p-ADIC COHOMOLOGY THEORIES AND POINT COUNTING (UNFINISHED DRAFT VERSION 2023.6.26.909)

RUBÉN MUÑOZ--BERTRAND

Abstract. These notes contain an introduction to Monsky–Washnitzer cohomology, and to the algorithm of Kedlaya which counts points on hyperelliptic curves in odd characteristic.

At the end of 2022, I gave an eight-hour mini-course at the Université Toulouse III - Paul Sabatier entitled "*Théories cohomologiques p-adiques et comptage de points*". These notes contains an extended version of the lecture.

The ultimate goal of this paper is to present Kedlaya's algorithm in its original form [Ked]. This algorithm computes the number of points on an hyperelliptic curve over a finite field of characteristic $p \geqslant 3$. To achieve this, it employs a tool called p-adic cohomology.

There exists numerous variants of p-adic cohomology, and providing a full exposition would be an impossible task for a mini-course. Here, we will rather focus on two of the most explicit p-adic cohomology theories: Monsky–Washnitzer and overconvergent de Rham–Witt cohomology. We will give proofs of some standard theorems which will be necessary for the algorithm.

The construction of these theories is inspired from results in differential topology. By combining Lefschetz–Hopf and de Rham theorems, we have in modern terms the following result.

Theorem. *Let $n \in \mathbb{N}$. Let X be a compact, smooth n-manifold with boundary. Let $f\colon X \to X$ be a smooth map. Denote by $\operatorname{Fix}(f)$ the set of fixed points of f.*

Suppose that these fixed points are all isolated, and that none of them lays on the boundary of X. For all $x \in \operatorname{Fix}(f)$, we let $i_f(x)$ be the fixed point index of f at x.

Then, we have the following formula using the de Rham cohomology of X:

$$\sum_{x \in \operatorname{Fix}(f)} i_f(x) = \sum_{i=0}^{n} (-1)^i \operatorname{tr}\left(H^i_{\mathrm{dR}}(f)\right).$$

Proof. See [RS, theorem 4.4.2] for the proof and terminology. □

Roughly, the idea is to get a similar result when X is a smooth scheme over a perfect field of positive characteristic, and when f is related to the Frobenius endomorphism. The difficulty resides in the definition of a suitable complex a la de Rham.

In the first part, we will first see why the naive definitions of the de Rham complex fail to provide such a formula. We then introduce Monsky–Washnitzer cohomology to get around the problems we shall encounter.

In the last part of this paper, we describe Kedlaya's algorithm.

This paper targets a wide audience of mathematicians, but we still assume that the reader has some background. For instance, it is necessary for them to be familiar with the algebraic de Rham complex [Sta, 0FKF], and with the theory of smooth morphisms of schemes [Sta, 01V5]. We also presume that they know how the cohomology groups of a cochain complex are defined [Sta, 010V], and what adic topologies are [Sta, 07E8]. By now, it should be clear that we will often rely on [Sta] to reference some basic facts, in hope that it will make the reading more accessible.

Part 1. Monsky–Washnitzer cohomology

The cohomology theory we are about to define was introduced by Monsky and Washnitzer in [MW]. Their aim was to give a cohomological interpretation of Dwork's work.

Throughout this section, p is any prime number.

1.1. Naive de Rham cohomology

Let us first explain why we cannot simply use the algebraic de Rham cohomology of a scheme X over a perfect field of characteristic p.

Example 1.1.1. Simply consider the commutative $\mathbb{F}_p$-algebra $\mathbb{F}_p[X]$. Then the algebraic de Rham complex can be interpreted as:

$$\cdots \longrightarrow 0 \longrightarrow \mathbb{F}_p[X] \xrightarrow{\frac{\partial}{\partial X}} \mathbb{F}_p[X] \longrightarrow 0 \longrightarrow \cdots \tag{1.1.2}$$

Remember that our main goal is to have a formula similar to Lefschetz–Hopf theorem, that is, using traces. In particular, we want our cohomology spaces to be finite dimensional vector spaces.

Here, the associated cohomology spaces are obviously infinite dimensional. Indeed for each $n \in \mathbb{N}$, we have:

$$X^{p^n-1}\frac{\partial}{\partial X}(X) \neq 0,$$
$$\frac{\partial}{\partial X}\left(X^{p^n}\right) = 0.$$

So it is clear from the beginning that we have to work in characteristic zero. Before we explain how we proceed in general, let us just consider the case where our base field is $\mathbb{F}_p$. The obvious characteristic zero p-adic candidate for the base ring is $\mathbb{Z}_p$.

In all this course, we are going to be working with lifts.

Definition 1.1.3. Let V be a commutative ring, and let I be an ideal of V. Let $\overline{A}$ be a commutative V/I-algebra. A **lift of** $\overline{A}$ is a commutative V-algebra A such that $\overline{A} \cong A \otimes_V V/I$ as V-algebras.

We say that such a lift is **flat** (respectively **smooth**) when the structural morphism $V \to A$ is flat (respectively smooth).

Similarly, if $\overline{F}\colon \overline{A} \to \overline{B}$ is a morphism of commutative V/I-algebras, and if A and B are two respective lifts of $\overline{A}$ and $\overline{B}$, then a **lift of** $\overline{F}$ is a morphism $F\colon A \to B$ of V-algebras such that $\overline{F} \cong F \otimes_V V/I$ as morphisms of V-algebras.

Of course, these definitions depend on the choices of V and I, but in context in will always be clear what our base ring is. In the examples that follow, we will only be working with $V = \mathbb{Z}_p$ and $I = \langle p \rangle$.

However, even in that simple case, lifting leads to infinite dimensional cohomology groups.

Example 1.1.4. Let us consider again $\mathbb{F}_p[X]$, with lift $\mathbb{Z}_p[X]$. The de Rham complex associated with $\mathbb{Z}_p[X]$ is:

$$\cdots \longrightarrow 0 \longrightarrow \mathbb{Z}_p[X] \xrightarrow{\frac{\partial}{\partial X}} \mathbb{Z}_p[X] \longrightarrow 0 \longrightarrow \cdots \tag{1.1.5}$$

This time, the kernel of $\frac{\partial}{\partial X}$ is just $\mathbb{Z}_p$. But in the cokernel, for all $n \in \mathbb{N}^*$ the element $X^{p^n-1}\frac{\partial}{\partial X}(X)$ is a non zero element with p^n-torsion. So again, we get an infinitely generated cohomology group in degree 1.

To get rid of these torsion elements, we tensor our complex with $\mathbb{Q}$; or in other words, we invert p.

Before we carry on with yet another problematic example, let us just comment in this paragraph that you have just read a lie. The real problem here is that the morphism of schemes $\operatorname{Spec}(\mathbb{F}_p[X]) \to \operatorname{Spec}(\mathbb{F}_p)$ is not proper. In crystalline cohomology, one has actually a p-adic cohomology theory with finite dimensional $\mathbb{Z}_p$-modules for proper and smooth schemes over $\mathbb{F}_p$, amongst other base fields, in which p-torsion play an important role [Ber74]. This goes however far beyond the scope of this course, so let us go back to our quest for finite dimensional vector spaces associated to any smooth scheme over a perfect field of characteristic p.

We stumble on another problem: there are infinitely many lifts for a ring of positive characteristic to characteristic zero, thus leading to different de Rham complexes and cohomologies; and this also happens when one consider smooth lifts.

Example 1.1.6. We will consider two smooth lifts of $\mathbb{F}_p[X]$, namely $\mathbb{Z}_p[X]$ and $A := \mathbb{Z}_p[T,X] / \langle pTX + T - 1\rangle$.

To see that the second lift is indeed smooth, use [Sta, 00T7] by noticing that $\frac{\partial}{\partial T}(pTX + T - 1) = pX + 1$, so that $(pX+1)T = 1$ in A.

We first invert p in the de Rham complex (1.1.5), and we get:

$$\cdots \longrightarrow 0 \longrightarrow \mathbb{Q}_p[X] \xrightarrow{\frac{\partial}{\partial X}} \mathbb{Q}_p[X] \longrightarrow 0 \longrightarrow \cdots$$

It is easy to notice that $\frac{\partial}{\partial X}$ is surjective, hence the H^1 associated to this complex is reduced to $\{0\}$.

Let us now turn to A. We will be working in $A \otimes_{\mathbb{Z}} \mathbb{Q}$, which is isomorphic as a $\mathbb{Q}_p$-algebra to $\mathbb{Q}_p[T,X] / \langle pTX + T - 1\rangle$. For that reason, any element in $A \otimes_{\mathbb{Z}} \mathbb{Q}$ as a unique representative of the form:

$$P(T) + Q(X) \in \mathbb{Q}_p[T,X], \tag{1.1.7}$$

with $P(T) \in \mathbb{Q}_p[T]$ satisfying $P(0) = 0$ and $Q(X) \in \mathbb{Q}_p[X]$.

Indeed, if $S(T,X) \in \mathbb{Q}_p[T,X]$ has a monomial of the form T^aX^b with $a, b \in \mathbb{N}^*$, then one can replace it with $\frac{1}{p}\left(T^{a-1}X^{b-1} - T^aX^{b-1}\right)$ now that p is invertible in $A \otimes_{\mathbb{Z}} \mathbb{Q}$ to get a new representative for the same class. Repeating the process removes all the monomials divided by TX as wanted.

As of unicity, notice that if $P(T) + Q(X) = (pTX + T - 1)\,S(T,X)$ for some $S(T,X) \in \mathbb{Q}_p[T,X]$, then if $S(T,X) \neq 0$ the monomials with the highest total degree in $P(T) + Q(X)$ must be divisible by TX, which is impossible.

