Jean-Marc Fontaine and Yi Ouyang

Theory of p-adic Galois Representations

Springer

Preface

In Fall 2003, Jean-Marc Fontaine was appointed as Chair Professor of Arithmetic Geometry at Tsinghua University in Beijing. This was the starting point of broad Sino-French cooperation in number theory and arithmetic geometry. One can read my tribute to him in the Gazette (The China Legacy of Jean-Marc Fontaine. Gaz. Math. No. 162 (2019), 15–17) for more details about his great effort to develop modern arithmetic geometry in China. He gave a one-month lecture in Fall 2003 and then a one-semester course in Fall 2004 about the theory of p-adic Galois representations. The audiences consisted of mostly senior undergraduate and graduate students, young postdocs and junior faculties from Tsinghua University and nearby Peking University and Chinese Academy of Sciences. This book grew out of the course notes given in these two courses, first prepared by students attending the class.

From the very beginning, Jean-Marc would like to write a textbook in the subject of p-adic Galois representations, for which he laid a firm foundation during his lifetime work. He even had a more ambitious plan to have a book series for all lecture notes given in the Chair Professorship Program. However, this project took much more time than we expected and I had to carry on by myself at last. We had a plan to finish the book in 2009/2010, then he found the exciting result that B_e is a PID and consequently most of his time was devoted to studying the p-adic fundamental curve of Laurent Fargues and himself. Then the more exciting development of Peter Scholze's theory of perfectoid spaces came out in 2011/2012. After all these great developments, finally when he had more time, I arranged him to visit USTC for three months after the second Sino-French Conference in Arithmetic Geometry at Sanya in October 2016 to complete this book project. Just before he was going to depart from Paris to China, he was found to have cancer. It is really a pity that he did not get more time to finish this project.

The theory of p-adic Galois representation contains a huge amount of materials which could not be filled in a 300-page book. During the many years' preparation of this book, Jean-Marc and I had many discussions about which to be included and which not. Sadly this time I don't have Jean-Marc to consult with and have to apply my own judgment.

The main purpose of this book, as well as Fontaine's courses in 2003/2004, is to give an introduction of p-adic Hodge theory, which treats p-adic Galois representations over certain p-adic local field K. Fontaine's great idea is to construct several big (topological) rings containing $\mathbb{Q}_p$ and with continuous G_K-adction, say B, and then divide the category of p-adic Galois representations into subcategories consisting of B-admissible representations, each equivalent to a category consisting of finite dimensional vector spaces with easily described extra structures (Frobenius action, monodromy action, filtration etc), so that it can be studied by linear or semi-linear algebra methods.

Let me first explain briefly about the main content of this book, which covers Chapters 3 to 10. We first define the notion of B-admissible representations and study their properties. We then relate p-adic Galois representations of fields of characteristic p with étale φ-modules. After that, we construct and study successively the big rings C, R, B_{HT}, B_{dR}, B_{cris} and B_{st}, and study the associated C-admissible, Hodge-Tate, de Rham, crystalline and semi-stable representations. We then prove two fundamental results in p-adic Hodge theory: *de Rham is potentially semi-stable* (Theorem A, the p-adic Monodromy Conjecture) and *weakly admissible is admissible* (Theorem B), which were proved by Berger and Colmez-Fontaine a few years before Fontaine's courses. Finally we prove the celebrated theorem of Cherbonnier-Colmez that all p-adic representations are overconvergent.

Now let me explain the reason why many beautiful results are left out here. We don't include the integral p-adic Hodge theory of Breuil, Kisin and others, and only include a tiny part of the theory of (φ, Γ)-modules of Fontaine, Colmez, Berger, Herr and many others. We thought they deserve a whole new book and Fontaine had the vision to write a volume II for them. In fact, Colmez' adaptation of Sen's method is so elegant that it deserves more applications than just the classification of C-representations, which is the only reason I open a new chapter (Chapter 10) to include Cherbonnier-Colmez's Theorem. As the main theme of this book is algebraic, not geometric, other than the overview of ℓ-adic representations in Chapter 2 and several remarks scattering in the book, the geometric applications including the comparison theorems and the relative theory are both not covered. The theory of perfectoid spaces of Scholze, the crowning achievement of p-adic Hodge theory, deserves another new book written by the experts.

We thought seriously about to include the p-adic fundamental curve of Fargues and Fontaine, before the publication of their new book. Fontaine promised to write a new proof of Colmez's Fundamental Lemma based on the classification of vector bundles of this curve, and then apply it to show Proposition 2A in §9.3 (for k arbitrary), which is essential to prove Theorem A. To my knowledge, to achieve this, many new notions and concepts have to be introduced. To make the book as concise as possible, I decided to apply the method in Plût's thesis to prove Colmez' result, which is a highly technical proof. Probably one can come out with a new proof without using the theory of (φ, Γ)-modules (as the proof by Berger).

To the readers

This book grew out of Fontaine's course notes in 2003/2004. His lectures covered roughly § 1.1, part of § 1.2, § 1.5, Chapter 2, Chapter 3, §4.1-4.2, Chapter 5, Chapter 6, §7.1, Chapter 8 and §9.1 in this book. The main purpose of this book is to give an introduction of p-adic Hodge theory, and to prove two fundamental results: *de Rham is potentially semi-stable* (Theorem A, the p-adic Monodromy Conjecture) and *weakly admissible is admissible* (Theorem B). The following is the content chapter-by-chapter.

Chapter 1 is a preliminary chapter. We give a brief introduction here about inverse limits, Galois theory, Witt and Cohen rings, ramification theory of local fields and continuous cohomology.

In Chapter 2 we give a brief overview about linear ℓ-adic representations. Most results here are not proved, but the references are (not yet!) given.

In Chapter 3 we introduce the notion of B-admissible representations. We then study the $\mathbb{F}_p$-, $\mathbb{Z}_p$- and p-adic Galois representations of local fields of characteristic p, which are associated with the category of étale φ-modules. Results in Chapter 3 are essential to later development.

From Chapter 4 on, the field K is assumed to be a p-adic field with perfect residue field k of characteristic p. In Chapter 4, we study properties about the field C and then classify C-representations by Sen's method.

In Chapter 5 we construct the ring R and study its properties, most notably the theorem of Fontaine and Wintenberger (Theorem 5.13). This also leads to the basic theory of (φ, Γ)-modules.

In Chapter 6 we construct the Hodge-Tate ring B_{HT} and more importantly the field of p-adic periods B_{dR}. We also introduce Hodge-Tate representations and de Rham representations, and associate the latter with filtered K-vector spaces.

Chapter 7 is devoted to the construction and properties of the ring B_{cris}. We prove the fundamental exact sequence of p-adic Hodge theory. We introduce the ring B_e and the Lubin-Tate elements, prove the Fundamental Lemma of Colmez and then prove that B_e is a PID.

In Chapter 8 we introduce the ring B_{st} and semi-stable representations. We also study filtered (φ, N)-modules and their admissibility. Then we give the statements of Theorem A and Theorem B.

Chapter 9 is devoted to the proof of Theorem A and Theorem B based on a prepublication of Fontaine. Along the way, we classify admissible (φ, N)-modules with trivia filtration or of dimension ≤ 2 and representations of dimension 1. We introduce the fundamental complex, and prove Hyodo's result $H^1_g = H^1_{\mathrm{st}}$ when k is finite.

Finally we prove that all p-adic representations are overconvergent (Theorem of Cherbonnier-Colmez) by Colmez' adaptation of Sen's method in Chapter 10, which is essential in the theory of (φ, Γ)-modules.

Attention: The following are a few highly technical results whose statement is needed but whose actual proof is not:

(a) Sen's Filtration Theorem (Theorem 1.92) in §1.4.1, which is needed in §1.4.2 and §4.4.2 (to prove Theorem 4.47).
(b) Theorem 4.47. Actually only its corollary, Proposition 4.43, is needed.
(c) Fundamental Lemma of Colmez (Theorem 7.41) in §7.4, which is needed to prove B_e is a PID and then in §9.5.
(d) Dieudonné-Manins Classification Theorem (Theorem 8.25) of φ-modules in §8.2.2.

Acknowledgment

To be filled.

Yi Ouyang
May 24, 2022

Contents

1

Preliminary

1.1 Inverse limits and Galois theory

1.1.1 Inverse limits.

In this subsection, we always assume that $\mathscr{A}$ is a category with arbitrary products. In particular, one can suppose $\mathscr{A}$ is the category of sets, of (topological) groups, of (topological) rings, of left (topological) modules over a certain ring. Recall that a partially ordered set I is called a *directed set* if for any two elements $i, j \in I$, there exists $k \in I$ such that $i \leq k$ and $j \leq k$.

Definition 1.1. *Let $\mathscr{A}$ be a category with arbitrary products and I be a directed set.*

A family $(A_i)_{i\in I}$ of objects in the category $\mathscr{A}$ is called an inverse system *(or a* projective system*) of $\mathscr{A}$ over the index set I if for each pair $i \leq j$ in I, there exists a morphism $\varphi_{ji} : A_j \to A_i$ such that the following two conditions are satisfied:*

(i) $\varphi_{ii} = \mathrm{Id}$*;*
(ii) *For every triple $i \leq j \leq k$, $\varphi_{ki} = \varphi_{ji}\varphi_{kj}$.*

The inverse limit *(or* projective limit*) of a given inverse system $A_\bullet = (A_i)_{i\in I}$ is the object A in $\mathscr{A}$ given by*

$$A := \varprojlim_{i\in I} A_i = \Big\{(a_i) \in \prod_{i\in I} A_i : \ \varphi_{ji}(a_j) = a_i \text{ for every pair } i \leq j\Big\}, \qquad (1.1)$$

such that the natural projection

$$\varphi_i : A \to A_i, \ a = (a_j)_{j\in I} \mapsto a_i$$

is a morphism in $\mathscr{A}$ for each $i \in I$.

Remark 1.2. The condition that the set I is a directed set is not needed to define an inverse system. For example, if I is a set with trivial ordering, i.e. $i \leq j$ if and only if $i = j$, then $\varprojlim_{i \in I} A_i = \prod_{i \in I} A_i$. However, this condition is usually satisfied and often needed in application.

By the inverse system condition, one can see immediately that $\varphi_i = \varphi_{ji}\varphi_j$ for every pair $i \leq j$. Actually, A is the solution of the following universal problem.

Proposition 1.3. *Let (A_i) be an inverse system in $\mathscr{A}$, A be its inverse limit and B be an object in $\mathscr{A}$. If there exist morphisms $f_i : B \to A_i$ for all $i \in I$ such that for every pair $i \leq j$, $f_i = \varphi_{ji} \circ f_j$, then there exists a unique morphism $f : B \to A$ such that $f_j = \varphi_j \circ f$, i.e. the diagram*

$$\begin{tikzcd}
 & & A_j \arrow[dd, "\varphi_{ji}"] \\
B \arrow[urr, "f_j"] \arrow[r, "\exists\,!\,f"] \arrow[drr, "f_i"'] & A \arrow[ur, "\varphi_j"] \arrow[dr, "\varphi_i"'] & \\
 & & A_i
\end{tikzcd}$$

is commutative.

Proof. This is an easy exercise.

By definition, if $\mathscr{A}$ is the category of topological spaces, i.e., if the objects X_i are all topological spaces and the morphisms φ_{ij} are continuous maps, then the inverse limit $X = \varprojlim_{i \in I} X_i$ is a topological space equipped with a natural topology, the *weakest topology* such that all the projections φ_i are continuous maps. Recall that the product topology of the topological spaces $\prod_{i \in I} X_i$ is the *weakest topology* such that the projections pr_i from $\prod_{i \in I} X_i$ to X_i are continuous maps. Thus the natural topology of the inverse limit X is the topology induced as a closed subset of $\prod_{i \in I} X_i$ with the product topology.

For example, if each X_i is endowed with the discrete topology, then X is endowed with the topology of the inverse limit of discrete topological spaces. In particular, if each X_i is a finite set endowed with discrete topology, then X is called a *profinite set* (inverse limit of finite sets). In this case, since $\varprojlim X_i \subset \prod_{i \in I} X_i$ is closed, and since $\prod_{i \in I} X_i$, as the product space of compact spaces, is still compact, $\varprojlim X_i$ is also compact. In this case one can see that $\varprojlim X_i$ is also totally disconnected.

If moreover, each X_i is a (topological) group and if the φ_{ij}'s are (continuous) homomorphisms of groups, then $\varprojlim X_i$ is a (topological) group with $\varphi_i : \varprojlim_j X_j \to X_i$ a (continuous) homomorphism of groups.

If the X_i's are finite groups endowed with discrete topology, the inverse limit in this case is a *profinite group*. Thus a profinite group is always compact and totally disconnected. As a consequence, all open subgroups of a profinite group are closed, and a closed subgroup is open if and only if it is of finite index.

Example 1.4. (1) On the set of positive integers $\mathbb{N}^*$, we define a partial order by $n \leq m$ if $n \mid m$. For the inverse system $(\mathbb{Z}/n\mathbb{Z})_{n\in\mathbb{N}^*}$ of finite rings where the transition map φ_{mn} is the natural projection, the inverse limit is the compact topological commutative ring

$$\widehat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}^*} \mathbb{Z}/n\mathbb{Z}. \tag{1.2}$$

(2) Let ℓ be a prime number, for the sub-index set $\{\ell^n : n \in \mathbb{N}\}$ of $\mathbb{N}^*$,

$$\mathbb{Z}_\ell = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/\ell^n\mathbb{Z}$$

is the ring of ℓ-adic integers. The ring $\mathbb{Z}_\ell$ is a complete discrete valuation ring with the maximal ideal generated by ℓ, the residue field $\mathbb{Z}/\ell\mathbb{Z} = \mathbb{F}_l$, and the fraction field

$$\mathbb{Q}_\ell = \mathbb{Z}_\ell\left[\frac{1}{\ell}\right] = \bigcup_{m=0}^{\infty} \ell^{-m}\mathbb{Z}_\ell$$

being the field of ℓ-adic numbers.

If $N \geq 1$, let $N = \ell_1^{r_1}\ell_2^{r_2}\cdots\ell_h^{r_h}$ be its primary factorization. Then the isomorphism

$$\mathbb{Z}/N\mathbb{Z} \cong \prod_{i=1}^{h} \mathbb{Z}/\ell_i^{r_i}\mathbb{Z}$$

induces an isomorphism of commutative topological rings

$$\widehat{\mathbb{Z}} \cong \prod_{\ell \text{ prime number}} \mathbb{Z}_\ell. \tag{1.3}$$

1.1.2 Galois theory.

Let K be a field and L be a (finite or infinite) Galois extension of K, which means that L/K is a separable and normal field extension. The Galois group $\mathrm{Gal}(L/K)$ is the group of the K-automorphisms of L, i.e.,

$$\mathrm{Gal}(L/K) := \{g : L \xrightarrow{\sim} L,\ g(\gamma) = \gamma \text{ for all } \gamma \in K\}. \tag{1.4}$$

Denote by $\mathscr{I}$ the set of finite Galois extensions of K contained in L and order this set by inclusion. Then for any pair $E, F \in \mathscr{I}$, one has $EF \in \mathscr{I}$, thus $\mathscr{I}$ is in fact a directed set and $L = \bigcup_{E\in\mathscr{I}} E$. As a consequence, we can study the inverse limits of objects over this directed set. For the Galois groups, by definition,

$$\gamma = (\gamma_E) \in \varprojlim_{E \in \mathscr{I}} \mathrm{Gal}(E/K) \text{ if and only if } (\gamma_F)|_E = \gamma_E \text{ for } E \subset F \in \mathscr{I}.$$

Galois theory tells us that the map

$$\begin{aligned} \mathrm{Gal}(L/K) &\xrightarrow{\sim} \varprojlim_{E \in \mathscr{I}} \mathrm{Gal}(E/K) \\ g \quad &\longmapsto (g|_E) : g|_E \text{ the restriction of } g \text{ in } E \end{aligned}$$

is an isomorphism. From now on, we identify these two groups via this isomorphism. Given the discrete topology on each finite group $\mathrm{Gal}(E/K)$, the group $G = \mathrm{Gal}(L/K)$ is then a profinite group, endowed with a compact and totally disconnected topology, which is called the *Krull topology.* We have

Theorem 1.5 (Fundamental Theorem of Galois Theory). *There is a one-to-one correspondence between intermediate field extensions $K \subset K' \subset L$ and closed subgroups H of $\mathrm{Gal}(L/K)$ given by*

$$K' \mapsto \mathrm{Gal}(L/K') \quad \textit{and} \quad H \mapsto L^H$$

where

$$L^H = \{x \in L \mid g(x) = x \textit{ for all } g \in H\}$$

is the invariant field of H.

Moreover, the above correspondence gives one-to-one correspondences between finite extensions (resp. finite Galois extensions, Galois extensions) of K contained in L and open subgroups (resp. open normal subgroups, closed normal subgroups) of $\mathrm{Gal}(L/K)$.

Remark 1.6. We have the following remarks about the above theorem:

(a) Given an element g and a sequence $(g_n)_{n\in\mathbb{N}}$ of $\mathrm{Gal}(L/K)$, the sequence $(g_n)_{n\in\mathbb{N}}$ converges to g if and only if for all $E \in \mathscr{I}$, there exists $n_E \in \mathbb{N}$ such that if $n \geq n_E$, then $g_n|_E = g|_E$.

(b) The open normal subgroups of G are the groups $\mathrm{Gal}(L/E)$ for $E \in \mathscr{I}$. In this case there is an exact sequence

$$1 \longrightarrow \mathrm{Gal}(L/E) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E/K) \longrightarrow 1.$$

(c) A subgroup of G is open if and only if it contains an open normal subgroup. A subset X of G is an open set if and only if for every element $x \in X$, there exists an open normal subgroup H_x such that the coset $xH_x \subseteq X$.

(d) If H is a subgroup of $\mathrm{Gal}(L/K)$, then $L^H = L^{\overline{H}}$ with $\overline{H}$ being the closure of H in $\mathrm{Gal}(L/K)$.

We now give an easy example:

Example 1.7. Let $K = \mathbb{F}_p$ be the finite field with $q = p^f$ elements, and let $\overline{K}$ be an algebraic closure of K with Galois group $G = \mathrm{Gal}(\overline{K}/K)$.

For each $n \in \mathbb{N}$, $n \geq 1$, there exists a unique extension K_n of degree n of K contained in $\overline{K}$. The extension K_n/K is a cyclic extension whose Galois group $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/n\mathbb{Z} = \langle \varphi_n \rangle$ where $\varphi_n = (x \mapsto x^q)$ is the *arithmetic Frobenius* of $\mathrm{Gal}(K_n/K)$. We have the following diagram

$$\begin{tikzcd} G \arrow[r, "\sim"] \arrow[d, "\wr"] & \varprojlim \mathrm{Gal}(K_n/K) \arrow[d, "\wr"] \\ \widehat{\mathbb{Z}} \arrow[r, "\sim"] & \varprojlim \mathbb{Z}/n\mathbb{Z}. \end{tikzcd}$$

Thus the Galois group $G \cong \widehat{\mathbb{Z}}$ is topologically generated by $\sigma_q = (\varphi_n)_n \in G$: $\sigma_q(x) = x^q$ for $x \in \overline{K}$, i.e., with obvious convention, any elements of G can be written uniquely as $g = \sigma_q^a$ with $a \in \widehat{\mathbb{Z}}$. The element σ_q is called the *arithmetic Frobenius* and its inverse σ_q^{-1} is called the *geometric Frobenius* of K.

If $K = \mathbb{F}_p$, the arithmetic Frobenius $\sigma_p = (x \mapsto x^p)$ is called the *absolute Frobenius*. From now on, we simply denote σ_p as σ. Moreover, for any field k of characteristic p, we call the endomorphism $\sigma : x \mapsto x^p$ the *absolute Frobenius* of k. Note that σ is an automorphism if and only if k is perfect.

Definition 1.8. *Let K be a field and K^s be the separable closure of K. The* absolute Galois group *of K, denoted as G_K, is the group* $\mathrm{Gal}(K^s/K)$.

In the case $K = \mathbb{Q}$, the structure of $G_{\mathbb{Q}}$ is far from being completely understood. The inverse problem of Galois theory asks for a given finite group J, if there exists a finite Galois extension of $\mathbb{Q}$ whose Galois group is isomorphic to J. There are cases where the answer is known (eg. J is abelian, $J = S_n$, $J = A_n$, etc), but the general case is still wide open.

For each place p of $\mathbb{Q}$ (i.e., a prime number or ∞), let $\overline{\mathbb{Q}}_p$ be a chosen algebraic closure of the p-adic completion $\mathbb{Q}_p$ of $\mathbb{Q}$ (for $p = \infty$, we let $\mathbb{Q}_p = \mathbb{R}$ and $\overline{\mathbb{Q}}_p = \mathbb{C}$). Choose for each p an embedding $\sigma_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. From the diagram

$$\begin{tikzcd} \overline{\mathbb{Q}} \arrow[r] & \overline{\mathbb{Q}}_p \\ \mathbb{Q} \arrow[r] \arrow[u] & \mathbb{Q}_p \arrow[u] \end{tikzcd}$$

one can identify $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with a closed subgroup of $G_{\mathbb{Q}}$, called the *decomposition subgroup* of G at p. To study $G_{\mathbb{Q}}$, it is necessary and important to study $G_{\mathbb{Q}_p}$ for all p, which is the philosophy called the local-global principle.

This phenomenon is not unique. There is a generalization of the above facts to number fields, i.e. finite extensions of $\mathbb{Q}$ whose completions are finite extensions of $\mathbb{Q}_p$, and to global function fields, i.e. finite extensions of the field of rational functions $k(x)$ with k a finite field whose completions are fields of power series with coefficients in finite extensions of k. As a consequence, we are led to study properties of local fields.

Representation theory is an essential tool to the study of groups in general and the absolute Galois groups of fields in particular. The main theme of this book is introduce the theory of p-adic Galois representations.

1.2 Witt vectors and complete discrete valuation rings

1.2.1 Nonarchimedean fields and local fields.

Let us first recall the definition of valuation.

Definition 1.9. *Let A be a commutative ring with unit. If $v : A \to \mathbb{R} \cup \{+\infty\}$ is a function satisfying the following properties*

(i) $v(a) = +\infty$ *if and only if* $a = 0$,
(ii) $v(ab) = v(a) + v(b)$,
(iii) $v(a + b) \geq \min\{v(a), v(b)\}$,

and if there exists $0 \neq a \in A$ *such that* $v(a) \neq 0$, *then v is called a (nontrivial)* valuation *on A. If $v(A \backslash \{0\})$ is a discrete subset of $\mathbb{R}$, then v is called a* discrete valuation.

Remark 1.10. The valuation defined above is usually called *a valuation of height* 1.

For a ring A with a valuation v, we define the *absolute value* or *metric* on $a \in A$ by $|a| = \gamma^{v(a)}$ for some constant $\gamma \in (0, 1)$, then A becomes a topological space with a basis of neighborhood of 0 given by $\{x \mid v(x) > n\} = \{x \mid |x| < \gamma^n\}$ for $n \in \mathbb{N}$ which is independent of the choice of γ. We shall keep in mind that for $a \in A$,

$$a \text{ is small} \Leftrightarrow |a| \text{ is small} \Leftrightarrow v(a) \text{ is big.}$$

Two valuations v_1 and v_2 on A are called *equivalent* if there exists $r \in \mathbb{R}$, $r > 0$, such that $v_2(a) = rv_1(a)$ for any $a \in A$. Thus v_1 and v_2 are equivalent if and only if the respective induced topologies in A are equivalent.

If A is a ring with a valuation v, then A is always a domain: if $ab = 0$ but $b \neq 0$, then $v(b) < +\infty$ and $v(a) = v(ab) - v(b) = +\infty$, hence $a = 0$. Let K be the fraction field of A, we may extend the valuation to K by setting

$$v(a/b) := v(a) - v(b).$$

Then the *ring of valuations* (often called the *ring of integers*)

$$\mathcal{O}_K = \{a \in K \mid v(a) \geq 0\} \tag{1.5}$$

is a local ring, with the maximal ideal

$$\mathfrak{m}_K = \{a \in K \mid v(a) > 0\}, \tag{1.6}$$

and the residue field $k_K = \mathcal{O}_K/\mathfrak{m}_K$.

Definition 1.11. *A* valuation field *is a field K equipped with a valuation v.*

A valuation field is nonarchimedean: the absolute value $|\ |$ defines a metric on K, which is *ultrametric*, since $|a+b| \leq \max(|a|,|b|)$. Let $\widehat{K}$ denote the completion of K of the valuation v. Then $\widehat{K}$ is again a valuation field with the unique valuation extending v. Take any $0 \neq u \in \mathfrak{m}_K$, then

$$\mathcal{O}_{\widehat{K}} = \varprojlim \mathcal{O}_K/(u^m)$$

is the ring of integers of $\widehat{K}$ and $\widehat{K} = \mathcal{O}_{\widehat{K}}[1/u]$.

Remark 1.12. The ring $\mathcal{O}_{\widehat{K}}$ does not depend on the choice of u. Indeed, if $v(u) = r > 0$, $v(u') = s > 0$, for any $n \in \mathbb{N}$, there exists $m_n \in \mathbb{N}$, such that $u^{m_n} \in u'^n \mathcal{O}_K$, so

$$\varprojlim \mathcal{O}_K/(u^m) \xrightarrow{\sim} \varprojlim \mathcal{O}_K/(u'^n).$$

Definition 1.13. *A field complete with respect to a valuation v is called a* complete nonarchimedean field*.*

We quote the following well-known result of valuation theory:

Proposition 1.14. *If F is a complete nonarchimedean field with a valuation v, and F' is any algebraic extension of F, then there is a unique valuation v' on F' such that $v'(x) = v(x)$ for any $x \in F$. Moreover,*

(1) *F' is complete if and only if F'/F is finite.*
(2) *If $\alpha, \alpha' \in F'$ are conjugate over F, then $v'(\alpha) = v'(\alpha')$.*

Remark 1.15. By abuse of notations, from now on we shall also write the extended valuation v.

If F is a complete field with respect to a discrete valuation v, then $v(F^\times) = r\mathbb{Z}$ for some constant $r > 0$. We denote $v_F = \frac{1}{r}$ and call it the *normalized valuation* of F, thus v_F is the unique valuation equivalent to v such that $v_F(F^\times) = \mathbb{Z}$. In this case, an element $\pi \in F$ such that $v_F(\pi) = 1$ is a generator of $\mathfrak{m}_F$, called a uniformizing parameter or uniformizer of F.

If F is a valuation field, for any $0 \neq a \in \mathfrak{m}_F$, let v_a denote the unique valuation of F equivalent to the given valuation such that $v_a(a) = 1$.

Definition 1.16. *A* local field *is a complete discrete valuation field whose residue field is perfect of characteristic $p > 0$.*

A p-adic field *is a local field of characteristic* 0.

Example 1.17. A finite extension of $\mathbb{Q}_p$ is a p-adic field. In fact, it is the only p-adic field whose residue field is finite.

