $c = 1$, the composite of all four arrows equals $F \circ F^{c-1} = F^c$ (note that T_V^1 obviously commutes with F). The proof is complete. \square

DEFINITION 11.19. *Let V be a (finite-dimensional) k -vector space. Let $W \subset V$ be a k -linear subspace, of codimension $c \geq 1$. By the universal property of divided powers, there exists a unique $\mathbf{W}(k)$ -linear map*

$$\begin{aligned} \Gamma^{p^{n+rc}}(V) &\longrightarrow \Gamma^{p^n}(W), \\ [v]_{p^{n+rc}} &\mapsto [T_{W,V}(v)]_{p^n}. \end{aligned}$$

We shall denote it by $\Gamma T_{W,V}^n$. It is the Transfer, for divided powers.

Let $H \subset V$ be a k -rational hyperplane.

In view of the preceding definition, it is natural to wonder whether we can define, by passing to the quotient, a descending transfer

$$\Omega^{i+r}(V) \longrightarrow \Omega^i(H),$$

for $i \geq 0$. It is doable for $i \leq 1$. After a few unsuccessful attempts to do so for $i \geq 2$, we noticed that the difficulty can be bypassed, by considering only the submodule of $\Omega^n(V)$ generated by pure symbols. Since k is finite, this submodule, for n large, is much smaller than $\Omega^n(V)$. In particular, its rank (as a $\mathbf{W}(k)$ -module) is bounded by the cardinality of the finite projective space $\mathbb{P}_k(V)$, whereas that of the whole space $\Omega^n(V)$ grows (a priori doubly exponentially!) to infinity with n .

At the present moment, we do believe that the submodule of $\Omega^n(V)$ generated by pure k -rational symbols is the right object, for applications to Galois cohomology- and perhaps to other areas. It is the small Omega power functor. We elaborate on this new object in the next section.

12. SMALL OMEGA POWERS.

In this section, k is a finite field, of cardinality $q = p^r$. We denote by m a positive integer.

DEFINITION 12.1. (*Small Omega powers.*) Let M be a $\mathbf{W}_m(k)$ -module. Let n be a positive integer.

We define

$$\underline{\Omega}_m^n(V) \subset \Omega_m^n(V)$$

to be the $\mathbf{W}_{n+m}(k)$ -submodule spanned by all pure symbols $(x)_n$, with $x \in M$. It is the n -th Small Omega power of M . We will simply denote it by $\underline{\Omega}^n(M)$, if the dependence in m is understood.

Remark 12.2. The small Omega power $\underline{\Omega}^n$ is a functor, from the category of $\mathbf{W}_m(k)$ -modules to that of $\mathbf{W}_{n+m}(k)$ -modules. Contrary to medium and big Omega powers, it is clear from the definition that small Omega powers do not commute to extending scalars to a larger finite field.

We will now show that small Omega powers naturally occur as a direct summand of medium Omega powers. This can be compared to the occurrence of medium Omega powers as a direct summand of big Omega powers. We will need a computation in finite fields, which presents similarities with Gauss sums.

12.1. SMALL OMEGA POWERS AS A DIRECT FACTOR OF MEDIUM OMEGA POWERS. Let k'/k be 'the' finite field extension, of degree s . The field k' has q^s elements.

DEFINITION 12.3. We put

$$\kappa' := \text{Hom}_{k'}(k', k).$$

It is the k -linear dual of k' , viewed as a k -vector space.

Denote by $\tau : k' \rightarrow \mathbf{W}(k')$ the Teichmüller representative of k' . Its restriction to k is the Teichmüller representative τ of k .

12.1.1. *A funny computation in finite fields.* Denote by $\tau : k' \rightarrow \mathbf{W}(k')$ the Teichmüller representative of k' . Its restriction to k is the Teichmüller representative of k . Denote by

$$\text{tr} : k' \rightarrow k$$

the trace map. We know that the Galois group of the extension k'/k is cyclic of order s , generated by the Frobenius $x \mapsto x^q$. Hence, for $z \in k'^*$, we have

$$\text{tr}(z) = \sum_{i=0}^{s-1} z^{q^i}.$$

LEMMA 12.4. Put

$$C = C(k, k') := \sum_{z \in k'^*} \tau(z)^{-1} \tau(\text{tr}(z)) \in \mathbf{W}(k').$$

Then C belongs to \mathbb{Z}_p , and C is congruent to -1 modulo p .

Proof. The fact that C belongs to \mathbb{Z}_p is clear: $C \in \mathbf{W}(k')$ is invariant by the Frobenius of $\mathbf{W}(k')/\mathbb{Z}_p$.

Modulo p , we have

$$C \equiv \sum_{z \in k'^*} z^{-1} \left(\sum_{i=0}^{s-1} z^{q^i} \right) = -1 \in \mathbf{W}(k')/p = k'.$$

Indeed, for any integer N , the quantity

$$\sum_{y \in k'^*} y^N$$

vanishes, except when $(q^s - 1)$ divides N , in which case its value is -1 . □

DEFINITION 12.5. *The number $C = C(k, k') \in \mathbb{Z}_p^\times$ of the previous Lemma will be called the conductor of the extension k'/k .*

For each linear form $f \in \kappa'$, denote by $y \in k'$ the unique element such that

$$f(\cdot) = \text{tr}(y \cdot).$$

We put

$$C(f) := \frac{1}{C} \tau(y).$$

PROPOSITION 12.6. *Let C be the conductor of k'/k .*

For every $x \in k'^$, we have the formula*

$$\tau(x) = \frac{1}{C} \sum_{y \in k'^*} \tau(y)^{-1} \tau(\text{tr}(xy)) \in \mathbf{W}(k').$$

Proof. This is clear from the previous Lemma, setting $z = xy$. □

COROLLARY 12.7. *For every $x \in k'^*$, we have the formula*

$$\tau(x) = \sum_{f \in \kappa'} C(f) \tau(f(x)) \in \mathbf{W}(k').$$

Remark 12.8. The authors are grateful to Pierre Colmez for helping us to clarify the exposition of the previous formula.

12.1.2. Perfect duality for small Omega powers. We first need a reformulation of Lemma 12.7. We use freely the notation of the preceding subsection.

LEMMA 12.9. *Let V be a (finite-dimensional) k -vector space. Let n be a positive integer. Let k'/k be a finite field extension, of degree s . Put $V' := V \otimes_k k'$. Pick an element $\phi' \in V'^{*'} (= V^* \otimes_k k')$. For each k -linear form $f \in \kappa'$, denote by $f(\phi') \in V^*$ the composite*

$$V \xrightarrow{x \mapsto x \otimes 1} V' \xrightarrow{\phi'} k' \xrightarrow{f} k.$$

We then have the relation

$$\langle X, (\phi')_n \rangle = \sum_{f \in \kappa'} C(f) \langle X, (f \circ \phi')_n \rangle \in \mathbf{W}_{n+1}(k'),$$

for all $X \in \underline{\Omega}^n(V)$.

Proof.

It is enough to check this when X is a pure symbol $(v)_n$, for $v \in V$. The formula follows from Lemma 12.7, applied (modulo p^{n+1}) to $x := \phi'(v)^{p^n} \in k'$. \square

The next Proposition is a key.

PROPOSITION 12.10. *Let M be a (finite) $\mathbf{W}_m(k)$ -module. Let n be a positive integer.*

Consider the natural embeddings

$$\underline{\Omega}^n(M) \longrightarrow \Omega^n(M)$$

and

$$\underline{\Omega}^n(M^\vee) \longrightarrow \Omega^n(M^\vee).$$

The perfect duality

$$\Omega^n(M) \times \Omega^n(M^\vee) \longrightarrow \mathbf{W}_{m+n}(k)$$

yields by restriction a duality

$$\underline{\Omega}^n(M) \times \underline{\Omega}^n(M^\vee) \longrightarrow \mathbf{W}_{m+n}(k).$$

This duality is perfect.

Proof. We reduce to the case $m = 1$, by induction. We have to show the following. Let $X \in \underline{\Omega}^n(M)$ be orthogonal to $\underline{\Omega}^n(M^\vee)$. Then X is orthogonal to the whole of $\Omega^n(M^\vee)$ (and hence vanishes). To do so, let k'/k be a finite field extension, such that k' has cardinality greater than p^n . Put $M' := M \otimes_{\mathbf{W}(k)} \mathbf{W}(k')$. Denote by Ω' the (small or medium) Omega powers of $\mathbf{W}(k')$ -modules. By Lemma 6.12, the inclusion $\underline{\Omega}^n(M') \subset \Omega^n(M')$ is an equality. Since we now that the formation of medium Omega powers commutes to base change, it is enough to show that, for every $\phi' \in (M')^\vee$, we have

$$\langle X, (\phi')_n \rangle = 0 \in \mathbf{W}_{n+1}(k').$$

This follows from the preceding Lemma, since X is orthogonal to $\underline{\Omega}^n(M^\vee)$. \square

Remark 12.11. Note that the perfect duality

$$\underline{\Omega}^n(M) \times \underline{\Omega}^n(M^\vee) \longrightarrow \mathbf{W}_{m+n}(k)$$

of the previous Proposition is given on pure symbols by

$$\langle (x)_n, (\phi)_n \rangle = \bar{\tau}_n(\phi(x)).$$

COROLLARY 12.12. *With the notation of the preceding Proposition, we have a natural direct sum decomposition*

$$\underline{\Omega}^n(M) = \underline{\Omega}^n(M) \bigoplus \underline{\Omega}^n(M^\vee)^\perp.$$

Proof. Clear. \square

The next Lemma is helpful for defining the Transfer for small Omega powers, in the next section.

LEMMA 12.13. *Let M be a $\mathbf{W}_m(k)$ -module. Let n be a positive integer. Then the canonical map*

$$\underline{\Omega}^n(M) \longrightarrow \bigoplus_L \underline{\Omega}^n(L)$$

is injective, where the direct sum is taken over all split surjective linear maps

$$M \longrightarrow L$$

of M onto a (not necessarily free) $\mathbf{W}_m(k)$ -module of rank one.