Now, compute in $\Omega^1_{A/\mathbb{Z}_p} \otimes_{\mathbb{Z}} \mathbb{Q}$:

$$\begin{aligned} d(T) &= d(T \times 1) \\ &= d(T \times (pTX + T)) \\ d(T) &= 2pTXd(T) + pT^2d(X) + 2Td(T). \end{aligned}$$

So that:

$$-pT^2d(X) = (2pTX + 2T - 1)\,d(T) = d(T). \tag{1.1.8}$$

In particular, by using the unique writing (1.1.7), the universal derivation can be computed as follows:

$$d(P(T) + Q(X)) = \left(\frac{\partial}{\partial X}(Q(X)) - pT^2\frac{\partial}{\partial T}(P(T))\right)d(X) \tag{1.1.9}$$

Without using dimensional arguments, applying (1.1.8) implies that all elements in $\Omega^1_{A/\mathbb{Z}_p}\otimes_{\mathbb{Z}}\mathbb{Q}$ are cocyles. But (1.1.9) shows us, using the unique writing (1.1.7) and [Sta, 00T7], that $Td\,(X)$ is a non-zero cochain which is not a coboundary. Actually, one sees that here the H^1 is the free $\mathbb{Q}_p$-vector space of dimension 1 generated by the class of $Td\,(X)$, so we have indeed two non isomorphic degree 1 cohomology groups.

This last example shows us that we have to do better than smooth lifts to find a canonical lift.

1.2. Completion and pathologies

In this section, we let V be a commutative ring, and we fix $\pi \in V$. Here, we will study the properties of lifts of π-adically complete and T_2 (also called Hausdorff) lifts of formally smooth algebras. For our definition of formally smooth ring maps, we follow [Sta, 00TI].

Lemma 1.2.1. *Let A be a flat commutative V-algebra. If $A/\pi V$ is a formally smooth $V/\pi V$-algebra, then for all $n \in \mathbb{N}^*$ the ring $A/\pi^n A$ is a formally smooth $V/\pi^n V$-algebra.*

Proof. By hypothesis, we already have shown the case $n = 1$, so suppose that we have proven the formal smoothness for some $n \in \mathbb{N}^*$. In that case, the ideal $\pi^n A/\pi^{n+1}A$ has square zero in $A/\pi^{n+1}A$. Moreover, by base change [Sta, 00HI] the ring $A/\pi^{n+1}A$ is a flat $V/\pi^{n+1}V$-algebra. So applying [Sta, 031L], we get that $A/\pi^{n+1}A$ is a formally smooth $V/\pi^{n+1}V$-algebra. □

Lemma 1.2.2. *Let A and B be two commutative V-algebras. Consider a morphism $\varphi_1\colon A/\pi A \to B/\pi B$ of $V/\pi V$-algebras. Assume that A is a flat V-algebra and that $A/\pi A$ is a formally smooth $V/\pi V$-algebra.*

Then there is a projective system, indexed by $n \in \mathbb{N}^*$, of morphisms of $V/\pi^n V$-algebras $\varphi_n\colon A/\pi^n A \to B/\pi^n B$.

Proof. We fix $n \in \mathbb{N}^*$ and we apply lemma 1.2.1. Then, by definition of a formally smooth morphism there exists a dotted morphism making the following diagram of $V/\pi^{n+1}V$-algebras commutative:

$$\begin{tikzcd}
A/\pi^{n+1}A \arrow[r] \arrow[rrd, dotted, "\varphi_{n+1}"] & A/\pi^n A \arrow[r, "\varphi_n"] & B/\pi^n B \\
V/\pi^{n+1}V \arrow[u] \arrow[rr] & & B/\pi^{n+1}B. \arrow[u]
\end{tikzcd}$$

□

The next proposition illustrates how π-adic T_2 completion yields canonical lifts. We do not state it in full generality, nevertheless we are also about to see that these lifts are still not satisfying for our purpose, so there is no need for the entire machinery.

Proposition 1.2.3. *Let A and B be two π-adically complete and T_2 commutative V-algebras. Let $\varphi_1\colon A/\pi A \to B/\pi B$ be an isomorphism of formally smooth $V/\pi V$-algebras. If A is flat and B has no π-torsion, then A and B are isomorphic as V-algebras. Moreover, this isomorphism is a lift of φ_1.*

Proof. By hypothesis, $A \cong \lim A/\pi^n A$ and so does B. So from the projective system of morphisms given by lemma 1.2.2, we have a morphism of V-algebras $\varphi\colon A \to B$. Let $a \in A$. If $\varphi\,(a) = 0$, then $a = \pi a_1$ for some $a_1 \in A$ because φ_1 is injective. Since B has no π-torsion we find $\varphi(a_1) = 0$. By repeating this process, we get $a \in \bigcap_{n\in\mathbb{N}^*} \pi^n A$. So it is zero.

As of surjectivity, if $b_1 \in B$, then we can find $a_1 \in A$ and $b_2 \in B$ such that $\varphi(a_1) = b_1 - \pi b_2$ because φ_1 is surjective. We can do it again with b_2, and carry on infinitely many times, so that $\varphi\left(\sum_{n\in\mathbb{N}^*} \pi^{n-1} a_n\right) = b_1$. □

A fortiori, we find the following well-known proposition.

Proposition 1.2.4. *If V is Noetherian and π-torsion free, then the π-adic T_2 completions of two smooth lifts of the same smooth commutative $V/\pi V$-algebra are isomorphic.*

Proof. Let $\overline{A}$ be a smooth commutative $V/\pi V$-algebra. Let A and B be two smooth lifts of $\overline{A}$. These lifts are Noetherian because V is Noetherian. We can thus apply [Sta, 00MB], which informs us that these π-adic T_2 completions are two flat lifts, with same smooth reduction modulo π. The flatness property implies that the completions are π-torsion free, so we can apply proposition 1.2.3. □

However, such flat, π-adically complete and T_2 lifts still do not provide a suitable setting for our quest for an appropriate de Rham complex. First of all, the universal derivation is in general not continuous for the p-adic topology.

Example 1.2.5. Let $A := \widehat{\mathbb{Z}_p[X]}$ be a flat, p-adically complete and T_2 lift of $\mathbb{F}_p[X]$. The module $\Omega^1_{A/\mathbb{Z}_p} \otimes_{\mathbb{Z}} \mathbb{Q}$ is not a $A \otimes_{\mathbb{Z}} \mathbb{Q}$-module of rank 1 as one could candidly expect.

To see this, we first have to remind the reader that there exists an injective morphism of $\mathbb{Z}_p$-algebras $\mathbb{Z}_p[Y_i \mid i \in \mathbb{N}] \to \mathbb{Z}_p[\![T]\!]$ from the ring of polynomials with countably many variables to the ring of formal power series. One way to see this is to read the second proof of [MS, lemma 2.], and see that it still holds in the case of an integral domain (or, similarly, that the power series constructed in the proof can be chosen in the ring of integers of $\mathbb{Q}_p$).

Consider now the injective morphism of $\mathbb{Z}_p$-algebras $\mathbb{Z}_p[\![T]\!] \to A$ sending T to pX. Inverting p gives us the following sequence of injective $\mathbb{Q}_p$-algebras:

$$\mathbb{Q}_p[Y_i \mid i \in \mathbb{N}] \longrightarrow \mathbb{Z}_p[\![T]\!] \otimes_{\mathbb{Z}} \mathbb{Q} \longrightarrow A \otimes_{\mathbb{Z}} \mathbb{Q}.$$

In turn, there is an injective morphism $\mathbb{Q}_p[Y_i \mid i \in \mathbb{N}] \to \mathrm{Frac}(A)$ of $\mathbb{Q}_p$-algebras. In other words, the transcendence degree of $\mathrm{Frac}(A)$ over $\mathbb{Q}_p$ is infinite.

Now, [Bou07b, théorème 2. p. V.125] tells us that $\Omega^1_{\mathrm{Frac}(A)/\mathbb{Q}_p}$ is an infinite dimensional $\mathrm{Frac}(A)$-vector space. Using [Sta, 00RT] we get isomorphisms of $\mathrm{Frac}(A)$-modules $\Omega^1_{\mathrm{Frac}(A)/\mathbb{Q}_p} \cong \Omega^1_{\mathrm{Frac}(A)/\mathbb{Z}_p} \cong \Omega^1_{A/\mathbb{Z}_p} \otimes_A \mathrm{Frac}(A)$. This means that $\Omega^1_{A/\mathbb{Z}_p}$ must be an infinitely generated A-module, but also that $\Omega^1_{A/\mathbb{Z}_p} \otimes_{\mathbb{Z}} \mathbb{Q}$ is an infinitely generated $A \otimes_{\mathbb{Z}} \mathbb{Q}$-module.

Where do all these elements come from? One could ingenuously think that the derivative $\frac{\partial}{\partial X}$ extended to formal series would be universal.

To understand what goes wrong, take a power series $P(X) \in A$ transcendental over $\mathbb{Z}_p$, and algebraically independent with X. What [Bou07b, théorème 2. p. V.125] unveils is that the element $\frac{\partial}{\partial X}(P(X))\, d(X) - d(P(X)) \in \Omega^1_{A/\mathbb{Z}_p} \otimes_{\mathbb{Z}} \mathbb{Q}$ is not zero. Notably, the universal differential is not continuous for the p-adic topology, which of course would cause us huge practical problems. In particular, we still do not get infinite dimensional cohomology groups...

Moreover, we see that $\bigcap_{n\in\mathbb{N}} p^n \Omega^1_{A/\mathbb{Z}_p}$ is an infinitely generated A-module. Indeed, all the elements of the form $\frac{\partial}{\partial X}(P(X))\, d(X) - d(P(X))$ are divisible by all powers of p. To sum up, our main issue here is that $\Omega^1_{A/\mathbb{Z}_p}$ is not T_2 for the p-adic topology.

To circumvolve this last issue, one idea is to slightly change the universal property of our module of differentials.

Let A be a commutative V-algebra. For each A-module M, we denote by $\mathrm{Der}_V(A, M)$ the set of V-derivations from A into M. Recall that this rule defines a functor from the category of A-modules to the category of sets, and that it is representable by the A module $\Omega^1_{A/V}$.