Let K be a local field with normalized valuation v_K and perfect residue field k such that $\mathrm{char}\, k = p > 0$ (equivalently $p \in \mathfrak{m}_K$). Let π_K be a uniformizing parameter of K. Then $v_K(\pi_K) = 1$ and $\mathfrak{m}_K = (\pi_K)$. One has topological isomorphisms

$$\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\mathfrak{m}_K^n \cong \varprojlim_n \mathcal{O}_K/\pi_K^n\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/p^n\mathcal{O}_K, \tag{1.7}$$

where $\mathcal{O}_K/p^n\mathcal{O}_K = \mathcal{O}_K$ if $\mathrm{char}\, K = p$. We have the following propositions:

Proposition 1.18. *The local field K is locally compact, equivalently $\mathcal{O}_K$ is compact, if and only if its residue field k is finite.*

Proposition 1.19. *Let S be a set of representatives of k in $\mathcal{O}_K$. Then every element $x \in \mathcal{O}_K$ can be written uniquely as*

$$x = \sum_{\substack{i \geq 0 \\ s_i \in S}} s_i \pi_K^i \tag{1.8}$$

and $x \in K$ can be written uniquely as

$$x = \sum_{\substack{i \geq -n \\ s_i \in S}} s_i \pi_K^i. \tag{1.9}$$

By the binomial theorem, since $p \in \mathfrak{m}_K$, we have the following extremely useful fact:

Lemma 1.20. *For $a, b \in \mathcal{O}_K$,*

$$a \equiv b \bmod \mathfrak{m}_K \quad \Longrightarrow \quad a^{p^n} \equiv b^{p^n} \bmod \mathfrak{m}_K^{n+1} \text{ for } n \geq 0. \tag{1.10}$$

Proposition 1.21. *There exists a unique multiplicative section $s : k \to \mathcal{O}_K$ for the projection $\mathcal{O}_K \to k$.*

Proof. Let $a =\in k$. Since k is perfect, we can find successfully a unique sequence (a_n) in k such that $a_0 = a$, $a_1^p = a_0$, $\cdots$, $a_n^p = a_{n-1}$, in particular $a_n^{p^n} = a$. Let $\widehat{a}_n$ be a(ny) lifting of a_n in $\mathcal{O}_K$.

By (1.10), $\widehat{a}_{n+1}^p \equiv \widehat{a}_n \bmod \mathfrak{m}_K$ implies that $\widehat{a}_{n+1}^{p^{n+1}} \equiv \widehat{a}_n^{p^n} \bmod \mathfrak{m}_K^{n+1}$. Therefore $s(a) := \lim_{n\to\infty} \widehat{a}_n^{p^n}$ exists. By (1.10) again, $s(a)$ is found to be independent of the choice of the liftings. It is easy to check that s is a section of $\mathcal{O}_K \to k$ and is multiplicative. Moreover, if t is another section, we can always choose $\widehat{a}_n = t(a_n)$, then

$$s(a) = \lim_{n\to\infty} \widehat{a}_n^{p^n} = \lim_{n\to\infty} t(a_n)^{p^n} = t(a),$$

hence follows the uniqueness.

Remark 1.22. The element $s(a)$ is called the *Teichmüller representative* of a, and often denoted as $[a]$.

If $\mathrm{char}(K) = p$, then $s(a+b) = s(a) + s(b)$ since $(\widehat{a}_n + \widehat{b}_n)^{p^n} = \widehat{a}_n^{p^n} + \widehat{b}_n^{p^n}$. Thus $s : k \to \mathcal{O}_K$ is a homomorphism of rings. We can and will use it to identify k with a subfield of $\mathcal{O}_K$. Furthermore, we have

Theorem 1.23. *Assume $\mathcal{O}_K$ is a complete discrete valuation ring, k is its residue field and K is its field of fractions. Let π_K be a uniformizing parameter of $\mathcal{O}_K$. Suppose that $\mathcal{O}_K$ (hence K) and k have the same characteristic, then*

$$\mathcal{O}_K = k[[\pi_K]], \quad K = k((\pi_K)).$$

Proof. We only need to show the case that $\mathrm{char}(k) = 0$. In this case, the composite homomorphism $\mathbb{Z} \hookrightarrow \mathcal{O}_K \twoheadrightarrow k$ is injective, hence the homomorphism $\mathbb{Z} \hookrightarrow \mathcal{O}_K$ extends to $\mathbb{Q} \hookrightarrow \mathcal{O}_K$. In this way $\mathcal{O}_K$ contains the field $\mathbb{Q}$. By Zorn's lemma, there exists a maximal subfield of $\mathcal{O}_K$. We denote it by S. Let $\overline{S} \neq 0$ be its image in k. Then $S \to \overline{S}$ is an isomorphism. It suffices to show that $\overline{S} = k$.

First we show k is algebraic over $\overline{S}$. If not, there exists $a \in \mathcal{O}_K$ whose image $\bar{a} \in k$ is transcendental over $\overline{S}$. The subring $S[a]$ maps to $\overline{S}[\bar{a}]$, hence is isomorphic to $S[X]$, and $S[a] \cap \mathfrak{m}_K = 0$. Therefore $\mathcal{O}_K$ contains the field $S(a)$ of rational functions of a, which is contradiction to the maximality of S.

Now for any $\alpha \in k$, let $\bar{f}(X)$ be the minimal polynomial of $\overline{S}(\alpha)$ over $\overline{S}$. Since $\mathrm{char}(k) = 0$, $\bar{f}$ is separable and α is a simple root of $\bar{f}$. Let $f \in S[X]$ be a lifting of $\bar{f}$. By Hensel's Lemma, there exists $x \in \mathcal{O}_K$, $f(x) = 0$ and $\bar{x} = \alpha$. One can lift $\overline{S}[\alpha]$ to $S[x]$ by sending x to α. By the maximality of S, $x \in S$. and thus $k = \overline{S}$.

If K is a p-adic field and $\mathrm{char}(K) = 0$, then in general $s(a+b) \neq s(a)+s(b)$. Witt vectors are very useful in this situation.

1.2.2 Witt vectors.

Assume p is a prime number. Let X, Y, X_i, Y_i ($i \in \mathbb{N}$) be indeterminates. Write $\underline{X} := (X_0, X_1, \cdots)$ and $\underline{Y} := (Y_0, Y_1, \cdots)$.

Definition 1.24. *The n-th* Witt polynomial *of $\underline{X}$ is*

$$\mathtt{W}_n(\underline{X}) = \mathtt{W}_n(X_0, \cdots, X_n) := \sum_{i=0}^{n} p^i X_i^{p^{n-i}}.$$

Remark 1.25. One can easily check that $X_n \in \mathbb{Z}[p^{-1}][\mathtt{W}_0, \cdots, \mathtt{W}_n]$ for each n.

Lemma 1.26. *For every $\Phi(X,Y) \in \mathbb{Z}[X,Y]$, there exists a unique sequence $\{\Phi_n\}_{n\in\mathbb{N}}$ of polynomials*

$$\Phi_n \in \mathbb{Z}[X_0, X_1, \cdots, X_n; Y_0, Y_1, \cdots, Y_n]$$

such that for every $n \in \mathbb{N}$,

$$\Phi(\mathtt{W}_n(\underline{X}), \mathtt{W}_n(\underline{Y})) = \mathtt{W}_n(\Phi_0, \cdots, \Phi_n). \tag{1.11}$$

Replacing the coefficient ring $\mathbb{Z}$ by $\mathbb{Z}_p$, the result still holds.

Proof. First we work in $\mathbb{Z}[\frac{1}{p}][\underline{X}, \underline{Y}]$. Set $\Phi_0(\underline{X}, \underline{Y}) = \Phi(X_0, Y_0)$ and define Φ_n inductively by

$$\Phi_n(\underline{X}, \underline{Y}) = \frac{1}{p^n}\left(\Phi\Big(\sum_{i=0}^{n} p^i X_i^{p^{n-i}}, \sum_{i=0}^{n} p^i Y_i^{p^{n-i}}\Big) - \sum_{i=0}^{n-1} p^i \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}}\right).$$

Clearly Φ_n exists, is unique in $\mathbb{Z}[\frac{1}{p}][\underline{X}, \underline{Y}]$, and is in $\mathbb{Z}[\frac{1}{p}][X_0, \cdots, X_n; Y_0, \cdots, Y_n]$. We only need to prove that Φ_n has coefficients in $\mathbb{Z}$.

This is done by induction on n. For $n = 0$, Φ_0 certainly has coefficients in $\mathbb{Z}$. Assuming Φ_i has coefficients in $\mathbb{Z}$ for $i \leq n$, to show that Φ_{n+1} has coefficients in $\mathbb{Z}$, it suffices to prove that

$$\begin{aligned}&\Phi(X_0^{p^n} + \cdots + p^n X_n; Y_0^{p^n} + \cdots + p^n Y_n)\\ \equiv&\Phi_0(\underline{X}, \underline{Y})^{p^n} + p\Phi_1(\underline{X}, \underline{Y})^{p^{n-1}} + \cdots + p^{n-1}\Phi_{n-1}(\underline{X}, \underline{Y})^p \bmod p^n.\end{aligned}$$

One can verify that

$$\begin{aligned}LHS &\equiv \Phi(X_0^{p^n} + \cdots + p^{n-1}X_{n-1}^p; Y_0^{p^n} + \cdots + p^{n-1}Y_{n-1}^p) \bmod p^n\\ &\equiv \Phi_0(\underline{X}^p, \underline{Y}^p)^{p^{n-1}} + p\Phi_1(\underline{X}^p, \underline{Y}^p)^{p^{n-2}} + \cdots + p^{n-1}\Phi_{n-1}(\underline{X}^p, \underline{Y}^p) \bmod p^n.\end{aligned}$$

By induction, $\Phi_i(\underline{X}, \underline{Y}) \in \mathbb{Z}[\underline{X}, \underline{Y}]$, hence $\Phi_i(\underline{X}^p, \underline{Y}^p) \equiv (\Phi_i(\underline{X}, \underline{Y}))^p \bmod p$, and

$$p^i\Phi_i(\underline{X}^p, \underline{Y}^p)^{p^{n-1-i}} \equiv p^i \cdot \Phi_i(\underline{X}, \underline{Y})^{p^{n-i}} \bmod p^n.$$

Putting all these congruences together, the lemma is proven.

Definition 1.27. *The polynomials*

$$S_n, P_n \in \mathbb{Z}[X_0, \cdots, X_n; Y_0, \cdots, Y_n]$$

are the polynomials associated to $\Phi(X, Y) = X + Y$ and XY, i.e., defined inductively by

$$\mathtt{W}_n(\underline{X}) + \mathtt{W}_n(\underline{Y}) = \mathtt{W}_n(S_0, S_1, \cdots, S_n), \tag{1.12}$$

$$\mathtt{W}_n(\underline{X}) \cdot \mathtt{W}_n(\underline{Y}) = \mathtt{W}_n(P_0, P_1, \cdots, P_n). \tag{1.13}$$

For $\lambda \in \mathbb{Z}_p$, the polynomials $M(\lambda)_n(X_0, \cdots, X_n) \in \mathbb{Z}_p[X_0, \cdots, X_n]$ are polynomials associated to $\Phi(X) = \lambda X$, i.e., defined inductively by

$$\lambda\mathtt{W}_n(\underline{X}) = \mathtt{W}_n(M(\lambda)_0, \cdots, M(\lambda)_n). \tag{1.14}$$

It is clear that

$$S_0 = X_0 + Y_0, \quad P_0 = X_0 Y_0, \quad M(\lambda)_0 = \lambda X_0. \tag{1.15}$$

From $(X_0 + Y_0)^p + p\,S_1 = X_0^p + p\,X_1 + Y_0^p + p\,Y_1$, we get

$$S_1 = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_0^i\, Y_0^{p-i}. \tag{1.16}$$

From $(X_0^p + p\,X_1)\,(Y_0^p + p\,Y_1) = X_0^p\, Y_0^p + p\,P_1$, we get

$$P_1 = X_1\, Y_0^p + X_0^p\, Y_1 + p\, X_1\, Y_1. \tag{1.17}$$

From $\lambda(X_0^p + p\,X_1) = M(\lambda)_0^p + pM(\lambda)_1$, we get

$$M(\lambda)_1 = \lambda X_1 + \frac{\lambda^p - \lambda}{p} X_0^p. \tag{1.18}$$

For general n, it is too complicated to write down S_n, P_n and $M_n(\lambda)$ explicitly. However, from the definition equations, we have

Lemma 1.28. *Assign X_n and Y_n with weight p^n. Then*

(1) *$S_n = X_n + Y_n$ + terms of degree ≥ 2, of which all monomials have same weight p^n.*
(2) *$P_n = p^n X_n Y_n$ + terms of degree ≥ 3, of which all monomials have same $\underline{X}$-weight and $\underline{Y}$-weight p^n, and $P_n(X_0, 0, \cdots, 0; Y_0, \cdots, Y_n) = X_0^{p^n} Y_n$.*
(3) *$M(\lambda)_n = \lambda X_n$ + terms of degree ≥ 2, of which all monomials have same weight p^n.*
(4) *$M(p)_n \equiv X_{n-1}^p \bmod p$ for $n \geq 1$.*

Proof. By induction. The proof of (4) needs the fact that if $a \equiv b \bmod p$, then $a^{p^m} \equiv b^{p^m} \bmod p^{m+1}$.

Remark 1.29. Let S_n^- be the associated integer polynomial to $\Phi(X,Y) = X - Y$. Then

$$\mathtt{W}_n(\underline{X}) - \mathtt{W}_n(\underline{Y}) = \mathtt{W}_n(S_0^-, S_1^-, \cdots, S_n^-). \tag{1.19}$$

Then $S_n^- = X_n - Y_n +$terms of degree ≥ 2, of which all monomials have same weight p^n. Moreover, if $p > 2$, by the fact $-\mathtt{W}_n(Y) = \mathtt{W}_n(-Y)$, then

$$S_n^-(\underline{X}, \underline{Y}) = S_n(\underline{X}, -\underline{Y}). \tag{1.20}$$

Now suppose A is a commutative ring. For $n \geq 1$, let $W_n(A) = A^n$ as a set. For two elements $a = (a_0, a_1, \cdots, a_{n-1}), b = (b_0, b_1, \cdots, b_{n-1}) \in W_n(A)$, define

$$a + b = (s_0, s_1, \cdots, s_{n-1}), \quad a \cdot b = (p_0, p_1, \cdots, p_{n-1}), \tag{1.21}$$

where

$$s_i = S_i(a_0, a_1, \cdots, a_i; b_0, b_1, \cdots, b_i),$$
$$p_i = P_i(a_0, a_1, \cdots, a_i; b_0, b_1, \cdots, b_i).$$

For $a \in W_n(A)$, set

$$w_i = \mathtt{W}_i(a) = a_0^{p^i} + p\, a_1^{p^{i-1}} + \cdots + p^i\, a_i. \tag{1.22}$$

By definition, then

$$w_i(a+b) = w_i(a) + w_i(b) \quad \text{and} \quad w_i(ab) = w_i(a)\, w_i(b).$$

Moreover, let $s_i^{-1} = S_i^{-1}(a_0, \cdots, a_i; b_0, \cdots, b_i)$ and

$$a - b = (s_0^-, \cdots, s_{n-1}^-). \tag{1.23}$$

then $-a = 0 - a \in W_n(A)$,

$$w_i(a-b) = w_i(a) - w_i(b) \quad \text{and} \quad w_i(-a) = -w_i(a).$$

Definition 1.30. *Denote the map*

$$\rho : W_n(A) \longrightarrow A^n, \quad (a_0, \cdots, a_{n-1}) \longmapsto (w_0, \cdots, w_{n-1}).$$

Then

$$\rho(a+b) = \rho(a) + \rho(b) \quad \text{and} \quad \rho(a \cdot b) = \rho(a) \cdot \rho(b).$$

Proposition 1.31. $(W_n(A); +, \cdot)$ *defined by* (1.21) *is a commutative ring with* $0 = (0, \cdots, 0)$ *and* $1 = (1, 0, \cdots, 0)$*, and ρ is a homomorphism of commutative rings. Moreover, for $\lambda \in \mathbb{Z}$ (or $\in \mathbb{Z}_p$ if A is a $\mathbb{Z}_p$-module), define the scalar multiplication $\lambda \cdot a$ in $W_n(A)$ by*

$$\lambda \cdot a = (M_i(\lambda)(a_0, \cdots, a_i))_{0 \le i \le n},$$

then ρ preserves the $\mathbb{Z}$-module (or $\mathbb{Z}_p$-module) structure.

Proof. Note that $X_n \in \mathbb{Z}[p^{-1}][\mathtt{W}_0, \cdots, \mathtt{W}_n]$. Then

(1) If p is invertible in A, ρ is bijective and therefore $W_n(A)$ is a ring isomorphic to A^n.
(2) If A has no p-torsion, by the injection $A \hookrightarrow A[\frac{1}{p}]$, then $W_n(A) \subset W_n(A[\frac{1}{p}])$. If $a, b \in W_n(A)$, then $a - b \in W_n(A)$, so $W_n(A)$ is a subring of $W_n(A[\frac{1}{p}])$.
(3) In general, any commutative ring can be written as $A = R/I$ with R having no p-torsion. Then $W_n(R)$ is a ring, and

$$W_n(I) = \{(a_0, a_1, \cdots, a_{n-1}) \mid a_i \in I\}$$

is an ideal of $W_n(R)$. Then $W_n(R/I)$ is the quotient of $W_n(R)$ by $W_n(I)$, again a ring itself.

The rest is clear.

For the sequence of rings $W_n(A)$, consider the restriction maps

$$\begin{aligned} \mathrm{res}: \ W_{n+1}(A) &\longrightarrow W_n(A) \\ (a_0, a_1, \cdots, a_n) &\longmapsto (a_0, a_1, \cdots, a_{n-1}). \end{aligned}$$

These are surjective homomorphisms of rings. Define

$$W(A) = \varprojlim_n W_n(A). \tag{1.24}$$

Put the topology of inverse limit with the discrete topology on each $W_n(A)$, then $W(A)$ can be viewed as a topological ring. Moreover, if A is already a topological ring, $W_n(A)$ and $W(A)$ are then endowed with the induced topological structures.

Definition 1.32. *The ring $W_n(A)$ is called the* ring of Witt vectors of length n *of A, an element of $W_n(A)$ is called a* Witt vector of length n*.*

The ring $W(A)$ is called the ring of Witt vectors *of A (of infinite length), an element of $W(A)$ is called a* Witt vector*.*

By construction, $W(A)$ as a set is isomorphic to $A^{\mathbb{N}}$. For two Witt vectors $a = (a_0, a_1, \cdots, a_n, \cdots), b = (b_0, b_1, \cdots, b_n, \cdots) \in W(A)$, the addition and multiplication laws are given by

$$a + b = (s_0, s_1, \cdots, s_n, \cdots), \quad a \cdot b = (p_0, p_1, \cdots, p_n, \cdots). \tag{1.25}$$

The map

$$\rho : W(A) \to A^{\mathbb{N}}, \quad (a_0, a_1, \cdots, a_n, \cdots) \mapsto (w_0, w_1, \cdots, w_n, \cdots) \tag{1.26}$$

is a homomorphism of commutative rings and moreover is an isomorphism if p is invertible in A.

The operators W_n and W are actually functorial. Indeed, let $h : A \to B$ be a ring homomorphism, then we get the ring homomorphisms

$$\begin{aligned} W_n(h): \qquad\qquad W_n(A) &\longrightarrow W_n(B) \\ (a_0, a_1, \cdots, a_{n-1}) &\longmapsto (h(a_0), h(a_1), \cdots, h(a_{n-1})) \end{aligned}$$

for $n \geq 1$ and hence the homomorphism $W(h) : W(A) \to W(A)$. Moreover, $W_n(h)$ and $W(h)$ commute with ρ.

Remark 1.33. In fact, W_n is represented by the affine group scheme $\mathbf{W}_n$ over $\mathbb{Z}$:

$$\mathbf{W}_n = \mathrm{Spec}(B), \quad \text{where } B = \mathbb{Z}[X_0, X_1, \cdots, X_{n-1}].$$

with the comultiplication

$$m^* : B \longrightarrow B \otimes_{\mathbb{Z}} B \simeq \mathbb{Z}[X_0, X_1, \cdots, X_{n-1}; Y_0, Y_1, \cdots, Y_{n-1}]$$

given by

$$X_i \longmapsto X_i \otimes 1, \quad Y_i \longmapsto 1 \otimes X_i, \quad m^* X_i = S_i(X_0, X_1, \cdots, X_i; Y_0, Y_1, \cdots, Y_i).$$

Remark 1.34. If A is killed by p, then

$$\begin{aligned} W_n(A) &\xrightarrow{w_i} A \\ (a_0, a_1, \cdots, a_{n-1}) &\longmapsto a_0^{p^i}. \end{aligned}$$

So ρ is given by

$$\begin{aligned} W_n(A) &\xrightarrow{\rho} A^n \\ (a_0, a_1, \cdots, a_{n-1}) &\longmapsto (a_0, a_0^p, \cdots, a_0^{p^{n-1}}). \end{aligned}$$

In this case ρ certainly is not an isomorphism. As a consequence $\rho : W(A) \to A^{\mathbb{N}}$ is not an isomorphism either.

We now define the shift map (the Verschiebung) $\mathtt{V}$, the Teichmüller map s and the Frobenius map φ related to $W(A)$.

Definition 1.35. *Let A be a commutative ring.*

(i) *The* shift map *or* Vershiebung *is the map*

$$\mathtt{V} : W(A) \to W(A), \quad (a_0, \cdots, a_n, \cdots) \mapsto (0, a_0, \cdots, a_n, \cdots). \tag{1.27}$$

and

$$\mathtt{V} : W_n(A) \to W_{n+1}(A), \quad (a_0, \cdots, a_{n-1}) \mapsto (0, a_0, \cdots, a_{n-1}). \tag{1.28}$$

(ii) *The Teichmüller map s is the section*

$$s : A \to W(A), \quad x \mapsto [x] = (x, 0, \cdots, 0, \cdots).$$

(iii) *If A is a ring of characteristic p, the* Frobenius map *φ is the ring homomorphism:*

$$\varphi : W(A) \to W(A), \quad (a_0, a_1, \cdots) \mapsto (a_0^p, a_1^p, \cdots).$$

If moreover, $A = k$ is a perfect field, the Frobenius on $W(k)$ is often denoted as σ.

Proposition 1.36. *The maps $\mathtt{V}$ and s commute with ring homomorphisms. Moreover,*

(1) *The shift map $\mathtt{V}$ is an additive map, and the sequences*

$$0 \longrightarrow W_k(A) \xrightarrow{\mathtt{V}^r} W_{k+r}(A) \longrightarrow W_r(A) \longrightarrow 0 \tag{1.29}$$

are exact.

(2) *The Teichmüller map s is a multiplicative section of $W(A) \to A$, and*

$$(a_0, a_1, \cdots) = \sum_{n=0}^{\infty} \mathtt{V}^n([a_n]), \quad a_i \in A \tag{1.30}$$

$$[x] \cdot (a_0, \cdots) = (xa_0, x^p a_1, \cdots, x^{p^n} a_n, \cdots), \;\; x, a_i \in A. \tag{1.31}$$

Proof. By definition, it is easy to check the commutativity. Because of this, one can reduce the proof of (1) and (2) to the case that p is invertible in A, and then apply the isomorphism $\rho : W(A) \to A^{\mathbb{N}}$. One can also show this fact by just applying Lemma 1.28.

Lemma 1.37. *If A is of characteristic p, then over the Witt ring $W(A)$, one has $\mathtt{V}\varphi = \varphi\mathtt{V} = p$.*

Proof. By Lemma 1.28(4), $p(a_0, a_1, \cdots) = (0, a_0^p, a_1^p, \cdots)$, hence $\mathtt{V}\varphi = \varphi\mathtt{V} = p$.

Recall a commutative ring A of characteristic p is called *perfect* if the endomorphism $x \mapsto x^p$ of A is an automorphism, i.e., if every element of $x \in A$ has a unique p-th root $x^{p^{-1}}$ in A.

Proposition 1.38. *If A is a perfect ring, then every element in $W(A)$ can be written in two forms*

$$(a_0, a_1, \cdots) = \sum_{n=0}^{+\infty} p^n [a_n^{p^{-n}}]. \tag{1.32}$$

Consequently

(1) *The projection $W(A) \to W_n(A)$, $(a_0, a_1, \cdots) \mapsto (a_0, \cdots, a_{n-1})$ induces $W(A)/p^n W(A) \cong W_n(A)$. In particular, $W(A)/pW(A) \cong A$.*
(2) *$W(A)$ is complete and separated by the p-adic topology, i.e. $W(A) = \varprojlim_n W(A)/p^n W(A)$.*

Proof. Clear from the above two results.

Example 1.39. $W(\mathbb{F}_p) = \mathbb{Z}_p$ by identifying the Teichmüller representative $[x]$ of $x \in \mathbb{F}_p$.

1.2.3 Structure of complete discrete valuation rings with mixed characteristic.

As an application of Witt vectors, we discuss the structure of complete discrete valuation rings in the mixed characteristic case. The exposition in this subsection follows the content in Serre [Ser80], Chap. II, §5.

Definition 1.40. *A topological ring A is called a* p-ring *if there exists a decreasing filtration of ideals $\mathfrak{a}_1 \supset \mathfrak{a}_2 \cdots$ satisfying $\mathfrak{a}_m \cdot \mathfrak{a}_n \subset \mathfrak{a}_{m+n}$ such that*

(i) *$A/\mathfrak{a}_1$ is perfect of characteristic p;*
(ii) *$A \cong \varprojlim_n A/\mathfrak{a}_n$.*

A p-ring A is called a strict p-ring *if furthermore p is not a zero-divisor in A and the ideal $\mathfrak{a}_n = p^n A$.*

Example 1.41. Suppose k is a perfect ring of characteristic p.

(1) If k is the residue field of local field K, then $\mathcal{O}_K$ with the filtration $\{\mathfrak{m}_K^n\}$ is a p-ring.
(2) In general, the Witt ring $W(k)$ is a strict p-ring with residue ring k.

Proposition 1.42. *Let A be a p-ring with residue ring k.*

(1) *There exists one and only one system of representatives $f : k \to A$ which commutes with p-th powers: $f(\lambda^p) = f(\lambda)^p$.*
(2) *For $a \in A$, $a \in S = f(k)$ if and only if a is a p^n-th power for all $n \geq 0$.*
(3) *This system of representatives is multiplicative, i.e., one has $f(\lambda\mu) = f(\lambda)f(\mu)$ for all $\lambda, \mu \in k$.*
(4) *If A has characteristic p, this system of representatives is additive, i.e., $f(\lambda + \mu) = f(\lambda) + f(\mu)$.*

Proof. Similar to the proof of Proposition 1.21. We leave it as an exercise.

Remark 1.43. For Example 1.41, f is nothing but the Teichmüller representative $x \mapsto [x]$.