Proof. We can assume that M is a $\mathbf{W}_m(k)$ -module of finite-type. By perfect duality (Proposition 12.10), it is then equivalent to show that the canonical map

$$\bigoplus_{L^\vee} \underline{\Omega}^n(L^\vee) \longrightarrow \underline{\Omega}^n(M^\vee)$$

is surjective, where the direct sum is taken over all split injections $L^\vee \subset M^\vee$. This holds (almost) by definition: small Omega powers are generated by pure symbols. \square

13. THE TRANSFER, FOR SMALL OMEGA POWERS.

In this section, we study the -exemplary- compatibility of the Transfer with small Omega powers.

Here k is a finite field, of cardinality $q = p^r$.

PROPOSITION 13.1. *Let V be a (finite-dimensional) k -vector space. Let $W \subset V$ be a k -linear subspace, of codimension $c \geq 1$. Let n be a positive integer. Then the Transfer*

$$\Gamma_{W,V}^n : \Gamma^{p^{rc+n}}(V) \longrightarrow \Gamma^{p^n}(W)$$

is compatible with the formation of small Omega powers. It thus induces a $\mathbf{W}(k)$ -linear map

$$\underline{\Omega}^{rc+n}(V) \longrightarrow \underline{\Omega}^n(W).$$

Proof. By induction (see Lemma 11.14), we can assume that $c = 1$. The statement is clear if V is two-dimensional: we know that the duality Δ on $\Gamma^{p^{r+n}}(V)$ is perfect in this case. In general, let $H \subset W$ be a k -rational hyperplane. Then H is of codimension two in V . We have a commutative diagram

$$\begin{array}{ccc} \Gamma^{p^{r+i}}(V) & \xrightarrow{\Gamma_{W,V}} & W \\ \downarrow & & \downarrow \\ \Gamma^{p^{r+i}}(V/H) & \xrightarrow{\Gamma_{W/H,V/H}^i} & \Gamma^{p^i}(W/H), \end{array}$$

where the vertical maps are induced by the canonical surjections. Forming the direct sum

$$\begin{array}{ccc} \Gamma^{p^{r+i}}(V) & \xrightarrow{\Gamma_{W,V}^i} & \Gamma^{p^i}(W) \\ \downarrow & & \downarrow \\ \bigoplus_H \Gamma^{p^{r+i}}(V/H) & \xrightarrow{\bigoplus_H \Gamma_{W/H,V/H}^i} & \bigoplus_H \Gamma^{p^i}(W/H), \end{array}$$

over all hyperplanes H , yields the result. Indeed, the composite arrows vanish on $\text{Ker}(\Delta)$ by the two-dimensional case, and we can apply Lemma 12.13 (the vertical arrow on the right induces an injection on small Omega powers).

□

The following Definition thus makes sense.

DEFINITION 13.2. (*Ascending and Descending Transfer for small Omega powers.*)
 Let V be a (finite-dimensional) k -vector space. Let n be a positive integer.
 Let $W \subset V$ be a k -linear subspace, of codimension $c \geq 1$. The $\mathbf{W}(k)$ -linear map

$$\underline{\Omega}^{rc+n}(V) \longrightarrow \underline{\Omega}^n(W)$$

of the preceding Proposition is the Descending Transfer, from V to W , for small Omega powers. We denote it by $\underline{DT}_{W,V}^n$.

Dually, let

$$\pi : V \longrightarrow W$$

be a surjection between (finite-dimensional) k -vector spaces, such that $\text{Ker}(\pi)$ has dimension c . Using Pontryagin duality, the dual of $\underline{DT}_{W,V}^n$ is a $\mathbf{W}(k)$ -linear map

$$\underline{\Omega}^n(W) \longrightarrow \underline{\Omega}^{n+rc}(V).$$

It is the Ascending Transfer, from W to V , for small Omega powers. We denote it by $\underline{AT}_{V,W}^n$.

Remark 13.3. For $v \in V$, we have

$$\underline{DT}_{W,V}((v)_{n+rc}) = (v)_n$$

if $v \in W$, and

$$\underline{DT}_{W,V}((v)_{n+rc}) = 0$$

if $v \notin W$. The surprising fact is that this simple formula on symbols indeed defines a $\mathbf{W}(k)$ -linear map!

The next Proposition gives a simple formula for the ascending transfer.

PROPOSITION 13.4. *Let*

$$\pi : V \longrightarrow W$$

be a surjection between k -vector spaces, such that $\text{Ker}(\pi)$ has dimension c .

Let n be a positive integer. Put

$$X_\pi := \sum_{w \in \text{Ker}(\pi)} (w)_{n+cr} \in \Omega^{n+cr}(V).$$

(Note that $X_\pi = 0$ if k has at least 3 elements.)

Pick an element $w \in W$. Then we have the formula

$$\underline{AT}_{V,W}((w)_n) = -X_W + \sum_{v \in \pi^{-1}(w)} (v)_{n+cr}.$$

Proof.

Denote by

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

the Teichmüller representative, and by

$$\pi^* : W^* \subset V^*$$

the inclusion of the c -codimensional subspace which is dual to W . Pick an arbitrary linear form $\phi \in V^*$. By definition of the ascending transfer, we have

$$\langle \underline{AT}_{V,W}((x)_n), (\phi)_{n+cr} \rangle = p^{rc} \langle (x)_n, \underline{DT}_{W^*,V^*}((\phi)_{n+cr}) \rangle \in \mathbf{W}_{n+rc+1}(k).$$

Denote this quantity by a .

Note that we used here the natural injection (Verschiebung)

$$\mathbf{W}_{n+1}(k) \xrightarrow{1 \rightarrow p^{rc}} \mathbf{W}_{n+rc+1}(k).$$

Put

$$a' := -X_\pi + \sum_{v \in \pi^{-1}(w)} (v)_{n+cr}, (\phi)_{n+cr} \rangle \in \mathbf{W}_{n+rc+1}(k).$$

By perfect duality, it suffices to show that $a = a'$: indeed, the symbols $(\phi)_{n+cr}$ span the $\mathbf{W}(k)$ -module $\underline{\Omega}^{n+cr}(V^*)$.

We distinguish two cases.

Case i): The linear form does not belong to W^* .

Case ii) The linear form ϕ belongs to W^* .

By Remark 13.3, $\underline{DT}_{W^*,V^*}((\phi)_{n+cr})$ is equal to zero in Case i), and to $(\phi)_n$ in Case ii). Hence, $a = 0$ in Case i), and

$$a = p^{rc} \tau(\phi(x))^{p^n} \in \mathbf{W}_{n+rc+1}(k)$$

in Case ii). Clearly, we have

$$\begin{aligned} a' &= \left(- \sum_{v \in \text{Ker}(\pi)} \tau(\phi(v))^{p^{n+rc}} + \sum_{v \in \pi^{-1}(w)} \tau(\phi(v))^{p^{n+rc}} \right) \\ &= \left(- \sum_{v \in \text{Ker}(\pi)} \tau(\phi(v))^{p^n} + \sum_{v \in \pi^{-1}(w)} \tau(\phi(v))^{p^n} \right) \end{aligned}$$

(remember that $x^q = x$ for every $x \in k$). Assume that we are in Case i), i.e. that ϕ does not vanish on $\text{Ker}(\pi)$. Then

$$\phi|_{\pi^{-1}(w)} : \pi^{-1}(w) \longrightarrow k$$

and

$$\phi|_{\text{Ker}(\pi)} : \text{Ker}(\pi) \longrightarrow k$$

are both surjective maps, between k -affine spaces. Hence, the cardinality of the fiber of any element of k by these two maps is the same, from which we get $a' = 0$. Assume now that we are in case ii). Then ϕ vanishes on $\text{Ker}(\pi)$, and the p^{rc} other terms occuring in the sum defining a' are all equal to $\tau(\phi(w))^{p^n}$. Again, we conclude that $a = a'$ and the Proposition is proved. □

13.1. THE TRANSFER, AS A CONTRAVARIANT FUNCTOR.

DEFINITION 13.5. *Let n be a positive integer. Let*

$$f : V \longrightarrow W$$

be a linear map between finite-dimensional k -vector spaces. Then f factors canonically as the composite

$$V \twoheadrightarrow V/\text{Ker}(f) = \text{Im}(f) \hookrightarrow W.$$

Denote by $\rho := \delta(\text{Im}(f))$ the rank of f .

We denote by $\underline{T}^n(f)$ (or simply by $\underline{T}(f)$) the composite

$$\underline{\Omega}^{n+r\delta(W)}(W) \xrightarrow{DT_{\text{Im}(f),W}} \underline{\Omega}^{n+r\rho}(\text{Im}(f)) = \underline{\Omega}^{n+r\rho}(V/\text{Ker}(f)) \xrightarrow{AT_{V,V/\text{Ker}(f)}} \underline{\Omega}^{n+r\delta(V)}(V). \blacksquare$$

It is the Transfer, for small Omega powers.

PROPOSITION 13.6. *Let n be a positive integer. Let*

$$f : V \longrightarrow W$$

be a linear map between finite-dimensional k -vector spaces. Put

$$X_f := \sum_{v \in \text{Ker}(f)} (v)_{n+r\delta(V)} \in \underline{\Omega}^{n+r\delta(V)}(V).$$

Note that we always have $X_f = 0$ if k has at least 3 elements.

Then

$$\underline{T}(f) : \underline{\Omega}^{n+r\delta(W)}(W) \longrightarrow \underline{\Omega}^{n+r\delta(V)}(V)$$

is given, on pure symbols, by the formula

$$(w)_{n+r\delta(W)} \mapsto -X_f + \sum_{v \in f^{-1}(\{w\})} (v)_{n+r\delta(V)}.$$

Proof. It is easy to check that, if $g : W \longrightarrow Z$ is another linear map between finite-dimensional k -vector spaces, then the formula of the Proposition is true for $g \circ f : V \longrightarrow Z$, if it is true for both f and g . Hence, it suffices to check the formula if f is injective or surjective.