Consider the full subcategory $\mathsf{(A,\pi)\text{-}T_2Mod}$ of A-modules whose objects are T_2 for the π-adic topology. We can restrict the above functor to $\mathsf{(A,\pi)\text{-}T_2Mod}$.

Proposition 1.2.6. *The restriction of the functor* $\mathrm{Der}_V(A, \bullet)$ *to the category* $\mathsf{(A,\pi)\text{-}T_2Mod}$ *is representable by a A-module, T_2 for the π-adic topology,* $\Omega^1_{A/V}$.

In other words, there exists a A-module $\Omega^1_{A/V}$, which is T_2 for the π-adic topology, and a V-derivation $d\colon A \to \Omega^1_{A/V}$ such that for all A-module M, T_2 for the π-adic topology, and any V-derivation $\partial\colon A \to M$, there exists a unique morphism of A-modules $\varphi\colon \Omega^1_{A/V} \to M$ such that the following diagram is commutative:

$$\begin{tikzcd} & \Omega^1_{A/V} \arrow[dr, dotted, "\varphi"] & \\ A \arrow[ur, "d"] \arrow[rr, "\partial"] & & M \end{tikzcd}$$

Proof. By the universal property of the quotient, and the universal property of Kähler differentials, it is immediate to see that $\Omega^1_{A/V} \coloneqq \Omega^1_{A/V} / \bigcap_{n\in\mathbb{N}} p^n \Omega^1_{A/V}$, endowed with the quotiented universal derivation, satisfies the universal property. □

As usual, we define the associated de Rham complex by taking the exterior product $\Omega_{A/V} \coloneqq \bigwedge \Omega^1_{A/V}$ endowed with the differential induced by the universal derivation. Alternatively, if A is π-adically separated (and it will be), we could have defined it as the quotient $\Omega_{A/V} / \bigcap_{n\in\mathbb{N}} p^n \Omega_{A/V}$.

Do not fear to mingle both complexes in the following of the paper: as of now, we shall only consider the T_2 complex. These extremely close notations have been chosen here on purpose: in the literature, some authors denote the T_2 complex the same way as the de Rham complex.

It seems that we have finally have worked through all the issues in our quest for a suitable de Rham cohomology for affine schemes over a perfect field of characteristic p. Unless... Convergence is not fast enough.

Example 1.2.7. As usual, we work with the $\mathbb{F}_p$-algebra $\mathbb{F}_p[X]$. Again, we consider the flat, p-adically complete and T_2 lift $A \coloneqq \widehat{\mathbb{Z}_p[X]}$.

For all $n \in \mathbb{N}$, consider the following element in $\Omega^1_{A/\mathbb{Z}_p} \otimes_{\mathbb{Z}} \mathbb{Q}$:

$$\sum_{l\in\mathbb{N}^*} p^{nl} X^{p^{nl}-1} d(X). \tag{1.2.8}$$

Looking at the following commutative diagram:

$$\begin{tikzcd} A \otimes_{\mathbb{Z}} \mathbb{Q} \arrow[r, "d"] \arrow[d, "i"] & \Omega^1_{A/\mathbb{Z}_p} \otimes_{\mathbb{Z}} \mathbb{Q} \arrow[d] \\ \mathbb{Z}_p[\![X]\!] \otimes_{\mathbb{Z}} \mathbb{Q} \arrow[r] & \Omega^1_{\mathbb{Z}_p[\![X]\!]/\mathbb{Z}_p} \otimes_{\mathbb{Z}} \mathbb{Q}, \end{tikzcd}$$

in which i is the obvious inclusion, one sees that if (1.2.8) was the image through d of some element $a \in A \otimes_{\mathbb{Z}} \mathbb{Q}$, then we would have:

$$i\left(a\right) = \sum_{l \in \mathbb{N}^*} X^{p^{nl}}$$

which is not convergent for the p-adic topology. Thus, we again get an infinite dimensional cohomology group in degree 1.

The annoying phenomenon here is that the degree of the monomials grows too fast in comparison to the p-adic valuation of their coefficients. Because of that, when one would like to integrate the series, the powers of p disappear, and the integrated series does not converge any longer. So we want to have some control on the pace of convergence of our series.

1.3. Weak completions

In all this section, we let V be a commutative Noetherian ring, and $\pi \in V$. If A is a commutative V-algebra, we denote by $\widehat{A} = \lim A/\pi^n A$ the π-adic T_2 completion of A (with n varying in $\mathbb{N}$ and the canonical projective system).

The next definition allows us to get rid of the problem shown in example 1.2.7. For the moment, we shall review the basic properties of this notion in full generality.

Definition 1.3.1. Let A be a commutative V-algebra, and let $S \subset A$ be a subset. We shall denote by $\left(S \subset A\right)^\dagger$ the subset of $\widehat{A}$ whose elements are the ones for which there exists $n \in \mathbb{N}$, depending of the given element, such that it can be written as:

$$\sum_{j \in \mathbb{N}} \pi^j P_j\left(\underline{a}\right)$$

with $\underline{a} \in S^n$ and $P_j \in V\left[X_1, \ldots, X_n\right]$ for all $j \in \mathbb{N}$. In addition, we require that there exists $c \in \mathbb{N}$ such that:

$$\forall j \in \mathbb{N},\ \deg\left(P_j\right) \leqslant c\left(j+1\right).$$

When $S = A$, we shall simply write $A^\dagger := \left(A \subset A\right)^\dagger$, and call this set the **weak completion of** A.

We will call series of the form above **overconvergent**.

Of course, this definition and the ones to follow depend on the choices of V and π. But in practice, it will be very clear what they are, so we do not keep them in our notations.

Proposition 1.3.2. *Let A be a commutative V-algebra, and let S be a subset of A. Then $\left(S \subset A\right)^\dagger$ is a commutative V-algebra such that $\left(S \subset A\right)^\dagger \cong \left(S \subset A\right)^{\dagger\dagger}$ as V-algebras.*

Proof. Let $s \in \widehat{A}\left[\!\left[\pi\right]\!\right]$ be a formal series which has a representation for some fixed $n \in \mathbb{N}$:

$$s = \sum_{j \in \mathbb{N}} \pi^j P_j\left(s_1, \ldots, s_n\right),$$

with $\left(s_1, \ldots, s_n\right) \in {\left(S \subset A\right)^{\dagger}}^n$ and $P_j \in V\left[X_1, \ldots, X_n\right]$ for all $j \in \mathbb{N}$. We will also assume the existence of $c \in \mathbb{N}$ such that:

$$\forall j \in \mathbb{N},\ \deg\left(P_j\right) \leqslant c\left(j+1\right).$$

We can assume without loss of generality that $c \neq 0$. By definition, for all $i \in [\![1, n]\!]$, we have:

$$s_i = \sum_{k \in \mathbb{N}} \pi^k Q_{i,k}\left(\underline{a}\right),$$

with $\underline{a} \in S^m$ and $Q_{i,k} \in V[X_1, \ldots, X_m]$ for all $k \in \mathbb{N}$ and some fixed $m \in \mathbb{N}$. Furthermore, there exists $e \in \mathbb{N}$ such that:

$$\forall k \in \mathbb{N},\ \deg(Q_{i,k}) \leqslant e(k+1).$$

Notice that it is possible to choose such m and e commonly for all $i \in [\![1, n]\!]$.

For now, let us fix $j \in \mathbb{N}$. We claim that for all $l \in \mathbb{N}$, there exists polynomials $F_{j,l} \in V[X_1, \ldots, X_m]$ such that we have the following inequality in $\widehat{A}$:

$$P_j(s_1, \ldots, s_n) = \sum_{l \in \mathbb{N}} \pi^l F_{j,l}(\underline{a}),$$
$$\forall l \in \mathbb{N},\ \deg(F_{j,l}) \leqslant e(l + \deg(P_j)).$$

This is actually a general fact about polynomials, that we can show by induction on their total degree. If $\deg(P_j) \leqslant 1$, the claim is obvious. Otherwise, for all $i \in [\![1, n]\!]$ we can find $R_{j,i} \in V[Y_1, \ldots, Y_n]$ and $v \in V$ such that:

$$P_j(s_1, \ldots, s_n) = v + \sum_{i=1}^{n} R_{j,i}(s_1, \ldots, s_n) s_i,$$
$$\forall i \in [\![1, n]\!],\ \deg(R_{j,i}) \leqslant \deg(P_j) - 1.$$

Fix such an i, and suppose that the claim is shown for $R_{j,i}$; that is, suppose we have polynomials $G_{j,l} \in V[X_1, \ldots, X_n]$ for all $l \in \mathbb{N}$ satisfying:

$$R_{j,i}(s_1, \ldots, s_n) = \sum_{l \in \mathbb{N}} \pi^l G_{j,l}(\underline{a}),$$
$$\forall l \in \mathbb{N},\ \deg(G_{j,l}) \leqslant e(l + \deg(P_j) - 1).$$

So that we can now write:

$$R_{j,i}(s_1, \ldots, s_n) s_i = \sum_{l \in \mathbb{N}} \pi^l G_{j,l}(\underline{a}) \sum_{k \in \mathbb{N}} \pi^k Q_{i,k}(\underline{a}) = \sum_{t \in \mathbb{N}} \pi^t \sum_{\substack{l,k \in \mathbb{N} \\ l+k=t}} G_{j,l}(\underline{a}) Q_{i,k}(\underline{a}).$$

Of course we find for all $l + k = t$ as in the double series above:

$$\deg(G_{j,l} Q_{i,k}) \leqslant e(l + \deg(P_j) - 1 + k + 1) = e(t + \deg(P_j)),$$

and the claim follows. Notice that this very argument implies that $(S \subset A)^\dagger$ is a commutative V-algebra, so that we can see the element $s \in \widehat{A}[\![\pi]\!]$ we started with as an element in $(S \subset A)^{\dagger^\dagger}$ instead. To conclude, by examining the following commutative diagram:

$$\begin{tikzcd}
\widehat{A} & \widehat{(S \subset A)}^\dagger \arrow[l] \\
(S \subset A)^\dagger \arrow[u] \arrow[r] & (S \subset A)^{\dagger^\dagger}, \arrow[u]
\end{tikzcd}$$

we see that the bottom arrow is injective because so is the left one, and by our previous claim we get:

$$s = \sum_{k \in \mathbb{N}} \pi^k \sum_{\substack{j,l \in \mathbb{N} \\ j+l=k}} F_{j,l}(\underline{a}).$$

To conclude, since we assumed that $c \neq 0$, we find for all $j + l = k$ as above:

$$\deg(F_{j,l}) \leqslant e(l + \deg(P_j)) \leqslant e(l + c(j+1)) \leqslant ec(k+1).$$

Which implies that the bottom map is also onto. □

Definition 1.3.3. A V-algebra is said to be **weakly complete** if it is isomorphic to $A^\dagger$ for some commutative V-algebra A.