By Proposition 1.42, if A is a p-ring, let $f : k = A/\mathfrak{a}_1 \to A$ be the system of multiplicative representatives, then for every sequence (α_i) of elements in $A/\mathfrak{a}_1$, the series

$$\sum_{i=0}^{\infty} f(\alpha_i)p^i \tag{1.33}$$

converges to an element $a \in A$. Furthermore if A is a strict p-ring, every element $a \in A$ can be uniquely expressed in the form of a series of type (1.33). In this case, let $\beta_i = \alpha_i^{p^i}$, then $a = \sum\limits_{i=0}^{\infty} f(\beta_i^{p^{-i}})p^i$. We call $\{\beta_i\}$ the *coordinates* of a.

Example 1.44. Let $\{X_\alpha\}$ be a family of indeterminates and $S = \bigcup\limits_{n\geq 0} \mathbb{Z}[X_\alpha^{p^{-n}}]$. Let $\widehat{S} = \widehat{\mathbb{Z}[X_\alpha^{p^{-\infty}}]}$, the completion of S by the p-adic filtration $\{p^n S\}_{n\geq 0}$. Then $\widehat{S}$ is a strict p-ring, whose residue ring $\widehat{S}/p\widehat{S} = F_p[X_\alpha^{p^{-\infty}}]$ is perfect of characteristic p. Since X_α admits p^n-th roots for all n, we identify X_α in $\widehat{S}$ with its image in the residue ring.

Suppose $X_0, \cdots, X_n, \cdots$ and $Y_0, \cdots, Y_n, \cdots$ are indeterminates in the ring $\widehat{\mathbb{Z}[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]}$. Consider the two elements

$$x = \sum_{i=0}^{\infty} X_i p^i, \quad y = \sum_{i=0}^{\infty} Y_i p^i.$$

If $*$ is one of the operations $+, \times, -$, then $x * y$ is also an element in the ring and can be written uniquely of the form

$$x * y = \sum_{i=0}^{\infty} f(Q_i^*)p^i, \quad \text{with} \quad Q_i^* \in \mathbb{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}].$$

As Q_i^* are $p^{-\infty}$-polynomials with coefficients in the prime field $\mathbb{F}_p$, one can evaluate it in a perfect ring k of characteristic p. More precisely,

Proposition 1.45. *If A is a p-ring with residue ring k and $f : k \to A$ is the system of multiplicative representatives of A. Suppose $\{\alpha_i\}$ and $\{\beta_i\}$ are two sequences of elements in k. Then*

$$\sum_{i=0}^{\infty} f(\alpha_i)p^i * \sum_{i=0}^{\infty} f(\beta_i)p^i = \sum_{i=0}^{\infty} f(\gamma_i)p^i$$

with $\gamma_i = Q_i^*(\alpha_0, \alpha_1, \cdots; \beta_0, \beta_1, \cdots)$.

Proof. One sees immediately that there is a homomorphism

$$h : \mathbb{Z}[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}] \to A$$

which sends X_i to $f(\alpha_i)$ and Y_i to $f(\beta_i)$. This homomorphism extends by continuity to $\widehat{\mathbb{Z}[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}]} \to A$, which sends $x = \sum X_i p^i$ to $\alpha = \sum f(\alpha_i)p^i$ and $y = \sum Y_i p^i$ to $\beta = \sum f(\beta_i)p^i$. Again h induces, on the residue rings, a homomorphism $\bar{h} : \mathbb{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}] \to k$ which sends X_i to α_i and Y_i to β_i. Since h commutes with the multiplicative representatives, one thus has

$$\begin{aligned} \sum f(\alpha_i)p^i * \sum f(\beta_i)p^i =& h(x) * h(y) = h(x * y) \\ =& \sum h(f(Q_i^*))p^i = \sum f(\bar{h}(Q_i^*))p^i, \end{aligned}$$

this completes the proof of the proposition, as $\bar{h}(Q_i^*)$ is nothing but γ_i.

Theorem 1.46. *Suppose A and A' are two p-rings with residue rings k and k', suppose A is also strict. For every homomorphism $\bar{g} : k \to k'$, there exists exactly one homomorphism $g : A \to A'$ such that the diagram*

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d] & A' \arrow[d] \\ k \arrow[r, "\bar{g}"] & k' \end{tikzcd}$$

is commutative. Consequently,

(1) *Two strict p-rings with same residue ring are canonically isomorphic.*
(2) *For every perfect ring k of characteristic p, $W(k)$ is the only strict p-ring with residue ring k up to unique canonical isomorphism.*

Proof. For $a = \sum_{i=0}^{\infty} f_A(\alpha_i)p^i \in A$, if g is defined, then

$$g(a) = \sum_{i=0}^{\infty} g(f_A(\alpha_i)) \cdot p^i = \sum_{i=0}^{\infty} f_{A'}(\bar{g}(\alpha_i)) \cdot p^i,$$

hence follows the uniqueness. But by Proposition 1.45, the map g defined above is indeed a homomorphism.

Corollary 1.47. *If k and k' are two perfect rings of characteristic p, then* $\mathrm{Hom}(k, k') = \mathrm{Hom}(W(k), W(k'))$.

Definition 1.48. *Let A be a complete discrete valuation ring, with residue field k. Suppose A has characteristic 0 and k has characteristic $p > 0$. The integer $e = e_A := v(p)$ is called the* absolute ramification index *of A. If $e = 1$, i.e., if p is a local uniformizer of A, then A is called* absolutely unramified.

Theorem 1.49. (1) *For every perfect field k of characteristic p, $W(k)$ is the unique complete discrete valuation ring of characteristic 0 (up to unique isomorphism) which is absolutely unramified and has k as its residue field.*

(2) *Let A be a complete discrete valuation ring of characteristic 0 with a perfect residue field k of characteristic $p > 0$. Let e be its absolute ramification index. Then there exists a unique homomorphism of $\iota : W(k) \to A$ which makes the diagram*

$$\begin{tikzcd} W(k) \arrow[rr, "\iota"] \arrow[dr] & & A \arrow[dl] \\ & k & \end{tikzcd}$$

commutative, moreover ι is injective, and A is a free $W(k)$-module of rank equal to e.

Proof. (1) is a special case of Theorem 1.46.

For (2), the existence and uniqueness of ι follow from Theorem 1.46, since A is a p-ring. As A is of characteristic 0, ι is injective. If π_A is a uniformizer of A, then every $a \in A$ can be uniquely written as $a = \sum_{i=0}^{\infty} f(\alpha_i)\pi_A^i$ for $\alpha_i \in k$. Replaced π_A^e by $p \times$ (unit), then a is uniquely written as

$$a = \sum_{j=0}^{e-1} \left(\sum_{i=0}^{\infty} f(\alpha_{ij})p^i \right) \pi_A^j, \qquad \alpha_{ij} \in k.$$

Thus $\{1, \pi_A, \cdots, \pi_A^{e-1}\}$ is a basis of A as a $W(k)$-module.

1.2.4 Cohen rings.

We have seen that if k is a perfect field, then the ring of Witt vectors $W(k)$ is the unique complete discrete valuation ring which is absolutely unramified and with residue field k. However, if k is not perfect, the situation is more complicated. We first quote two theorems without proof from Commutative Algebra (cf. Matsumura [Mat86], § 29, pp 223-225):

Theorem 1.50 (Theorem 29.1, [Mat86]). *Let $(A, \varpi A, k = A/\varpi A)$ be a discrete valuation ring and K a field extension of k, then there exists a discrete valuation ring $(B, \varpi B, K)$ containing A.*

Theorem 1.51 (Theorem 29.2, [Mat86]). *Let $(A, \mathfrak{m}_A, k_A)$ be a complete local ring, and $(R, \mathfrak{m}_R, k_R)$ be an absolutely unramified discrete valuation ring of characteristic 0 (i.e., $\mathfrak{m}_R = pR$). Then for every homomorphism $h : k_R \to k_A$, there exists a local homomorphism $g : R \to A$ which induces h on the ground field.*

Remark 1.52. The above theorem is a generalization of Proposition 1.46. However, in this case there are possibly many g inducing h. For example, let $k = \mathbb{F}_p(x)$ and $A = \mathbb{Z}_p(x)$, then the homomorphism $x \mapsto x + \alpha$ in A for any $\alpha \in p\mathbb{Z}_p$ induces the identity map in k.

Applying $A = \mathbb{Z}_p$ to Theorem 1.50, then if K is a given field of characteristic p, there exists an absolutely unramified complete discrete valuation ring R of characteristic 0 with residue field K. By Theorem 1.51, this ring R is unique up to isomorphism.

Definition 1.53. *Let k be a field of characteristic $p > 0$, the* Cohen ring $\mathcal{C}(k)$ *is the unique (up to isomorphism) absolutely unramified complete discrete valuation ring of characteristic 0 whose residue field is k.*

We now give an explicit construction of $\mathcal{C}(k)$. Recall that a *p-basis* of a field k is a set B of elements of k, such that

(i) $[k^p(b_1, \cdots, b_r) : k^p] = p^r$ for any r distinct elements $b_1, \cdots, b_r \in B$;
(ii) $k = k^p(B)$.

If k is perfect, only the empty set is a p-basis of k; if k is imperfect, there always exist nonempty sets satisfying condition (i), then any maximal such set (which must exist, by Zorn's Lemma) must also satisfy (ii) and hence is a p-basis.

Let B be a fixed p-basis of k, then $k = k^{p^n}(B)$ for every $n > 0$, and $B^{p^{-n}} = \{b^{p^{-n}} \mid b \in B\}$ is a p-basis of $k^{p^{-n}}$. Let $I_n = \bigoplus_B \{0, \cdots, p^n - 1\}$, then

$$T_n = \left\{ \mathfrak{b}^\alpha = \prod_{b \in B} b^{\alpha_b}, \alpha = (\alpha_b)_{b \in B} \in I_n \right\}$$

generates k as a k^{p^n}-vector space, and in general $T_n^{p^m}$ is a basis of k^{p^m} over $k^{p^{n+m}}$. Set

$$\begin{aligned}\mathcal{C}_{n+1}(k) = \text{the subring of } W_{n+1}(k) \text{ generated by}\\ W_{n+1}(k^{p^n}) \text{ and } [b] \text{ for } b \in B.\end{aligned}$$

For $x \in k$, we define the Teichmüller representative $[x] = (x, 0, \cdots, 0) \in W_{n+1}(k)$. We also define the shift map V on $W_{n+1}(k)$ by $V((x_0, \cdots, x_n)) = (0, x_0, \cdots, x_{n-1})$. Then every element $x \in W_{n+1}(k)$ can be written as

$$x = (x_0, \cdots, x_n) = [x_0] + V([x_1]) + \cdots + V^n([x_n]).$$

We also has

$$[y]V^r(x) = V^r([y^{p^r}]x).$$

Then $\mathcal{C}_{n+1}(k)$ is nothing but the additive subgroup of $W_{n+1}(k)$ generated by $\{V^r([(\mathfrak{b}^\alpha)^{p^r}x]) \mid \mathfrak{b}^\alpha \in T_{n-r}, x \in k^{p^n}, r = 0, \cdots, n\}$. By Lemma 1.37, one sees that

$$V^r(\varphi^r([x])) = p^r[x] \bmod V^{r+1}.$$

Let $\mathscr{U}_r$ be ideals of $\mathcal{C}_{n+1}(k)$ defined by

$$\mathscr{U}_r = \mathcal{C}_{n+1}(k) \cap V^r(W_{n+1}(k)).$$

Then $\mathscr{U}_r$ is the additive subgroup generated by $\{V^m([(\mathfrak{b}^\alpha)^{p^m}x]) \mid \mathfrak{b}^\alpha \in T_{n-m}, x \in k^{p^n}, m \geq r\}$. Then we have $\mathcal{C}_{n+1}(k)/\mathscr{U}_1 \simeq k$ and the multiplication

$$p^r : \mathcal{C}_{n+1}(k)/\mathscr{U}_1 \longrightarrow \mathscr{U}_r/\mathscr{U}_{r+1}$$

induces an isomorphism for all $r \leq n$. Thus $\mathscr{U}_n$ is generated by p^n and by decreasing induction, one has $\mathscr{U}_r = p^r\mathcal{C}_{n+1}(k)$. Moreover, for any $x \in \mathcal{C}_{n+1}(k) - \mathscr{U}_1$, let y be a preimage of $\bar{x}^{-1} \in \mathcal{C}_{n+1}(k)/\mathscr{U}_1$, then $xy = 1 - z$ with $z \in \mathscr{U}_1$ and $xy(1 + z + \cdots + z^n) = 1$, thus x is invertible. In conclusion, we have

Proposition 1.54. *The ring $\mathcal{C}_{n+1}(k)$ is a local ring whose maximal ideal is generated by p, whose residue field is isomorphic to k. For every $r \leq n$, the multiplication by p^r induces an isomorphism of $\mathcal{C}_{n+1}(k)/p\mathcal{C}_{n+1}(k)$ with $p^r\mathcal{C}_{n+1}(k)/p^{r+1}\mathcal{C}_{n+1}(k)$, and $p^{n+1}\mathcal{C}_{n+1}(k) = 0$.*

Lemma 1.55. *The canonical projection* $\mathrm{pr} : W_{n+1}(k) \to W_n(k)$ *induces a surjective homomorphism $\vartheta : \mathcal{C}_{n+1}(k) \to \mathcal{C}_n(k)$.*

Proof. By definition, the image of $\mathcal{C}_{n+1}(k)$ by pr is the subring of $W_n(k)$ generated by $W_n(k^{p^n})$ and $[b]$ for $b \in B$, but $\mathcal{C}_n(k)$ is the subring generated by $W_n(k^{p^{n-1}})$ and $[b]$ for $b \in B$, thus the map ϑ is well defined.

For $n \geq 1$, the filtration $W_n(k) \supset V(W_n(k)) \cdots \supset V^{n-1}(W_n(k)) \supset V^n(W_n(k)) = 0$ induces the filtration of $\mathcal{C}_n(k) \supset p\mathcal{C}_n(k) \cdots \supset p^{n-1}\mathcal{C}_n(k) \supset$

$p^n\mathcal{C}_n(k) = 0$. To show ϑ is surjective, it suffices to show that the associate graded map is surjective. But for $r < n$, we have the following commutative diagram

$$\begin{array}{ccc} p^r\mathcal{C}_{n+1}(k)/p^{r+1}\mathcal{C}_{n+1}(k) & \xrightarrow{\operatorname{gr}\vartheta} & p^r\mathcal{C}_n(k)/p^{r+1}\mathcal{C}_n(k) \\ {\scriptstyle j}\big\downarrow & & {\scriptstyle j'}\big\downarrow \\ V^rW_{n+1}(k)/V^{r+1}W_{n+1}(k) \simeq k & \xrightarrow{\operatorname{gr}\mathrm{pr}=\mathrm{Id}} & V^rW_n(k)/V^{r+1}W_n(k) \simeq k. \end{array}$$

Since the inclusion j(resp. j') identifies $p^r\mathcal{C}_{n+1}(k)/p^{r+1}\mathcal{C}_{n+1}(k)$ (resp. $p^r\mathcal{C}_n(k)/p^{r+1}\mathcal{C}_n(k)$) to k^{p^r}, thus $\operatorname{gr}\vartheta$ is surjective for $r < n$. For $r = n$, $p^n\mathcal{C}_n(k) = 0$. Then $\operatorname{gr}\vartheta$ is surjective at every grade and hence ϑ is surjective.

By Proposition 1.54, we thus have

Theorem 1.56. *The ring* $\varprojlim_n \mathcal{C}_n(k)$ *is the Cohen ring* $\mathcal{C}(k)$ *of* k.

Remark 1.57. (a) By construction, $\mathcal{C}(k)$ can be identified with a subring of $W(k)$; moreover $\mathcal{C}(k)$ contains $W(k_0)$ where $k_0 = \bigcap_{n\in N} k^{p^n}$ is the maximal perfect subfield of k.

(b) As $\mathcal{C}(k)$ contains the multiplicative representatives $[b]$ for $b \in B$, it contains all elements $[B^\alpha]$ and $[B^{-\alpha}]$ for $n \in N$ and $\alpha \in I_n$.

1.3 Galois groups of extensions of local fields

In this section, we let K be a local field with residue field $k = k_K$ perfect of characteristic p and normalized valuation v_K. Let $\mathcal{O}_K$ be the ring of integers of K, whose maximal ideal is $\mathfrak{m}_K$. Let $U_K = \mathcal{O}_K^\times = \mathcal{O}_K - \mathfrak{m}_K$ be the group of units and $U_K^i = 1 + \mathfrak{m}_K^i$ for $i \geq 1$. Replacing K by L, a finite separable extension of K, we get corresponding notations $k_L, v_L, \mathcal{O}_L, \mathfrak{m}_L$, U_L and U_L^i. Recall the following notations:

(i) $e_{L/K} \in \mathbb{N}^*$: the ramification index defined by $v_K(L^\times) = \frac{1}{e_{L/K}}\mathbb{Z}$;
(ii) $e'_{L/K}$: the prime-to-p part of $e_{L/K}$;
(iii) $p^{r_{L/K}}$: the p-part of $e_{L/K}$;
(iv) $f_{L/K}$: the index of residue field extension $[k_L : k]$.

From previous section, if $\operatorname{char}(K) = p > 0$, then $K = k((\pi_K))$ for π_K a uniformizing parameter of $\mathfrak{m}_K$; if $\operatorname{char}(K) = 0$, let $K_0 = \operatorname{Frac} W(k) = W(k)[1/p]$, then $[K : K_0] = e_K = v_K(p)$, and K/K_0 is totally ramified.

1.3.1 Ramification groups of finite Galois extensions.

Let L/K be a finite Galois extension with Galois group $G = \mathrm{Gal}(L/K)$. Then G acts on the ring $\mathcal{O}_L$. We fix an element x of $\mathcal{O}_L$ which generates $\mathcal{O}_L$ as an $\mathcal{O}_K$-algebra (such an x exists by p-adic analysis).

Lemma 1.58. *Let $s \in G$, and let i be an integer ≥ -1. Then the following three conditions are equivalent:*

(1) *s operates trivially on the quotient ring $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$.*
(2) *$v_L(s(a) - a) \geq i + 1$ for all $a \in \mathcal{O}_L$.*
(3) *$v_L(s(x) - x) \geq i + 1$.*

Proof. This is a trivial exercise.

Proposition 1.59. *For each integer $i \geq -1$, let G_i be the set of $s \in G$ satisfying the conditions of Lemma 1.58. Then the G_i's form a decreasing sequence of normal subgroups of G. Moreover, $G_{-1} = G$, G_0 is the inertia subgroup of G and $G_i = \{1\}$ for i sufficiently large.*

Proof. The sequence is clearly a decreasing sequence of subgroups of G. We want to show that G_i is normal for all i. For every $s \in G$ and every $t \in G_i$, since G_i acts trivially on the quotient ring $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$, we have $sts^{-1}(x) \equiv x \bmod \mathfrak{m}_L^{i+1}$, namely, $sts^{-1} \subseteq G_i$. Thus, G_i is a normal subgroup for all i. The remaining parts follow just by definition.

Definition 1.60. *The group G_i is called the i-*th ramification group *of G or of the extension L/K.*

By convention, the inertia subgroup G_0 is also denoted by $I(L/K)$ and its invariant field by $L_0 = (L/K)^{\mathrm{ur}}$; the group G_1 is also denoted by $P(L/K)$ and is called the wild inertia subgroup *of G, and its invariant field denoted by $L_1 = (L/K)^{\mathrm{tame}}$.*

Remark 1.61. Let H be a subgroup of G and $K' = L^H$. If $x \in \mathcal{O}_L$ is a generator of the $\mathcal{O}_K$-algebra $\mathcal{O}_L$, then it is also a generator of the $\mathcal{O}_{K'}$-algebra $\mathcal{O}_L$. Then the i-th ramification group H_i of H is nothing but $G_i \cap H$. In particular, the higher ramification groups of G are equal to those of G_0, therefore the study of higher ramification groups can always be reduced to the totally ramified case.

In the following, we describe the ramifications groups in more detail.

Proposition 1.62. *Let π_L be a uniformizer of L. For any $s \in G_0$ and $i \in \mathbb{N}$,*

$$s \in G_i \iff s(\pi_L)/\pi_L = 1 \bmod \mathfrak{m}_L^i \iff s(\pi_L)/\pi_L \in U_L^i.$$

Proof. Replacing G by G_0 reduces us to the case of a totally ramified extension. In this case π_L is a generator of $\mathcal{O}_L$ as an $\mathcal{O}_K$-algebra. Since the formula $v_L(s(\pi_L) - \pi_L) = 1 + v_L(s(\pi_L)/\pi_L - 1)$, we have $s(\pi_L)/\pi_L \equiv 1 \bmod \mathfrak{m}_L^i \Leftrightarrow s \in G_i$.

We recall the following result from study of units of local fields:

Proposition 1.63. (1) $U_L/U_L^1 = k_L^\times$;

(2) *For $i \geq 1$, the group U_L^i/U_L^{i+1} is canonically isomorphic to the group $\mathfrak{m}_L^i/\mathfrak{m}_L^{i+1}$, which is itself isomorphic (non-canonically) to the additive group of the residue field k_L.*

Then we have a more precise description of G_i/G_{i+1}:

Proposition 1.64. *The map*

$$G_i \longrightarrow U_L^i, \quad s \longmapsto s(\pi_L)/\pi_L$$

induces an injective homomorphism

$$\theta_i : G_i/G_{i+1} \hookrightarrow U_L^i/U_L^{i+1} \tag{1.34}$$

of groups which is independent of the choice of the uniformizer π. Moreover,

(1) *The group G_0/G_1 is cyclic of order prime to $p = \operatorname{char} k$, and is isomorphic to a subgroup of the group of roots of unity $\boldsymbol{\mu}(k_L)$ of k_L via the map θ_0.*
(2) *The quotients G_i/G_{i+1} for $i \geq 1$ are abelian groups of p-power order, and in fact are direct products of cyclic groups of order p.*
(3) *The group G_1 is a p-group, the inertia group G_0 is the semi-direct product of a cyclic group of order prime to p with a normal subgroup whose order is a power of p.*

Remark 1.65. (a) By definition, L_0 is the maximal unramified subextension inside L. By Proposition 1.64, L_1 is the maximal subextension of L with ramification index prime to p, which is called the *maximal tamely ramified subextension* inside L.
(b) Proposition 1.64 also implies that G_0 is solvable, and so is G if k is finite.

In fact, we can describe the cyclic group $G_0/G_1 = I(L/K)/P(L/K)$ more explicitly.

Let $N = e'_{L/K} = [L_1 : L_0]$. The image of θ_0 in $k_L^\times$ is a cyclic group of order N prime to p, thus $k_L = k_{L_0}$ contains a primitive N^{th}-root of 1 and $\operatorname{Im}\theta_0 = \boldsymbol{\mu}_N(k_L) = \{\varepsilon \in k_L \mid \varepsilon^N = 1\}$ is of order N. By Hensel's lemma, L_0 contains a primitive N-th root of unity. By Kummer theory, there exists a uniformizing parameter ϖ of L_0 such that

$$L_1 = L_0(\alpha) \text{ with } \alpha \text{ a root of } X^N - \varpi.$$

The homomorphism θ_0 is the canonical isomorphism

$$\begin{aligned} \operatorname{Gal}(L_1/L_0) &\xrightarrow{\sim} \boldsymbol{\mu}_N(k_L) \\ g &\longmapsto \varepsilon \quad \text{if } g\,\alpha = [\varepsilon]\,\alpha, \end{aligned}$$

where $[\varepsilon]$ is the Teichmüller representative of ε.

By the short exact sequence

$$1 \longrightarrow \mathrm{Gal}(L_1/L_0) \longrightarrow \mathrm{Gal}(L_1/K) \longrightarrow \mathrm{Gal}(k_L/k) \longrightarrow 1,$$

$\mathrm{Gal}(L_1/K)$ acts on $\mathrm{Gal}(L_1/L_0)$ by conjugation. Because the group $\mathrm{Gal}(L_1/L_0)$ is abelian, this action factors through an action of $\mathrm{Gal}(k_L/k)$. The isomorphism $\mathrm{Gal}(L_1/L_0) \xrightarrow{\sim} \boldsymbol{\mu}_N(k_L)$ then induces an action of $\mathrm{Gal}(k_L/k)$ over $\boldsymbol{\mu}_N(k_L)$, which is the natural action of $\mathrm{Gal}(k_L/k)$.

Suppose $L/M/K$ is a tower of finite Galois extensions. Let $G = \mathrm{Gal}(L/K)$ and $G' = \mathrm{Gal}(M/K)$, let $N = e'_{L/K}$ and $N' = e'_{M/K}$. Then one has a commutative diagram

$$\begin{tikzcd} G_0/G_1 \arrow[r, "\theta_0"] \arrow[d, "\mathrm{res}"'] & \mu_N(k_L) \arrow[d, "\varepsilon \mapsto \varepsilon^{N/N'}"] \\ G'_0/G'_1 \arrow[r, "\theta_0"] & \mu_{N'}(k_M). \end{tikzcd} \tag{1.35}$$

1.3.2 The Galois group of K^s/K.

Let K^s be a separable closure of K and $G_K = \mathrm{Gal}(K^s/K)$. Let $\mathcal{L}$ be the set of finite Galois extensions L of K contained in K^s, then

$$K^s = \bigcup_{L \in \mathcal{L}} L, \qquad G_K = \varprojlim_{L \in \mathcal{L}} \mathrm{Gal}(L/K).$$

Let

$$K^{\mathrm{ur}} = \bigcup_{\substack{L \in \mathcal{L} \\ L/K \text{ unramified}}} L, \qquad K^{\mathrm{tame}} = \bigcup_{\substack{L \in \mathcal{L} \\ L/K \text{ tamely ramified}}} L.$$

Then K^{ur} and K^{tame} are the maximal unramified and maximal tamely ramified extensions of K contained in K^s respectively.

The valuation of K extends uniquely to K^s, but the valuation on K^s is no more discrete, actually $v_K((K^s)^\times) = \mathbb{Q}$, and K^s is no more complete for the valuation.

The field $\bar{k} = \mathcal{O}_{K^{\mathrm{ur}}}/\mathfrak{m}_{K^{\mathrm{ur}}}$ is the algebraic closure of k. We use the notations

(i) $I_K = \mathrm{Gal}(K^s/K^{\mathrm{ur}})$ is the inertia subgroup, which is a closed normal subgroup of G_K;
(ii) $G_K/I_K = \mathrm{Gal}(K^{\mathrm{ur}}/K) = \mathrm{Gal}(\bar{k}/k) = G_k$;
(iii) $P_K = \mathrm{Gal}(K^s/K^{\mathrm{tame}})$ is the wild inertia subgroup, which is a closed normal subgroup of I_K and of G_K;
(iv) $I_K/P_K =$ the tame quotient of the inertia subgroup.

Note that P_K is a pro-p-group, the inverse limit of finite p-groups.