The formula is obviously true if f is injective, by the very definition of the descending transfer (Remark 13.3). That the formula is true if f is surjective is the content of Proposition 13.4. \square

PROPOSITION 13.7. *Let n be a positive integer. The association*

$$\begin{aligned} V &\mapsto \underline{\Omega}^{n+r\delta(V)}(V), \\ f &\mapsto \underline{T}(f) \end{aligned}$$

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

Proof. This follows from the expression of $T(f)$ given in Proposition 13.6. \square

PROPOSITION 13.8. *Let*

$$f : V \longrightarrow W$$

be a linear map between finite-dimensional k -vector spaces. Then the following is true.

i) If f is injective, then the composite

$$\underline{\Omega}^{n+r\delta(W)}(V) \xrightarrow{\underline{\Omega}(f)} \underline{\Omega}^{n+r\delta(W)}(W) \xrightarrow{\underline{T}(f)} \underline{\Omega}^{n+r\delta(V)}(V)$$

equals $\text{Frob}^{r(\delta(W)-\delta(V))}$.

ii) If f is surjective, then the composite

$$\underline{\Omega}^{n+r\delta(W)}(W) \xrightarrow{\underline{T}(f)} \underline{\Omega}^{n+r\delta(V)}(V) \xrightarrow{\underline{\Omega}(f)} \underline{\Omega}^{n+r\delta(V)}(W)$$

equals $\text{Ver}^{r(\delta(V)-\delta(W))}$.

Proof. Computation, using Proposition 13.6. \square

PROPOSITION 13.9. *Let n be a nonnegative integer. Let*

$$\begin{array}{ccc} V & \xrightarrow{f_2} & W_1 \\ \downarrow f_1 & & \downarrow g_2 \\ W_2 & \xrightarrow{g_1} & Z \end{array}$$

be a cartesian diagram in the category of finite-dimensional k -vector spaces. Then we have

$$\underline{\Omega}(f_2) \circ \underline{T}(f_1) = \underline{T}(g_2) \circ \underline{\Omega}(g_1),$$

as $\mathbf{W}(k)$ -linear maps $\underline{\Omega}^{n+r\delta(W_2)}(W_2) \longrightarrow \underline{\Omega}^{n+r\delta(V)}(W_1)$

Proof. Using Proposition 13.6, we compute that both composites are given, on symbols, by the formula

$$(x). \mapsto \sum_{y \in W_1, g_2(y) = g_1(x)} (y).,$$

and the claim is proved. \square

We conclude this section with an important Proposition. Its content is that the modules $\underline{\Omega}^n(V)/p^m$ are *induced from dimension one*, if $n - m$ is large enough.

PROPOSITION 13.10. *Let V be a finite-dimensional k -vector space, of dimension ≥ 2 . Let n, m be positive integers, satisfying*

$$n - m \geq r(\delta(V) - 1) - 1.$$

For each line $L \subset V$, functoriality of small Omega powers yields a canonical map

$$\underline{\Omega}^n(L)/p^m \xrightarrow{f_L} \underline{\Omega}^n(V)/p^m.$$

Then the map

$$f : \bigoplus_{L \in \mathbb{P}_k(V)} \underline{\Omega}^n(L)/p^m \xrightarrow{\sum f_L} \underline{\Omega}^n(V)/p^m$$

is an isomorphism of free $\mathbf{W}_m(k)$ -modules.

Proof. The map f is obviously surjective: $\underline{\Omega}^n(V)$ is generated by symbols $(v)_n$, for v ranging through the nonzero vectors of V , and such a v belongs to a unique L ! For each line $L \hookrightarrow V$, we have the transfer

$$\underline{DT}_{L,V} : \underline{\Omega}^n(V) \longrightarrow \underline{\Omega}^{n-r(\delta(V)-1)}(L).$$

But $\underline{\Omega}^{n-r(\delta(V)-1)}(L)$ is a free $\mathbf{W}_{p^{n-r(\delta(V)-1)+1}}(k)$ -module of rank one. Under our assumption on m , the quotient $\underline{\Omega}^{n-r(\delta(V)-1)}(L)/p^m$ is then a free $\mathbf{W}_m(k)$ -module of rank one. Using the canonical isomorphism $L \simeq L^{(r)}$, we see (via the Frobenius) that there is a canonical isomorphism

$$\underline{\Omega}^{n-r(\delta(V)-1)}(L)/p^m \simeq \underline{\Omega}^n(L)/p^m,$$

through which the transfer can be seen, modulo p^m , as a $\mathbf{W}(k)/p^m$ -linear map

$$g_L : \underline{\Omega}^n(V)/p^m \longrightarrow \underline{\Omega}^n(L)/p^m,$$

sending a symbol $(v)_n$ to zero if $v \notin L$, or to $(v)_n$ if $v \in L$.

The sum of the g_L 's is a $\mathbf{W}(k)/p^m$ -linear map

$$g : \underline{\Omega}^n(V)/p^m \longrightarrow \bigoplus_{L \in \mathbb{P}(V)} \underline{\Omega}^n(L)/p^m,$$

which is seen to be the inverse of f (check this on pure symbols). □

13.2. THE INTEGRAL FORMULAS FOR THE FROBENIUS AND THE VERSCHIEBUNG. The purpose of this section is to state and prove Integral Formulas for the Frobenius and the Verschiebung, for small Omega powers. These formulas say that averaging all descending (resp. ascending) transfers over all linear subspaces of a given dimension yields the Frobenius (resp. the Verschiebung). These formulas are reminiscent of motivic integration.

Recall that $\text{Gr}_k(m, n)$, the Grassmannian of m dimensional subspaces of k^n , has cardinality

$$|\text{Gr}_k(m, n)| = \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-m+1} - 1)}{(q^m - 1)(q^{m-1} - 1) \dots (q - 1)}.$$

In particular, all these numbers are congruent to 1 modulo p .

PROPOSITION 13.11. (*Frobenius Integral Formula.*) *Let n be a positive integer. Let V be a nonzero finite-dimensional k -vector space. Let $1 \leq m \leq \delta(V) - 1$ be an integer. For each linear subspace $W \in \text{Gr}(\delta(V) - m, V)$, denote by*

$$i_W : W \hookrightarrow V$$

the canonical inclusion. We have the formula

$$\frac{1}{|\text{Gr}_k(m, \delta(V) - 1)|} \sum_{W \in \text{Gr}(m, V)} \underline{\Omega}(i_W) \circ \underline{T}(i_W) = \text{Frob}^{mr},$$

as $\mathbf{W}(k)$ -linear maps

$$\underline{\Omega}^{n+mr}(V) \longrightarrow \underline{\Omega}^n(V).$$

Proof. This is an easy computation, using the formula for the transfer given by Proposition 13.6. Pick a nonzero vector $v \in V$. For $W \in \text{Gr}(\delta(V) - m, V)$, the quantity $\underline{\Omega}(i_W) \circ \underline{T}(i_W)((v)_{n+rm})$ equals zero if $v \notin W$, or $(v)_n$ otherwise. It is clear that the set of subspaces $W \in \text{Gr}(\delta(V) - m, V)$ containing v is in bijection with $\text{Gr}(\delta(V) - m - 1, V / \langle v \rangle)$, hence has cardinality $|\text{Gr}_k(m, \delta(V) - 1)|$. The formula follows. □

PROPOSITION 13.12. (*Verschiebung Integral Formula.*) *Let n be a positive integer. Let V be a nonzero finite-dimensional k -vector space. Let $1 \leq m \leq \delta(V) - 1$ be an integer. For each linear subspace $W \in \text{Gr}(m, V)$, denote by*

$$\pi_W : V \twoheadrightarrow V/W$$

the quotient map. We have the formula

$$\frac{1}{|\text{Gr}_k(m - 1, \delta(V) - 1)|} \sum_{W \in \text{Gr}(m, V)} \underline{T}(\pi_W) \circ \underline{\Omega}(\pi_W) = \text{Ver}^{mr},$$

as $\mathbf{W}(k)$ -linear maps

$$\underline{\Omega}^n(V) \longrightarrow \underline{\Omega}^{n+mr}(V).$$

Proof. This follows, by Pontryagin duality, from the Frobenius Integral Formula for V^* . □

14. AXIOMATIZING HILBERT'S THEOREM 90.

In this section, we explain a possible way to axiomatize the consequences of Hilbert's Theorem 90 (Kummer theory) for the cohomology of profinite groups. The key notion here is that of cyclotomic modules, and smooth profinite groups.

14.1. THE NOTION OF n -SURJECTIVITY. In this section, k is a perfect field of characteristic p , and G is a profinite group.

DEFINITION 14.1. *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 14.2. 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 14.3. *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. □

Exercise 14.4. Prove the preceding Lemma without using the connecting map, i.e. without invoking cohomology groups in degree $n + 1$.

Remark 14.5. (0-surjectivity). 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 0-surjective if and only if it possesses a G -equivariant *-set-theoretic-* section. This situation appears in the study of rationality questions for algebraic tori, through the use of (co)flasque resolutions of their character lattice. We refer here to the work of Endo and Miyata [EM], of Colliot-Thélène and Sansuc [CTS], and of Voskresenskii [Vos].

Exercise 14.6. It is clear that a split surjection is n -surjective for every n . In this exercise, we show that the converse implication is false in general. This exercise, though by no means easy, provides good practice for understanding the ideas developed in this paper.

For simplicity, we assume here that $k = \mathbb{F}_p$.

Let X be a finite G -set. Let

$$V \subset \mathbb{F}_p^X$$

be a sub- (\mathbb{F}_p, G) -module. Put

$$W := \mathbb{F}_p^X / V.$$

Let M be a $(\mathbb{Z}/p^2\mathbb{Z}, G)$ -module, which is free of rank one as a $\mathbb{Z}/p^2\mathbb{Z}$ -module, together with an isomorphism of (\mathbb{F}_p, G) -modules

$$M/p \simeq \mathbb{F}_p.$$

The exact sequence

$$0 \longrightarrow (pM)^X \longrightarrow M^X \longrightarrow (M/pM)^X \longrightarrow 0$$

can thus be viewed as an exact sequence

$$0 \longrightarrow \mathbb{F}_p^X \longrightarrow M^X \longrightarrow \mathbb{F}_p^X \longrightarrow 0.$$

Pulling it back by the inclusion $V \longrightarrow \mathbb{F}_p^X$ and pushing it forward by the surjection $\mathbb{F}_p^X \longrightarrow W$ yields an extension

$$\mathcal{E} : 0 \longrightarrow W \longrightarrow E \xrightarrow{\pi} V \longrightarrow 0.$$

- i) Show that \mathcal{E} is an exact sequence of (\mathbb{F}_p, G) -modules.
- ii) Show that \mathcal{E} depends neither on M nor on the choice of the isomorphism $M/p \simeq \mathbb{F}_p$ (up to isomorphism of short exact sequences of (\mathbb{F}_p, G) -modules).
- iii) Show that π is 0-surjective.