Notice that we have a canonical morphism of V-algebras $A \to A^\dagger$.

Proposition 1.3.4. *Let A be a commutative V-algebra. Then it is weakly complete if and only if the canonical morphism $A \to A^\dagger$ is an isomorphism.*

Proof. One direction by definition of being weakly complete, the other is simply proposition 1.3.2 with $S = A$. □

We can associate functorialy to each morphism of V-algebras $A \to B$ another morphism $\widehat{A} \to \widehat{B}$. It is clear that the restriction of this morphism to $A^\dagger$ has image in $B^\dagger$, so that we get a weak completion functor.

Proposition 1.3.5. *Let A be a weakly complete V-algebra. Then πA is included in the Jacobson radical $\mathrm{J}(A)$ of A.*

Proof. We have to prove that for all $a \in A$, then $1 + \pi a$ is a unit in A. Of course, $\sum_{i \in \mathbb{N}} (-\pi a)^i$ is an overconvergent series, and an inverse of $1 + \pi a$ in A. □

Definition 1.3.6. Let A be a weakly complete V-algebra. We say that S is a set of **weak generators of** A if $(S \subset A)^\dagger = A$.

Weak generators play an important role in the theory of weak completions, because most of the time, the weak completion of a commutative V-algebra of finite type is not of finite type. Nevertheless, weak generators provide the good framework to retrieve a notion similar to being of finite type.

Definition 1.3.7. A V-algebra is said to be **wcfg** is it is a weakly complete V-algebra having a finite subset of weak generators.

This definition stands for "weakly complete, weakly finitely generated".

Example 1.3.8. The V-algebra $V[X_1, \dots, X_n]^\dagger$ is wcfg, with $S = \{X_1, \dots, X_n\}$. Indeed, one can replace the P_j in the definition above with $P_j(\underline{a})$. If d is the greatest of the degrees in $\underline{a}$, then $\deg(P_j) \leqslant dc(j+1)$.

All wcfg V-algebras are the homomorphic image of $V[X_1, \dots, X_n]^\dagger$ for some $n \in \mathbb{N}$. To see this, it suffices to define the V-algebra morphism sending the weak generators of $V[X_1, \dots, X_n]^\dagger$ to the ones of the considered wcfg algebra.

For the same reason, the weak completion of a finitely generated commutative V-algebra is wcfg.

Proposition 1.3.9. *Any wcfg V-algebra is Noetherian.*

Proof. The proof of this result of Fulton is not very long nor too difficult, but it is slightly technical, so we omit it here. It can be found in [Ful, theorem p. 592]. □

As expected, the universal module of π-adically T_2 differentials has nice properties regarding weak completion.

Proposition 1.3.10. *Let A be a commutative V-algebra. Let $n \in \mathbb{N}$ be an integer. Then $\Omega^1_{A[X_1,\dots,X_n]^\dagger/A}$ is a free $A[X_1, \dots, X_n]^\dagger$-module with basis $\{d(X_i)\}_{i \in [\![1,n]\!]}$.*

Proof. Recall that we defined the universal module of π-adically T_2 differentials as a quotient $\Omega^1_{A[X_1,\dots,X_n]^\dagger/A} = \Omega^1_{A[X_1,\dots,X_n]^\dagger/A} / \bigcap_{n \in \mathbb{N}} \pi^n \Omega^1_{A[X_1,\dots,X_n]^\dagger/A}$ of the $A[X_1, \dots, X_n]^\dagger$-module of Kähler differentials, which is by construction generated by the set $\{d(a)\}_{a \in A[X_1,\dots,X_n]^\dagger}$.

Let $a \in \sum_{j \in \mathbb{N}} \pi^j P_j \in A[X_1, \dots, X_n]^\dagger$, where $P_j \in A[X_1, \dots, X_n]$ for all $j \in \mathbb{N}$. Then for all $k \in \mathbb{N}$ we have:

$$d(a) - \sum_{i=1}^{n} \sum_{j \in \mathbb{N}} \pi^j \frac{\partial}{\partial X_i}(P_j)\, d(X_i) \in \pi^{k+1} \Omega^1_{A[X_1,\dots,X_n]^\dagger/A}.$$

Turning back to our π-adically T_2 differentials, this implies that $\{d(X_i)\}_{i\in[\![1,n]\!]}$ is a generating set of $\Omega^1_{A[X_1,\dots,X_n]^\dagger/A}$, and it is linearly independent because it is known to be modulo π^k for all $k \in \mathbb{N}$ [Sta, 00RX]. □

Proposition 1.3.11. *Let A be a commutative V-algebra of finite type. Then the inclusion morphism $A^\dagger \to \widehat{A}$ is faithfully flat, and the canonical morphism $A \to A^\dagger$ is flat.*

Proof. Since the natural composition $A/\pi^n A \to A^\dagger/\pi^n A^\dagger \to \widehat{A}/\pi^n\widehat{A}$ is an isomorphism, the first arrow is injective. It is also surjective because every element in $A^\dagger$ can be written as $a + \pi^n a'$ with $a \in A$ and $a' \in A^\dagger$.

Since A is of finite type, $A^\dagger$ is Noetherian by virtue of proposition 1.3.9, so by [Sta, 0912] the inclusion morphism $A^\dagger \to \widehat{A}$ is flat. Let $\mathfrak{m} \in \operatorname{Spec}\left(A^\dagger\right)$ be a closed point, that is, a maximal ideal of $A^\dagger$. Notice that $\mathfrak{m}\widehat{A} \cap A^\dagger = \mathfrak{m}$ using proposition 1.3.5, so by [Sta, 00HQ] it is also faithfully flat.

The second part of the statement is [Sta, 039V]. □

1.4. Dagger smoothness

As in the previous section, we let V be a commutative Noetherian ring, and $\pi \in V$. We now introduce a very important property which all lifts of smooth $V/\pi V$-algebras shall have.

Definition 1.4.1. A weakly complete V-algebra A is **very smooth**, or **dagger smooth**, if $A/\pi A$ is a smooth $V/\pi V$-algebra, and if for all pairs of morphisms of weakly complete V-algebras $\varphi\colon A \to B$ and $p\colon C \to B$, such that p is surjective and that there exists a morphism of $V/\pi V$-algebras $\overline{\psi}\colon A/\pi A \to C/\pi C$ satisfying $\varphi \otimes_V V/\pi V = (p \otimes_V V/\pi V) \circ \overline{\psi}$, then there exists a morphism of V-algebras $\psi\colon A \to C$ such that the following diagram commutates:

$$\begin{tikzcd}
A \arrow[rrr] \arrow[dd, "\varphi"'] \arrow[dr, dotted, "\psi"] & & & A/\pi A \arrow[dl, "\overline{\psi}"'] \arrow[dd, "\varphi\otimes_V V/\pi V"] \\
& C \arrow[r] \arrow[dl, "p"] & C/\pi C \arrow[dr, "p\otimes_V V/\pi V"'] & \\
B \arrow[rrr] & & & B/\pi B
\end{tikzcd}$$

The term "very smooth" is the only one in the literature, but the author finds it quite confusing. Indeed, as we shall see, very smooth algebras are not always smooth, and the weak completion of a smooth algebra is very smooth. So we will talk about "dagger smooth" algebras instead.

The following two theorems will be the first ones for which we do not provide proofs, and whose demonstrations are not straightforward.

Theorem 1.4.2. *Let $\overline{A}$ be a smooth commutative $V/\pi V$-algebra. Then there exists a smooth V-algebra A which is a lift of $\overline{A}$.*

Proof. This is a result of Arabia [Ara, 1.3.1.] which generalizes a theorem of Elkik [Elk, théorème 6]. She has shown the existence of a smooth lift in the context of Noetherian henselian pairs, which is actually general enough in the context of the algorithm we shall study.

See also: [Sta, 07M8]. □

Theorem 1.4.3. *Let $\overline{A}$ be a smooth commutative $V/\pi V$-algebra. For every smooth V-algebra A lifting $\overline{A}$ which always exist by theorem 1.4.2, its weak completion $A^\dagger$ is a dagger smooth V-algebra A which is a lift of $\overline{A}$.*

Proof. This result is due to Arabia [Ara, 3.3.2.]. □

This theorem actually also implies the existence of lifts of morphisms between smooth commutative $V/\pi V$-algebras.

Proposition 1.4.4. *Let $\overline{\varphi}\colon \overline{A} \to \overline{B}$ be a morphism of smooth commutative $V/\pi V$-algebras. Let A be a dagger smooth, weakly complete V-algebra. Let B be a weakly complete V-algebra. Suppose that A and B are lifts of $\overline{A}$ and $\overline{B}$ respectively.*

Then there exists a morphism of V-algebras $\varphi\colon A \to B$ which is a lift of $\overline{\varphi}$.