For each integer N prime to p, the N-th roots of unity $\boldsymbol{\mu}_N(\bar{k})$ is cyclic of order N. We get a canonical isomorphism

$$I_K/P_K \xrightarrow{\sim} \varprojlim_{\substack{N\in\mathbb{N} \\ N \text{ prime to } p \\ \text{ordering} = \text{divisibility}}} \boldsymbol{\mu}_N(\bar{k}),$$

by the diagram (1.35). Therefore we get

Proposition 1.66. *If write $\mathbb{Z}_\ell(1) = \varprojlim_n \mu_{\ell^n}$, which is the Tate twist of $\mathbb{Z}_\ell$, then*

$$I_K/P_K \xrightarrow[\textit{canonically}]{\simeq} \prod_{\ell\neq p} \mathbb{Z}_\ell(1). \tag{1.36}$$

As $G_K/I_K \simeq \mathrm{Gal}(\bar{k}/k) = G_k$, the action by conjugation of G_k on I_K/P_K gives the natural action on $\mathbb{Z}_\ell(1)$.

1.3.3 The functions Φ and Ψ.

Assume L/K is a finite Galois extension and $G = \mathrm{Gal}(L/K)$. Set

$$i_G: \quad G \to \mathbb{N}, \quad s \mapsto v_L(s(x)-x). \tag{1.37}$$

The function i_G has the following properties:

(i) $i_G(s) \geq 0$ and $i_G(1) = +\infty$;
(ii) $i_G(s) \geq i+1 \Longleftrightarrow s \in G_i$;
(iii) $i_G(tst^{-1}) = i_G(s)$;
(iv) $i_G(st) \geq \min\{i_G(t), i_G(s)\}$.

Let H be a subgroup of G. Let K' be the subextension of L fixed by H. Following Remark 1.61, we have

Proposition 1.67. *For every $s \in H$, $i_H(s) = i_G(s)$, and $H_i = G_i \cap H$.*

Suppose in addition that the subgroup H is normal, then the quotient group G/H may be identified with the Galois group of K'/K.

Proposition 1.68. *For every $\delta \in G/H$,*

$$i_{G/H}(\delta) = \frac{1}{e'} \sum_{s\to\delta} i_G(s), \tag{1.38}$$

where $e' = e_{L/K'}$ is the ramification index of L over K'.

Proof. For $\delta = 1$, both sides are equal to $+\infty$, so the equation holds.

Suppose $\delta \neq 1$. Let x(resp. y) be an $\mathcal{O}_K$-generator of $\mathcal{O}_L$(resp. $\mathcal{O}_{K'}$). By definition

$$e' i_{G/H}(\delta) = e' v_{K'}(\delta(y)-y) = v_L(\delta(y)-y), \text{ and } i_G(s) = v_L(s(x)-x).$$

If we choose one $s \in G$ representing δ, the other representatives have the form st for some $t \in H$. Hence it comes down to showing that the elements $a = s(y) - y$ and $b = \prod_{t \in H}(st(x) - x)$ generate the same ideal in $\mathcal{O}_L$.

Let $f(X) = \sum_i c_i X^i \in \mathcal{O}_{K'}[X]$ be the minimal polynomial of x over the intermediate field K'. For $s \in G$, denote by $s(f)(X) = \sum_i s(c_i)X^i$. Then

$$f(X) = \prod_{t \in H}(X - t(x)), \quad s(f)(X) = \prod_{t \in H}(X - st(x)).$$

As $s(f) - f$ has coefficients divisible by $s(y) - y$, one sees that $a = s(y) - y$ divides $s(f)(x) - f(x) = s(f)(x) = \pm b$.

It remains to show that b divides a. Write $y = g(x)$ as a polynomial in x, with coefficients in $\mathcal{O}_K$. The polynomial $g(X) - y \in \mathcal{O}_{K'}[X]$ has x as a root, therefore

$$g(X) - y = f(X)h(X) \text{ with some } h \in \mathcal{O}_{K'}[X].$$

Transform this equation by s and substitute x for X in the result; ones gets $y - s(y) = s(f)(x)s(h)(x)$, which shows that $b = \pm s(f)(x)$ divides a.

Let u be a real number ≥ 0. Define $G_u := G_i$ where i is the smallest integer $\geq u$. Thus

$$s \in G_u \Longleftrightarrow i_G(s) \geq u + 1.$$

Put

$$\Phi(u) := \int_0^u (G_0 : G_t)^{-1} dt, \tag{1.39}$$

where for $-1 \leq u \leq 0$,

$$(G_0 : G_u) := \begin{cases} (G_{-1} : G_0)^{-1}, & \text{when } u = -1; \\ 1, & \text{when} -1 < u \leq 0. \end{cases}$$

Thus the function $\Phi(u)$ is equal to u between -1 and 0. For $m \leq u \leq m + 1$ where m is a nonnegative integer, we have

$$\Phi(u) = \frac{1}{g_0}\Big(g_1 + g_2 + ... + g_m + (u - m)g_{m+1}\Big), \text{ with } g_i = |G_i|. \tag{1.40}$$

In particular,

$$\Phi(m) + 1 = \frac{1}{g_0}\sum_{i=0}^{m} g_i. \tag{1.41}$$

Immediately one can verify

Proposition 1.69. *The function $\Phi : [-1, +\infty) \to [-1, +\infty)$ is continuous, piecewise linear, increasing and concave, and*

(1) $\Phi(0) = 0$, $\Phi(-1) = -1$*;*

(2) *if denote by Φ'_r and Φ'_l the right and left derivatives of Φ, then*

$$\Phi'_l(u) = \frac{1}{(G_0 : G_u)}, \qquad \Phi'_r(u) = \begin{cases} \frac{1}{(G_0:G_u)}, & \text{if } u \notin \mathbb{Z}; \\ \frac{1}{(G_0:G_{u+1})}, & \text{if } u \in \mathbb{Z}. \end{cases}$$

Moreover, Φ is characterized by these properties.

Proposition 1.70. $\Phi(u) = \frac{1}{g_0} \sum_{s\in G} \min\{i_G(s), u+1\} - 1.$

Proof. Let $\theta(u)$ be the function on the right hand side. It is continuous and piecewise linear. One has $\theta(0) = 0$, and if $m \geq -1$ is an integer and $m < u < m+1$, then

$$\theta'(u) = \frac{1}{g_0}\#\{s \in G \mid i_G(s) \geq m+2\} = \frac{1}{(G_0 : G_{m+1})} = \Phi'(u).$$

Hence $\theta = \Phi$.

Theorem 1.71 (Herbrand). *Let K'/K be a Galois subextension of L/K and $H = G(L/K')$. Then one has $G_u(L/K)H/H = G_v(K'/K)$ where $v = \Phi_{L/K'}(u)$.*

Proof. Let $G = G(L/K)$, $H = G(L/K')$. For every $s' \in G/H$, we choose a preimage $s \in G$ of maximal value $i_G(s)$ and show that

$$i_{G/H}(s') - 1 = \Phi_{L/K'}(i_G(s) - 1). \tag{1.42}$$

Let $m = i_G(s)$. If $t \in H$ belongs to $H_{m-1} = G_{m-1}(L/K')$, then $i_G(t) \geq m$, and $i_G(st) \geq m$ and so that $i_G(st) = m$. If $t \notin H_{m-1}$, then $i_G(t) < m$ and $i_G(st) = i_G(t)$. In both cases we therefore find that $i_G(st) = \min\{i_G(t), m\}$. Applying Proposition 1.68, since $i_G(t) = i_H(t)$ and $e' = e_{L/K'} = |H_0|$, this gives

$$i_{G/H}(s') = \frac{1}{e'}\sum_{t\in H} i_G(st) = \frac{1}{e'}\sum_{t\in H} \min\{i_G(t), m\}.$$

Proposition 1.70 gives the formula (1.42), which in turn yields

$$\begin{aligned} & s' \in G_u(L/K)H/H \iff i_G(s) - 1 \geq u \\ \iff & \Phi_{L/K'}(i_G(s) - 1) \geq \Phi_{L/K'}(u) \iff i_{K'/K}(s') - 1 \geq \Phi_{L/K'}(u) \\ \iff & s' \in G_v(K'/K), v = \Phi_{L/K'}(u). \end{aligned}$$

Herbrand's Theorem is proved.

Since the function Φ is a homeomorphism of $[-1, +\infty)$ onto itself, its inverse exists. We denote by $\Psi : [-1, +\infty) \to [-1, +\infty)$ the inverse function of Φ. The functions Φ and Ψ satisfy the following transitivity condition:

Proposition 1.72. *If K'/K is a Galois subextension of L/K, then*

$$\Phi_{L/K} = \Phi_{K'/K} \circ \Phi_{L/K'} \quad \textit{and}\ \Psi_{L/K} = \Psi_{L/K'} \circ \Psi_{K'/K}.$$

Proof. For the ramification indices of the extensions L/K, K'/K and L/K' we have $e_{L/K} = e_{K'/K} e_{L/K'}$. From Herbrand's Theorem, we obtain $G_u/H_u = (G/H)_v$ with $v = \Phi_{L/K'}(u)$. Thus

$$\frac{1}{e_{L/K}}|G_u| = \frac{1}{e_{K'/K}}|(G/H)_v| \, \frac{1}{e_{L/K'}}|H_u|.$$

The equation is equivalent to

$$\Phi'_{L/K}(u) = \Phi'_{K'/K}(v)\Phi'_{L/K'}(u) = \left(\Phi_{K'/K} \circ \Phi_{L/K'}\right)'(u).$$

As $\Phi_{L/K}(0) = (\Phi_{K'/K} \circ \Phi_{L/K'})(0)$, it follows that $\Phi_{L/K} = \Phi_{K'/K} \circ \Phi_{L/K'}$. The formula for Ψ follows similarly.

We define the ramification groups in *upper numbering* by

$$G^v := G_u, \text{ where } u = \Psi(v). \tag{1.43}$$

Then $G^{\Phi(u)} = G_u$. We have $G^{-1} = G$, $G^0 = G_0$ and $G^v = 1$ for $v \gg 0$. We also have

$$\Psi(v) = \int_0^v [G^0 : G^w] dw. \tag{1.44}$$

The advantage of the ramification groups in upper numbering is that it is invariant when passing from L/K to a Galois subextension.

Proposition 1.73. *Let K'/K be a Galois subextension of L/K and $H = G(L/K')$, then one has $G^v(L/K)H/H = G^v(K'/K)$.*

Proof. We put $u = \Psi_{K'/K}(v), G' = G_{K'/K}$, apply Herbrand's Theorem and Proposition 1.72, and get

$$\begin{aligned} G^v H/H =& G_{\Psi_{L/K}(v)} H/H = G'_{\Phi_{L/K'}(\Psi_{L/K}(v))} \\ =& G'_{\Phi_{L/K'}(\Psi_{L/K'}(u))} = G'_u = G'^v. \end{aligned}$$

The proposition is proved.

1.3.4 Ramification groups of infinite Galois extensions.

Let L/K be an infinite Galois extension of local fields with Galois group $G = \mathrm{Gal}(L/K)$. Then G^v, the *ramification groups in upper numbering* of G, is defined by

$$G^v := \varprojlim_{L'/K \text{ finite Galois inside } L} \mathrm{Gal}(L'/K)^v. \tag{1.45}$$

Thus $\{G^v\}$ forms a filtration of G which is *left continuous*:

$$G^v = \bigcap_{w<v} G^w.$$

Moreover, Herbrand's Theorem remains true.

Proposition 1.74. *Let L/K be an infinite Galois extension with group G. If H is a closed normal subgroup of G, corresponding to the invariant field $L^H = L'$. Then*

(1) *If H is also open in G, then $G^v \cap H = H^{\psi_{G/H}(v)}$ where $\Psi_{G/H} := \Psi_{L'/K}$.*
(2) *In general, $(G/H)^v = G^v H/H$.*

Proof. (1) As H is open in G,

$$G = \varprojlim_{\substack{N \lhd H \lhd G \\ N \text{ open in } G}} G/N, \quad H = \varprojlim_{\substack{N \lhd H \lhd G \\ N \text{ open in } G}} H/N, \quad G^v = \varprojlim_{\substack{N \lhd H \lhd G \\ N \text{ open in } G}} (G/N)^v.$$

Let $L^N = L''$, consider the finite Galois extensions $L''/L'/K$, then $(G/N)^v \cap H/N = (H/N)^{\Psi_{G/H}(v)}$. Passing to the limit, then $G^v \cap H = H^{\Psi_{G/H}(v)}$.

(2) If G/H is finite, for any normal open subgroup N of G contained in H, by Herbrand's Theorem, $(G/H)^v = (G/N)^v \cdot (H/N)/(H/N)$. Passing to the limit, then $(G/H)^v = G^v H/H$ in this case. In general,

$$(G/H)^v = \varprojlim_{\substack{H \lhd M \lhd G \\ M \text{ open in } G}} (G/M)^v = \varprojlim_{\substack{H \lhd M \lhd G \\ M \text{ open in } G}} G^v M/M = G^v H/H.$$

We thus have the proposition.

Definition 1.75. *An Galois extension L/K is called an* arithmetically profinite extension *and in abbreviation APF if for any $v \geq -1$, G^v is an open subgroup of $G = \mathrm{Gal}(L/K)$. .*

If L/K is APF, then we can define

$$\Psi_{L/K}(v) = \begin{cases} \int_0^v (G^0 : G^w) dw, & \text{if } v \geq 0; \\ v, & \text{if } -1 \leq v \leq 0. \end{cases} \tag{1.46}$$

As in the finite extension case, $\Psi_{L/K}(v)$ is a homeomorphism of $[-1, +\infty)$ to itself which is continuous, piecewise linear, increasing and concave and satisfies $\Psi(0) = 0$. Let $\Phi_{L/K}$ be the inverse function of Ψ. One can then define the ramification group G_u in lower numbering by

$$G_u := G^{\Phi(u)}. \tag{1.47}$$

If the extension L'/L is APF and L/K is finite, then the transitive formulas $\Phi_{L'/K} = \Phi_{L/K} \circ \Phi_{L'/L}$ and $\Psi_{L'/K} = \Psi_{L'/L} \circ \Psi_{L/K}$ still hold.

1.3.5 Different and discriminant.

Let L/K be a finite separable extension of local fields. The ring of integers $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of finite rank. The trace map $\mathrm{Tr} = \mathrm{Tr}_{L/K}$ defines a non-degenerate bilinear form on L which makes L self dual as a K-vector space.

Definition 1.76. *The* different $\mathfrak{D}_{L/K}$ *of* L/K *is the inverse of the dual* $\mathcal{O}_K$*-module of* $\mathcal{O}_L$ *to the trace map inside* L*, i.e.,* $\mathfrak{D}_{L/K}^{-1}$ *is given by*

$$\mathfrak{D}_{L/K}^{-1} := \{x \in L \mid \mathrm{Tr}(xy) \in \mathcal{O}_K \text{ for all } y \in \mathcal{O}_L\}. \tag{1.48}$$

The discriminant $\delta_{L/K}$ *is the ideal of* K *given by*

$$\delta_{L/K} := [\mathfrak{D}_{L/K}^{-1} : \mathcal{O}_L] = (\det(\rho)) \tag{1.49}$$

where $\rho : \mathfrak{D}_{L/K}^{-1} \xrightarrow{\sim} \mathcal{O}_L$ *is an isomorphism of* $\mathcal{O}_K$*-modules and* $\det \rho$ *is under any given* K*-basis of* L*.*

For every $x \in \mathfrak{D}_{L/K}^{-1}$, certainly $\mathrm{Tr}(x) \in \mathcal{O}_K$; moreover, $\mathfrak{D}_{L/K}^{-1}$ is the maximal $\mathcal{O}_L$-module satisfying this property.

Suppose $\{e_i\}$ is a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$, let $\{e_i^*\}$ be the dual basis of $\mathfrak{D}_{L/K}^{-1}$. Define the isomorphism ρ by setting $e_i = \rho(e_i^*)$, then

$$\delta_{L/K} = (\det \rho)$$

and

$$\det \mathrm{Tr}(e_i, e_i) = \det \rho \cdot \det \mathrm{Tr}(e_i, e_i^*) = \det \rho.$$

Thus the discriminant $\delta_{L/K}$ is given by

$$\delta_{L/K} = (\det \mathrm{Tr}(e_i e_j)) = (\det(\sigma_j(e_i)))^2 \tag{1.50}$$

where σ_j runs through K-embeddings of L into the separable closure K^s of K. Note that $(\det \rho^{-1})$ is the norm of the fractional ideal $\mathfrak{D}_{L/K}^{-1}$, thus

$$\delta_{L/K} = N_{L/K}(\mathfrak{D}_{L/K}). \tag{1.51}$$

Proposition 1.77. *Let* $\mathfrak{a}$ *(resp.* $\mathfrak{b}$*) be a fractional ideal of* K *(resp.* L*), then*

$$\mathrm{Tr}(\mathfrak{b}) \subset \mathfrak{a} \Longleftrightarrow \mathfrak{b} \subset \mathfrak{a} \cdot \mathfrak{D}_{L/K}^{-1}.$$

Proof. The case $\mathfrak{a} = 0$ is trivial. For $\mathfrak{a} \neq 0$,

$$\begin{aligned} \mathrm{Tr}(\mathfrak{b}) \subset \mathfrak{a} &\Longleftrightarrow \mathfrak{a}^{-1} \mathrm{Tr}(\mathfrak{b}) \subset \mathcal{O}_K \Longleftrightarrow \mathrm{Tr}(\mathfrak{a}^{-1}\mathfrak{b}) \subset \mathcal{O}_K \\ &\Longleftrightarrow \mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{D}_{L/K}^{-1} \Longleftrightarrow \mathfrak{b} \subset \mathfrak{a} \cdot \mathfrak{D}_{L/K}^{-1}. \end{aligned}$$

Corollary 1.78. *Let $M \supseteq L \supseteq K$ be finite separable extensions. Then*

$$\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L} \cdot \mathfrak{D}_{L/K}, \quad \delta_{M/K} = (\delta_{L/K})^{[M:L]} N_{L/K}(\delta_{M/L}).$$

Proof. Repeating the equivalence of Proposition 1.77 to show that

$$\mathfrak{c} \subset \mathfrak{D}_{M/L}^{-1} \Longleftrightarrow \mathfrak{c} \subset \mathfrak{D}_{L/K} \cdot \mathfrak{D}_{M/K}^{-1}.$$

Corollary 1.79. *Let L/K be a finite extension of p-adic fields with ramification index e. Let $\mathfrak{D}_{L/K} = \mathfrak{m}_L^m$. Then for any integer n, $\mathrm{Tr}(\mathfrak{m}_L^n) = \mathfrak{m}_K^r$ where $r = [(m+n)/e]$, the largest integer $\leq (m+n)/e$.*

Proof. Since the trace map is $\mathcal{O}_K$-linear, $\mathrm{Tr}(\mathfrak{m}_L^n)$ is an ideal in $\mathcal{O}_K$. Now the proposition implies that $\mathrm{Tr}(\mathfrak{m}_L^n) \subset \mathfrak{m}_K^r$ if and only if

$$\mathfrak{m}_L^n \subset \mathfrak{m}_K^r \cdot \mathfrak{D}_{L/K}^{-1} = \mathfrak{m}_L^{er-m},$$

i.e., if $r \leq (m+n)/e$.

Proposition 1.80. *Let $x \in \mathcal{O}_L$ such that $L = K[x]$, let $f(X)$ be the minimal polynomial of x over K. Then $\mathfrak{D}_{L/K} = (f'(x))$ and $\delta_{L/K} = (N_{L/K} f'(x))$.*

We first need the following formula of Euler:

Lemma 1.81 (Euler). *Let $n = \deg f$. Then*

$$\mathrm{Tr}(x^i/f'(x)) = \begin{cases} 0, & \text{if } i = 0, \cdots, n-2; \\ 1, & \text{if } i = n-1. \end{cases} \tag{1.52}$$

Proof. Let x_k $(k = 1, \cdots, n)$ be the conjugates of x in the splitting field of $f(X)$. Then $\mathrm{Tr}(x^i/f'(x) = \sum_k x_k^i/f'(x_k)$. Expanding both sides of the identity

$$\frac{1}{f(X)} = \sum_{k=1}^{n} \frac{1}{f'(x_k)(X - x_k)}$$

into power series of $1/X$, and comparing the coefficients in degree $\leq n$, then the lemma follows.

Proof (Proof of Proposition 1.80). Since $\{1, \cdots, x^{n-1}\}$ is a basis of $\mathcal{O}_L$, by induction and the above Lemma, one sees that $\mathrm{Tr}(x^m/f'(x)) \in \mathcal{O}_K$ for every $m \in \mathbb{N}$. Thus $x^i/f'(x) \in \mathfrak{D}_{L/K}^{-1}$. Moreover, the matrix (a_{ij}), $0 \leq i, j \leq n-1$ for $a_{ij} = \mathrm{Tr}(x^{i+j}/f'(x))$ satisfies $a_{ij} = 0$ for $i+j < n-1$ and $= 1$ for $i+j = n-1$, thus the matrix has determinant $(-1)^{n(n-1)/2}$. Hence $x^j/f'(x)$, $0 \leq j \leq n-1$ is a basis of $\mathfrak{D}_{L/K}^{-1}$.

Proposition 1.82. *Let L/K be a finite Galois extension of local fields with Galois group G. Then*

$$\begin{aligned} v_L(\mathfrak{D}_{L/K}) &= \sum_{s\neq 1} i_G(s) = \sum_{i=0}^{\infty}(|G_i|-1) \\ &= \int_{-1}^{\infty}(|G_u|-1)du = |G_0|\int_{-1}^{\infty}(1-|G^v|^{-1})dv. \end{aligned} \tag{1.53}$$

Thus

$$v_K(\mathfrak{D}_{L/K}) = \int_{-1}^{\infty}(1-|G^v|^{-1})dv. \tag{1.54}$$

Proof. Let x be a generator of $\mathcal{O}_L$ over $\mathcal{O}_K$ and let f be its minimal polynomial. Then $\mathfrak{D}_{L/K}$ is generated by $f'(x)$ by the above proposition. Thus

$$v_L(\mathfrak{D}_{L/K}) = v_L(f'(x)) = \sum_{s\neq 1} v_L(x-s(x)) = \sum_{s\neq 1} i_G(s).$$

The second and third equalities of (1.53) are easy. For the last equality,

$$\int_{-1}^{\infty}(1-|G^v|^{-1})dv = \int_{-1}^{\infty}(1-|G_u|^{-1})\Phi'(u)du = \frac{1}{|G_0|}\int_{-1}^{\infty}(|G_u|-1)du.$$

(1.54) follows easily from (1.53), since $v_K = \frac{1}{|G_0|}v_L$.

Corollary 1.83. *Let $L \supseteq M \supseteq K$ be finite Galois extensions of local fields. Then*

$$v_K(\mathfrak{D}_{L/M}) = \int_{-1}^{\infty}\left(\frac{1}{|\operatorname{Gal}(M/K)|^v} - \frac{1}{|\operatorname{Gal}(L/K)|^v}\right)dv. \tag{1.55}$$

Proof. This follows from the transitive relation $\mathfrak{D}_{L/K} = \mathfrak{D}_{L/M}\mathfrak{D}_{M/K}$ and (1.54).

1.4 Ramification in *p*-adic Lie extensions

1.4.1 Sen's filtration Theorem.

In this subsection, we shall give the proof of Sen's theorem that the Lie filtration and the ramification filtration agree in a totally ramified p-adic Lie extension. We follow the beautiful paper of Sen [Sen72].

Let K be a p-adic field with perfect residue field k. Let L be a totally ramified Galois extension of K with Galois group $G = \operatorname{Gal}(L/K)$. Let $e = e_G = v_K(p)$ be the absolute ramification index of K.

If G is abelian, let $(G)^n := \{g^n \mid g \in G\}$ and $G[n]$ be the n-torsion subgroup of G.

If G is finite, put

$$v_G := \inf\{v \mid v \geq 0, G^v = 1\}, \tag{1.56}$$

$$u_G := \inf\{u \mid u \geq 0, G_u = 1\}. \tag{1.57}$$

Then

$$u_G = \Psi_G(v_G) \leq |G|v_G. \tag{1.58}$$

Lemma 1.84. *Assume L/K is a totally ramified finite Galois extension with group G. There is a complete non-archimedean field extension L'/K' with the same Galois group G such that the residue field of K' is algebraically closed and the ramification groups of L/K and L'/K' coincide.*

Proof. Pick a separable closure K^s of K containing L, then the maximal unramified extension K^{ur} of K inside K^s and L are linearly disjoint over K. Let $K' = \widehat{K^{\mathrm{ur}}}$ and $L' = \widehat{LK^{\mathrm{ur}}}$, then $\mathrm{Gal}(L'/K') = \mathrm{Gal}(L/K)$. Moreover, if x generates $\mathcal{O}_L$ as $\mathcal{O}_K$-algebra, then it also generates $\mathcal{O}_{L'}$ as $\mathcal{O}_{K'}$-algebra, thus the ramification groups coincide.

Proposition 1.85. *Suppose G is a finite abelian p-group. Then*

$$\begin{cases} (G^v)^p \subseteq G^{pv}, & \text{if } v \leq \frac{e_G}{p-1}; \\ (G^v)^p = G^{v+e_G}, & \text{if } v > \frac{e_G}{p-1}. \end{cases} \tag{1.59}$$

Proof. By the above lemma, we can assume that the residue field k is algebraic closed. In this case, one can always find a quasi-finite field k_0, such that k is the algebraic closure of k_0(cf. [Ser80], Ex.3, p.192). Regard $K_0 = W(k_0)[\frac{1}{p}]$ as a subfield of K. By general argument from field theory (cf. [Ser80], Lemma 7, p.89), one can find a finite extension K_1 of K_0 inside K and a finite totally ramified extension L_1 of K_1, such that

(i) K/K_1 is unramified and hence L_1 and K are linearly disjoint over K_1;
(ii) $L_1K = L$.

Thus $\mathrm{Gal}(L_1/K_1) = \mathrm{Gal}(L/K)$ and their ramification groups coincide. As the residue field of K_1 is a finite extension of k_0, hence it is quasi-finite. The proposition is reduced to the case that the residue field k is quasi-finite.

Now the proposition follows from the well-known facts that

$$\begin{cases} U_v^p \subset U_{pv}, & \text{if } v \leq \frac{e_G}{p-1} \\ U_v^p = U_{v+e}, & \text{if } v > \frac{e_G}{p-1}. \end{cases}$$

and the following lemma.

Lemma 1.86. *Suppose K is a complete discrete valuation field with quasi-finite residue field. Let L/K be an abelian extension with Galois group G. Then the image of U_K^n under the reciprocity map $K^\times \to G$ is dense in $(G)^n$.*

Proof. This is an application of local class field theory, see Serre [Ser80], Theorem 1, p.228 for the proof.