From now on, we assume that G is "the" absolute Galois group of a field F of characteristic not p , containing the p -th roots of unity for simplicity. We make no extra assumption on X .

- iv) Using Kummer theory, show that π is 1-surjective. *Hint: choose $M = \mu_{p^2}$.*
- v) Using the Bloch-Kato conjecture, show that π is n -surjective, for every $n \geq 1$.
- vi) Give an example (of F and X) where \mathcal{E} is not split.

14.2. CYCLOTOMIC MODULES AND SMOOTHNESS.

DEFINITION 14.7. We put

$$\overline{\mathbb{N}} := \mathbb{N}_{\geq 1} \cup \{\infty\},$$

and $\mathbf{W}_{\infty}(k) = \mathbf{W}(k)$.

DEFINITION 14.8. Pick an element $d \in \overline{\mathbb{N}}$. Let \mathcal{T} be a free $\mathbf{W}_{d+1}(k)$ -module of rank one.

For i a non negative integer, we put

$$\mathcal{T}(i) = \mathcal{T}^{\otimes_{\mathbf{W}_{d+1}(k)} i}.$$

For negative i , we put

$$\mathcal{T}(i) = \mathrm{Hom}_{\mathbf{W}_{d+1}(k)}(\mathcal{T}(-i), \mathbf{W}_{d+1}(k)).$$

For any $(\mathbf{W}_{d+1}(k), G)$ -module M , we put

$$M(i) = \mathcal{T}(i) \otimes_{\mathbf{W}_{d+1}(k)} M,$$

the dependence in \mathcal{T} being implicit.

DEFINITION 14.9. (Cyclotomic module.) Let $n \geq 0$ and $d \in \overline{\mathbb{N}}$ be integers. Let \mathcal{T} be a free $\mathbf{W}_{d+1}(k)$ -module of rank one, endowed with a continuous $\mathbf{W}_{d+1}(k)$ -linear action of G .

The module \mathcal{T} is said to be n -cyclotomic (relative to k and G) if the following condition holds.

For every integer $s \geq 1$, the quotient map

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

is n -surjective.

If $\mathcal{T}(n)$ is n -cyclotomic for every $n \geq 1$, we shall say that \mathcal{T} is cyclotomic (relative to k and G).

The integer d is the depth of \mathcal{T} . It will be denoted by $\delta(\mathcal{T})$.

Remark 14.10. If \mathcal{T} has finite depth, it suffices of course to require n -surjectivity for $s = \delta(\mathcal{T})$ in the previous Definition.

Remark 14.11. The preceding Definition has an interest only if $n \geq 1$.

Remark 14.12. A cyclotomic G -module is given by a continuous character

$$\chi : G \longrightarrow \mathbf{W}_{\delta(\mathcal{T})+1}(k)^{\times},$$

which shall, in our theory, play the rôle of the cyclotomic character in Galois theory. Indeed, we will see in a moment that Kummer theory (a consequence of Hilbert's Theorem 90) implies that the cyclotomic character at p of a field of characteristic not p is 1-cyclotomic, in our sense. That it is in fact cyclotomic is the main content of the norm-residue isomorphism theorem (the Bloch-Kato conjecture).

Exercise 14.13. Let \mathcal{T} be an n -cyclotomic G -module. Show that the quotient map

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

is n -surjective, for every $s \geq 1$.

LEMMA 14.14. *Let $n \geq 0$ be an integer. Let k'/k be a field extension. Let \mathcal{T} be a n -cyclotomic G -module over k . Put*

$$\mathcal{T}' := \mathcal{T} \otimes_{\mathbf{W}(k)} \mathbf{W}(k').$$

Then \mathcal{T}' is n -cyclotomic over k' .

Proof. This is clear, since $\mathbf{W}(k')$ is a free $\mathbf{W}(k)$ -module. \square

Remark 14.15. In the Definition of a cyclotomic module, it might be worth allowing the case where \mathcal{T} is free of rank ≥ 2 : this would enable restriction of scalars for finite field extensions k'/k . We shall not consider this possibility here.

LEMMA 14.16. *Let k'/k be an (arbitrary) field extension. Let n be a positive integer.*

Assume that G is a pro- p -group, and that there exists an n -cyclotomic G -module over k' , of depth 1. Then, there exists an n -cyclotomic G -module over k , of depth 1.

Proof.

Let \mathcal{T}' be an n -cyclotomic G -module over k' , of depth 1; in particular, \mathcal{T}' is a free $\mathbf{W}_2(k')$ -module of rank one. Consider the exact sequence

$$0 \longrightarrow \mathcal{T}'/p \simeq p\mathcal{T}' \longrightarrow \mathcal{T}' \longrightarrow \mathcal{T}'/p \longrightarrow 0.$$

Since G is a pro- p -group, it acts trivially on the one-dimensional k' -vector space \mathcal{T}'/p . As an exact sequence of $(\mathbf{W}(k'), G)$ modules, the preceding sequence can thus be rewritten as

$$\mathcal{E}' : 0 \longrightarrow k' \longrightarrow \mathcal{T}' \longrightarrow k' \longrightarrow 0.$$

Choose a linear form $\phi \in \text{Hom}_k(k', k)$, such that $\phi(1) = 1$. Denote by $i : k \longrightarrow k'$ the canonical inclusion. Then $\phi_*(i^*(\mathcal{E}'))$ is an sequence of $(\mathbf{W}(k), G)$ modules of the shape

$$\mathcal{E} : 0 \longrightarrow k \longrightarrow \mathcal{T} \longrightarrow k \longrightarrow 0,$$

where \mathcal{T} is a free $\mathbf{W}_2(k)$ -module of rank one, equipped with an action of G . From Lemma 14.3, it follows that \mathcal{T} is n -cyclotomic, qed. \square

Remark 14.17. The preceding Lemma can probably be generalized to cyclotomic modules of arbitrary depth.

DEFINITION 14.18. (*Smooth profinite group.*) *Let n and d be positive integers. The group G is said to be (d, n) -smooth (resp. d -smooth) relative to k , if there exists an n -cyclotomic (resp. cyclotomic) G -module over k , of depth d .*

The group G is said to be n -smooth (resp. smooth) relative to k , if there exists an n -cyclotomic (resp. cyclotomic) G -module over k , of infinite depth.

The fundamental example of 1-smoothness is that of absolute Galois groups. It can be extended to a broader class of Galois groups, as follows.

PROPOSITION 14.19. *Let E/F be an extension of fields of characteristic not p . Assume that the multiplicative group E^\times is p -divisible (i.e. the map $E^\times \xrightarrow{x \mapsto x^p} E^\times$ is onto), and contains all p -th roots of unity (hence also all roots of unity of order a power of p). Put*

$$G := \text{Gal}(E/F)$$

and

$$\mu = \varprojlim_n \mu_{p^n}(E).$$

Then μ is a cyclotomic G -module (relative to $k = \mathbb{F}_p$).

Proof.

By our assumptions on E , we have a diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mu_p(E) & \longrightarrow & \mu_{p^{s+1}}(E) & \xrightarrow{x \mapsto x^p} & \mu_{p^s}(E) & \longrightarrow & 1 \\ & & \parallel & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mu_p(E) & \longrightarrow & E^\times & \xrightarrow{x \mapsto x^p} & E^\times & \longrightarrow & 1, \end{array}$$

given by classical Kummer theory. The surjection in the lower line is obviously 1-surjective by Hilbert's Theorem 90 for \mathbb{G}_m . By Lemma 14.3, the surjection in the upper line is 1-surjective as well, yielding the result. \square

It is natural to ask whether all 1-cyclotomic modules occur this way. We did not investigate this question, but we expect a positive answer—possibly given by a simple construction. We now formulate it precisely.

Problem 14.20. Let G be a profinite group. Let M be a 1-cyclotomic G -module of infinite depth, for $k = \mathbb{F}_p$. Let l be zero or a prime number distinct from p . Find an extension E/F of fields of characteristic l , such that the multiplicative group E^\times is p -divisible, contains all p -th roots of unity, and such that the following holds.

There is an isomorphism

$$\phi : G \longrightarrow \text{Gal}(E/F)$$

of profinite groups, and an isomorphism

$$\psi : M \longrightarrow \varprojlim_n \mu_{p^n}(E)$$

of \mathbb{Z}_p -modules, such that

$$\psi(g.m) = \phi(g).\psi(m),$$

for all $g \in G$ and $m \in M$.

14.3. THE SMOOTHNESS CONJECTURE. Recall that G is a profinite group.

DEFINITION 14.21. Let $n \geq 1$ be an integer. Let L be a one-dimensional (k, G) -module.

Cohomology classes in the image of the natural cup-product map

$$H^1(G, L)^n \longrightarrow H^n(G, L^{\otimes n})$$

are called *symbols* (relative to L).

If $H \subset G$ is an open subgroup, the image of a symbol in $H^n(H, L^{\otimes n})$ by the corestriction (norm)

$$\text{Cor} : H^n(H, L^{\otimes n}) \longrightarrow H^n(G, L^{\otimes n})$$

is called an *H-quasi-symbol* (relative to L).

A class which can be written as a sum $a_1 + \dots + a_N$, where the H_i 's are open subgroups of G , and a_i is an H_i -quasi-symbol, will be called a *quasi-symbol* (relative to L).