Proof. Since A is dagger smooth, the existence of φ is given by the definition applied to the following commutative diagram:

$$\begin{tikzcd}
A \arrow[rrr] \arrow[dr, dotted, "\varphi"] \arrow[dd] & & & A/\pi A \arrow[dl, "\overline{\varphi}"'] \arrow[dd, "\overline{\varphi}"] \\
& B \arrow[r] \arrow[dl] & B/\pi B \arrow[dr, "\mathrm{Id}_{B/\pi B}"'] & \\
B/\pi B \arrow[rrr, "\mathrm{Id}_{B/\pi B}"'] & & & B/\pi B.
\end{tikzcd}$$

□

Example 1.4.5. Assume that $V/\pi V$ has characteristic p. Let $\overline{A}$ be a smooth commutative $V/\pi V$-algebra. Denote by $\mathrm{Frob}_{V/\pi V}$ and $\mathrm{Frob}_{\overline{A}}$ the Frobenius endomorphisms of $V/\pi V$ and $\overline{A}$ respectively. Let $\overline{A}_{[\mathrm{Frob}_{V/\pi V}]}$ be the $V/\pi V$-algebra that we obtain from $\overline{A}$ by restriction of scalars through $\mathrm{Frob}_{V/\pi V}$.

Assume also that there exists a lift $F\colon V \to V$ of the Frobenius endomorphism on $V/\pi V$, and that F is an isomorphism. Let A be a dagger smooth, weakly complete lift of $\overline{A}$. Denote by $A_{[F]}$ the V-algebra that we obtain from A by restriction of scalars trough F.

Notice that $A_{[F]}$ is a weakly complete lift of $\overline{A}_{[\mathrm{Frob}_{V/\pi V}]}$. Moreover, since the Frobenius endomorphism $\mathrm{Frob}_{\overline{A}}\colon \overline{A} \to \overline{A}_{[\mathrm{Frob}_{V/\pi V}]}$ is actually a morphism of $V/\pi V$-algebras, then we can apply proposition 1.4.4 to get a lift $F\colon A \to A_{[F]}$ of $\mathrm{Frob}_{\overline{A}}$.

It is of course less confusing to think of F as a endomorphism of rings on A, which is the Frobenius endormorphism modulo π. However for functoriality reasons, we need to be more careful.

By proposition 1.2.3, we are in the situation of the above example when $V/\pi V$ is a perfect commutative ring of characteristic p, and when V is a π-adically complete T_2 and π-torsion free commutative ring. In practice, we will always work in such a setting: think of V as a complete discrete valuation ring of mixed characteristic.

The lifting of morphisms also imply the unicity of dagger smooth lifts. But to prove this, we first need to demonstrate the "formal inversion lemma".

Lemma 1.4.6. *Let $c, n \in \mathbb{N}$. For all $i \in [\![1, n]\!]$ and all $j \in \mathbb{N}^*$, fix a polynomial $P_{i,j} \in V[X_1, \ldots, X_n]$ satisfying* $\deg(P_{i,j}) \leqslant c(j+1)$.

Then, for all $i \in [\![1, n]\!]$, there exists unique $S_i \in V[X_1, \ldots, X_n][\![\Pi]\!]$ such that:

$$X_i = S_i + \sum_{j \in \mathbb{N}^*} \Pi^j P_{i,j}(S_1, \ldots, S_n).$$

Moreover, when one writes:

$$S_i = X_i + \sum_{j \in \mathbb{N}^*} \Pi^j Q_{i,j}(X_1, \ldots, X_n),$$

then all the polynomials $Q_{i,j}$ satisfy the same inequality on their degree as the $P_{i,j}$.

Proof. The ring $V[X_1,\dots,X_n][\![\Pi]\!]^n$ has a product metric induced by the Π-adic topology, and it is complete for it. Consider the map:

$$f\colon \begin{array}{rl} V[X_1,\dots,X_n][\![\Pi]\!]^n & \to V[X_1,\dots,X_n][\![\Pi]\!]^n \\ (U_1,\dots,U_n) & \mapsto \left(-\sum_{j\in\mathbb{N}^*}\Pi^j P_{i,j}(X_1+U_1,\dots,X_n+U_n)\right)_{i\in[\![1,n]\!]} \end{array}.$$

We see that it is a contraction, so by Banach's theorem it has a unique fixed point $(Z_1,\dots,Z_n)$. Since $f((Z_1,\dots,Z_n))=(Z_1,\dots,Z_n)$, we see that Π divides $(Z_1,\dots,Z_n)$. Then defining $S_i\coloneqq X_i+Z_i$ for all $i\in[\![1,n]\!]$ answers the first point.

Fix $i\in[\![1,n]\!]$. Write uniquely $S_i=X_i+\sum_{j\in\mathbb{N}^*}\Pi^jQ_{i,j}(X_1,\dots,X_n)$ as in the statement. Then:

$$\sum_{j\in\mathbb{N}^*}\Pi^jQ_{i,j}(X_1,\dots,X_n)+\sum_{j\in\mathbb{N}^*}\Pi^jP_{i,j}(S_1,\dots,S_n)=0. \tag{1.4.7}$$

Using the multivariate Taylor expansion, we get for all $j\in\mathbb{N}^*$:

$$P_{i,j}(S_1,\dots,S_n)=P_{i,j}(X_1,\dots,X_n)+\sum_{(a_1,\dots,a_n)\in\mathbb{N}^n}\frac{\partial^{\sum_{l=1}^n a_l}}{\prod_{l=1}^n\partial {X_l}^{a_l}}(P_{i,j})(X_1,\dots,X_n)\prod_{l=1}^n(S_l-X_l)^{a_l}.$$

The sum is finite, and it is divisible by Π because for all $l\in[\![1,n]\!]$ we have $S_l-X_l=\sum_{k\in\mathbb{N}^*}\Pi^kQ_{l,k}(X_1,\dots,X_n)$.

Injecting these formulas in (1.4.7) gives us, by induction on $j\in\mathbb{N}^*$, the inequalities on the degrees. □

The next proposition is paramount is the sense that it provides us the unicity of flat wcfg lifts of smooth algebras.

Proposition 1.4.8. *Let A and B be two flat wcfg lifts of a smooth commutative $V/\pi V$-algebra $\overline{A}$. Then A and B are dagger smooth, and isomorphic as V-algebras.*

Proof. By theorem 1.4.3, it is enough to prove the proposition when A is dagger smooth. Indeed proposition 1.3.11 guarantees us that A is a flat V-algebra. Then by proposition 1.4.4, there exist a morphism $\varphi\colon A\to B$ of V-algebras, which is a lift of the identity on $\overline{A}$.

For the injectivity of the morphism, since $A/\pi A\cong B/\pi B$ as V-modules, we find in the same category $(A/\pi A)\otimes_V\left(\pi^iV/\pi^{i+1}V\right)\cong(B/\pi B)\otimes_V\left(\pi^iV/\pi^{i+1}V\right)$ for all $i\in\mathbb{N}$. By the flatness hypothesis, we find that φ induces an isomorphism $\pi^iA/\pi^{i+1}A\cong\pi^iB/\pi^{i+1}B$ of V-modules. In particular $\operatorname{Ker}(\varphi)\subset\bigcap_{i\in\mathbb{N}}\pi^iA$, and we can conclude because A is wcfg and in particular T_2 for the π-adic topology.

As of surjectivity, consider S a finite set of weak generators of B. Denote by s_i with $i\in[\![1,\#S]\!]$ each element of S. By hypothesis, for all $s_i\in S$, there exists $x_i\in A$ and $b_i\in B$ such that $\varphi(x_i)=s_i+\pi b_i$. Then there exists $c\in\mathbb{N}$, and for each $i\in[\![1,\#S]\!]$ and all $j\in\mathbb{N}^*$ there exists $P_{i,j}\in V[X_1,\dots,X_{\#S}]$ satisfying $\deg(P_{i,j})\leqslant c(j+1)$ and:

$$\varphi(x_i)=s_i+\sum_{j\in\mathbb{N}^*}\pi^jP_{i,j}(s_1,\dots,s_{\#S}).$$

Then, by the formal inversion lemma 1.4.6, for all $i\in[\![1,\#S]\!]$, there exists unique $S_i\in V[X_1,\dots,X_{\#S}][\![\Pi]\!]$ such that:

$$X_i=S_i+\sum_{j\in\mathbb{N}^*}\Pi^jP_{i,j}(S_1,\dots,S_{\#S}).$$

Moreover, one has polynomials $Q_{i,j} \in V[X_1, \ldots, X_n]$ for all $i \in [\![1, \#S]\!]$ and all $j \in \mathbb{N}^*$ with the same overconvergence inequalities as above, and such that:

$$S_i = X_i + \sum_{j \in \mathbb{N}^*} \pi^j Q_{i,j}(X_1, \ldots, X_{\#S}).$$

In particular, we have:

$$s_i = \varphi(x_i) + \sum_{j \in \mathbb{N}^*} \Pi^j Q_{i,j}(\varphi(x_1), \ldots, \varphi(x_{\#S})).$$

This shows that each s_i is in the image of φ by proposition 1.3.4 applied to A. The same proposition also implies that φ is surjective. □

Take care that the previous proposition fails when considering weakly complete lifts instead of wcfg ones. Indeed, the T_2 completion of a wcfg lift is a weakly complete lift, which is in general not wcfg.

We now make a quick digression through Hensel's lemma following [DLZ].

Proposition 1.4.9. *Let C be a weakly complete V-algebra. Let $P(X) \in C[X]$. Let $\overline{c} \in C/\pi C$ such that $P(\overline{c}) = 0$ and $P'(\overline{c})$ is a unit in $C/\pi C$. Then, there exists a unique $c \in C$ such that $P(c) = 0$ and that its reduction modulo π is $\overline{c}$.*

Proof. The unicity is Hensel's lemma applied to $\widehat{C} \supset C$.