Corollary 1.87. *Suppose G is a finite abelian Galois p-group and denote $G[n]$ for the n-torsion subgroup of G. If $v_G \leq \frac{p}{p-1}e_G$, then $v_G \geq p^m v_{G/G[p^m]}$ for all $m \geq 1$; if $v_G > \frac{p}{p-1}e_G$, then $v_G = v_{G/G[p]} + e_G$.*

Proof. If $v_G \leq \frac{p}{p-1}e_G$, then $t_m := p^{-m}v_G \leq \frac{1}{p-1}e_G$, and $(G^{t_m+\varepsilon})^{p^m} = G^{p^m t_m+\varepsilon} = G^{v_G+\varepsilon} = 1$ for $\varepsilon > 0$, then $G^{t_m+\varepsilon} \subset G[p^m]$ and thus $v_{G/G[p^m]} \leq p^{-m}v_G$.

If $v_G > \frac{p}{p-1}e_G$, then $t := v_G - e_G > \frac{1}{p-1}e_G$, and $(G^{t+\varepsilon})^p = G^{t+\varepsilon+e_G} = G^{v_A+\varepsilon}$ for $\varepsilon \geq 0$. Thus $v_G = v_{G/G[p]} + e_G$.

Definition 1.88. *We call a finite abelian Galois p-group G* small *if $v_G \leq \frac{p}{p-1}e_G$, or equivalently, if $(G^x)^p \subseteq G^{px}$ for all $x \geq 0$.*

Lemma 1.89. *If G is small, then for every $m \geq 1$,*

$$u_G \geq p^{m-1}(p-1)(G[p^m] : G[p])u_{G/G[p]}. \tag{1.60}$$

Proof. For every $\varepsilon > 0$, we have

$$\begin{aligned} u_G =&\Psi_G(v_G) = \int_0^{v_G} (G : G^t)dt \geq \int_{p^{-1}v_G+\varepsilon}^{v_G} (G : G^t)dt \\ \geq&(v_G - p^{-1}v_G - \varepsilon)(G : G^{p^{-1}v_G+\varepsilon}) \geq \left(v_G \cdot \frac{p-1}{p} - \varepsilon\right)(G : G[p]). \end{aligned}$$

The last inequality holds since $(G^{p^{-1}v_G+\varepsilon})^p = 1$ by Proposition 1.85. Then by Corollary 1.87,

$$u_G \geq \frac{p}{p-1}(G : G[p])v_G \geq p^{m-1}(p-1)(G : G[p])v_{G/G[p^m]}.$$

Since $u_{G/G[p^m]} \leq (G : G[p^m])v_{G/G[p^m]}$ by (1.58), we have the desired result.

We now suppose G is a p-adic Lie group of dimension $d > 0$ with a Lie filtration $\{G(n)\}$, which means that $G(1)$ is a non-trivial pro-p group and that

$$G(n) = G(n+1)^{p^{-1}} = \{s \in G \mid s^p \in G(n+1)\}.$$

For $n \geq 1$, we denote

$$\Psi_n = \Psi_{G/G(n)},\ v_n = v_{G/G(n)}, \quad u_n = u_{G/G(n)} = \Psi_n(v_n),\ e_n = e_{G(n)}. \tag{1.61}$$

Proposition 1.90. *For each $n \geq 1$ we have $G^v \cap G(n) = G(n)^{\Psi_n(v)}$ for $v \geq 0$. In particular,*

$$G^v = G(n)^{u_n+(v-v_n)(G:G(n))}, \quad \text{for } v > v_n, \tag{1.62}$$

i.e.,

$$G^{v_n+te} = G(n)^{u_n+te_n}, \quad \text{for } t > 0. \tag{1.63}$$

As a consequence, for $n,\ r \geq 1$,

$$v_{G(n)/G(n+r)} = u_n + (v_{n+r} - v_n)(G : G(n)). \tag{1.64}$$

Proof. The first equality follows from Proposition 1.74. For $v > v_n$, then $G^v \subset G(n)$ and

$$\Psi_n(v) = \Psi_n(v_n) + \int_{v_n}^{v} (G : G(n))dv = u_n + (v - v_n)(G : G(n)).$$

Now $v = v_{G(n)/G(n+r)}$ is characterized by the fact that $G(n)^v \nsubseteq G(n+r)$ and $G(n)^{v+\varepsilon} \subseteq G(n+r)$ for all $\varepsilon \geq 0$, but $x = v_{n+r}$ is characterized by the fact that $G^x \nsubseteq G(n+r)$ and $G^{x+\varepsilon} \subseteq G(n+r)$ for all $\varepsilon \geq 0$, thus (1.64) follows from (1.62).

Proposition 1.91. *There exists an integer n_1 and a constant c such that for all $n \geq n_1$,*

$$v_{n+1} = v_n + e \quad \textit{and} \quad v_n = ne + c.$$

Proof. By (1.63), we can replace G by $G(n_0)$ for some fixed n_0 and $G(n)$ by $G(n_0 + n)$. Thus we can suppose $G = \exp \mathscr{L}$, where $\mathscr{L}$ is an order in the Lie algebra Lie(G) such that $[\mathscr{L}, \mathscr{L}] \subset p^3\mathscr{L}$ and that $G(n) = \exp p^n\mathscr{L}$. Then $(G : G(n)) = p^{nd}$ for all n, and for $r \leq n+1$, there are isomorphisms

$$G(n)/G(n+r) \xrightarrow{\log} p^n\mathscr{L}/p^{n+r}\mathscr{L} \xrightarrow{p^{-n}} \mathscr{L}/p^r\mathscr{L} \cong (\mathbb{Z}/p^r\mathbb{Z})^d. \tag{1.65}$$

Thus $G(n)/G(n+d+3)$ is abelian for sufficient large n.

If $G(n)/G(n+r)$ is abelian and small for $r \geq 2$, then apply Lemma 1.89 with finite Galois group $A = G(n)/G(n+r)$, $m = r-1$. Note that in this case $u_{n+r} = u_A$ and $u_{n+1} = u_{A/A[p^{r-1}]}$, then

$$\frac{u_{n+r}}{e_{n+r}} \geq (p-1)p^{r-2-d} \cdot \frac{u_{n+1}}{e_{n+1}}.$$

But note that the sequence $u_n/e_n \leq \frac{1}{p-1}$ is bounded, then for $r = d+3$, $G(n)/G(n+d+3)$ can not be all small.

We can thus assume $G(n_0)/G(n_1+1)$ is not small, then by Corollary 1.87,

$$v_{G(n_0)/G(n_1+1)} = v_{G(n_0)/G(n_1)} + e_{n_0},$$

and by (1.64), then

$$v_{n_1+1} = v_{n_1} + e.$$

Hence $G(n_1)/G(n_1+2)$ is not small and $v_{n_1+2} = v_{n_1+1} + e$. Continue this procedure inductively, we have the proposition.

Theorem 1.92. *There is a constant c such that*

$$G^{ne+c} \subset G(n) \subset G^{ne-c} \tag{1.66}$$

for all n.

Remark 1.93. The above theorem means that the filtration of G by upper numbering ramification subgroups agrees with the Lie filtration. In particular this means that a totally ramified p-adic Lie extension is always APF.

If $G = \mathbb{Z}_p$, the above results were shown to be true by Wyman [Wym69], without using class field theory.

Proof. We can assume the assumptions in the first paragraph of the proof of Proposition 1.91 and (1.65) hold. We assume $n \geq n_1 > 1$.

Let c_1 be the constant given in Proposition 1.91. Let $c_0 = c_1 + \frac{\alpha e}{p-1}$ for some constant $\alpha \geq 1$. By Proposition 1.91, $G^{ne+c_0} \subset G(n)$ for large n.

By (1.63),

$$G^{ne+c_0} = G^{v_n + \frac{\alpha e}{p-1}} = G(n)^{u_n + \frac{\alpha e_n}{p-1}}.$$

Apply Proposition 1.85 to the finite abelian Galois group $A = G(n)/G(2n+1)$, since $u_n + \frac{\alpha e_n}{p-1} > \frac{e_n}{p-1}$, we have

$$(G^{ne+c_0})^p G(2n+1) = G^{(n+1)e+c_0} G(2n+1). \tag{1.67}$$

Put

$$M_n = p^{-n} \log(G^{ne+c_0} G(2n)/G(2n)) \subset \mathscr{L}/p^n\mathscr{L}.$$

Then (1.67) implies that M_n is the image of M_{n+1} under the canonical map $\mathscr{L}/p^{n+1}\mathscr{L} \to \mathscr{L}/p^n\mathscr{L}$. Let

$$M = \varprojlim_n M_n \subset \mathscr{L}.$$

Then $M_n = (M + p^n\mathscr{L})/p^n\mathscr{L}$. We let

$$I = \mathbb{Q}_p M \cap \mathscr{L}.$$

Since the ramification subgroups G^{ne+c_0} are invariant in G, each M_n and hence M is stable under the adjoint action of G on $\mathscr{L}$. Hence $\mathbb{Q}_p M$, as a subspace of $\mathrm{Lie}(G)$, is stable under the adjoint action of G, hence is an ideal of $\mathrm{Lie}(G) = \mathbb{Q}_p\mathscr{L}$. As a result, I is an ideal in $\mathscr{L}$. Let $N = \exp I$ and $\overline{G} = G/N$. Then $\overline{G}$ is a p-adic Lie group filtered by $\overline{G}(n) = \exp p^n \overline{\mathscr{L}}$ where $\overline{\mathscr{L}} = \mathscr{L}/I$.

A key fact of Sen's proof is the following Lemma:

Lemma 1.94. $\dim \overline{G} = 0$, *i.e.,* $\overline{G} = 1$.

Proof (Proof of the Lemma). If not, we can apply the previous argument to $\overline{G}$ to get a sequence $\bar{v}_n$ and a constant $\bar{c}_1$ such that $\bar{v}_n = ne + \bar{c}_1$ for $n \geq \bar{n}_1$. But on the other hand, we have

$$\overline{G}^{ne+c_0} = G^{ne+c_0} N/N \subset G(2n)N/N = \overline{G}(2n)$$

since

$$\begin{aligned} G^{ne+c_0}G(2n)/G(2n) &= \exp(p^n M_n) \\ &\subset \exp((p^n I + p^{2n}\mathscr{L})/p^{2n}\mathscr{L}) = N(n)G(2n)/G(2n). \end{aligned}$$

Hence for all $n \geq n_1$ and $\bar{n}_1$, one gets $ne + c_0 > \bar{v}_{2n} = 2ne + \bar{c}_1$, which is a contradiction.

By the lemma, thus we have $I = \mathscr{L}$, i.e., $p^{n_0}\mathscr{L} \subset M$ for some n_0. Then for large n,

$$p^{n_0}\mathscr{L}/p^n\mathscr{L} \subset (p^{n_0}\mathscr{L} + M)/p^n\mathscr{L} = M_n.$$

Applying the operation $\exp \circ p^n$, we get

$$G(n + n_0)/G(2n) \subset G^{ne+c_0}G(2n)/G(2n).$$

Thus G^{ne+c_0} contains elements of $G(n + n_0)$ which generate $G(n + n_0)$ modulo $G(n + n_0 + 1)$. It follows that $G^{ne+c_0} \supset G(n + n_0)$ as $G^{ne+c_0} = \varprojlim_m G^{ne+c_0}G(m)/G(m)$ is closed. This completes the proof of the theorem.

1.4.2 Totally ramified $\mathbb{Z}_p$-extensions.

Let K be a p-adic field and K_∞ be a totally ramified extension of K with Galois group $\Gamma \cong \mathbb{Z}_p$. Let K_n be the subfield of K_∞ which corresponds to the closed subgroup $\Gamma_n = \Gamma^{p^n} \cong p^n\mathbb{Z}_p$. Let γ be a topological generator of Γ. Then $\gamma_n := \gamma^{p^n}$ is a topological generator of Γ_n.

For the higher ramification groups Γ^v of Γ with the upper numbering, suppose $\Gamma^v = \Gamma_n$ for $v_n < v \leq v_{n+1}$, then by Proposition 1.91 or by Wyman's result [Wym69], we have $v_{n+1} = v_n + e$ for $n \gg 0$. By Herbrand's Theorem (Theorem 1.71),

$$\operatorname{Gal}(K_n/K)^v = \Gamma^v\Gamma_n/\Gamma_n = \begin{cases} \Gamma_i/\Gamma_n, & \text{if } v_i < v \leq v_{i+1},\ i \leq n; \\ 1, & \text{otherwise.} \end{cases} \tag{1.68}$$

Proposition 1.95. *If L be a finite extension of K_∞, then*

$$\operatorname{Tr}_{L/K_\infty}(\mathcal{O}_L) \supset \mathfrak{m}_{K_\infty}.$$

Proof. Replace K by K_n if necessary, we may assume $L = L_0K_\infty$ such that L_0/K is finite and linearly disjoint from K_∞ over K. We may also assume that L_0/K is Galois. Put $L_n = L_0K_n$. Then by (1.55),

$$v_K(\mathfrak{D}_{L_n/K_n}) = \int_{-1}^{\infty} \left(|\operatorname{Gal}(K_n/K)^v|^{-1} - |\operatorname{Gal}(L_n/K)^v|^{-1}\right) dv.$$

Suppose that $\operatorname{Gal}(L_0/K)^v = 1$ for $v \geq h$, then $\operatorname{Gal}(L/K)^v \subseteq \Gamma$ and $\operatorname{Gal}(L_n/K)^v = \operatorname{Gal}(K_n/K)^v$ for $v \geq h$. We have

$$v_K(\mathfrak{D}_{L_n/K_n}) \leq \int_{-1}^{h} |\operatorname{Gal}(K_n/K)^v|^{-1} dv \to 0$$

as $n \to \infty$ by (1.68). Now the proposition follows from Corollary 1.79.

Corollary 1.96. *For any $a > 0$, there exists $x \in L$, such that*

$$v_K(x) > -a \text{ and } \mathrm{Tr}_{L/K_\infty}(x) = 1. \tag{1.69}$$

Proof. For any $a > 0$, find $\alpha \in \mathcal{O}_L$ such that $v_K(\mathrm{Tr}_{L/K_\infty}(\alpha))$ is less than a. Let $x = \frac{\alpha}{\mathrm{Tr}_{L/K_\infty}(\alpha)}$, then x satisfies (1.69).

Remark 1.97. Clearly the proposition and the corollary are still true if replacing K_∞ by any field M such that $K_\infty \subset M \subset L$. (1.69) is called the *almost étale condition*.

Proposition 1.98. *There is a constant c such that*

$$v_K(\mathfrak{D}_{K_n/K}) = en + c + p^{-n}a_n \tag{1.70}$$

where a_n is bounded.

Proof. We apply (1.68) and (1.54), then

$$v_K(\mathfrak{D}_{K_n/K}) = \int_{-1}^{\infty}(1 - |\operatorname{Gal}(K_n/K)^v|^{-1})dv = en + c + p^{-n}a_n.$$

Corollary 1.99. *There is a constant c which is independent of n such that for all $x \in K_n$,*

$$v_K(p^{-n}\,\mathrm{Tr}_{K_n/K}(x)) \geq v_K(x) - c. \tag{1.71}$$

Proof. By the above proposition, $v_K(\mathfrak{D}_{K_{n+1}/K_n}) = e + p^{-n}b_n$ with b_n bounded. Let $\mathcal{O}_n$ be the ring of integers of K_n and $\mathfrak{m}_n$ its maximal ideal. Suppose $\mathfrak{D}_{K_{n+1}/K_n} = \mathfrak{m}_{n+1}^d$. By Corollary 1.79, we have

$$\mathrm{Tr}_{K_{n+1}/K_n}(\mathfrak{m}_{n+1}^i) = \mathfrak{m}_n^j,$$

where $j = \left[\frac{i+d}{p}\right]$. Thus

$$v_K(p^{-1}\,\mathrm{Tr}_{K_{n+1}/K_n}(x)) \geq v_K(x) - ap^{-n}$$

for some a independent of n. The corollary then follows.

Definition 1.100. *For $n \geq 0$,* Tate's normalized trace map $R_n : K_\infty \to K_n$ *is the map*

$$R_n(x) = p^{-m}\,\mathrm{Tr}_{K_{n+m}/K_n}(x) \text{ if } x \in K_{n+m}. \tag{1.72}$$

Denote $R_0(x) = R(x)$.

Remark 1.101. Using the transitive properties of the trace map, one can easily see the definition is indenpent of the choice of m.

Proposition 1.102. *There exists a constant $d > 0$ such that for all $x \in K_\infty$,*

$$v_K(x - R(x)) \geq v_K(\gamma x - x) - d. \tag{1.73}$$

Proof. We prove by induction on $n \geq 1$ the inequality

$$v_K(x - R(x)) \geq v_K(\gamma x - x) - c_n, \text{ if } x \in K_n \tag{1.74}$$

with $c_1 = e$, $c_{n+1} = c_n + ap^{-n}$ for some constant $a > 0$.

For $x \in K_{n+1}$, then

$$px - \mathrm{Tr}_{K_{n+1}/K_n}(x) = px - \sum_{i=0}^{p-1} \gamma_n^i x = \sum_{i=1}^{p-1} (1 + \gamma_n + \cdots + \gamma_n^{i-1})(1 - \gamma_n)x,$$

thus

$$v_K(x - p^{-1}\,\mathrm{Tr}_{K_{n+1}/K_n}(x)) \geq v_K(x - \gamma_n x) - e.$$

In particular, let $c_1 = e$, (1.74) holds for $n = 1$.

In general, for $x \in K_{n+1}$, then

$$R(\mathrm{Tr}_{K_{n+1}/K_n} x) = pR(x), \text{ and } (\gamma - 1)\,\mathrm{Tr}_{K_{n+1}/K_n}(x) = \mathrm{Tr}_{K_{n+1}/K_n}(\gamma x - x).$$

By induction,

$$\begin{aligned} v_K(\mathrm{Tr}_{K_{n+1}/K_n}(x) - pR(x)) \geq & v_K(\mathrm{Tr}_{K_{n+1}/K_n}(\gamma x - x)) - c_n \\ \geq & v_K(\gamma x - x) + e - ap^{-n} - c_n, \end{aligned}$$

thus

$$\begin{aligned} v_K(x - R(x)) &\geq \min(v_K(x - p^{-1}\,\mathrm{Tr}_{K_{n+1}/K_n}(x)), v_K(\gamma x - x) - c_n - ap^{-n}) \\ &\geq v_K(\gamma x - x) - \max(c_1, c_n + ap^{-n}) \end{aligned}$$

which establishes the inequality (1.74) for $n + 1$.

Remark 1.103. If we take K_n as the ground field instead of K and replace $R(x)$ by $R_n(x)$, from the proof the corresponding inequality with the same constant d holds.

By Corollary 1.99, the linear operator R_n is continuous on K_∞ for each n and therefore extends to $\widehat{K}_\infty$ by continuity. Denote

$$X_n := \{x \in \widehat{K}_\infty, R_n(x) = 0\}. \tag{1.75}$$

Proposition 1.104. *For each n, X_n is a closed subspace of $\widehat{K}_\infty$. Moreover,*

(1) $\widehat{K}_\infty = K_n \oplus X_n$.
(2) *The operator $\gamma_n - 1$ is bijective on X_n and has a continuous inverse such that*

$$v_K((\gamma_n - 1)^{-1}(x)) \geq v_K(x) - d$$

for $x \in X_n$.
(3) *If λ is a principal unit which is not a root of unity, then $\gamma_n - \lambda$ has a continuous inverse on $\widehat{K}_\infty$.*

Proof. It suffices to prove the case $n = 0$.

(1) follows immediately from the fact that $R = R \circ R$ is idempotent.

(2) For $m \in \mathbb{N}$, let $K_{m,0} = K_m \cap X_0$, then $K_m = K \oplus K_{m,0}$ and X_0 is the completion of $K_{\infty,0} = \cup K_{m,0}$. Note that $K_{m,0}$ is a finite dimensional K-vector space, the operator $\gamma - 1$ is injective on $K_{m,0}$, and hence bijective on $K_{m,0}$ and on $K_{\infty,0}$. By Proposition 1.102, then

$$v_K((\gamma - 1)^{-1}y) \geq v_K(y) - d$$

for $y = (\gamma - 1)x \in K_{m,0}$. Hence $(\gamma - 1)^{-1}$ extends by continuity to X_0 and the inequality still holds.

(3) Since $\gamma - \lambda$ is obviously bijective and has a continuous inverse on K for $\lambda \neq 1$, we can restrict our attention to its action on X_0. Note that

$$\gamma - \lambda = (\gamma - 1)(1 - (\gamma - 1)^{-1}(\lambda - 1)),$$

we just need to show that $1 - (\gamma - 1)^{-1}(\lambda - 1)$ has a continuous inverse. If $v_K(\lambda - 1) > d$ for the d in Proposition 1.102, then $v_K((\gamma - 1)^{-1}(\lambda - 1)(x)) > 1$ in X_0 and

$$1 - (\gamma - 1)^{-1}(\lambda - 1) = \sum_{k \geq 0}((\gamma - 1)^{-1}(\lambda - 1))^k$$

is the continuous inverse in X_0 and $\gamma - \lambda$ has a continuous inverse in X.

In general, as d is not changed if replacing K by K_n, we can assume $v_K(\lambda^{p^n} - 1) > d$ for $n \gg 0$. Then $\gamma^{p^n} - \lambda^{p^n}$ has a continuous inverse in X and so does $\gamma - \lambda$.

1.5 Continuous Cohomology

1.5.1 Abelian cohomology.

Let G be a group.

Definition 1.105. *A* G-module *is an abelian group with a linear action of* G. *If* G *is a topological group, a* topological G-module *is a topological abelian group equipped with a linear and continuous action of* G.

Let $\mathbb{Z}[G]$ be the ring algebra of G over $\mathbb{Z}$, that is,

$$\mathbb{Z}[G] = \{\sum_{g \in G} a_g g : a_g \in \mathbb{Z}, a_g = 0 \text{ for almost all } g\}.$$

A G-module M may be viewed as a *left* $\mathbb{Z}[G]$*-module* by setting

$$(\sum a_g g)(x) = \sum a_g g(x), \text{for all } a_g \in \mathbb{Z},\ g \in G,\ x \in M.$$

The G-modules form an *abelian category.*

Let M be a topological G-module. The abelian group of continuous n-cochains $C^n_{\text{cont}}(G,M)$ is defined as the group of continuous maps $G^n \to M$ for $n > 0$ and $C^0_{\text{cont}}(G,M) := M$. Let

$$d_n : C^n_{\text{cont}}(G,M) \longrightarrow C^{n+1}_{\text{cont}}(G,M)$$

be given by

$$\begin{aligned}
&(d_0 a)(g) = g(a) - a;\\
&(d_1 f)(g_1,g_2) = g_1(f(g_2)) - f(g_1 g_2) + f(g_1);\\
&(d_n f)(g_1,g_2,\cdots,g_n,g_{n+1}) = g_1(f(g_2,\cdots,g_n,g_{n+1}))\\
&\qquad\qquad + \sum_{i=1}^{n} (-1)^i f(\cdots,g_{i-1},g_i g_{i+1},g_{i+2},\cdots)\\
&\qquad\qquad + (-1)^{n+1} f(g_1,g_2,\cdots,g_n).
\end{aligned}$$

We have $d_{n+1}d_n = 0$, thus the sequence $C^\bullet_{\text{cont}}(G.M)$:

$$C^0_{\text{cont}}(G,M) \xrightarrow{d_0} C^1_{\text{cont}}(G,M) \xrightarrow{d_1} C^2_{\text{cont}}(G,M) \xrightarrow{d_2} \cdots \xrightarrow{d_{n-1}} C^n_{\text{cont}}(G,M) \xrightarrow{d_n} \cdots$$

is a cochain complex.

Definition 1.106. *Set*

$$\begin{aligned}
&Z^n_{\text{cont}}(G,M) = \operatorname{Ker} d_n, \qquad B^n_{\text{cont}}(G,M) = \operatorname{Im} d_{n-1},\\
&H^n_{\text{cont}}(G,M) = Z^n/B^n = H^n(C^\bullet(G,M)).
\end{aligned}$$

These groups are called the group of continuous n-cocycles*, the group of* continuous n-coboundaries *and the* n-th continuous cohomology group *of M respectively.*

Proposition 1.107. *For $n = 0, 1$, one has*

$$H^0_{\text{cont}}(G,M) = M^G = \{a \in M \mid g(a) = a, \textit{for all } g \in G\}, \tag{1.76}$$

$$H^1_{\text{cont}}(G,M) = \frac{\{f : G \to M \mid f \textit{ continuous}, \ f(g_1 g_2) = g_1 f(g_2) + f(g_1)\}}{\{s_a = (g \mapsto g \cdot a - a) : a \in M\}}. \tag{1.77}$$

Corollary 1.108. *When G acts trivially on M, then*

$$H^0_{\text{cont}}(G,M) = M, \quad H^1_{\text{cont}}(G,M) = \operatorname{Hom}(G,M).$$

The cohomological functors $H^n(G,-)$ are functorial. If $\eta : M_1 \to M_2$ is a morphism of topological G-modules, then it induces a morphism of complexes $C^\bullet_{\text{cont}}(G,M_1) \to C^\bullet_{\text{cont}}(G,M_2)$, which in turn induces morphisms from $Z^n_{\text{cont}}(G,M_1)$ (resp. $B^n_{\text{cont}}(G,M_1)$, resp. $H^n_{\text{cont}}(G,M_1)$) to $Z^n_{\text{cont}}(G,M_2)$ (resp. $B^n_{\text{cont}}(G,M_2)$, resp. $H^n_{\text{cont}}(G,M_2)$).

Proposition 1.109. *For a short exact sequence of topological G-modules*

$$0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{j} M'' \longrightarrow 0,$$

then there is an exact sequence

$$0 \to M'^G \to M^G \to M''^G \xrightarrow{\delta} H^1_{\mathrm{cont}}(G, M') \to H^1_{\mathrm{cont}}(G, M) \to H^1_{\mathrm{cont}}(G, M''),$$

where for any $a \in (M'')^G$, $\delta(a)$ is defined as follows: choose $x \in M$ such that $j(x) = a$, then define $\delta(a)$ to be the continuous 1-cocycle $g \mapsto i^{-1}(g(x) - x)$.

Proof. Note that for any $g \in G$, $j(g(x) - x) = g(j(x)) - j(x) = g(a) - a = 0$, thus $g(x) - x \in \mathrm{Im}\, i$, so that $i^{-1}(g(x) - x)$ is meaningful.

The proof of the exactness is routine. We omit it here.

From the above proposition, the functor $H^0_{\mathrm{cont}}(G, -)$ is left exact. In general, the category of topological G-modules *does not* have sufficiently many injective objects, so it is not possible to have a long exact sequence involving all H^n.

However, for the following two extremely useful cases, a short exact sequence *do* induce a long exact sequence involving all higher continuous cohomology groups.