Remark 14.22. Assume that \mathcal{T} is a 1-cyclotomic G -module (of any depth). Let n and s be positive integers. It is straightforward that any symbol (and hence any quasi-symbol) in $H^n(G, \mathcal{T}(n)/p)$ can be lifted to a class in $H^n(G, \mathcal{T}(n)/p^s)$.

DEFINITION 14.23. *We say that G has the weak Bloch-Kato property (at p) if the following holds. For every integer $n \geq 1$ and for every open subgroup $H \subset G$, every class in $H^n(H, k)$ is a quasi-symbol (relative to $L = k$).*

The following Remark is elementary, but important.

Remark 14.24. Let G_p be a pro- p -Sylow of G . By the standard restriction-corestriction argument, it is straightforward to prove the following two assertions.
i) The group G has the weak Bloch-Kato property at p if and only if G_p has it.
ii) In the preceding definition, we may replace the trivial (k, G) -module $L = k$ by -any- one-dimensional (k, G) -module L .

We now state the Smoothness Conjecture, which we plan to prove in a future work.

CONJECTURE. 14.25. *Let G be a profinite group. If G is 1-smooth, then it has the weak Bloch-Kato property. In particular, it is smooth.*

Remark 14.26. The Smoothness Conjecture implies the (surjectivity part of the) Bloch-Kato conjecture, using a classical input from Milnor K -theory: the Lemma of Rosset and Tate. It implies that a quasi-symbol in $H^n(\text{Gal}(F_{\text{sep}}/F), \mu_p^{\otimes n})$ is in fact a sum of symbols. Note that this Lemma, whose proof uses Euclidean division for polynomials, is of highly effective nature.

We conclude this section with an instructive exercise.

Exercise 14.27. Let k be an arbitrary perfect field of characteristic p .

Let G be a finite p -group.

- i) Assume that $|G| \geq 3$. Show that G is not smooth.
- ii) Assume that $p = 2$ and $G = \mathbb{Z}/2\mathbb{Z}$. Show that G is 1-smooth. What are the possible cyclotomic modules for G ?

14.4. EXACT SEQUENCES OF KUMMER TYPE.

DEFINITION 14.28. *Let a and b be positive integers.*

The extension (of $(\mathbf{W}(k), G)$ -modules with trivial G -action)

$$0 \longrightarrow \mathbf{W}_b(k) \xrightarrow{1 \mapsto p^a} \mathbf{W}_{a+b}(k) \longrightarrow \mathbf{W}_a(k) \longrightarrow 0$$

will be called the elementary Kummer extension, of type (a, b) . We shall denote it by $\mathcal{K}_{a,b}$. The integer $a + b - 1$ is called the depth of $\mathcal{K}_{a,b}$.

We denote $\mathcal{K}_{d,1}$ simply by \mathcal{K}_d . It is the elementary Kummer extension, of depth d .

Remark 14.29. Let a and b be positive integers.

Then Pontryagin duality exchanges $\mathcal{K}_{a,b}$ and $\mathcal{K}_{b,a}$.

The diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbf{W}_b(k) & \longrightarrow & \mathbf{W}_{a+b}(k) & \longrightarrow & \mathbf{W}_a(k) \longrightarrow 0 \\ & & \parallel & & \downarrow 1 \mapsto p & & \downarrow 1 \mapsto p \\ 0 & \longrightarrow & \mathbf{W}_b(k) & \longrightarrow & \mathbf{W}_{a+b+1}(k) & \longrightarrow & \mathbf{W}_{a+1}(k) \longrightarrow 0 \end{array}$$

is clearly a pullback diagram. This shows that $\mathcal{K}_{a,b}$ is a pullback of $\mathcal{K}_{a+1,b}$. Dually, $\mathcal{K}_{a,b}$ is a pushforward of $\mathcal{K}_{a,b+1}$.

DEFINITION 14.30. *Let d be a positive integer.*

We denote by $\mathcal{K}_d(G)$ the smallest class of extensions

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

of $(\mathbf{W}(k), G)$ -modules, containing the extension

$$0 \longrightarrow k \longrightarrow \mathbf{W}_{d+1}(k) \longrightarrow \mathbf{W}_d(k) \longrightarrow 0,$$

and stable by the following operations.

i) Arbitrary finite direct sums, pullbacks and pushforwards (of extensions of $(\mathbf{W}(k), G)$ -modules).

ii) Induction from open subgroups: if $H \subset G$ is an open subgroup, and if

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

belongs to $\mathcal{K}_d(H)$, then

$$0 \longrightarrow \text{Ind}_H^G(A) \longrightarrow \text{Ind}_H^G(B) \longrightarrow \text{Ind}_H^G(C) \longrightarrow 0$$

belongs to $\mathcal{K}_d(G)$.

iii) Composition (on the right): if $f : A \longrightarrow B \longrightarrow 0$ and $g : B \longrightarrow C \longrightarrow 0$ are the epimorphisms of extensions belonging to $\mathcal{K}_d(G)$, then

$$0 \longrightarrow \text{Ker}(f \circ g) \longrightarrow A \xrightarrow{f \circ g} C \longrightarrow 0$$

belongs to $\mathcal{K}_d(G)$.

Extensions belonging to $\mathcal{K}_d(G)$ are said to be of Kummer type, of depth $\leq d$.

We put

$$\mathcal{K}(G) = \bigcup_{d \geq 1} \mathcal{K}_d(G).$$

Extensions belonging to $\mathcal{K}(G)$ are said to be of Kummer type.

Epimorphisms or monomorphisms fitting into an exact sequence of Kummer type, will also be called of Kummer type.

REMARK 14.31. Using Remark 14.29 and property iii) of the previous Definition, we see that the Kummer extension of type (a, b) belongs to $\mathcal{K}_{a+b-1}(G)$, for every positive integers a and b .

LEMMA 14.32. *Let d be a positive integer. The following assertions are true.*

a) The class $\mathcal{K}_d(G)$ is stable by composition on the left. In other words, if $f : 0 \longrightarrow A \longrightarrow B$ and $g : 0 \longrightarrow B \longrightarrow C$ are the monomorphisms of extensions belonging to $\mathcal{K}_d(G)$, then

$$0 \longrightarrow A \xrightarrow{f \circ g} C \xrightarrow{h} \text{Coker } f \circ g \longrightarrow 0$$

belongs to $\mathcal{K}_d(G)$ as well.

b) The class $\mathcal{K}_d(G)$ is stable under Pontryagin duality.

Proof. Point a) is obviously Pontryagin dual to point iii) of the definition of $\mathcal{K}_d(G)$, whereas point i) and ii) are self dual (Pontryagin duality exchanges pullbacks and pushforwards, and Pontryagin duality commutes to induction from open subgroups). By Remarks 14.29 and 14.31, we thus see that b) follows from a). We now prove a).

Forming the pullback of

$$0 \longrightarrow B \xrightarrow{g} C \longrightarrow C/B \longrightarrow 0$$

by the natural quotient map

$$C/A \longrightarrow C/B$$

yields the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & C \oplus B/A & \xrightarrow{\text{can}} & C/A & \longrightarrow & 0 \\ & & \parallel & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & B & \longrightarrow & C & \longrightarrow & C/B & \longrightarrow & 0, \end{array}$$

where *can* is the sum of the canonical inclusion and of the canonical surjection. By point i) of the definition of $\mathcal{K}_d(G)$ (for pullbacks), the upper row is of Kummer type. By assumption on f , and by point i) again (but for direct sums), the natural surjection

$$C \oplus B \longrightarrow C \oplus B/A$$

belongs to $\mathcal{K}_d(G)$ as well. By point iii), we see that the composite surjection

$$C \oplus B \longrightarrow C \oplus B/A \longrightarrow C/A$$

belongs to $\mathcal{K}_d(G)$. Noting that it equals the composite

$$C \oplus B \xrightarrow{\Sigma} C \xrightarrow{h} C/A,$$

we finally conclude (using point i), for pushforwards this time) that h belongs to $\mathcal{K}_d(G)$. \square

Remark 14.33. A surjection of Kummer type can be intuitively thought of as 'a surjection through which cohomology classes can be lifted', in the spirit of model categories. This is made precise in the Proposition below.

PROPOSITION 14.34. *Let n and d be positive integers. Assume that G is (d, n) -smooth. Let \mathcal{T} be an n -cyclotomic G -module, of depth d . Let*

$$0 \longrightarrow A \longrightarrow B \xrightarrow{f} C \longrightarrow 0$$

be a exact sequence of Kummer type, of depth $\leq d$. Then the sequence

$$0 \longrightarrow A(n) \longrightarrow B(n) \xrightarrow{f^{(n)}} C(n) \longrightarrow 0$$

is n -surjective.

Proof. This property holds, by the definition of an n -cyclotomic G -module of depth d , for the exact sequence \mathcal{K}_d . It remains to be checked that it is stable under the operations i), ii), iii) of the definition of an exact sequence of Kummer type. For point i), use Lemma 14.3. For point ii), use the definition of n -surjectivity. For point iii), there is almost nothing to do. \square

LEMMA 14.35. (*The Cross Lemma.*)
 Let

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \xrightarrow{h} & C_1 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 \longrightarrow 0 \\
 & & \downarrow f & & \downarrow g & & \downarrow \\
 0 & \longrightarrow & A_3 & \longrightarrow & B_3 & \longrightarrow & C_3 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

be a commutative diagram of $(\mathbf{W}(k), G)$ -modules, with exact rows and columns. Assume that g and h are of Kummer type, of depth $\leq d$. Then so is f .

Proof. Exercise in homological algebra for the reader. \square

15. ABOUT HILBERT'S THEOREM 90.

The authors now want make a brief digression, to stress the importance of Hilbert's Theorem 90. It is, by the way, the favorite Theorem of the second author of this paper, who is a big fan of descent statements. The theory developed here shows that this Theorem, contrary to what one could expect, is perhaps -the key ingredient to a 'short' proof of the Bloch-Kato conjecture, over a field F of characteristic not p . Indeed, the Stable Lifting Theorem in the next section, is the starting point of 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 for modules over Witt vectors. Choosing a basis for these is often misleading- except, perhaps, in some proofs.