Write uniquely $P(X) = \sum_{i=0}^{\deg(P(X))} t_i X^i$. Consider the multivariate polynomial $F(X) \coloneqq \sum_{i=0}^{\deg(P(X))} T_i X^i \in V\left[X, Y, T_0, \ldots, T_{\deg(F(X))}\right]$. We will work with the wcfg V-algebra $A \coloneqq V\left[X, Y, T_0, \ldots, T_{\deg(F(X))}\right] / \langle F(X), 1 - YF'(X)\rangle^{\dagger}$. We have $A/\pi A \cong (V/\pi V)\left[X, Y, T_0, \ldots, T_{\deg(F(X))}\right] / \langle F(X), 1 - YF'(X)\rangle$ as V-algebras.

The solution $\overline{c}$ defines a morphism of $V/\pi V$-algebras:

$$\overline{\psi}\colon (V/\pi V)\left[X, Y, T_0, \ldots, T_{\deg(F(X))}\right] / \langle F(X), 1 - YF'(X)\rangle \to C/\pi C,$$

by sending each T_i for $i \in [\![0, \deg(P(X))]\!]$ to the image of t_i modulo π, sending X to $\overline{c}$ and Y to $P'(\overline{c})^{-1}$.

Notice that $A/\pi A$ is a smooth V-algebra because:

$$\begin{vmatrix} \frac{\partial}{\partial X}(F(X)) & \frac{\partial}{\partial Y}(F(X)) \\ \frac{\partial}{\partial X}(1 - YF'(X)) & \frac{\partial}{\partial Y}(1 - YF'(X)) \end{vmatrix} = -F'(X)^2,$$

which maps to an unit in $V\left[X, Y, T_0, \ldots, T_{\deg(F(X))}\right] / \langle F(X), 1 - YF'(X)\rangle$, so that we can apply [Sta, 00T7]. Its weak completion A is dagger smooth according to theorem 1.4.3. By proposition 1.4.4, we can lift $\overline{\psi}$ to $\psi\colon A \to C$. The image of the class of X through ψ is then the solution to our problem. □

1.5. Monsky–Washnitzer cohomology groups

As in the previous two sections, we let V be a commutative Noetherian ring, and $\pi \in V$. We have seen that we can lift both objects and morphisms, and that two lifts of the same object are isomorphic. In contrast, this does not hold for lifts of the same morphism. Nevertheless, two lifts of the same morphism still bear a strong relationship.

Definition 1.5.1. Let $f, g\colon A \to B$ be two morphisms of weakly complete V-algebras. Let C be the weak completion of the commutative $V[T]$-algebra $B[T]$ with respect to T. For $i \in \{0; \pi\}$, consider the two natural morphisms $e_i\colon C \to B$ satisfying $e_i(T) = i$.

These morphisms are said to be **homotopic** if there exists a morphism of V-algebras $\varphi\colon A \to C$ such that $e_0 \circ \varphi = f$ and $e_\pi \circ \varphi = g$.

Originally, this definition was written with 1 instead of π, and without weak completion with respect to T. We draw inspiration from [ES], so that homotopy becomes an useful definition even without tensoring by $\mathbb{Q}$.

Proposition 1.5.2. *Let $f, g\colon A \to B$ be two morphisms of weakly complete V-algebras. If A is flat, dagger smooth and wcfg, and if $f \equiv g \mod \pi$, then the maps are homotopic.*

Proof. Let us keep the notations of definition 1.5.1. Consider $e_0 \oplus e_\pi\colon C \to B \oplus B$. We can obviously restrict this morphism to its image, so that it is onto and the image is a weakly complete $V[T]$-algebra with respect to T. Moreover, it is clear that its reduction modulo T is B, because $e_0 \oplus e_\pi(T) = 0 \oplus \pi$.

Notice that $\mathrm{Im}(f \oplus g) \subset \mathrm{Im}(e_0 \oplus e_\pi)$. Indeed, for all $a \in A$, by hypothesis on f and g there exists $b \in B$ such that:

$$f(a) \oplus g(a) = f(a) \oplus (f(a) + \pi b) = e_0 \oplus e_\pi (f(a) + Tb).$$

Let D be the weak completion of the commutative $V[T]$-algebra $A[T]$ with respect to T. We can uniquely extend $f \oplus g$ to a morphism $A[T] \to \mathrm{Im}(e_0 \oplus e_\pi)$ of $V[T]$-algebras. By functoriality, we thus get a morphism of weakly complete $V[T]$-algebras $D \to \mathrm{Im}(e_0 \oplus e_\pi)$.

This means that we have the following commutative diagram of $V[T]$-algebras, where the arrows on the left are the reduction mod π of the arrows on the right when present:

$$\begin{tikzcd}
D \arrow[rrr] \arrow[dd] & & & A \arrow[dl, "f"'] \arrow[dd, "f"] \\
& C \arrow[r] \arrow[dl, two heads, "e_0\oplus e_\pi"] & B \arrow[dr, "\mathrm{Id}_B"] & \\
\mathrm{Im}(e_0 \oplus e_\pi) \arrow[rrr] & & & B
\end{tikzcd}$$

By hypothesis, A is a wcfg V-algebra. Let $S \subset A$ be a finite subset of weak generators of A. Then S is also a set of weak generators of the weakly complete $V[T]$-algebra D. Also, $A[T]$ is a flat $V[T]$-algebra by [Sta, 00HI], so that D is also flat as a $V[T]$-algebra by proposition 1.3.11.

This implies that D is dagger smooth by proposition 1.4.8. So we have a morphism of $V[T]$-algebras $D \to C$, and composing with the canonical map $A \to D$ gives the morphism of V-algebras making f and g homotopic. □

Proposition 1.5.3. *Two homotopic maps induce the same map on cohomology.*

Proof. We shall use the notations of definition 1.5.1. Let $f, g\colon A \to B$ be two homotopic morphisms of weakly complete V-algebras. By homotopy and functoriality, we get morphisms $f_*, g_*\colon \Omega_{A/V} \to \Omega_{B/V}$, $e_{i*}\colon \Omega_{C/V} \to \Omega_{B/V}$ for $i \in \{0, p\}$ of V-differential graded algerbas which factor through some $\varphi_*\colon \Omega_{A/V} \to \Omega_{C/V}$. Here, the de Rham complexes are π-adically T_2, not T-adically. It is enough to show that both e_{i*} are homotopic.

But first, let us describe $\Omega_{C/V}$. Consider the tensor product of alternating B-algebras $\Omega_{B/V} \otimes_B \Omega_{B[\![T]\!]/B}$ as described in [Bou07a, proposition 14 p. III.54]. It is the same as the direct sum $\Omega_{B/V} \otimes_B B[\![T]\!] \oplus d(T)\, \Omega_{B/V} \otimes_B B[\![T]\!]$.

We can turn this tensor product into an alternating V-differential graded algebra by defining the following differential for each $i \in \mathbb{N}$:

$$d\colon \begin{array}{ll} \Omega_{B/V} \otimes_B \Omega_{B[\![T]\!]/B} & \to \Omega_{B/V} \otimes_B \Omega_{B[\![T]\!]/B} \\ \sum_{i\in\mathbb{N}} T^i x_i + d(T)\, T^i y_i & \mapsto \sum_{i\in\mathbb{N}} T^i d(x_i) + d(T)\, T^i \left((i+1)\, x_{i+1} - d(y_i)\right), \end{array}$$

where all $x_i, y_i \in \Omega_{B/V}$ for all $i \in \mathbb{N}$.

Similarly, we can consider the tensor product $\Omega_{B/V} \otimes_B \Omega_{C/B}$. By proposition 1.3.11, the canonical inclusion $C \to B\llbracket T \rrbracket$ is faithfully flat, and in particular universally injective [Sta, 05CK]. So we can include the latter tensor product into the former.

We can prove that d restricts well.

In degree zero, we retrieve the ring C. By the universal property of the T_2 de Rham complex, the morphism Id_C yields a morphism of V-differential graded algebras $\Omega_{C/V} \to \Omega_{B/V} \otimes_B \Omega_{C/B}$.

On the other hand, we can sum the identity morphism with the obvious B-linear map $d(T)\, C \to \Omega_{C/V}$. So the universal property of the tensor product gives us a morphism of graded B-modules $\Omega_{B/V} \otimes_B \Omega_{C/B} \to \Omega_{C/V}$. It is actually a morphism of V-differential graded algebras, and the universal properties we used show us that the two arrows we have constructed are inverse of each other. In particular, the remark made in the proof of [Van, theorem 2.4.4] holds for general V.

Now, the homotopy between the e_{i*} is given by the composition of the projection morphism $\Omega_{C/V} \to d(T)\, \Omega_{B/V} \otimes_B C$ and the integration morphism evaluated at π given by $d(T)\, \Omega_{B/V} \otimes_B C \to \Omega_{B/V}$. $\square$

We can now define the Monsky–Washnitzer cohomology groups, and the results we have just proven gives us a functor.

Definition 1.5.4. Let $\overline{A}$ be a smooth commutative $V/\pi V$-algebra. Let A be a dagger smooth lift of $\overline{A}$. Let $i \in \mathbb{Z}$. We call $H^i_{\mathrm{MW}}\left(\overline{A}\right)$ the ***i*-th Monsky–Washnitzer group of $\overline{A}$**, and define it as the i-th cohomology group of the localization of the π-adically T_2 de Rham complex $\Omega_{A/V} \otimes_{\mathbb{Z}} \mathbb{Q}$.

We will now assume the two following theorems, are their proofs are too long for this course.