(A) G is a group endowed with the discrete topology. This is the usual group cohomology. By convention,

$$H^n(G, M) := H^n_{\mathrm{cont}}(G, M).$$

(B) G is a profinite group and the modules are discrete G-modules. Here we call M a *discrete G-module* if the subgroup $G_a = \{g \in G \mid g(a) = a\}$ for all $a \in M$ is open in G. By convention, again set

$$H^n(G, M) := H^n_{\mathrm{cont}}(G, M).$$

The inflation map then induces a natural isomorphism

$$\varinjlim_{\substack{H \triangleleft G \\ H \text{ open}}} H^n(G/H, M^H) \xrightarrow{\sim} H^n(G, M). \tag{1.78}$$

Example 1.110. If K is a field and L is a Galois extension of K, then $G = \mathrm{Gal}(L/K)$ is a profinite group and $H^n(G, M) = H^n(L/K, M)$ is the so-called *Galois cohomology* of M. In particular, if $L = K^s$ is a separable closure of K, we write $H^n(G, M) = H^n(K, M)$.

Remark 1.111. If j admits a continuous set theoretic section $s : M'' \to M$, one can define a map

$$\delta_n : H^n_{\mathrm{cont}}(G, M'') \longrightarrow H^{n+1}_{\mathrm{cont}}(G, M'), \quad \text{for all } n \in \mathbb{N}$$

to get a long exact sequence (ref. Tate [Tat76]).

1.5.2 Non-abelian cohomology.

Let G be a topological group. Let M be a topological group which may be non-abelian, written multiplicatively. Assume M is a topological G-group, that is, M is equipped with a continuous action of G such that $g(xy) = g(x)g(y)$ for all $g \in G$, $x, y \in M$. From now on, we denote $g(x)$ by x^g, and denote a continuous map $c : G \to M$ by $(c_g)_{g\in G}$ where $c_g = c(g)$.

The 0-th cohomology is defined by

$$H^0_{\mathrm{cont}}(G, M) = M^G := \{x \in M \mid x^g = x \text{ for all } g \in G\}. \tag{1.79}$$

To define H^1, we first define the set of continuous 1-cocycles

$$Z^1_{\mathrm{cont}}(G, M) := \{c = (c_g) \text{ continuous} \mid c_{gh} = c_g c_h^g\}. \tag{1.80}$$

If $c, c' \in Z^1_{\mathrm{cont}}(G, M)$, we say that c and c' are *cohomologous* if there exists $a \in M$ such that $c'_g = a^{-1} c_g a^g$ for all $g \in G$. This defines an equivalence relation for the set of cocycles. The 1-st cohomology is defined by

$$H^1_{\mathrm{cont}}(G, M) := Z^1_{\mathrm{cont}}(G, M)/(\text{cohomologous relations}). \tag{1.81}$$

Note that $H^1_{\mathrm{cont}}(G, M)$ is actually a *pointed set* with the *distinguished point* being the trivial class $c = (1)$. We call $H^1_{\mathrm{cont}}(G, M)$ (abelian or non-abelian) *trivial* if it contains only the trivial element.

The above construction is functorial. If $\eta : M_1 \to M_2$ is a continuous homomorphism of topological G-modules, it induces a group homomorphism

$$M_1^G \to M_2^G$$

and a morphism of pointed sets

$$H^1_{\mathrm{cont}}(G, M_1) \to H^1_{\mathrm{cont}}(G, M_2).$$

For a sequence $X \overset{\lambda}{\to} Y \overset{\mu}{\to} Z$ of pointed sets which means that λ, μ are morphisms of pointed sets, it is called *exact* if $\lambda(X) = \{y \in Y \mid \mu(y) = z_0\}$, where z_0 is the distinguished element in Z.

Proposition 1.112. *Let $1 \to M' \xrightarrow{i} M \xrightarrow{j} M'' \to 1$ be an exact sequence of continuous topological G-groups. Then there exists a long exact sequence of pointed sets:*

$$1 \to M'^G \overset{i_0}{\to} M^G \overset{j_0}{\to} M''^G \overset{\delta}{\to} H^1(G, M') \overset{i_1}{\to} H^1(G, M) \overset{j_1}{\to} H^1(G, M''),$$

where the connecting map δ is defined as follows: Given $c \in M''^G$, pick $b \in M$ such that $j(b) = c$. Then

$$\delta(c) = (i^{-1}(b^{-1}b^g))_{g\in G}.$$

Proof. We first check that the map δ is well defined. First, $j(b^{-1}b^g) = c^{-1}c^g = 1$, then $b^{-1}b^g \in \operatorname{Ker} j = \operatorname{Im} i$, $a_g = i^{-1}(b^{-1}b^g) \in M'$. To simplify notations, from now on we take i to be the inclusion $M' \hookrightarrow M$. Then

$$a_{gh} = b^{-1}b^{gh} = b^{-1}b^g \cdot (b^{-1}b^h)^g = a_g a_h^g,$$

thus (a_g) is a 1-cocycle in M. If we choose b' other than b such that $j(b') = j(b) = c$, then $b' = bm$ for some $m \in M'$, and

$$a'_g = b'^{-1}b'^g = m^{-1}b^{-1}b^g m^g = m^{-1}a_g m^g$$

is cohomologous to a_g.

Now we check the exactness:

(1) Exactness at M'^G. This is trivial.

(2) Exactness at M^G. By functoriality, $j_0 i_0 = 1$, thus $\operatorname{Im} i_0 \subseteq \operatorname{Ker} j_0$. On the other hand, if $j_0(b) = 1$ and $b \in M^G$, then $j(b) = 1$ and $b \in M' \cap M^G = M'^G$.

(3) Exactness at M''^G. If $c \in j_0(B^G)$, then c can be lifted to an element in M^G and $\delta(c) = 1$. On the other hand, if $\delta(c) = 1$, then $1 = a_g = b^{-1}b^g$ for some $b \in j^{-1}(c)$ and for all $g \in G$, hence $b = b^g \in M^G$.

(4) Exactness at $H^1(G, M')$. A cocycle (a_g) maps to 1 in $H^1(G, M)$ is equivalent to say that $a_g = b^{-1}b^g$ for some $b \in M$. From the definition of δ, one then see $i_1\delta = 1$. On the other hand, if $a_g = b^{-1}b^s$ for every $g \in G$, then $j(b^{-1}b^g) = j(a_g) = 1$ and $j(b) \in M''^G$ and $\delta(j(b)) = (a_g)$.

(5) Exactness at $H^1(G, M)$. By functoriality, $j_1 i_1 = 1$, thus $\operatorname{Im} i_1 \subseteq \operatorname{Ker} j_1$. Now if (b_g) maps to $1 \in H^1(G, M'')$, then there exists $c \in M''$, $c^{-1}j(b_g)c^g = 1$ for all $g \in G$. Pick $b' \in M$ such that $j(b') = c$, then $j(b'^{-1}b_g b'^g) = 1$ and $(b'^{-1}b_g b'^g) = (a_g)$ is a cocycle of M'.

We adopt the same conventions as in the abelian case. If G is endowed with the discrete topology, or if G is a profinite group and M is a discrete G-module (i.e., M is endowed with the discrete topology and G acts continuously on M), then $H^n_{\text{cont}}(G, M)$ is simply denoted as $H^n(G, M)$. If G is the Galois group of a Galois extension, we again have Galois cohomology.

Let G be a topological group and let H be a closed normal subgroup of G, then for any topological G-module M, M is naturally regarded as an H-module and M^H a G/H-module. Then naturally we have the restriction map

$$\text{res}: \ H^1_{\text{cont}}(G, M) \longrightarrow H^1_{\text{cont}}(H, M).$$

Given a cocycle $(a_{\bar{g}}) : G/H \to M^H$, for any $g \in G$, just set $a_g = a_{\bar{g}}$, then (a_g) is a 1-cocycle in G with values in $M^H \subseteq M$, thus we have the inflation map

$$\text{Inf}: \ H^1_{\text{cont}}(G/H, M^H) \longrightarrow H^1_{\text{cont}}(G, M).$$

Proposition 1.113 (Inflation-restriction sequence). *One has the following exact sequence*

$$1 \longrightarrow H^1_{\text{cont}}(G/H, M^H) \xrightarrow{\text{Inf}} H^1_{\text{cont}}(G, M) \xrightarrow{\text{res}} H^1_{\text{cont}}(H, M). \tag{1.82}$$

Proof. By definition, it is clear that the composition map $\mathrm{res} \circ \mathrm{Inf}$ sends any element in $H^1_{\mathrm{cont}}(G/H, M^H)$ to the distinguished element in $H^1_{\mathrm{cont}}(H, M)$.

(1) Exactness at $H^1_{\mathrm{cont}}(G/H, M^H)$: If $(a_g)_g = (a_{\bar{g}})_g$ is equivalent to the distinguished element in $H^1(G, M)$, then $a_g = m^{-1}m^g$ for some $m \in M$, but for any $h \in H$, $a_g = a_{gh}$, thus $m^g = (m^h)^g$, thus $m = m^h$ and hence $m \in M^H$, so $(a_{\bar{g}})_{\bar{g}}$ is cohomologous to the trivial cocycle from G/H to M^H.

(2) Exactness at $H^1_{\mathrm{cont}}(G, M)$: If $a : G \to M$ is a cocycle whose restriction to H is cohomologous to 1, then $a_h = m^{-1}m^h$ for some $m \in M$ and all $h \in H$. Let $a'_g = ma_g(m^{-1})^g$, then a' is cohomologous to a and $a'_h = 1$ for all $h \in H$. By the cocycle condition, then $a'_{gh} = a'_g a'^g_h = a'_g$ if $h \in H$. Thus a'_g is constant on the cosets of H. Again using the cocycle condition, we get $a'_{hg} = a'^h_g$ for all $h \in H$, but $hg = gh'$ for some $h' \in H$, thus $a'_g = a'^h_g$ for all $h \in H$. We therefore get a cocycle $(a_{\bar{g}} = a'_g)_{\bar{g}} : G/H \to M^H$ which maps to a.

At the end of this section, we introduce the following classical result:

Theorem 1.114 (Hilbert's Theorem 90). *Let K be a field and L be a Galois extension of K, finite or not. Then*

(1) $H^1(L/K, L) = 0$;
(2) $H^1(L/K, L^\times) = 1$;
(3) *Moreover, for all $n \geq 1$, $H^1(L/K, \mathrm{GL}_n(L))$ is trivial.*

Proof. It suffices to show the finite extension case. (1) is a consequence of normal basis theorem: there exists a normal basis of L over K.

For (2) and (3), we have the following proof which is due to Cartier (cf. Serre [Ser80], Chap. X, Proposition 3).

Let c be a cocycle. Suppose x is a vector in L^n, we form $b(x) = \sum\limits_{s \in \mathrm{Gal}(L/K)} c_s(s(x))$. Then $b(x)$, $x \in K^n$ generates L^n as a L-vector space. In fact, if u is a linear form which is 0 at all $b(x)$, then for every $h \in L$,

$$0 = u(b(hx)) = \sum u(c_s s(h)s(x)) = \sum s(h)u(c_s(s(x))).$$

Varying h, we get a linear relation of $s(h)$. By Dedekind's linear independence theorem of automorphisms, $u(c_s s(x)) = 0$, and since c_s is invertible, $u = 0$.

By the above fact, suppose $x_1, \cdots, x_n$ are vectors in L^n such that the $y_i = b(x_i)$'s are linear independent over L. Let T be the transformation matrix from the canonical basis e_i of L^n to x_i, then the corresponding matrix of $b = \sum c_s s(T)$ sends e_i to y_i, which is invertible. It is easy to check that $s(b) = c_s^{-1}b$, thus the cocycle c is trivial.

2

ℓ-adic representations of local fields: an overview

2.1 ℓ-adic Galois representations

We let $G = \mathrm{Gal}(L/K)$, the Galois group of a Galois extension L/K, equipped with the natural profinite topology.

2.1.1 Definition and basic properties.

Definition 2.1. *Let E be a topological vector field. A* continuous linear representation of G with coefficients in E *or a* continuous E-representation *is a finite dimensional E-vector space V with induced topology equipped with a continuous linear action of G, equivalently, it is a continuous group homomorphism*

$$\rho : \quad G \longrightarrow \mathrm{Aut}_E(V).$$

The dimension of a representation is its dimension as an E-vector space.

If moreover, $G = G_K$ is the absolute Galois group of the field K, such a representation of G is called a Galois representation *of K.*

Remark 2.2. (1) If $\dim V = d$, one has an isomorphism $\mathrm{Aut}_E(V) \cong \mathrm{GL}_d(E)$ under a given E-basis of V, hence ρ extends to a homomorphism $G \to \mathrm{GL}_d(V)$. However this extension depends on the choice of the basis.

(2) If E is endowed with the discrete topology, then the continuous condition means that ρ factors through a suitable finite Galois extension F of K contained in L:

$$\begin{tikzcd} G \arrow[rr, "\rho"] \arrow[dr] & & \mathrm{Aut}_E(V). \\ & \mathrm{Gal}(F/K) \arrow[ur] & \end{tikzcd}$$

(3) Assume that E is a completion of a number field. Then either $E = \mathbb{R}$, $\mathbb{C}$ or a finite extension of $\mathbb{Q}_\ell$ for a suitable prime number ℓ.

(i) If $E = \mathbb{R}$ or $\mathbb{C}$, then ρ is continuous if and only if $\mathrm{Ker}\,(\rho)$ is an open normal subgroup of G.

(ii) If E is a finite extension of $\mathbb{Q}_\ell$ of degree d and V is an E-linear representation of G of dimension h, by the inclusion $\mathrm{Aut}_E(V) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$, V is naturally viewed as a $\mathbb{Q}_\ell$-representation of dimension hd and $E \hookrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell[G]}(V)$. Conversely, if V is a $\mathbb{Q}_\ell$-linear representation of G together with an embedding $E \hookrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell[G]}(V)$, then V is viewed as an E-representation of G.

Definition 2.3. *An* ℓ-adic representation *of G is a finite dimensional $\mathbb{Q}_\ell$-vector space equipped with a continuous and linear action of G.*

In particular a representation of G_K is called an ℓ-adic Galois representation *of K.*

Definition 2.4. *A* $\mathbb{Z}_\ell$-representation *of G is a finitely generated $\mathbb{Z}_\ell$-module, equipped with a linear and continuous action of G.*

Example 2.5. (1) The *trivial ℓ-adic representation* is $\mathbb{Q}_\ell$ with trivial G-action. The *trivial $\mathbb{Z}_\ell$-representation* is $\mathbb{Z}_\ell$.

(2) A $\mathbb{Z}_\ell$-representation killed by ℓ is nothing but an $\mathbb{F}_\ell$-representation.

Example 2.6. If V is a continuous ℓ-adic representation of G of dimension 1, write $V = \mathbb{Q}_\ell e$, then $g(e) = \eta(g)e$. The map $g \mapsto \eta(g)$ is a continuous homomorphism $\eta : G \to \mathbb{Q}_\ell^\times$. Conversely, given $\eta : G \to \mathbb{Q}_\ell^\times$, then $\mathbb{Q}_\ell \cdot e$ with the G-action $g(e) = \eta(g)e$ is an ℓ-adic representation of G of dimension 1. If $G = G_K$, we let $\mathbb{Q}_\ell(\eta)$ be the ℓ-adic Galois representation of K determined by η.

Similarly, a free $\mathbb{Z}_\ell$-representation of rank 1 is uniquely determined by a continuous homomorphism $\eta : G \to \mathbb{Z}_\ell^\times$. We let $\mathbb{Z}_\ell(\eta)$ be the free $\mathbb{Z}_\ell$-representation of G_K determined by η.

Recall a (full) *lattice* in a $\mathbb{Q}_\ell$-vector space W is a free $\mathbb{Z}_\ell$-submodule of W with generators forming a basis of W.

Lemma 2.7. *For any ℓ-adic representation V of G, there exists a lattice T of V which is stable by G-action and thus a free $\mathbb{Z}_\ell$-representation of G. In particular, there exists a basis of V, such that $\rho : G \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V) \cong \mathrm{GL}_d(\mathbb{Q}_\ell)$ factors through $\mathrm{GL}_d(\mathbb{Z}_\ell)$.*

Proof. Suppose V is an ℓ-adic representation. Let T_0 be a lattice of V, then for every $g \in G$, $g(T_0) = \{g(v) \mid v \in T_0\}$ is also a lattice. Moreover, the stabilizer $H = \{g \in G \mid g(T_0) = T_0\}$ of T_0 is an open subgroup of G and hence G/H is finite, the sum

$$T = \sum_{g \in G} g(T_0)$$

is a finite sum. T is again a lattice of V, and is stable under G-action, hence is a $\mathbb{Z}_\ell$-representation of G. If $\{e_1, \cdots, e_d\}$ is a basis of T over $\mathbb{Z}_\ell$, then it is also a basis of V over $\mathbb{Q}_\ell$, thus

$$\begin{tikzcd} G \arrow[rr, "\rho"] \arrow[dr] & & \mathrm{GL}_d(\mathbb{Q}_\ell). \\ & \mathrm{GL}_d(\mathbb{Z}_\ell) \arrow[ur, hook] & \end{tikzcd}$$

Remark 2.8. On the other hand, given a free $\mathbb{Z}_\ell$-representation T of rank d of G, we can get a d-dimensional ℓ-adic representation V by

$$V = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T, \quad g(\lambda \otimes t) = \lambda \otimes g(t), \quad \lambda \in \mathbb{Q}_\ell,\ t \in T.$$

For all $n \in \mathbb{N}$, G acts continuously on $T/\ell^n T$ with the discrete topology. Therefore we have

$$\begin{tikzcd} \rho: & G \arrow[r] \arrow[dr, "\rho_n"'] & \mathrm{Aut}_{\mathbb{Z}_\ell}(T) \arrow[d] & (\simeq \mathrm{GL}_d(\mathbb{Z}_\ell)) \\ & & \mathrm{Aut}(T/\ell^n T) & (\simeq \mathrm{GL}_d(\mathbb{Z}/\ell^n\mathbb{Z})) \end{tikzcd}$$

since $T/\ell^n T \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^d$ and $T = \varprojlim_{n\in\mathbb{N}} T/\ell^n T$. The group $H_n = \mathrm{Ker}\,(\rho_n)$ is a normal open subgroup of G and $\mathrm{Ker}\,(\rho) = \bigcap_{n\in\mathbb{N}} H_n$ is a closed subgroup.

As is well-known from linear algebra, one can define the direct sum, the tensor product, the dual, the symmetric power and the exterior power of vector spaces. We can build *new* representations starting from *old* ones:

Definition 2.9. *Suppose V_1, V_1 and V_2 are ℓ-adic representations of G.*

(1) *The direct sum $V_1 \oplus V_2$ of V_1 and V_2 is the vector space $V_1 \oplus V_2$, together with the G-action*
$$g(v_1, v_2) = (gv_1, gv_2). \tag{2.1}$$
(2) *The* tensor product $V_1 \otimes V_2$ *of V_1 and V_2 is the vector space $V_1 \otimes_{\mathbb{Q}_\ell} V_2$ together with the G-action*
$$g(v_1 \otimes v_2) = gv_1 \otimes gv_2. \tag{2.2}$$
(3) *The* dual representation V^* *of V is the dual vector space $\mathscr{L}_{\mathbb{Q}_\ell}(V, \mathbb{Q}_\ell)$ of V together with the G-action*
$$g \cdot \varphi = (v \mapsto \varphi(g^{-1} \cdot v)). \tag{2.3}$$
(4) *The r-th* symmetric power $\mathrm{Sym}^r_{\mathbb{Q}_\ell} V$ *of V is the r-th symmetric power vector space of V together with the inherited G-action from tensor products.*
(5) *The r-th* exterior power $\bigwedge^r_{\mathbb{Q}_\ell} V$ *of V is the r-th exterior power vector space of V together with the inherited G-action from tensor products.*

Remark 2.10. For finite free $\mathbb{Z}_\ell$-modules T, T_1 and T_2, one can define direct sum $T_1 \oplus T_2$, tensor product $T_1 \otimes_{\mathbb{Z}_\ell} T_2$ and dual $T^* = \mathscr{L}_{\mathbb{Z}_\ell}(T, \mathbb{Z}_\ell)$. Equipped with the obvious G-actions, we obtain the corresponding direct sum, tensor product and dual as free $\mathbb{Z}_\ell$-representations.

2.1.2 Examples of ℓ-adic Galois representations of K.

Assume that K is a field, K^s is separable closure of K and $G_K = \mathrm{Gal}(K^s/K)$.

(1). The Tate module of the multiplicative group $\mathbb{G}_m$.

Consider the exact sequence

$$1 \longrightarrow \boldsymbol{\mu}_{\ell^n}(K^s) \longrightarrow (K^s)^\times \xrightarrow{a \mapsto a^{\ell^n}} (K^s)^\times \longrightarrow 1,$$

where for a field F,

$$\boldsymbol{\mu}_{l^n}(F) = \{a \in F \mid a^{\ell^n} = 1\}. \tag{2.4}$$

Then $\boldsymbol{\mu}_{\ell^n}(K^s) \simeq \mathbb{Z}/\ell^n\mathbb{Z}$ if $\mathrm{char}\, K \neq \ell$ and $\simeq \{1\}$ if $\mathrm{char}\, K = \ell$. If $\mathrm{char}\, K \neq \ell$, the homomorphisms

$$\boldsymbol{\mu}_{\ell^{n+1}}(K^s) \to \boldsymbol{\mu}_{\ell^n}(K^s), \qquad a \mapsto a^\ell$$

form an inverse system, thus define the *Tate module of the multiplicative group* $\mathbb{G}_m$

$$T_\ell(\mathbb{G}_m) = \varprojlim_{n \in \mathbb{N}} \boldsymbol{\mu}_{\ell^n}(K^s). \tag{2.5}$$

$T_\ell(\mathbb{G}_m)$ is a free $\mathbb{Z}_\ell$-module of rank 1. Fix an element $t = (\varepsilon_n)_{n \in \mathbb{N}} \in T_\ell(\mathbb{G}_m)$ such that

$$\varepsilon_0 = 1,\ \varepsilon_1 \neq 1,\ \varepsilon_{n+1}^\ell = \varepsilon_n.$$

Then $T_\ell(G_m) = \mathbb{Z}_\ell t$ with

$$\lambda \cdot t = \left(\varepsilon_n^{\lambda_n}\right)_{n \in \mathbb{N}},\ \lambda_n \in \mathbb{Z},\ \lambda \equiv \lambda_n \bmod \ell^n \mathbb{Z}_\ell.$$

For any $g \in G_K$, then $g(t) = \chi(g)t$, with the *cyclotomic character*

$$\chi : G_K \longrightarrow \mathbb{Z}_\ell^\times. \tag{2.6}$$

Thus $T_\ell(\mathbb{G}_m) = \mathbb{Z}_\ell(\chi)$ is a free Z_ℓ-representation of G_K of rank 1. In convention, we write

$$T_\ell(\mathbb{G}_m) = \mathbb{Z}_\ell(1), \qquad V_\ell(\mathbb{G}_m) = \mathbb{Q}_\ell(1) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(1). \tag{2.7}$$

Set $\mathbb{Z}_\ell(-1) := \mathbb{Z}_\ell(1)^*$, and for $r \in Z$, set

$$\mathbb{Z}_\ell(r) = \mathbb{Z}_\ell t^r = \begin{cases} \mathbb{Z}_\ell(1)^{\otimes r}, & \text{if } r > 0; \\ \mathbb{Z}_\ell, & \text{if } r = 0; \\ \mathbb{Z}_\ell(-1)^{\otimes -r}, & \text{if } r < 0, \end{cases} \tag{2.8}$$

$$\mathbb{Q}_\ell(r) = \mathbb{Q}_\ell \cdot t^r = Q_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(r). \tag{2.9}$$

Then $g(t^r) = \chi^r(g) \cdot t^r$ for all $g \in G_K$, and

$$\mathbb{Z}_\ell(r) = \mathbb{Z}_\ell(\chi^r), \quad \mathbb{Q}_\ell(r) = \mathbb{Q}_\ell(\chi^r).$$

These representations are called the *Tate twists* of $\mathbb{Z}_\ell$. Moreover, for any ℓ-adic representation V, $V(r) = V \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell(r)$ are the Tate twists of V.

(2). The Tate module of an elliptic curve.

Assume $\operatorname{char} K \neq 2, 3$. Let $f(X) \in K[X]$, $\deg(f) = 3$ such that f is separable, then

$$f(x) = \lambda(X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$$

with distinct roots α_1, α_2, $\alpha_3 \in K^s$. Let E be the corresponding elliptic curve $Y^2 = f(X)$. Then

$$E(K^s) = \big\{(x, y) \in (K^s)^2 \mid y^2 = f(x)\big\} \cup \{\infty\}, \text{ where } O = \{\infty\}.$$

The set $E(K^s)$ is an abelian group on which G acts. One has the exact sequence

$$0 \longrightarrow E[\ell^n] \longrightarrow E(K^s) \xrightarrow{\times \ell^n} E(K^s) \longrightarrow 0,$$

where $E[\ell^n] = \{P \in E(K^s) \mid \ell^n P = O\}$. If $\ell \neq \operatorname{char} K$, then $E[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$. If $\ell = \operatorname{char} K$, then either $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z}$ in the ordinary case, or $E[\ell^n] = O$ in the supersingular case.

With the transition maps

$$E[\ell^{n+1}] \longrightarrow E[\ell^n], \quad P \longmapsto \ell\, P,$$

the *Tate module of* E is defined as

$$T_\ell(E) = \varprojlim_n E[\ell^n]. \tag{2.10}$$

The Tate module $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module of rank 2 if $\operatorname{char} K \neq \ell$; and 1 or 0 if $\operatorname{char} K = \ell$. Set $V_\ell(E) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(E)$. Then $V_\ell(E)$ is an ℓ-adic representation of G_K of dimension $2, 1, 0$ respectively.

(3). The Tate module of an abelian variety.

An *abelian variety* is a projective smooth variety A equipped with a group law

$$A \times A \longrightarrow A.$$

Set $\dim A = g$. Then

(i) $A(K^s)$ is an abelian group;
(ii) The ℓ^n-torsion group $A[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ if $\operatorname{char} K \neq \ell$, and $A[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^r$ with $0 \leq r \leq g$ if $\operatorname{char} K = \ell$,

We then get the $\mathbb{Z}_e ll$ and ℓ-adic Galois representations of A:

$$T_\ell(A) = \varprojlim A[\ell^n] \cong \begin{cases} \mathbb{Z}_\ell^{2g}, & \text{if } \operatorname{char} K \neq \ell; \\ \mathbb{Z}_\ell^r, & \text{if } \operatorname{char} K = \ell; \end{cases} \tag{2.11}$$

$$V_\ell(A) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(A). \tag{2.12}$$

(4). ℓ-adic étale cohomology.

Let Y be a proper and smooth variety over K^s (here K^s can be replaced by a separably closed field). One can define for $m \in \mathbb{N}$ the cohomology group

$$H^m(Y_{\text{ét}}, \mathbb{Z}/\ell^n\mathbb{Z}),$$

which is a finite abelian group killed by ℓ^n. Then the inverse limit $\varprojlim H^m(Y_{\text{ét}}, \mathbb{Z}/\ell^n\mathbb{Z})$, defined by the natural transition maps

$$H^m(Y_{\text{ét}}, \mathbb{Z}/\ell^{n+1}\mathbb{Z}) \longrightarrow H^m(Y_{\text{ét}}, \mathbb{Z}/\ell^n\mathbb{Z}),$$

is a finitely generated $\mathbb{Z}_\ell$-module. Define

$$H^m_{\text{ét}}(Y, \mathbb{Q}_\ell) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim H^m(Y_{\text{ét}}, \mathbb{Z}/\ell^n\mathbb{Z}),$$

then $H^m_{\text{ét}}(Y, \mathbb{Q}_\ell)$ is a finite dimensional $\mathbb{Q}_\ell$-vector space.