Since Hilbert's Theorem 90 is central in this paper, we decided to discuss, in this section, some of its most significant algebraic incarnations. They are probably folklore for some mathematicians. They make 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 . Before proceeding any further, we wish to remind the reader that Hilbert's Theorem 90 (for \mathbb{G}_m) is actually due to Kummer for cyclic field extensions, and that its generalization to arbitrary Galois extensions is due to Noether.

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

LEMMA 15.1. *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 15.2. *Let A be a Noetherian local ring. Let A'/A be a faithfully 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 that $S = M_n(D)$ 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 15.3. 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 $\text{Spec}(A)$, for the fppf topology, correspond to S -modules M as in the previous Lemma. We thus get

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

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

PROPOSITION 15.4. *Let A be a Noetherian local ring. Let A'/A be a faithfully 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

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

it is an A -algebra. It is a subalgebra of $\text{End}_A(N)$. Writing N as a quotient of a free module A^n , $\text{End}_A(N)$ 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

$$S' \longrightarrow \{f' \in \text{End}_{R'}(N'), f'(M'_1) \subset M'_1\}$$

is an isomorphism. The set

$$X := \{f' \in \text{GL}_{R'}(N'), f'(M'_1) = M'_1\}$$

is endowed with a simply transitive action of the multiplicative group S'^{\times} . As such (see Lemma 15.1), 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 $f \in \text{GL}_R(N)$ such that $f(M_1) = M_2$). We conclude by applying Lemma 15.2.

□

COROLLARY 15.5. *Let A be a Noetherian local ring. Let A'/A be a faithfully 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 $M \oplus N$. □

Remark 15.6. 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).

Remark 15.7. In all what precedes, the Noetherian assumptions may probably be dropped. They are here to simplify the proofs.

16. THE STABLE LIFTING THEOREMS.

In this section, k is a finite field of cardinality $q = p^r$ and G is a profinite group. We use small Omega powers here: we believe they are better behaved than medium (or big) Omega powers, for applications in Galois theory.

Let us explain how we intend to apply small Omega powers to prove Lifting Theorems in Galois cohomology- with an explicit proof of the Bloch-Kato conjecture as a main motivation.

Assume that G is s -smooth, and denote by \mathcal{T} a fixed s -cyclotomic G -module, of infinite depth.

Let V be a (k, G) -module, and let n be a nonnegative integer. Almost by definition of smoothness, we have that the (twist of) Frobenius

$$\text{Frob}(s) : \underline{\Omega}^{n+1}(V)(s) \longrightarrow \underline{\Omega}^n(V^{(1)})(s)$$

is s -surjective, if V is one-dimensional. Indeed, we can reduce to the case where G is a pro- p -group. For such a G , any one-dimensional V is isomorphic to the trivial (k, G) -module k , and the statement becomes nothing but the definition of s -surjectivity. It is then legitimate to wonder whether the same holds for an arbitrary (k, G) -module V . The next exercise shows that it is not the case in general. This is deeply related to the notion of R -equivalence, due to Manin.

Exercise 16.1. Let F be an infinite field of characteristic not p , with separable closure F_{sep}/F . Assume for simplicity that F contains the p^2 -th roots of unity. We denote by $H_{et}^1(., .)$ the first étale cohomology groups. In this exercise and in this exercise only, $s = 1$, $G := \text{Gal}(F_{sep}/F)$ and

$$\mathcal{T} := \mathbb{Z}/p^2\mathbb{Z}.$$

By Proposition 14.19, we know that \mathcal{T} is a 1-cyclotomic G -module.

In view of the assumptions, we can remove all twists (by Frobenius, and by roots of unity).

Let V be a finite commutative algebraic F -group of multiplicative type, killed by p . We shall identify V with the (\mathbb{F}_p, G) -module $V(F_{sep})$.

A cohomology class $c \in H_{et}^1(\text{Spec}(F), V) = H^1(G, V)$ is said to be (elementarily) R -trivial if the following holds. There exists an open subvariety $U \subset \mathbb{A}_F^1$, containing 0 and 1, and a class

$$C \in H_{et}^1(U, V),$$

whose specialization at 0 (resp at 1) is trivial (resp. equals c).

1) Assume that V has dimension one. Show that every class in $c \in H^1(G, V)$ is R -trivial.

Hint: reduce to the case $V = \mu_p$, and use Kummer theory.

2) Assume that the map

$$\text{Frob} : \underline{\Omega}^1(V) \longrightarrow V$$

is 1-surjective, for every V as above. Show that every element in $H^1(G, V)$ would then be R -trivial.

Hint: induction on the dimension of V , using the Frobenius Integral formula 11.18, and Shapiro's Lemma.

3) Using the work of Colliot-Thélène and Sansuc ([CTS]), give an example of a field F and of a V as above, such that not every class in $H_{et}^1(\text{Spec}(F), V)$ is R -trivial. Conclude.

4) Let $c \in H^1(G, V)$ be a Galois cohomology class, which is R -trivial. It is true that c is in the image of

$$\text{Frob}_* : H^1(G, \underline{\Omega}^1(V)) \longrightarrow H^1(G, V) ?$$

Hint: we don't know the answer...

The following Lifting Theorem brings hope that our approach will shortly lead to an 'elementary' proof of the Bloch-Kato conjecture. Note that, if this Theorem was true for $n = 0$ and V arbitrary, Galois cohomology would be much simpler, and the Bloch-Kato conjecture would follow quite easily.

THEOREM 16.2. (*First Stable Lifting Theorem.*)

Let V be a d -dimensional (k, G) -module. Let n be a positive integer, with

$$n \geq r(d-1) - 1.$$

Let t be an arbitrary positive integer.

The following assertions are true.

1) *The Frobenius homomorphism*

$$\text{Frob}^t : \underline{\Omega}^{n+t}(V) \longrightarrow \underline{\Omega}^n(V^{(t)})$$

is of Kummer type, of depth $\leq n+t$.

2) *If \mathcal{T} is an s -cyclotomic G -module of depth $n+t$, then the twist*

$$\text{Frob}(s) : \underline{\Omega}^{n+t}(V)(s) \longrightarrow \underline{\Omega}^n(V^{(t)})(s)$$

is s -surjective.

Proof. We prove part 1); part 2) will follow by Proposition 14.34.

The assertions are clear if V is one-dimensional, by the very definition of surjections of Kummer type. We can thus assume that $d \geq 2$.

Now, consider the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \underline{\Omega}^{n+t}(V)[p^t] & \longrightarrow & \underline{\Omega}^{n+t}(V) & \xrightarrow{\text{Frob}^t} & \underline{\Omega}^n(V^{(t)}) & \longrightarrow & 0 \\ & & \downarrow g & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \bigoplus_H \underline{\Omega}^{n+t}(V/H)[p^t] & \longrightarrow & \bigoplus_H \underline{\Omega}^{n+t}(V/H) & \xrightarrow{\bigoplus \text{Frob}_{V/H}} & \bigoplus_H \underline{\Omega}^n((V/H)^{(t)}) & \longrightarrow & 0, \end{array}$$

where the direct sums are taken over all k -rational hyperplanes $H \subset V$, and the vertical arrows are obtained by functoriality from the quotient maps $V \rightarrow V/H$. The Pontryagin dual of the map g is the map f of Proposition 13.10 (applied to V^* , $n+t$ and $m=t$). Since $n \geq r(d-1) - 1$, the same Proposition asserts that f , hence g , is an isomorphism.

Point 1) now follows, from the definition of a surjection of Kummer type: the lower row is induced from dimension one (the open subgroups involved are the stabilizers of hyperplanes of V). \square

The next Theorem is more precise: it asserts that the cohomology of a smooth profinite group, with values in a (twist of a) G -module of the type $\underline{\Omega}^n(V)$, is induced from dimension one, if n is large enough.

THEOREM 16.3. (*Second Stable Lifting Theorem.*) Let V be a d -dimensional (k, G) -module, with $d \geq 2$.

Let n be a positive integer, with

$$n \geq r(d-1) - 1.$$

For each line $L \in \mathbb{P}(V)$, functoriality of Omega powers yields a canonical injection

$$\underline{\Omega}^n(L) \longrightarrow \underline{\Omega}^n(V).$$

Then the following assertions are true.

1) The (surjective) G -equivariant map

$$\bigoplus_{L \in \mathbb{P}(V)} \underline{\Omega}^n(L) \longrightarrow \underline{\Omega}^n(V)$$

is of Kummer type (of depth $\leq n + r(d - 1)$).

2) If \mathcal{T} is an s -cyclotomic G -module of depth $n + r(d - 1)$, then the twisted G -equivariant map

$$\bigoplus_{L \in \mathbb{P}(V)} \underline{\Omega}^n(L)(s) \longrightarrow \underline{\Omega}^n(V)(s)$$

is s -surjective.

Proof. We prove part 1); part 2) will follow by Proposition 14.34.

By the previous Theorem, for $t = r(d - 1)$, we see that the map

$$\text{Frob}^{r(d-1)} : \underline{\Omega}^{n+r(d-1)}(V) \longrightarrow \underline{\Omega}^n(V)$$

is of Kummer type, of depth $\leq n + r(d - 1)$. By the Frobenius Integral formula 13.11, this map factors as

$$\underline{\Omega}^{n+r(d-1)}(V) \longrightarrow \bigoplus_{L \subset V} \underline{\Omega}^n(L) \longrightarrow \underline{\Omega}^n(V),$$

where the direct sum is taken over all lines $L \subset V$, and the first map is the sum of the Transfers, for all inclusions $L \subset V$. The claim follows, by the definition of a surjection of Kummer type. \square

The preceding Theorem has a very concrete consequence, for cohomology classes with values in two-dimensional Galois representations, over \mathbb{F}_p .

COROLLARY 16.4. *Let F be a field of characteristic not p . Denote by F_{sep}/F a separable closure of F . Let V be a two-dimensional Galois representation of $G := \text{Gal}(F_{\text{sep}}/F)$ over \mathbb{F}_p . For each $v \in V$, denote by $G_v \subset G$ the stabilizer of v . Denote by ϕ_v the composite*

$$H^1(G_s, \mathbb{F}_p) \longrightarrow H^1(G_s, V) \xrightarrow{\text{Cor}_{G_s}^G} H^1(G, V),$$

where the first map is induced by functoriality from the G_s -equivariant map

$$\mathbb{F}_p \xrightarrow{1 \mapsto v} V.$$

Then the map

$$\bigoplus_{v \in V} H^1(G_s, \mathbb{F}_p) \xrightarrow{\oplus \phi_v} H^1(G, V)$$

is surjective.