Theorem 1.5.5. *The Monsky–Wahsnitzer cohomology groups are finite dimensional, when V is a complete discrete valuation field of mixed characteristic* 0 *and p, with uniformizing parameter π.*

Proof. This has been demonstrated independently by Mebkhout [Meb, théorème 1.0–1.] and Berthelot [Ber97, corollaire 3.2.]. $\square$

Theorem 1.5.6. *Let $\overline{A}$ be a smooth $\mathbb{F}_q$-algebra, where $q = p^m$ for some $m \in \mathbb{N}$, of pure dimension n. Then the action of the Frobenius endomorphim $\mathrm{Frob}_{\overline{A}*}$ on the Monsky–Washitzer group, seen here as $\mathrm{Frac}\left(W\left(\mathbb{F}_q\right)\right)$-vector spaces, is bijective.*

Furthermore, if we denote by $N\left(\overline{A}\right)$ the number of morphisms of $\mathbb{F}_q$-algebra $\overline{A} \to \mathbb{F}_q$, we have:

$$N\left(\overline{A}\right) = \sum_{i=0}^{n} (-1)^i \operatorname{tr}\left(q^n {\mathrm{Frob}_{\overline{A}*}}^{-m} \mid H^i_{\mathrm{MW}}\left(\overline{A}\right)\right).$$

Proof. The bijectivity of the action of the Frobenius is a result of Monsky and Washnitzer [MW, theorem 8.6.]. The Lefschetz formula is a result of Monsky [Mon, theorem 4.5.] combined with Arabia's theorem 1.4.3. $\square$

Part 2. Kedlaya's algorithm

In this section, we briefly explain how Kedlaya's algorithm works.

2.1. The cohomology of a localized ring

We now assume that $p \neq 2$.

Let $m \in \mathbb{N}^*$ and $q \coloneqq p^m$. Let $\overline{Q}(X) \in \mathbb{F}_q[X]$ be a monic polynomial off degree $2g+1$ for $g \in \mathbb{N}^*$, such that $\overline{Q}(X) \wedge \overline{Q}'(X) = 1$. This data determines uniquely an hyperrelliptic curve $\mathcal{C}$ with a rational point at infinity.

Let $\overline{A} \coloneqq \mathbb{F}_q[X,Y,Z] / \langle Y^2 - \overline{Q}(X), YZ-1 \rangle$. We will explain later why we are interested in this ring.

Let $Q(X) \in W(\mathbb{F}_q)[X]$ be a monic polynomial whose reduction mod p is $\overline{Q}(X)$ We can lift $\overline{A}$ to a standard smooth $W(\mathbb{F}_q)$-algebra:

$$A \coloneqq W(\mathbb{F}_q)[Y,Z,X] / \langle Y^2 - Q(X), YZ-1 \rangle.$$

Its weak completion $A^\dagger$ is wcfg and dagger smooth. We find the following isomorphism of $W(\mathbb{F}_q)$-algebras:

$$A^\dagger \cong W(\mathbb{F}_q)[X,Y,Z]^\dagger / \langle Y^2 - Q(X), YZ-1 \rangle.$$

In particular, if with the obvious convention $Y^{-1} = Z$ we have:

$$A^\dagger = \left\{ \sum_{i=0}^{2g} \sum_{j\in\mathbb{Z}} a_{i,j} X^i Y^j \in W(\mathbb{F}_q)[\![X,Y,Z]\!] \mid \right.$$
$$\left. \exists c \in \mathbb{N},\ \forall i \in [\![0,2g]\!],\ \forall j \in \mathbb{Z},\ j \leqslant c\left(\mathrm{v}_p(a_{i,j})+1\right) \right\}.$$

Proposition 2.1.1. *The $A^\dagger$-module $\Omega^1_{A^\dagger/W(\mathbb{F}_q)}$ is free of rank 1, is generated by $d(X)$, and has relations:*

$$d(Z) = -Z^2 d(Y),$$
$$d(Y) = \frac{1}{2} Z Q'(X)\, d(X).$$

As the p-adically T_2 de Rham complex is alternated, we have in particular $\Omega^i_{A^\dagger/W(\mathbb{F}_q)} \cong \{0\}$ for all integers $i \geqslant 2$.

Proof. By functoriality, we have a surjective morphism of $W(\mathbb{F}_q)[X,Y,Z]^\dagger$-modules $\Omega^1_{W(\mathbb{F}_q)[X,Y,Z]^\dagger/W(\mathbb{F}_q)} \to \Omega^1_{A^\dagger/W(\mathbb{F}_q)}$. In particular, the $A^\dagger$-module is generated by the set $\{d(X); d(Y); d(Z)\}$.

Moreover, we compute:

$$\begin{aligned} d(Z) &= 2d(Z) - d\left(Z^2 Y\right) \\ &= 2d(Z) - 2YZd(Z) - Z^2 d(Y) \\ d(Z) &= -Z^2 d(Y), \end{aligned}$$

from which we derive:

$$\begin{aligned} d(Y) &= \frac{1}{2}\left(d\left(ZY^2\right) + d(Y)\right) \\ &= \frac{1}{2}\left(Zd\left(Y^2\right) + Y^2 d(Z) + d(Y)\right) \\ &= \frac{1}{2}\left(Zd(Q(X)) - Y^2Z^2 d(Y) + d(Y)\right) \\ d(Y) &= \frac{1}{2} Z Q'(X)\, d(X). \end{aligned}$$

$\square$

There is an involution $\iota\colon \mathcal{C} \to \mathcal{C}$. On the ring $\mathbb{F}_q[X,Y]/\left\langle Y^2 - \overline{Q}(X)\right\rangle$, this involution satisfies $\iota(X) = X$ and $\iota(Y) = -Y$. On $\overline{A}$, this involution satisfies $\iota(X) = X$, $\iota(Y) = -Y$ and $\iota(Z) = -Z$. This involution lifts with the same relations to $A^\dagger$.

We can then split the p-adically T_2 de Rham complex in two eigenspaces for the involution, namely:

$$\begin{aligned} A_+^\dagger &\coloneqq \left\{ \sum_{i=0}^{2g} \sum_{\substack{j\in\mathbb{Z} \\ j\equiv 0 \mod 2}} a_{i,j} X^i Y^j \in A^\dagger \right\}, \\ \Omega_+ &\coloneqq A_+^\dagger d(X), \\ A_-^\dagger &\coloneqq \left\{ \sum_{i=0}^{2g} \sum_{\substack{j\in\mathbb{Z} \\ j\equiv 1 \mod 2}} a_{i,j} X^i Y^j \in A^\dagger \right\}, \\ \Omega_- &\coloneqq A_-^\dagger d(X). \end{aligned}$$

Lemma 2.1.2. *Let $n \in \mathbb{N}^*$. We have:*

$$\#\mathcal{C}(\mathbb{F}_{q^n}) = q^n + 1 - \operatorname{tr}\left(q^n \mathrm{Frob}_{\overline{A}*}{}^{-nm} \mid H^1_{\mathrm{MW}}\left(\overline{A}\right)_-\right).$$

Proof. Recall that $Y^2 = Q(X)$ in $A^\dagger$. We then see that the positive eigenspace of the involution is actually the p-adically T_2 de Rham complex associated to the ring $\mathbb{F}_q[X]\left[\frac{1}{\overline{Q}(X)}\right]$.

If (x,y) is a rational point, so is $\iota((x,y))$. This defines a second distinct point, except when $y = 0$. In this case, we simply have $\overline{Q}(x) = 0$.

As $p \neq 0$, we see that these eigenspaces are also stable by the action of the Frobenius on the Monsky-Washnitzer cohomology. Hence, the Lefschetz trace formula yields:

$$\begin{aligned} &\#\mathcal{C}(\mathbb{F}_{q^n}) = \#\overline{A}(\mathbb{F}_{q^n}) + \left(q^n - \#\mathbb{F}_{q^n}[X]\left[\frac{1}{\overline{Q}(X)}\right](\mathbb{F}_{q^n})\right) + 1 \\ &= \operatorname{tr}\left(q^n \mathrm{Frob}_{\overline{A}*}{}^{-nm} \mid H^0_{\mathrm{MW}}\left(\overline{A}\right)_-\right) - \operatorname{tr}\left(q^n \mathrm{Frob}_{\overline{A}*}{}^{-nm} \mid H^1_{\mathrm{MW}}\left(\overline{A}\right)_-\right) + q^n + 1. \end{aligned}$$

For $i \in [\![0, 2g]\!]$, write $B_i(X)$ We have:

(2.1.3) $\quad \forall i \in [\![0,2g]\!], \ \forall j \in \mathbb{Z},$

$$d\left(X^i Y^j\right) = \left(\frac{j}{2} X^i Y^{j-2} Q'(X) + i X^{i-1} Y^j\right) d(X).$$

This implies in particular that $H^0_{\mathrm{MW}}\left(\overline{A}\right)_-$ is a $\mathrm{Frac}(W(\mathbb{F}_q))$-vector space of dimension 0. To convince yourself consider the leading monomial in $X^i Y^{j-2} Q'(X)$. $\square$

Proposition 2.1.4. *Let $P(X) \in \mathrm{Frac}(W(\mathbb{F}_q))[X]$ and $j \in \mathbb{Z}$ odd. Then there is an algorithm to reduce $\left[P(X) Y^j d(X)\right] \in H^1_{\mathrm{MW}}\left(\overline{A}\right)_-$ to a linear combination of cohomology classes in the set $\left\{\left[X^i Y^{-1} d(X)\right] \mid i \in [\![0, 2g-1]\!]\right\}$.*

Proof. Assume first that $j < -1$. Let $R(X), S(X) \in \operatorname{Frac}(W(\mathbb{F}_q))[X]$ be two polynomials such that $P(X) = R(X) Q(X) + S(X) Q'(X)$.

$$\begin{aligned}
&\left[P(X) Y^j d(X)\right] \\
&\quad = \left[R(X) Q(X) Y^j d(X) + S(X) Q'(X) Y^j d(X)\right] \\
&\quad = \left[R(X) Y^{j+2} d(X) + S(X) Q'(X) Y^j d(X) - d\left(\frac{2}{j+2} S(X) Y^{j+2}\right)\right] \\
&\quad = \left[\left(R(X) - \frac{2}{j+2} S'(X)\right) Y^{j+2} d(X)\right].
\end{aligned}$$