Let X be a proper and smooth variety over K, and

$$Y = X_{K^s} = X \otimes K^s = X \times_{\operatorname{Spec} K} \operatorname{Spec}(K^s).$$

Then $H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)$ gives rise to an ℓ-adic representation of G_K.

Example 2.11. If X is an abelian variety of dimension g, then

$$H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell) = \bigwedge\nolimits^m_{\mathbb{Q}_\ell} (V_\ell(X))^*.$$

If $X = \mathbb{P}^d_K$, then

$$H^m(\mathbb{P}^d_{K^s}, \mathbb{Q}_\ell) = \begin{cases} 0, & \text{if } m \text{ is odd or } m > 2d; \\ \mathbb{Q}_\ell\left(-\frac{m}{2}\right), & \text{if } m \text{ is even, } 0 \le m \le 2d. \end{cases}$$

Remark 2.12. This construction extends to more generality and conjecturally to motives. To any motive M over K, one expects to associate an ℓ-adic realization.

2.2 ℓ-adic representations of finite fields

In this section, let p be a prime, $K = \mathbb{F}_q$ be the finite field of order $q = p$-power and K^s be a fixed algebraic closure of K. Let $\varphi_K = (x \mapsto x^q)$ be the Frobenius and $\tau_K = \varphi_K^{-1}$ be the geometric Frobenius of K, which are both topological generators of the absolute Galois group $G_K\widehat{\mathbb{Z}}$. Let K_n be the unique extension of K of degree n inside K^s.

2.2.1 ℓ-adic Galois representations of finite fields.

As $\tau_K(x)$ is a topological generator of G_K, an ℓ-adic representation $\rho : G_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ is uniquely determined by $\rho(\tau_K) = u \in \mathrm{Aut}_{\mathbb{Q}_ell}(V)$: for $n \in \mathbb{Z}$, $\rho(\tau_K^n) = u^n$; for $n \in \widehat{\mathbb{Z}}$,

$$\rho(\tau_K^n) = \lim_{\substack{m \in \mathbb{Z} \\ m \mapsto n}} u^m, \tag{2.13}$$

which means the limit must make sense.

Lemma 2.13. *Given any $u \in \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$. There exists a continuous homomorphism $\rho : G_K \longmapsto \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ such that $\rho(\tau_K) = u$ if and only if the eigenvalues of u in a chosen algebraic closure of $\mathbb{Q}_\ell$ are ℓ-adic units, i.e. $P_u(t) = \det(u - t\,\mathrm{Id}_V)$ as a polynomial in $\mathbb{Q}_\ell[t]$ must have coefficients in $\mathbb{Z}_\ell$ and the constant term $P_u(0) \in \mathbb{Z}_\ell^\times$ is a unit.*

Proof. Choose a basis $\{e_1, \cdots, e_d\}$ of V, then u is represented by a matrix A in $\mathrm{GL}_d(\mathbb{Q}_\ell)$. We then write $A = P^{-1}UP$ with $P, U \in \mathrm{GL}_d(\overline{\mathbb{Q}}_\ell)$ and U is the Jordan canonical form of A. The limit in (2.13) exists if and only if $\lim\limits_{\substack{m \in \mathbb{Z} \\ m \mapsto n}} U^m$ exists.

If there exists ρ such that $\rho(\tau_K) = u$, then limits of the form $\lim\limits_{\substack{m \in \mathbb{Z} \\ m \mapsto n}} U^m$ make sense, which implies the diagonal elements of U (the eigenvalues of u) can not have absolute value > 1. Apply the argument to u^{-1}, then the eigenvalues of u^{-1} can not have absolute value > 1. Hence the eigenvalues of u must all be ℓ-adic units.

If all eigenvalues of u are units, it is easy to check the limit $\lim\limits_{\substack{m \in \mathbb{Z} \\ m \mapsto n}} U^m$ exists, so does the limit in (2.13).

Definition 2.14. *The* characteristic polynomial of the representation V *is the polynomial* $P_V(t) = \det(\mathrm{Id}_V - t\tau_K)$.

We have $P_V(t) = (-t)^d P_V(1/t)$.

Remark 2.15. The representation V is semi-simple if and only if $u = \rho(\tau_K)$ is semi-simple. As a result, isomorphism classes of semi-simple ℓ-adic representations V of G are determined by $P_V(t)$.

2.2.2 ℓ-adic geometric representations of finite fields.

Let X be a projective, smooth and geometrically connected variety over K. Let $C_n = C_n(X) = \#X(K_n) \in \mathbb{N}$ be the number of K_n-rational points of X. The zeta function of X is defined by:

$$Z_X(t) := \exp\left(\sum_{n=1}^{\infty} \frac{C_n}{n} t^n\right) \in \mathbb{Q}[[t]]. \tag{2.14}$$

Let $|X|$ be the underlying topological space of X. If x is a closed point of $|X|$, let $K(x)$ be the residue field of x and $\deg(x) = [K(x) : K]$. Then $Z_X(t)$ can be expressed as an Euler product

$$Z_X(t) = \prod_{\substack{x \in |X| \\ x \text{ closed}}} \frac{1}{1 - t^{\deg(x)}}. \tag{2.15}$$

Theorem 2.16 (Weil Conjecture, proved by Deligne). *Let X be a projective, smooth and geometrically connected variety of dimension d over the finite field K of cardinality q. Then*

(1) *There exist $P_0, P_1, \cdots, P_{2d} \in \mathbb{Z}[t]$, $P_m(0) = 1$, such that*

$$Z_X(t) = \frac{P_1(t)P_3(t)\cdots P_{2d-1}(t)}{P_0(t)P_2(t)\cdots P_{2d}(t)}. \tag{2.16}$$

(2) *There exists a functional equation*

$$Z_X\left(\frac{1}{q^d t}\right) = \pm q^{d\beta} t^{2\beta} Z_X(t) \tag{2.17}$$

where $\beta = \frac{1}{2}\sum_{m=0}^{2d}(-1)^m \beta_m$ and $\beta_m = \deg P_m$.

(3) *If we make an embedding of the ring of algebraic integers $\overline{\mathbb{Z}} \hookrightarrow \mathbb{C}$, and decompose*

$$P_m(t) = \prod_{j=1}^{\beta_m}(1 - \alpha_{m,j}t), \quad \alpha_{m,j} \in \mathbb{C}.$$

Then $|\alpha_{m,j}| = q^{\frac{m}{2}}$.

The proof of Weil's conjecture is why Grothendieck, M. Artin and others ([AGV73]) developed the étale theory, although the p-adic proof of the rationality of the zeta functions is due to Dwork [Dwo60]. One of the key ingredients of Deligne's proof ([Del74a, Del80]) is that for ℓ a prime number not equal to p, the characteristic polynomial of the ℓ-adic representation $H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)$ is

$$P_{H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)}(t) = P_m(t).$$

Definition 2.17. *Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and $w \in \mathbb{Z}$. A* Weil number of weight w *relative to $K = \mathbb{F}_q$ is an element $\alpha \in \overline{\mathbb{Q}}$ satisfying*

(i) *there exists $i \in \mathbb{N}$ such that $q^i\alpha \in \overline{\mathbb{Z}}$;*
(ii) *for any embedding $\sigma : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, $|\sigma(\alpha)| = q^{w/2}$.*

Moreover, α is said to be effective *if $\alpha \in \overline{\mathbb{Z}}$.*

Remark 2.18. (a) This is an *intrinsic notion.*

(b) If $i \in \mathbb{Z}$ and if α is a Weil number of weight w, then $q^i\alpha$ is a Weil number of weight $w + 2i$, hence is effective if $i \gg 0$.

Definition 2.19. *An ℓ-adic representation V of G_K is called* pure of weight w *if all reciprocal roots of $P_V(t)$ are Weil numbers of weight w, and is called* effective of weight w *if moreover all reciprocal roots are algebraic integers.*

Remark 2.20. (a) Let V be an ℓ-adic representation. If V is pure of weight w, then $V(i)$ is pure of weight $w-2i$. This is because G_K acts on $\mathbb{Q}_\ell(1)$ through χ with χ(arithmetic Frobenius)$= q$, so $\chi(\tau_K) = q^{-1}$. Therefore τ_K acts on $\mathbb{Q}_\ell(i)$ by multiplication by q^{-i}. If V is pure of weight w and if $i \in \mathbb{N}$, $i \gg 0$, then $V(-i)$ is effective.

(b) The Weil Conjecture implies that $V = H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)$ is pure and effective of weight m, and $P_V(t) \in \mathbb{Q}[t]$.

Definition 2.21. *An ℓ-adic representation V of G_K is said to be* geometric *if the following two conditions hold:*

(i) *V is semi-simple;*
(ii) *V can be written as a direct sum $V = \bigoplus_{w\in\mathbb{Z}} V_w$, with V_w pure of weight w and almost all $V_w = 0$.*

Let $\mathbf{Rep}_{\mathbb{Q}_\ell}(G_K)$ be the category of ℓ-adic representations of G_K. We denote by $\mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{geo}}(G_K)$ the full sub-category of geometric representations, which is a sub-Tannakian category of $\mathbf{Rep}_{\mathbb{Q}_\ell}(G_K)$, i.e. stable under sub-objects, quotients, $\oplus$, $\otimes$, dual, and $\mathbb{Q}_\ell$ is the unit representation as a geometric one. We denote by $\mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{GEO}}(G_K)$ the smallest sub-Tannakian category of $\mathbf{Rep}_{\mathbb{Q}_\ell}(G_K)$ containing all objects isomorphic to $H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)$ for X projective smooth varieties over K and $m \in \mathbb{N}$, which is also the smallest full sub-category of $\mathbf{Rep}_{\mathbb{Q}_\ell}(G_K)$ containing the objects isomorphic to $H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)(i)$ for all X, $m \in \mathbb{N}$ and $i \in \mathbb{Z}$, and stable under sub-objects and quotients.

Conjecture 2.22. $\mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{geo}}(G_K) = \mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{GEO}}(G_K)$.

Theorem 2.23. *We have* $\mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{geo}}(G_K) \subseteq \mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{GEO}}(G_K)$.

The only thing left in Conjecture 2.22 is to prove that $H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)$ is geometric. We know that it is pure of weight m, but do not know in general if it is semi-simple.

2.3 ℓ-adic representations of local fields

2.3.1 ℓ-adic representations of local fields.

In this section we assume K is a local field, whose residue field k is perfect of characteristic $p > 0$. Recall I_K and P_K are the inertia subgroup and the wild inertia subgroup of the absolute Galois group G_K. Assume $\ell \neq p$ is a fixed prime number.

We have the following two exact sequences

$$\begin{aligned} 1 \longrightarrow I_K \longrightarrow & G_K \longrightarrow G_k \longrightarrow 1, \\ 1 \longrightarrow P_K \longrightarrow & I_K \longrightarrow I_K/P_K \longrightarrow 1. \end{aligned}$$

Under the isomorphism

$$I_K/P_K \cong \widehat{\mathbb{Z}}'(1) = \prod_{\ell \neq p} \mathbb{Z}_\ell(1) = \mathbb{Z}_\ell(1) \times \prod_{\ell' \neq \ell, p} \mathbb{Z}_{\ell'}(1),$$

we define $P_{K,\ell}$ to be the inverse image of $\prod_{\ell' \neq p, \ell} \mathbb{Z}_{\ell'}(1)$ in I_K and $G_{K,\ell} := G_K/P_{K,\ell}$. Then we have

$$I_K/P_{K,\ell} \cong \mathbb{Z}_\ell(1)$$

and the short exact sequences

$$1 \longrightarrow \mathbb{Z}_\ell(1) \longrightarrow G_{K,\ell} \longrightarrow G_k \longrightarrow 1. \tag{2.18}$$

Let V be an ℓ-adic representation of G_K and T be a $\mathbb{Z}_\ell$-lattice stable under G_K-action. Hence we have

$$\begin{tikzcd} G_K \arrow[r, "\rho"] \arrow[dr] & \mathrm{Aut}_{\mathbb{Z}_\ell}(T) \arrow[d, hook] & \simeq \mathrm{GL}_d(\mathbb{Z}_\ell) \\ & \mathrm{Aut}_{\mathbb{Q}_\ell}(V) & \simeq \mathrm{GL}_d(\mathbb{Q}_\ell) \end{tikzcd}$$

where $d = \dim_{\mathbb{Q}_\ell}(V)$. The image $\rho(G_K)$ is a closed subgroup of $\mathrm{Aut}_{\mathbb{Z}_\ell}(T)$.

Consider the following sequence

$$1 \longrightarrow N_1 \longrightarrow \mathrm{GL}_d(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_d(\mathbb{F}_\ell) \longrightarrow 1,$$

where N_1 is the kernel of the reduction map. Let N_n be the subgroup of matrices congruent to $1 \bmod \ell^n$ for $n \geq 1$. As N_1/N_n is a finite ℓ-group, $N_1 \simeq \varprojlim N_1/N_n$ is a pro-ℓ group. By the exact sequence

$$1 \longrightarrow P_K \longrightarrow P_{K,\ell} \longrightarrow \prod_{\ell' \neq p,\, \ell} \mathbb{Z}_{\ell'}(1) \longrightarrow 1,$$

note that P_K is a pro-p group, then $P_{K,\ell}$ is the inverse limit of finite groups with prime-to-ℓ orders, thus $\rho(P_{K,\ell}) \cap N_1 = \{1\}$. Hence $\rho(P_{K,\ell}) \hookrightarrow \mathrm{GL}_d(\mathbb{F}_\ell)$ is a finite group.

Definition 2.24. *Let V be an ℓ-adic Galois representation of K with the associated homomorphism $\rho : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$.*

(i) *V is* unramified *or has* good reduction *if I_K acts trivially.*

(ii) *V has* potentially good reduction *if $\rho(I_K)$ is finite, in other words, if there exists a finite extension K'/K inside K^s such that V as an ℓ-adic Galois representation of K' has good reduction.*
(iii) *V is* semi-stable *if I_K acts unipotently, in other words, if the semi-simplification of V has good reduction.*
(iv) *V is* potentially semi-stable *if there exists a finite extension K' of K contained in K^s such that V is semi-stable as a representation of $G_{K'}$.*

Remark 2.25. Notice that (4) is equivalent to the condition that there exists an open subgroup of I_K which acts unipotently, or that the semi-simplification of V has potentially good reduction.

Theorem 2.26. *Assume that the group $\boldsymbol{\mu}_{\ell^\infty}(K(\mu_\ell)) = \{\varepsilon \in K(\mu_\ell) \mid \exists\, n$ such that $\varepsilon^{\ell^n} = 1\}$ is finite. Then any ℓ-adic representation of G_K is potentially semi-stable. In particular, this is the case if k is finite.*

Proof. Replacing K by a suitable finite extension we may assume that $P_{K,\ell}$ acts trivially, then ρ factors through $G_{K,\ell}$:

$$\begin{tikzcd} G_K \arrow[rr, "\rho"] \arrow[dr] & & \mathrm{Aut}_{\mathbb{Q}_\ell}(V) \\ & G_{K,\ell} \arrow[ur, "\bar\rho"'] & \end{tikzcd}$$

Consider the sequence

$$1 \longrightarrow \mathbb{Z}_\ell(1) \longrightarrow G_{K,\ell} \longrightarrow G_k \longrightarrow 1.$$

Let t be a topological generator of $\mathbb{Z}_\ell(1)$. So $\bar\rho(t) \in \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$. Choose a finite extension E of $\mathbb{Q}_\ell$ such that the characteristic polynomial of $\bar\rho(t)$ splits in E. Let $V' = E \otimes_{\mathbb{Q}_\ell} V$. Then V' is an E-representation of $G_{K,\ell}$ via the action

$$g(\lambda \otimes v) = \lambda \otimes g(v).$$

Let a be an eigenvalue of $\bar\rho(t)$ and $0 \neq v \in V'$ be an eigenvector of a, i.e. $\bar\rho(t)(v) = a \cdot v$.

If $g \in G_{K,\ell}$, then $gtg^{-1} = t^{\chi_\ell(g)}$, where $\chi_\ell : G_{K,\ell} \longrightarrow \mathbb{Z}_\ell^\times$ is the cyclotomic character. Then

$$\bar\rho(gtg^{-1})(v) = \bar\rho\left(t^{\chi_\ell(g)}\right)(v) = a^{\chi_\ell(g)}v.$$

Therefore

$$\bar\rho(t)(g^{-1}(v)) = t(g^{-1}v) = (tg^{-1})(v) = g^{-1}(a^{\chi_\ell(g)}v) = a^{\chi_\ell(g)}g^{-1}v.$$

This implies, if a is an eigenvalue of $\bar\rho(t)$, then for all $n \in \mathbb{Z}$ such that there exists $g \in G_{K,\ell}$ with $\chi_\ell(g) = n$, a^n is also an eigenvalue of $\bar\rho(t)$. The condition

$\boldsymbol{\mu}_{\ell^\infty}(K(\mu_\ell))$ is finite $\Longleftrightarrow \mathrm{Im}(\chi_\ell)$ is open in $\mathbb{Z}_\ell^\times$. Thus there are infinitely many such n's. This implies a must be a root of 1. Therefore there exists an $N \geq 1$ such that t^N acts unipotently. The closure of the subgroup generated by t^N acts unipotently and is an open subgroup of $\mathbb{Z}_\ell(1)$. Since $I_K \twoheadrightarrow \mathbb{Z}_\ell(1)$ is surjective, the theorem now follows.

Corollary 2.27 (Grothendieck's ℓ-adic monodromy Theorem). *Let K be a local field. Then any ℓ-adic representation of G_K* coming from algebraic geometry *(eg. $V_\ell(A)$, $H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)(i), \cdots$) is potentially semi-stable.*

Proof. Let X be a projective and smooth variety over K. Let K_0 be the field of finite type over the prime field of K by joining all coefficients of the defining equations of X. Let K_1 be the closure of K_0 in K. Then K_1 is a complete discrete valuation field whose residue field k_1 is of finite type over $\mathbb{F}_p$. Let k_2 be the radical closure of k_1, and K_2 be a complete separable field contained in K and containing K_0, whose residue field is k_2. Then $\boldsymbol{\mu}_{\ell^\infty}(k_2) = \boldsymbol{\mu}_{\ell^\infty}(k_1)$, which is finite. Then

$$X = X_0 \times_{K_0} K, \quad X_2 = X_0 \times_{K_0} K_2, \quad X = X_2 \times_{K_2} K,$$

where X_0 is defined over K_0. The action of G_K on V comes from the action of G_{K_2}, hence the corollary follows from the theorem.

Theorem 2.28. *Assume k is algebraically closed. Then any potentially semi-stable ℓ-adic representation of G_K* comes from algebraic geometry.

Proof. We proceed the proof in two steps. First note that k is algebraically closed implies $I_K = G_K$.

(I): assume the Galois representation (V, ρ) is semi-stable. Then the action of $P_{K,\ell}$ must be trivial from the above discussion, hence the representation factors through $G_{K,\ell}$. Identify $G_{K,\ell}$ with $\mathbb{Z}_\ell(1)$, and let t be a topological generator of this group. Then $\rho : G_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ factors through $\bar{\rho} : G_{K,\ell} = \mathbb{Z}_\ell(1) \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ and is uniquely determined by $\bar{\rho}(t) \in \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$.

For each integer $n \geq 1$, there exists a unique (up to isomorphism) representation V_n of dimension n which is semi-stable and in-decomposable. Write it as $V_n = \mathbb{Q}_\ell^n$, and we can assume

$$\bar{\rho}(t) = \begin{pmatrix} 1 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}.$$

As $V_n \cong \mathrm{Sym}^{n-1}_{\mathbb{Q}_\ell}(V_2)$, it is enough to prove that V_2 comes from algebraic geometry. Write

$$0 \longrightarrow \mathbb{Q}_\ell \longrightarrow V_2 \longrightarrow \mathbb{Q}_\ell \longrightarrow 0,$$

where V_2 is a non-trivial extension. It is enough to produce a non-trivial extension of two trivial ℓ-adic representations of dimension 1 from algebraic geometry.

For $0 \neq q \in \mathfrak{m}_K$, let E be the Tate elliptic curve over K such that $E(K^s) \cong (K^s)^\times/q^{\mathbb{Z}}$, then

$$E[\ell^n] = \left\{ a \in (K^s)^\times \mid \exists\, m \in \mathbb{Z} \text{ such that } a^{\ell^n} = q^m \right\} \Big/ q^{\ell^n}$$

and

$$V_\ell(E) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(E), \quad T_\ell(E) = \varprojlim E[\ell^n].$$

An element $\alpha \in T_\ell(E)$ is given by

$$\alpha = (\alpha_n)_{n\in\mathbb{N}}, \quad \alpha_n \in E[\ell^n], \quad \alpha_{n+1}^\ell = \alpha_n.$$

From the exact sequence

$$0 \longrightarrow \boldsymbol{\mu}_{\ell^n}(K^s) \longrightarrow E[\ell^n] \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z} \longrightarrow 0,$$

and noting that $\boldsymbol{\mu}_{\ell^n}(K^s) = \boldsymbol{\mu}_{\ell^n}(K)$ as k is algebraically closed, we have a non-trivial extension

$$0 \longrightarrow \mathbb{Q}_\ell \longrightarrow V_\ell(E) \longrightarrow \mathbb{Q}_\ell \longrightarrow 0.$$

(II): assume V is potentially semi-stable. Then there exists a finite extension K' of K contained in K^s such that $I_{K'} = G_{K'}$ acts unipotently on V.

Let q be a uniformizing parameter of K'. Let E be the Tate elliptic curve associated to q defined over K', and let $V_\ell(E)$ be the semi-stable Galois representation of $G_{K'}$. From the *Weil scalar restriction of* E, we get an abelian variety A over K and

$$V_\ell(A) = \mathrm{Ind}_{G_{K'}}^{G_K} V_\ell(E)$$

is an ℓ-adic representation of G_K of dimension $2 \cdot [K' : K]$. All ℓ-adic representations of G_K which are semi-stable ℓ-adic representations of $G_{K'}$ come from $V_\ell(A)$.

2.3.2 An alternative description of potentially semi-stability.

Let the notations be as in the previous subsection. To any $0 \neq q \in \mathfrak{m}_K$, let E be the corresponding Tate elliptic curve, whose Tate module

$$V_\ell(E) = V_\ell\left((K^s)^\times/q^{\mathbb{Z}}\right) = \mathbb{Q}_\ell \otimes \varprojlim \left((K^s)^\times/q^{\mathbb{Z}}\right)[\ell^n].$$

Then one has a short exact sequence of ℓ-adic representations of K

$$0 \longrightarrow \mathbb{Q}_\ell \longrightarrow V_\ell(E)(-1) \longrightarrow \mathbb{Q}_\ell(-1) \longrightarrow 0.$$

Let t be a generator of $\mathbb{Q}_\ell(1)$. Let $u \in V_\ell(E)(-1)$ be a lifting of the generator t^{-1} of $\mathbb{Q}_\ell(-1)$. Put

$$B_\ell := \mathbb{Q}_\ell[u], \tag{2.19}$$

and define the following $\mathbb{Q}_\ell$-linear map

$$\begin{aligned} N : B_\ell &\longrightarrow B_\ell(-1) = B_\ell \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell(-1) \\ b \ &\longmapsto -b' \otimes t^{-1} = -\tfrac{db}{du} \otimes t^{-1}. \end{aligned} \tag{2.20}$$

Note that N commutes with the action of G_K. For any ℓ-adic representation V of G_K, set

$$\mathbf{D}_\ell(V) := \varinjlim_{\substack{H \triangleleft I_K \\ \text{open}}} \left(B_\ell \otimes_{\mathbb{Q}_\ell} V\right)^H . \tag{2.21}$$

Then the map N extends to $N : \mathbf{D}_\ell(V) \longrightarrow \mathbf{D}_\ell(V)(-1)$.

Definition 2.29. *Denote by $\mathscr{C}$ the category of pairs (D, N), where*

(i) *D is an ℓ-adic representation of G_K with potentially good reduction.*
(ii) *$N : D \longrightarrow D(-1)$ is a $\mathbb{Q}_\ell$-linear map commuting with the action of G_K, and is* nilpotent*. Here* nilpotent *means the following: write $N(\delta) = N_t(\delta) \otimes t^{-1}$, where $N_t : D \longrightarrow D$, then that N_t (or N) is* nilpotent *means that the composition of the maps*

$$D \xrightarrow{N} D(-1) \xrightarrow{N(-1)} D(-2) \longrightarrow \cdots \xrightarrow{N(-r+1)} D(-r)$$

is zero for r large enough. The smallest such r is called the length *of D.*
(iii) $\mathrm{Hom}_{\mathscr{C}}((D, N), (D', N'))$ *is the set of the maps $\eta : D \longrightarrow D'$ where η is $\mathbb{Q}_\ell$-linear, commutes with the action of G_K, and the diagram*

$$\begin{array}{ccc} D & \xrightarrow{\ \eta\ } & D' \\ {\scriptstyle N}\downarrow & & \downarrow{\scriptstyle N'} \\ D(-1) & \xrightarrow[\eta(-1)]{} & D'(-1) \end{array}$$

commutes.

One can check immediately that

$$\mathbf{D}_\ell : \mathbf{Rep}_{\mathbb{Q}_\ell}(G_K) \longrightarrow \mathscr{C}$$

is a functor. In the other direction, we can define the functor

$$\mathbf{V}_\ell : \mathscr{C} \longrightarrow \mathbf{Rep}_{\mathbb{Q}_\ell}(G_K).$$

Suppose the Galois group G_K acts diagonally on $B_\ell \otimes_{\mathbb{Q}_\ell} D$. Since

$$(B_\ell \otimes_{\mathbb{Q}_\ell} D)(-1) = (B_\ell \otimes_{\mathbb{Q}_\ell} D) \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell(-1) = B_\ell(-1) \otimes_{\mathbb{Q}_\ell} D = B_\ell \otimes_{\mathbb{Q}_\ell} D(-1),$$

define the map $N : B_\ell \otimes_{\mathbb{Q}_\ell} D \to (B_\ell \otimes_{\mathbb{Q}_\ell} D)(-1)$ by

$$N(b \otimes \delta) = Nb \otimes \delta + b \otimes N\delta.$$

Set

$$\mathbf{V}_\ell(D, N) := \mathrm{Ker}\,(N : B_\ell \otimes_{\mathbb{Q}_\ell} D \longrightarrow (B_\ell \otimes_{\mathbb{Q}_\ell} D)(-1))\,. \tag{2.22}$$

Theorem 2.30. (1) *If V is any ℓ-adic representation of G_K, then*

$$\mathbf{V}_\ell\left(\mathbf{D}_\ell(V)\right) \hookrightarrow V$$

is injective and is an isomorphism if and only if V is potentially semi-stable.