In other words, classes in $H^1(G, V)$ are 'induced from dimension one'.

Proof.

The statement is the concrete form of Theorem 16.3, for $\mathcal{T} = \mu_{p^2}$ (which is 1-smooth by Kummer theory), $s = 1$, $r = 1$, $d = 2$ and $n = 0$. \square

Exercise 16.5. Show that, for $p = 2$, the preceding Corollary is true for any profinite group G , and any two-dimensional (\mathbb{F}_2, G) -module.

17. AN APPLICATION TO p -ADIC DEFORMATION THEORY.

We finish this paper with an application of our point of view to p -adic deformation theory. It uses very few of the theory of Omega powers that we have explained before. In truth, it uses only the divided power functor $\Gamma_{\mathbb{Z}}^p$, for \mathbb{Z} -modules of p -primary torsion.

Recall that we have seen that p -typical Witt vectors of level n may be defined, in a pretty elementary way, as a quotient of a divided power module over \mathbb{Z} (cf. Proposition 6.8).

In this section, we give another elementary application of this point of view, to the problem of lifting \mathbb{F}_p -algebras to flat $(\mathbb{Z}/p^2\mathbb{Z})$ -algebras.

17.1. THE CASE OF PERFECT \mathbb{F}_p -ALGEBRAS.

DEFINITION 17.1. *A p -nice ring is a commutative ring R , satisfying the following three conditions.*

- i) The ring R is p -adically complete (i.e. complete with respect to the ideal $pR \subset R$).*
- ii) p is not a zero-divisor in R , i.e. R is torsion-free.*
- iii) The \mathbb{F}_p -algebra R/p is perfect, i.e. its Frobenius*

$$\begin{aligned} \text{Frob} : R/p &\longrightarrow R/p \\ x &\mapsto x^p \end{aligned}$$

is an isomorphism.

Recall the following result in p -adic deformation theory, well-known to experts.

PROPOSITION 17.2. *The reduction functor*

$$\begin{aligned} \Phi : \{p\text{- nice rings}\} &\longrightarrow \{\text{perfect } \mathbb{F}_p\text{- algebras}\}, \\ \mathcal{A} &\mapsto \mathcal{A}/p \end{aligned}$$

is an equivalence of categories (morphisms being ring homomorphisms on both sides).

Proof. The usual proof of this Proposition is through Illusie's cotangent complex, as explained in the work of Scholze ([S], Theorem 5.11 and Theorem 5.12). \square

It is possible to give a direct elementary proof of the preceding Proposition, using merely the functor $\Gamma_{\mathbb{Z}}^p$. Rather than giving more details, we prefer to state and prove a statement which is much more general- but, for the time being, for mod p^2 liftings only.

17.2. DESCENT FOR THE ARROW $\mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$. In Proposition 17.2, the crucial assumption is that the Frobenius map of R/p is surjective. The fact that it is injective (i.e. that R/p is reduced) is secondary. The authors believe that it is important to adapt this Proposition to the case of (possibly non reduced) \mathbb{F}_p -algebras whose Frobenius map is surjective. In a naive sense, these algebras are 'Frobenius-smooth' objects (existence of lifts by Frobenius), whereas perfect \mathbb{F}_p -algebras are "Frobenius-étale" objects (existence and uniqueness of lifts by Frobenius). To tackle this question, today's trend is to use Scholze's theory of perfectoid spaces, in which these algebras typically occur. We here suggest a first step towards an alternate approach, in the spirit of our paper: Proposition 17.9.

Its content is that deforming an \mathbb{F}_p -algebra A , whose Frobenius is surjective, to a flat $(\mathbb{Z}/p^2\mathbb{Z})$ -algebra \mathcal{A} , is equivalent to endowing the kernel of the Frobenius of A with a partial (level p) divided power operation $\gamma_p : I \rightarrow A$. Moreover, the Frobenius of A lifts to \mathcal{A} if, and only if, γ_p takes values in I .

DEFINITION 17.3. *Let R be a commutative ring in which $(p-1)!$ is invertible. For any integer i with $0 \leq i \leq p-1$ and $x \in R$, we set*

$$\gamma_i(x) := \frac{1}{i!}x^i.$$

DEFINITION 17.4. *A 2-wrinkled ring (relative to p) is the data of a pair (A, γ_p) , consisting of an \mathbb{F}_p -algebra A , whose Frobenius is surjective, and a map*

$$\gamma_p : \text{Ker}(\text{Frob}_A) \rightarrow A,$$

such that the relations

$$\gamma_p(ax) = a^p\gamma_p(x)$$

and

$$\gamma_p(x+x') = \sum_{i+i'=p} \gamma_i(x)\gamma_{i'}(x'),$$

hold for all $a \in A$ and all x, x' in $\text{Ker}(\text{Frob})$.

2-wrinkled rings obviously form a category: a morphism $(A, \gamma_p) \rightarrow (A', \gamma'_p)$ is a ring homomorphism $\phi : A \rightarrow A'$, such that $\gamma'_p \circ \phi = \phi \circ \gamma_p$.

Remark 17.5. Let (A, γ_p) be a 2-wrinkled ring. Put $I := \text{Ker}(\text{Frob}_A)$.

It is not hard to see that γ_p vanishes on I^2 , and that it is in fact given by a unique polynomial law of A -modules, which is homogeneous of degree p , from I/I^2 to A .

DEFINITION 17.6. *Denote by \mathcal{F}_2 the forgetful functor, from the category of 2-wrinkled rings to that of \mathbb{F}_p -algebras.*

A 2-liftable ring (relative to p) is an \mathbb{F}_p -algebra A , which lies in the essential image of \mathcal{F}_2 .

Remark 17.7. Note that a non-reduced (i.e. non-perfect) 2-liftable ring is not Noetherian (a surjective endomorphism of a Noetherian ring is an isomorphism...).

DEFINITION 17.8. *A 2-flat ring (relative to p) is a commutative $(\mathbb{Z}/p^2\mathbb{Z})$ -algebra R , satisfying the following conditions.*

i) R is a flat (i.e. free) $\mathbb{Z}/p^2\mathbb{Z}$ -module.

ii) The Frobenius map of R/p is surjective.

The 2-flat rings form a category, with morphisms been ring homomorphisms.

Let \mathcal{A} be a 2-flat ring. Put

$$A := \mathcal{A}/p.$$

We shall now see that A can be given the structure of a 2-wrinkled ring in a canonical way.

Put

$$I := \text{Ker}(\text{Frob}_A).$$

Let x be an element of the ideal I . Let $X \in \mathcal{A}$ be any lift of x . The quantity $X^p \in \mathcal{A}$ does not depend on the choice of X (cf. Lemma 6.1). By assumption, there exists $Y \in \mathcal{A}$ such that

$$X^p = pY.$$

Denote by $y \in A$ the reduction of Y . Since \mathcal{A} is a free $(\mathbb{Z}/p^2\mathbb{Z})$ -module, y does not depend on the choice of Y . We then put

$$\gamma_p(x) := \frac{1}{(p-1)!}y = -y \in A.$$

It is not hard to see that (A, γ_p) is a 2-wrinkled ring.

We have in fact built a functor

$$\Psi_2 : \{2\text{-flat rings}\} \longrightarrow \{2\text{-wrinkled rings}\},$$

by the formula

$$\Psi_2(\mathcal{A}) := (A, \gamma_p).$$

We can then prove the following result, which is a descent statement for the quotient map

$$\mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

It generalizes Proposition 17.2 (for mod p^2 deformations). Note that this Proposition may seem strange at first glance: the quotient map $\mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ is not quite flat, and descent statements in algebraic geometry are often the privilege of faithfully flat morphisms. However, the categorical data that allows descent here is not at all the usual one (it is non-linear).

PROPOSITION 17.9. *The functor Ψ_2 is an equivalence of categories. In particular, every 2-wrinkled ring admits a unique lift to a 2-flat ring.*

Proof.

Let \mathcal{A} be a 2-flat ring. Put $A = \mathcal{A}/p$. Denote by

$$\gamma_p : \text{Ker}(\text{Frob}_A) \longrightarrow A$$

the p -th divided power operation constructed above.

We know, by Lemma 6.1, that the polynomial law of \mathbb{Z} -modules

$$\begin{aligned} \mathcal{A} &\longrightarrow \mathcal{A}, \\ X &\mapsto X^p \end{aligned}$$

factors through the quotient map $\pi : \mathcal{A} \longrightarrow A$, yielding by the universal property of divided powers a group homomorphism

$$\begin{aligned} F : \Gamma_{\mathbb{Z}}^p(A) &\longrightarrow \mathcal{A}, \\ [\pi(X)]_p &\mapsto X^p. \end{aligned}$$

Note that pure symbols generate $\Gamma_{\mathbb{Z}/p^2\mathbb{Z}}^p(A) = \Gamma_{\mathbb{Z}/p^2\mathbb{Z}}^p(A)$, by Lemma 6.13. The group $\Gamma_{\mathbb{Z}}^p(A)$ bears a natural ring structure (formula on pure symbols: $[x]_p[y]_p = [xy]_p$), for which F is a ring homomorphism. Since the Frobenius of A is surjective, it is easily checked that F is onto. Let X_1, \dots, X_m be elements of \mathcal{A} , with reductions x_1, \dots, x_m in A . One has

$$[x_1]_p + \dots + [x_m]_p \in \text{Ker}(F)$$

if and only if

$$X_1^p + \dots + X_m^p = 0 \in \mathcal{A}.$$

Rewrite this equality as

$$(X_1 + \dots + X_m)^p = p \sum_{a_1, \dots, a_m} C_{a_1, \dots, a_m} X_1^{a_1} \dots X_m^{a_m} \in \mathcal{A},$$

where the sum ranges over all proper partitions of p , i.e. partitions

$$p = a_1 + \dots + a_m,$$

with $0 \leq a_i \leq p - 1$ for all i , and where

$$C_{a_1, \dots, a_m} := \frac{1}{p} \binom{p}{a_1, \dots, a_m} \in \mathbb{N}.$$

By the very definition of γ_p , this is equivalent to the combination of the two equalities

$$x_1 + \dots + x_m \in \text{Ker}(\text{Frob}_A)$$

and

$$-\gamma_p(x_1 + \dots + x_m) = \sum_{a_1, \dots, a_m} C_{a_1, \dots, a_m} x_1^{a_1} \dots x_m^{a_m} \in A.$$

The isomorphism $\Gamma_{\mathbb{Z}}^p(A)/\text{Ker}(F) \simeq \mathcal{A}$ thus yields a canonical presentation of \mathcal{A} , depending only on A and γ_p . We infer that Ψ_2 is fully faithful.