Assume now that $j \geqslant 1$. Let $F(X) \in \operatorname{Frac}(W(\mathbb{F}_q))[X]$ be a polynomial such that $F'(X) = P(X)$. Then we have:

$$\begin{aligned}
\left[P(X) Y^j d(X)\right] &= \left[P(X) Y^j d(X)\right] \\
&= \left[P(X) Y^j d(X) - d\left(F(X) Y^j\right)\right] \\
&= \left[P(X) Y^j d(X) - F'(X) Y^j d(X) - jF(X) Y^{j-1} d(Y)\right] \\
\left[P(X) Y^j d(X)\right] &= \left[-\frac{j}{2} F(X) Q'(X) Y^{j-2} d(X)\right].
\end{aligned}$$

We are now left with the case $j = -1$. If $\deg(P) \leqslant 2g - 1$, we have nothing left to do. Otherwise, for $r \coloneqq \deg(P) - 2g$ we have:

$$\begin{aligned}
d(X^r Y) &= rX^{r-1} Y d(X) + X^r d(Y) \\
&= \left(rX^{r-1} Q(X) + \frac{1}{2} X^r Q'(X)\right) Y^{-1} d(X).
\end{aligned}$$

So if α is the leading coefficient of $P(X)$, then we have:

$$\begin{aligned}
&\left[P(X) Y^{-1} d(X)\right] \\
&= \left[\left(P(X) - \frac{2\alpha r}{1 + 2g + 2r} X^{r-1} Q(X) - \frac{\alpha}{1 + 2g + 2r} X^r Q'(X)\right) Y^{-1} d(X)\right].
\end{aligned}$$

The degree of the polynomial in X in the right-hand side is strictly smaller than $\deg(P)$, so we are done. ☐

Proposition 2.1.5. *The set* $\left\{\left[X^i Y^{-1} d(X)\right] \mid i \in [\![0, 2g-1]\!]\right\}$ *forms a basis of* $H^1_{\mathrm{MW}}\left(\overline{A}\right)_-$.

Proof. We omit the proof for the time being. ☐

2.2. The action of the Frobenius endomorphism

In this section, we explain the three main steps of Kedlaya's algorithm.

Proposition 2.2.1. *Let* $\chi(T)$ *be the characteristic polynomial of* $\operatorname{Frob}_{\overline{A}*}{}^m$ *in* $H^1_{\mathrm{MW}}\left(\overline{A}\right)_-$. *We have:*

$$Z(\mathcal{C}) = \frac{T^{2g} \chi\left(\frac{1}{T}\right)}{(1 - T)(1 - qT)}.$$

Moreover, it is enough to compute $\chi(T)$ *up to precision* p^N, *where* N *is an integer such that* $N \geqslant \frac{gm}{2} + \log_p\left(\binom{2g}{g}\right)$.

Proof. By lemma 2.1.2, for all $n \in \mathbb{N}^*$ we have:

$$\#\mathcal{C}(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} {\alpha_i}^n$$

where all α_i are eigenvalues of $q\mathrm{Frob}_{\overline{A}*}^{-m}$ in $H^1_{\mathrm{MW}}\left(\overline{A}\right)_-$, seen as a $\mathbb{C}$-vector space by the inclusion $\mathrm{Frac}\left(W\left(\mathbb{F}_q\right)\right)$ given by the axiom of choice.

But:

$$\begin{aligned} Z\left(\mathcal{C}\right) &= \exp\left(\sum_{n\in\mathbb{N}^*} \#\mathcal{C}\left(\mathbb{F}_{q^n}\right)\frac{T^n}{n}\right) \\ &= \exp\left(\sum_{n\in\mathbb{N}^*}\frac{T^n}{n} + \sum_{n\in\mathbb{N}^*}\frac{(qT)^n}{n} - \sum_{i=1}^{2g}\sum_{n\in\mathbb{N}^*}\frac{(\alpha_i T)^n}{n}\right) \\ &= \exp\left(-\ln(1-T) - \ln(1-qT) + \sum_{i=1}^{2g}\ln(1-\alpha_i T)\right) \\ Z\left(\mathcal{C}\right) &= \frac{\prod_{i=1}^{2g}(1-\alpha_i T)}{(1-T)(1-qT)}. \end{aligned}$$

Weil conjectures imply that these eigenvalues satisfy, once ordered properly, $\alpha_i\alpha_{g+i} = q$ for all $i \in [\![1,g]\!]$. We then deduce that these eigenvalues are also the eigenvalues of $\mathrm{Frob}_{\overline{A}}{}^m{}_*$.

Write $\chi(T) = \sum_{i=0}^{2g} a_i T^i$. By Weil conjectures, we have:

$$\forall i \in [\![1,g]\!],\ |a_i| \leqslant \binom{2g}{i} q^{\frac{i}{2}} \leqslant \binom{2g}{g} q^{\frac{g}{2}}.$$

The now proven conjectures also imply that $\chi(T) = q^g T^{2g}\chi\left(\frac{1}{qT}\right)$, and $a_0 = 1$ so that $q^{g-i}a_i = a_{2g-i}$ for all $i \in [\![1,g]\!]$. So it suffices to compute the a_i for $i \in [\![g,2g]\!]$ up to precision p^N where $N \geqslant \frac{gm}{2} + \log_p\left(\binom{2g}{g}\right)$. □

Let σ be the canonical Frobenius lift on $W\left(\mathbb{F}_q\right)$. We define a Frobenius lift on $A^\dagger$ as follows:

$$\begin{aligned} F(X) &= X^p, \\ F(Y) &= Y^p\left(1 + \frac{\sigma(Q)(X^p) - Q(X)^p}{Y^{2p}}\right)^{\frac{1}{2}}, \\ F(Z) &= Y^{-p}\left(1 + \frac{\sigma(Q)(X^p) - Q(X)^p}{Y^{2p}}\right)^{-\frac{1}{2}}. \end{aligned}$$

So that for all $i \in [\![0, 2g-1]\!]$:

$$\begin{aligned} F\left(X^iY^{-1}d(X)\right) &= pX^{p(i+1)-1}Y^{-p}\left(1 + \frac{\sigma(Q)(X^p) - Q(X)^p}{Y^{2p}}\right)^{-\frac{1}{2}} d(X) \\ &= X^{p(i+1)-1}Y^{-p}\sum_{i\in\mathbb{N}}\frac{p^{i+1}}{i!}\prod_{k=0}^{i-1}\left(\frac{1}{2}-k\right)\left(\frac{\sigma(Q)(X^p) - Q(X)^p}{Y^{2p}}\right)^i d(X). \end{aligned}$$

Proposition 2.2.2. *The reduction of all $F\left(X^iY^{-1}d(X)\right)$ becomes integral after multiplication by a constant.*

Proof. We omit the proof. □

We thus now have an algorithm to compute a matrix M associated to $\mathrm{Frob}_{\overline{A}*}$ in $H^1_{\mathrm{MW}}\left(\overline{A}\right)_-$. To get the zeta function, we have to compute the characteristic polynomial of $\prod_{i=0}^{m-1}\sigma^i(M)$.

References

[Ara] Alberto Arabia, *Relèvement des algèbres lisses et de leurs morphismes*. Commentarii Mathematici Helvetici **76** (2001), pp. 607–639.

[Ber74] Pierre Berthelot, *Cohomologie cristalline des schémas de caractéristique $p > 0$*. Springer Lecture Notes in Mathematics **407** (1974).

[Ber97] Pierre Berthelot, *Finitude et pureté cohomologique en cohomologie rigide*. Inventiones Mathematicae **128** (1997), pp. 329–377.

[Bou07a] Nicolas Bourbaki, *Algèbre : Chapitres 1 à 3*. Springer-Verlag (2007).

[Bou07b] Nicolas Bourbaki, *Algèbre : Chapitres 4 à 7*. Springer-Verlag (2007).

[DLZ] Christopher Davis, Andreas Langer, Thomas Zink, *Overconvergent Witt vectors*. Journal für die reine und angewandte Mathematik **668** (2012), pp. 1–34.

[Elk] Renée Elkik, *Solutions d'équations à coefficients dans un anneau hensélien*. Annales scientifiques de l'É.N.S. 4 e série **6** (1973), pp. 553–603.

[ES] Veronika Ertl, Johannes Sprang, *Integral comparison of Monsky–Washnitzer and overconvergent de Rham–Witt cohomology*. Proceedings of the American Mathematical Society Series B **5** (2018), pp. 64–72.

[Ful] William Fulton, *A note on weakly complete algebras*. Bulletin of the American Mathematical Society **75** (1969), pp. 591–593.

[Ked] Kiran Sridhara Kedlaya, *Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology*. Journal of the Ramanujan Mathematical Society **16** (2001), pp. 323–338.

[MS] Saunders MacLane, Otto Franz Georg Schilling, *Zero-Dimensional Branches of Rank One on Algebraic Varieties*. Annals of Mathematics **40** (1939), pp. 507–520.

[Meb] Zoghman Mebkhout, *Sur le théorème de finitude de la cohomologie p-adique d'une variété affine non singulière*. American Journal of Mathematics **119** (1997), pp. 1027–1081.

[Mon] Paul Monsky, *Formal cohomology: III. Fixed point theorems*. Annals of Mathematics **93** (1971), pp. 315–343.

[MW] Paul Monsky, Gerard Washnitzer, *Formal cohomology: I*. Annals of Mathematics **88** (1968), pp. 181–217.

[RS] Joel William Robbin, Dietmar Arno Salamon, *Introduction to Differential Topology*. `https://people.math.ethz.ch/~salamon/PREPRINTS/difftop.pdf` (2018).

[Sta] The Stacks Project Authors, *Stacks Project*. `https://stacks.math.columbia.edu/` (2022).

[Van] Marius van der Put, *The cohomology of Monsky and Washnitzer*. Mémoires de la Société Mathématique de France 2 e série **23** (1986), pp. 33–59.