It remains to be shown that it is essentially surjective. To prove this, we first reset notation. Let (A, γ_p) be an arbitrary 2-wrinkled ring. We denote by

$$\mathcal{I} \subset \Gamma_{\mathbb{Z}}^p(A)$$

the subset consisting of elements X which can be written as

$$X = [x_1]_p + \dots + [x_m]_p,$$

where $x_1, \dots, x_m \in A$ are such that

$$x_1 + \dots + x_m \in \text{Ker}(\text{Frob}_A)$$

and

$$-\gamma_p(x_1 + \dots + x_m) = \sum_{a_1, \dots, a_m} C_{a_1, \dots, a_m} x_1^{a_1} \dots x_m^{a_m} \in A,$$

where the sum ranges over all proper partitions of p . From the equality

$$\gamma_p(x + x') = \sum_{i+i'=p} \gamma_i(x) \gamma_{i'}(x'),$$

which holds for all $x, x' \in \text{Ker}(\text{Frob}_A)$, we see that \mathcal{I} is in fact a subgroup of $\Gamma_{\mathbb{Z}}^p(A)$. It is thus an ideal of \mathcal{I} . We put

$$\mathcal{A} := \Gamma_{\mathbb{Z}}^p(A)/\mathcal{I}.$$

The surjection of rings

$$\begin{aligned} f : \Gamma_{\mathbb{Z}}^p(A) &\longrightarrow A, \\ [x]_p &\longmapsto x^p, \end{aligned}$$

clearly factors through \mathcal{I} , yielding a surjective ring homomorphism

$$\pi : \mathcal{A} \longrightarrow A.$$

Pick an element $X \in \text{Ker}(\pi)$. Write it as

$$X = [x_1]_p + \dots + [x_m]_p,$$

where $x_1, \dots, x_m \in A$. We have

$$x_1 + \dots + x_m \in \text{Ker}(\text{Frob}_A).$$

Choose $x_{m+1} \in A$ such that

$$x_{m+1}^p = \gamma_p(x_1 + \dots + x_m) \in A.$$

Then one has

$$[x_1]_p + \dots + [x_m]_p + p[x_{m+1}]_p \in \mathcal{I}$$

(verification left to the reader). We conclude that $X \in p\mathcal{A}$. Therefore, we have

$$\text{Ker}(\pi) = p\mathcal{A}.$$

Now, pick an element $Y \in \mathcal{A}[p]$. Write it as

$$Y = [y_1]_p + \dots + [y_m]_p,$$

where $y_1, \dots, y_m \in A$. From the equality

$$p[y_1]_p + \dots + p[y_m]_p \in \mathcal{I},$$

we see (by definition of \mathcal{I}) that

$$y_1^p + \dots + y_m^p = 0 \in A.$$

Hence Y belongs to $\text{Ker}(\pi) = p\mathcal{A}$. Altogether, we see that

$$\mathcal{A}[p] = p\mathcal{A},$$

i.e. that \mathcal{A} is a free $(\mathbb{Z}/p^2\mathbb{Z})$ -module. The ring \mathcal{A} is thus a 2-flat ring, with a canonical isomorphism $\mathcal{A}/p \simeq A$. From the definition of \mathcal{I} , it is straightforward to check that

$$\Psi(\mathcal{A}) = (A, \gamma_p),$$

which finishes the proof. □

Remark 17.10. The descent statement of the previous Proposition has a clear analogue in the classical context of (quasiprojective) complex varieties, as follows. It is standard that a complex variety may be view as a real variety, of double dimension. This is a simple form of Weil's restriction of scalars. It is also standard that the data of an anti-involution on a complex variety Y is equivalent to giving a real variety X and an isomorphism $Y \simeq X \times_{\mathbb{R}} \mathbb{C}$ of complex varieties. This is a simple (linear) descent statement.

Let us now switch to the p -adic setting. Then Greenberg's functor allows to consider a scheme over $\mathbb{Z}/p^2\mathbb{Z}$ as a scheme over \mathbb{F}_p , of double dimension. This is, in some sense, a non-linear analogue of Weil's scalar restriction, in which $\mathbb{Z}/p^2\mathbb{Z}$ (resp. \mathbb{F}_p) plays the rôle of \mathbb{C} (resp. \mathbb{R}).

Proposition 17.9 is then an analogue of the simple descent statement above, for the morphism $\mathbb{Z}/p^2\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$. But roles are exchanged in this second analogy: $\mathbb{Z}/p^2\mathbb{Z}$ now plays that of \mathbb{R} , whereas \mathbb{F}_p plays that of \mathbb{C} ! In a daring poetic sense, Proposition 17.9 is both a descent result and a lifting result: it just depends in which direction you choose to look...

We are grateful to Luc Illusie for his remarks, which led to the following improvement.

PROPOSITION 17.11. *Let \mathcal{A} be a 2-flat ring, corresponding to the 2-wrinkled ring (A, γ_p) (cf. Proposition 17.9).*

Denote by $I \subset A$ the kernel of the Frobenius homomorphism. Then the following conditions are equivalent.

- i) The Frobenius of A admits a (unique) lift to a (surjective) endomorphism of the ring \mathcal{A} .
 ii) The divided power operation $\gamma_p : I \rightarrow A$ takes values in I .

If these conditions are fulfilled, then there exists a unique structure of PD-ideal on I , with γ_p as p -th divided power operation.

Proof. By the preceding Proposition, i) holds if and only if the Frobenius of A commutes with γ_p . This is obviously equivalent to γ_p taking its values in I , qed. The last assertion follows from the fact that a divided power structure on an ideal, in our context, is uniquely determined by the data of γ_p , see for instance Stacks Project, Tag 07H4, Lemma 23.5.3. \square

Exercise 17.12. Let A be a 2-liftable ring. Put

$$I := \text{Ker}(\text{Frob}_A).$$

- 1) Show that the set of maps

$$\gamma_p : I \rightarrow A$$

such that (A, γ_p) is a 2-wrinkled ring is a principal homogeneous space of $\text{Hom}_{\text{Frob}}(I/I^2, A)$.

- 2) How is 1) connected to Illusie's theory of the cotangent complex?

Assume now that $I = I^2$, and that (A, γ_p) is a 2-wrinkled ring.

- 3) Show that $\gamma_p = 0$.
 4) Deduce that $I^p = 0$, hence that A is a perfect \mathbb{F}_p -algebra.

The generalisation of Proposition 17.9 to higher level descent statements is left to future considerations.

ACKNOWLEDGEMENTS

We are grateful to Patrick Brosnan for his support, and for spotting a mistake in the last part of the previous version of this paper, one year ago. We owe thanks to Michel Brion for precious comments on the first (correct) part of the previous version. We thank Ján Mináč for his kind and enthusiastic support. We thank Pierre Guillot and Fabien Morel for interesting discussions.

BIBLIOGRAPHY

- [CTS] COLLIOT-THÉLÈNE, J.-L., SANSUC, J.-J.— *La R-équivalence sur les tores*, Ann. sci. ÉNS 10 (1977), no. 2, 175-229.
 [EM] S. ENDÔ, T. MIYATA— *Integral representations with trivial first cohomology groups*, Nagoya Math. J. 85 (1982), 231-240.
 [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.

- [J] J. C. JANTZEN.— *Representations of algebraic groups. Second edition.*, Math. surveys and monographs 107, AMS (2003).
- [K1] D. KALEDIN.— *Witt vectors as a polynomial functor*, preprint, available on the arXiv server.
- [K2] D. KALEDIN.— *Witt vectors, commutative and non-commutative*, preprint, available on the arXiv server.
- [Ro] N. ROBY.— *Lois polynomes et lois formelles en théorie des modules*, Ann. Sci. ÉNS (3) 80 (1963), 213-348.
- [St] G. S. STÅHL.— *An Intrinsic Definition of the Rees Algebra of a Module*, Proc. Edinburgh Math. Soc. (2), to appear.
- [S] P. SCHOLZE.— *Perfectoid spaces*, Pub. Math. IHÉS 116 (2012), 245-313.
- [Se] J.-P. SERRE.— *Galois cohomology*, Springer-Verlag, 2002.
- [Sm] L. SMITH.— *An algebraic introduction to the Steenrod algebra*, Geo. & Top. Monographs 11 (2007), 327-348.
- [Vo] V. VOEVODSKY.— *On motivic cohomology with \mathbb{Z}/l -coefficients*, Ann. of Math. 174 (2011), 401-438.
- [Vos] V.E. VOSKRESENSKII.— *Algebraic groups and their birational invariants*, Trans. Math. Mono. AMS 179 (1998).

CHARLES DE CLERCQ, EQUIPE TOPOLOGIE ALGÈBRIQUE, LABORATOIRE ANALYSE, GÉOMÉTRIE ET APPLICATIONS, UNIVERSITÉ PARIS 13, 93430 VILLETANEUSE.

MATHIEU FLORENCE, EQUIPE DE TOPOLOGIE ET GÉOMÉTRIE ALGÈBRIQUES, INSTITUT DE MATHÉMATIQUES DE JUSSIEU, UNIVERSITÉ PIERRE ET MARIE CURIE, 4, PLACE JUSSIEU, 75005 PARIS.