(2) $\mathbf{V}_\ell(D, N)$ *is stable by G_K and* $\dim_{\mathbb{Q}_\ell} \mathbf{V}_\ell(D, N) = \dim_{\mathbb{Q}_\ell}(D)$ *and* $\mathbf{V}_\ell(D, N)$ *is potentially semi-stable.*

(3) $\mathbf{D}_\ell$ *induces an equivalence of categories between $\mathbf{Rep}_{\mathbb{Q}_\ell,\mathrm{pst}}(G_K)$, the category of potentially semi-stable ℓ-adic representations of G_K and the category $\mathscr{C}$, and $\mathbf{V}_\ell$ is the quasi-inverse functor of $\mathbf{D}_\ell$.*

Proof. (1) is a consequence of a more general result (Theorem 3.14) in next chapter. One needs to check that B_ℓ is so-called $(\mathbb{Q}_\ell, H)$-regular for any normal open subgroup H of I_K, i.e. it needs to satisfy: (i) $B_\ell^H = (\mathrm{Frac}\, B_\ell)^H$; (ii) for a non-zero element b such that the $\mathbb{Q}_\ell$-line generated by b is stable by H, then b is invertible in B_ℓ. This is easy to check: (i) $B_\ell^H = (\mathrm{Frac}\, B_\ell)^H = \mathbb{Q}_\ell$. (ii) $b \in \mathbb{Q}_\ell$ is invertible.

(2) is proved by induction to the length of D. If the length is 0, then $ND = 0$ and $\mathbf{V}_\ell(D, N) = B_\ell^{N=0} \otimes D = D$, and the result is evident. We also know that N is surjective on $B_\ell \otimes D$. In general, suppose D is of length $r+1$. Let $D_1 = \mathrm{Ker}\,(N : D \to D(-1))$ and $D_2 = \mathrm{Im}(N : D \to D(-1)$, and endow D_1 and D_2 with the induced nilpotent map N. Then both of them are objects in $\mathscr{C}$, D_1 is of length 0 and D_2 is of length r. The exact sequence

$$0 \longrightarrow D_1 \longrightarrow D \longrightarrow D_2 \longrightarrow 0$$

induces a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & B_\ell \otimes D_1 & \longrightarrow & B_\ell \otimes D & \longrightarrow & B_\ell \otimes D_2 & \longrightarrow & 0 \\
 & & {\scriptstyle N}\Big\downarrow & & {\scriptstyle N}\Big\downarrow & & {\scriptstyle N}\Big\downarrow & & \\
0 & \longrightarrow & B_\ell \otimes D_1(-1) & \longrightarrow & B_\ell \otimes D(-1) & \longrightarrow & B_\ell \otimes D_2(-1) & \longrightarrow & 0
\end{array}$$

and since N is surjective on $B_\ell \otimes D$, by the snake lemma, we have an exact sequence of $\mathbb{Q}_\ell$-vector spaces

$$0 \longrightarrow \mathbf{V}_\ell(D_1, N) \longrightarrow \mathbf{V}_\ell(D, N) \longrightarrow \mathbf{V}_\ell(D_2, N) \longrightarrow 0$$

which is compatible with the action of G. By induction, the result follows.

(3) follows from (1) and (2).

Exercise 2.31. Let (D,N) be an object of $\mathscr{C}$. The map

$$\begin{aligned} \mathbf{V}_\ell(D) \subset B_\ell \otimes_{\mathbb{Q}_\ell} D &\longrightarrow D \\ \textstyle\sum_i P_i(u) \otimes \delta_i &\longmapsto \textstyle\sum_i P_i(0) \otimes \delta_i \end{aligned}$$

induces an isomorphism of $\mathbb{Q}_\ell$-vector spaces between $V_\ell(D)$ and D (but it does not commute with the action of G_K). Describe the *new* action of G_K on D using the old action and N.

2.3.3 The finite residue field case.

Assume k is a finite field with q elements of characteristic p. Assume $\ell \neq p$. We identify $G_k = \overline{\langle \tau_k \rangle}$ with $\widehat{\mathbb{Z}}$.

Definition 2.32. *The* Weil group W_K *of* K *is the subgroup of* G_K *defined by*

$$\begin{tikzcd} 1 \arrow[r] & I_K \arrow[r] \arrow[d, equal] & G_K \arrow[r, "a"] & \widehat{\mathbb{Z}} \arrow[r] & 1 \\ 1 \arrow[r] & I_K \arrow[r] & W_K \arrow[r, "a"] \arrow[u, hook] & \widehat{\mathbb{Z}} \arrow[r] \arrow[u, hook] & 1, \end{tikzcd}$$

where $a(g) = m$ *if* $g|_{\bar{k}} = \tau_k^m$.

The Weil-Deligne group *of* K *(relative to* $\overline{K}/K$*), denoted as* WD_K*, is the group scheme over* $\mathbb{Q}$ *which is the semi-direct product of* W_K *by the additive group* $\mathbb{G}_a$*, over which* W_K *acts by*

$$wxw^{-1} = q^{-a(w)}x. \tag{2.23}$$

Suppose E is any field of characteristic 0.

Definition 2.33. *A* Weil representation *of* K *over* E *is a finite dimensional* E*-vector space* D *equipped with a homomorphism of groups* $\rho : W_K \longrightarrow \mathrm{Aut}_E(D)$ *whose kernel contains an open subgroup of* I_K.

A Weil-Deligne representation *is a Weil representation equipped with a nilpotent endomorphism* N *of* D *such that*

$$N \circ \rho(w) = q^{a(w)}\rho(w) \circ N \quad \text{for any } w \in W_K. \tag{2.24}$$

Remark 2.34. For an E-vector space D with an action of W_K, we can define $D(-1) = D \otimes_E E(-1)$, where $E(-1)$ is a one-dimensional E-vector space on which I_K acts trivially and the action of τ_k is multiplication by q^{-1}. Then an object of $\mathbf{Rep}_E(WD_K)$ is nothing but a pair (D,N) where D is an E-linear continuous representation of W_K and $N : D \longrightarrow D(-1)$ is a morphism of E-linear representation of W_K (which implies that N is nilpotent).

Example 2.35. Any ℓ-adic representation V of G_K which has potentially good reduction defines a continuous $\mathbb{Q}_\ell$-linear representation of W_K. As W_K is dense in G_K, the action of W_K determines the action of G_K. Let $\mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{pst}}(G_K)$ be the category of potentially semi-stable ℓ-adic representation of G_K. By results from previous subsection, we have a fully faithful functor

$$\begin{aligned} \mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{pst}}(G_K) &\longrightarrow \mathbf{Rep}_{\mathbb{Q}_\ell}(WD_K) \\ V &\longmapsto (\mathbf{D}_\ell(V), N). \end{aligned} \tag{2.25}$$

Definition 2.36. *Suppose E and F are two fields of characteristic* 0 *(for instance, $E = \mathbb{Q}_\ell$, and $F = \mathbb{Q}_{\ell'}$). Let D (resp. D') be an E-linear representation (resp. F-representation) of WD_K. D and D' are said to be* compatible *if for any field Ω and embeddings*

$$E \hookrightarrow \Omega \qquad \text{and} \qquad F \hookrightarrow \Omega,$$

$\Omega \otimes_E D \simeq \Omega \otimes_F D'$ are isomorphic as Ω-linear representations of WD_K.

Theorem 2.37. *Assume that A is an abelian variety over K. If ℓ and ℓ' are different prime numbers not equal to p, then $V_\ell(A)$ and $V_{\ell'}(A)$ are compatible.*

Conjecture 2.38. Let X be a projective and smooth variety over K. For any $m \in \mathbb{N}$, if ℓ, ℓ' are primes not equal to p, then

$$H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell) \text{ and } H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_{\ell'})$$

are compatible.

Remark 2.39. If X has good reduction, it is known that the two representations are unramified with the same characteristic polynomials of Frobenius by Weil's conjecture. It is expected that τ_k acts semi-simply, which would imply the conjecture in this case.

Definition 2.40. *An E-linear continuous representation V of W_K is called* pure of weight $w \in \mathbb{Z}$ *if all reciprocal roots of the characteristic polynomial of $\tau \in W_K$ a lifting of τ_k acting on V (in a chosen algebraic closure $\overline{E}$ of E) are Weil numbers of weight w relative to k, i.e. for any root λ, $\lambda \in \overline{\mathbb{Q}}$ and for any embedding $\sigma : \overline{\mathbb{Q}} \longrightarrow \overline{E}$, we have*

$$\mid \sigma(\lambda) \mid = q^{w/2}.$$

Remark 2.41. This definition is independent of the choices of τ and $\overline{E}$.

For V any E-linear continuous representation of W_K and $r \in \mathbb{N}$, set

$$D = D(V, r) := V \oplus V(-1) \oplus V(-2) \oplus \cdots \oplus V(-r)$$

with the nipotent map $N : D \longrightarrow D(-1)$ given by

$$N(v_0, v_{-1}, v_{-2}, \cdots, v_{-r}) = (v_{-1}, v_{-2}, \cdots, v_{-r}, 0).$$

Then D is a representation of WD_K.

Definition 2.42. *An E-linear representation of WD_K is called* elementary and pure of weight $w+r$ *if it is isomorphic to such a D with V satisfying*

(i) *V is pure of weight w;*
(ii) *V is semi-simple.*

Definition 2.43. *Let $m \in \mathbb{Z}$. A* geometric representation of WD_K pure of weight m *is a representation which is isomorphic to a direct sum of elementary and pure representation of weight m.*

Remark 2.44. The full sub-category $\mathbf{Rep}^m_{E,\,\mathrm{geo}}(WD_K)$ of $\mathbf{Rep}_E(WD_K)$ formed by geometric representations of WD_K pure of weight m is abelian category.

Definition 2.45. *An ℓ-adic representation of G_K is called* geometric *if the associated $\mathbb{Q}_\ell$-linear representation of WD_K is geometric.*

For $\ell \neq p$, let

$$\mathbf{Rep}^m_{\mathbb{Q}_\ell,\,\mathrm{geo}}(G_K)$$

be the category of pure geometric ℓ-adic representation of G_K of weight m, which is the category of those V such that $(\mathbf{D}_\ell(V), N)$ is in $\mathbf{Rep}^m_{\mathbb{Q}_\ell,\,\mathrm{geo}}(WD_K)$.

Conjecture 2.46. For $\ell \neq p$, the ℓ-adic representation $H^r_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)(i)$ should be an object of $\mathbf{Rep}^{r-2i}_{\mathbb{Q}_\ell,\,\mathrm{geo}}(WD_K)$ and objects of this form should generate the category.

In the category $\mathbf{Rep}_E(WD_K)$, let

Definition 2.47. *The category of* weighted E-linear representation of WD_K, *denoted as $\mathbf{Rep}^w_E(WD_K)$, is the category with*

(i) *An object is an E-linear representation D of WD_K equipped an increasing filtration*
$$\cdots \subseteq W_m D \subseteq W_{m+1} D \subseteq \cdots$$
where $W_m D$ is stable under WD_K, and
$$W_m(D) = \begin{cases} D, & \text{if } m \gg 0, \\ 0, & \text{if } m \ll 0. \end{cases}$$
(ii) *Morphisms are morphisms of WD_K-representations which respect the filtration.*

Then $\mathbf{Rep}^w_E(WD_K)$ is an additive category, but not an abelian category.

Definition 2.48. *The category of geometric weighted E-linear representations of WD_K, denoted by $\mathbf{Rep}^w_{E,\,\mathrm{geo}}(WD_K)$, is the full sub-category of $\mathbf{Rep}^w_E(WD_K)$ consisting of those D's such that for all $m \in \mathbb{Z}$,*

$$gr_m D = W_m D / W_{m-1} D$$

is a pure geometric representation of weight m.

Theorem 2.49. $\mathbf{Rep}^w_{E,\,\mathrm{geo}}(WD_K)$ *is an abelian category.*

It is expected that if M is a *mixed motive* over K, for any ℓ prime number $\neq p$, $H_\ell(M)$ should be an object of $\mathbf{Rep}^w_{\mathbb{Q}_\ell,\,\mathrm{geo}}(G_K)$.

3

p-adic Representations of fields of characteristic p

3.1 B-representations and regular (F, G)-rings

3.1.1 B-representations.

Let G be a topological group and B be a topological commutative ring equipped with a continuous action of G compatible with the structure of ring, that is, for all $g \in G$, and $b_1, b_2 \in B$,

$$g(b_1 + b_2) = g(b_1) + g(b_2), \qquad g(b_1 b_2) = g(b_1)g(b_2).$$

Example 3.1. Let L/K be a Galois extension. Set $B = L$ and $G = \mathrm{Gal}(L/K)$, both endowed with the discrete topology.

Definition 3.2. *A* B-representation X *of* G *is a* B*-module of finite type equipped with a semi-linear and continuous action of* G*, where* semi-linear *means that for all* $g \in G$*,* $\lambda \in B$*, and* $x, x_1, x_2 \in X$*,*

$$g(x_1 + x_2) = g(x_1) + g(x_2), \qquad g(\lambda x) = g(\lambda)g(x).$$

Remark 3.3. For a B-representation X, if G acts trivially on B, then X is just a linear representation of G.

In particular, if $B = \mathbb{F}_p$ endowed with the discrete topology, X is called a *mod p representation* instead of a $\mathbb{F}_p$-representation; if $B = \mathbb{Q}_p$ endowed with the p-adic topology, X is called a *p-adic representation* instead of a $\mathbb{Q}_p$-representation.

Definition 3.4. *A* free B-representation *of* G *is a* B*-representation such that the underlying* B*-module is free.*

Example 3.5. Let F be a closed subfield of B^G and V be an F-representation of G, let $X = B \otimes_F V$ be equipped with G-action by $g(\lambda \otimes x) = g(\lambda) \otimes g(x)$, where $g \in G, \lambda \in B, x \in X$, then X is a free B-representation.

Definition 3.6. *A free B-representation X of G is* trivial *if one of the following two equivalent conditions holds:*

(i) *There exists a basis of X consisting of elements of X^G;*
(ii) *$X \cong B^d$ which is equipped with natural component-wise action of G.*

We now give the classification of free B-representations of G of rank d for $d \in \mathbb{N}$ and $d \geq 1$.

Assume that X is a free B-representation of G with basis $\{e_1, \cdots, e_d\}$. For every $g \in G$, write

$$g(e_j) = \sum_{i=1}^{d} a_{ij}(g) e_i.$$

Write $A_g = (a_{ij}(g))_{i,j}$, then $A_g \in \mathrm{GL}_d(B)$ and

$$g(e_1, \cdots, e_d) = (e_1, \cdots, e_d) A_g. \tag{3.1}$$

Thus we define a continuous map

$$\alpha : G \longrightarrow \mathrm{GL}_d(B), \quad g \longmapsto A_g. \tag{3.2}$$

Moreover, on one hand

$$g_1 g_2 (e_1, \cdots, e_d) = (e_1, \cdots, e_d) A_{g_1 g_2}.$$

on the other hand,

$$g_1 g_2 (e_1, \cdots, e_d) = g_1((e_1, \cdots, e_d)) g_1(A_{g_2}) = (e_1, \cdots, e_d) A_{g_1} g_1(A_{g_2}),$$

hence

$$\alpha(g_1 g_2) = A_{g_1 g_2} = A_{g_1} g_1(A_{g_2}) = \alpha(g_1) g_1(\alpha(g_2))$$

and α is a 1-cocycle in $Z^1_{\mathrm{cont}}(G, \mathrm{GL}_d(B))$. Moreover, if $\{e'_1, \cdots, e'_d\}$ is another basis and if P is the transition matrix, write

$$g(e'_j) = \sum_{i=1}^{d} a'_{ij}(g) e'_i, \qquad \alpha'(g) = (a'_{ij}(g))_{1 \leq i,j \leq d},$$

then we have

$$\alpha'(g) = P^{-1} \alpha(g) g(P). \tag{3.3}$$

Therefore α and α' are cohomologous to each other. Hence the class of α in $H^1_{\mathrm{cont}}(G, \mathrm{GL}_d(B))$ is independent of the choice of the basis of X and we denote it by $[X]$.

Conversely, given a 1-cocycle $\alpha \in Z^1_{\mathrm{cont}}(G, \mathrm{GL}_d(B))$, there is a unique semi-linear action of G on $X = B^d$ such that, for every $g \in G$,

$$g(e_j) = \sum_{i=1}^{d} a_{ij}(g) e_i, \tag{3.4}$$

and $[X]$ is the class of α. Hence, we have the following proposition:

Proposition 3.7. *Suppose d is a positive integer. The correspondence $X \mapsto [X]$ defines a bijection between the set of equivalence classes of free B-representations of G of rank d and $H^1_{\mathrm{cont}}(G, \mathrm{GL}_d(B))$. Moreover X is trivial if and only if $[X]$ is the distinguished point in $H^1_{\mathrm{cont}}(G, \mathrm{GL}_d(B))$.*

The following proposition is thus a direct consequence of Hilbert's Theorem 90:

Proposition 3.8. *If L is a Galois extension of K and if L is equipped with the discrete topology, then any L-representation of $\mathrm{Gal}(L/K)$ is trivial.*

3.1.2 Regular (F,G)-rings.

In this subsection, we let B be a topological ring, G be a topological group which acts continuously on B. Set $E = B^G$, and assume it is a field. Let F be a closed subfield of E.

If B is a domain, then the action of G extends to $C = \operatorname{Frac} B$ by

$$g\left(\frac{b_1}{b_2}\right) = \frac{g(b_1)}{g(b_2)}, \quad \text{for all } g \in G,\ b_1, b_2 \in B. \tag{3.5}$$

Definition 3.9. *We say that B is* (F,G)-regular *if the following conditions hold:*

(i) *B is a domain.*
(ii) $B^G = C^G = E \supseteq F$.
(iii) *For $b \in B$, $b \neq 0$, if for any $g \in G$, there exists $\lambda = \lambda(g) \in F$ such that $g(b) = \lambda b$, then b is invertible in B.*

Remark 3.10. This is always the case if B is a field.

Let $\mathbf{Rep}_F(G)$ denote the category of continuous F-representations of G. This is an abelian category with additional structures:

(a) Tensor product: if V_1 and V_2 are F-representations of G, we set $V_1 \otimes V_2 = V_1 \otimes_F V_2$, with the G-action given by $g(v_1 \otimes v_2) = g(v_1) \otimes g(v_2)$;
(b) Dual representation: if V is a F-representation of G, we set $V^* = \mathscr{L}(V, F) = \{\text{continuous linear maps } V \to F\}$, with the G-action given by $(gf)(v) = f(g^{-1}(v))$;
(c) Unit representation: this is F with the trivial action.

We have obvious natural isomorphisms

$$V_1 \otimes (V_2 \otimes V_3) \cong (V_1 \otimes V_2) \otimes V_3, \quad V_2 \otimes V_1 \cong V_1 \otimes V_2, \quad V \otimes F \cong F \otimes V \simeq V.$$

With these additional structures, $\mathbf{Rep}_F(G)$ is a *neutral Tannakian category over F* (ref. e.g. Deligne [Del90] in the Grothendieck Festschrift, but we are not going to use the precise definition of Tannakian categories).

Definition 3.11. *A category $\mathscr{C}'$ is called a* strictly full sub-category *of a category $\mathscr{C}$ if it is a full sub-category such that if X is an object of $\mathscr{C}$ isomorphic to an object of $\mathscr{C}'$, then X is also an object of $\mathscr{C}'$.*

Definition 3.12. *A* sub-Tannakian category *of $\mathbf{Rep}_F(G)$ is a strictly full sub-category $\mathscr{C}$, such that*

(i) *The unit representation F is an object of $\mathscr{C}$;*
(ii) *If V is an object of $\mathscr{C}$ and V' is a sub-representation of V, then V' and V/V' are all in $\mathscr{C}$;*
(iii) *If V is an object of $\mathscr{C}$, so is V^*;*
(iv) *If V_1, V_2 are both objects of $\mathscr{C}$, so is $V_1 \oplus V_2$;*
(v) *If V_1, V_2 are both objects of $\mathscr{C}$, so is $V_1 \otimes V_2$.*

Definition 3.13. *Let V be an F-representation of G. We say that V is B-*admissible *if $B \otimes_F V$ is a trivial B-representation of G.*

Let V be any F-representation of G, then $B \otimes_F V$, equipped with the G-action by $g(\lambda \otimes x) = g(\lambda) \otimes g(x)$, is a free B-representation of G. Let

$$\mathbf{D}_B(V) := (B \otimes_F V)^G, \tag{3.6}$$

we get a map

$$\begin{aligned} \alpha_V : B \otimes_E \mathbf{D}_B(V) &\longrightarrow B \otimes_F V \\ \lambda \otimes x \quad &\longmapsto \quad \lambda x \end{aligned} \tag{3.7}$$

where $\lambda \in B$ and $x \in \mathbf{D}_B(V)$. α_V is B-linear and commutes with the action of G, where G acts on $B \otimes_E \mathbf{D}_B(V)$ via $g(\lambda \otimes x) = g(\lambda) \otimes x$.

Theorem 3.14. *Assume that B is (F,G)-regular. Then*

(1) *For any F-representation V of G, the map α_V is injective and $\dim_E \mathbf{D}_B(V) \leq \dim_F V$. Consequently*

$$\begin{aligned} \dim_E \mathbf{D}_B(V) = \dim_F V &\Leftrightarrow \alpha_V \text{ is an isomorphism} \\ &\Leftrightarrow V \text{ is } B\text{-admissible.} \end{aligned} \tag{3.8}$$

(2) *Let $\mathbf{Rep}_F^B(G)$ be the full subcategory of $\mathbf{Rep}_F(G)$ consisting of these representations V which are B-admissible. Then $\mathbf{Rep}_F^B(G)$ is a sub-Tannakian category of $\mathbf{Rep}_F(G)$ and the restriction of $\mathbf{D}_B$, regarded as a functor from the category $\mathbf{Rep}_F(G)$ to the category of E-vector spaces, on $\mathbf{Rep}_F^B(G)$ is an exact and faithful tensor functor, i.e., it is exact and satisfies the following three properties:*

(i) *If V_1 and V_2 are admissible, so is their tensor product $V_1 \otimes V_2$, and there is a natural isomorphism*

$$\mathbf{D}_B(V_1) \otimes_E \mathbf{D}_B(V_2) \cong \mathbf{D}_B(V_1 \otimes V_2). \tag{3.9}$$

(ii) *If V is admissible, so is its dual V^*, and there is a natural isomorphism*

$$\mathbf{D}_B(V^*) \cong (\mathbf{D}_B(V))^*. \tag{3.10}$$

(iii) *The unit representation F is B-admissible $\mathbf{D}_B(F) \cong E$.*

Proof. (1) Let $C = \operatorname{Frac} B$. Since B is (F,G)-regular, $C^G = B^G = E$. By the following commutative diagram:

$$\begin{tikzcd}
B \otimes_E \mathbf{D}_B(V) \arrow[r, "\alpha_{V,B}"] \arrow[d, hook] & B \otimes_F V \arrow[dd, hook] \\
B \otimes_E \mathbf{D}_C(V) \arrow[d, hook] & \\
C \otimes_E \mathbf{D}_C(V) \arrow[r, "\alpha_{V,C}"] & C \otimes_F V,
\end{tikzcd}$$

the injectivity of $\alpha_{V,C}$ implies that of $\alpha_{V,B}$, so we may assume that $B = C$ is a field. Now the injectivity of α_V means that given $h \geq 1$, if $x_1, ..., x_h \in \mathbf{D}_B(V)$ are linearly independent over E, then they are linearly independent over B. We prove this by induction on h.

The case $h = 1$ is trivial. We may assume $h \geq 2$. Assume that $x_1, \cdots, x_h$ are linearly independent over E, but not over B. Then there exist $\lambda_1, \cdots, \lambda_h \in B$, not all zero, such that $\sum\limits_{i=1}^{h} \lambda_i x_i = 0$. By induction, the λ_i's are all different from 0. Multiplying them by $-1/\lambda_h$, we may assume $\lambda_h = -1$, then we get $x_h = \sum\limits_{i=1}^{h-1} \lambda_i x_i$. For any $g \in G$,

$$x_h = g(x_h) = \sum_{i=1}^{h-1} g(\lambda_i) x_i,$$

then

$$\sum_{i=1}^{h-1} (g(\lambda_i) - \lambda_i) x_i = 0.$$

By induction, $g(\lambda_i) = \lambda_i$, for $1 \leq i \leq h-1$, i.e., $\lambda_i \in B^G = E$, which is a contradiction. This finishes the proof that α_V is injective.

If α_V is an isomorphism, then

$$\dim_E \mathbf{D}_B(V) = \dim_F V = \operatorname{rank}_B B \otimes_F V.$$

We need to show that if $\dim_E \mathbf{D}_B(V) = \dim_F V$, then α_V is an isomorphism.

Suppose $\{v_1, \cdots, v_d\}$ is a basis of V over F, by abuse of notation, write $v_i = 1 \otimes v_i$, then $v_1, \cdots, v_d$ is a basis of $B \otimes_F V$ over B. Let $\{e_1, \cdots, e_d\}$

be a basis of $\mathbf{D}_B(V)$ over E. Then $e_j = \sum_{i=1}^{d} b_{ij}v_i$, for $(b_{ij}) \in M_d(B)$. Let $b = \det(b_{ij})$, the injectivity of α_V implies that $b \neq 0$.

We need to prove b is invertible in B. Denote by $\det V = \bigwedge_F^d V = Fv$, where $v = v_1 \wedge \cdots \wedge v_d$. Then $g(v) = \eta(g)v$ with $\eta : G \to F^\times$ a homomorphism. Similarly let $e = e_1 \wedge \cdots \wedge e_d \in \bigwedge_E^d \mathbf{D}_B(V)$, then $g(e) = e$ for $g \in G$. We have $e = bv$, and $e = g(e) = g(b)\eta(g)v$, so $g(b) = \eta(g)^{-1}b$ for all $g \in G$, hence b is invertible in B by the assumption that B is (F,G)-regular (condition (3)).

The second equivalence is easy. The condition that V is B-admissible, means that there exists a B-basis $\{x_1, \cdots, x_d\}$ of $B \otimes_F V$ with each $x_i \in \mathbf{D}_B(V)$. Since $\alpha_V(1 \otimes x_i) = x_i$, and α_V is always injective, this condition is equivalent to that α_V is an isomorphism.

(2) Let V be a B-admissible F-representation of G, V' be a sub-F-vector space stable under G, set $V'' = V/V'$, then we have an exact sequences

$$0 \to V' \to V \to V'' \to 0$$

and

$$0 \to B \otimes_F V' \to B \otimes_F V \to B \otimes_F V'' \to 0.$$

Then the sequence

$$0 \to \mathbf{D}_B(V') \to \mathbf{D}_B(V) \to \mathbf{D}_B(V'') \dashrightarrow 0 \tag{3.11}$$

is exact at $\mathbf{D}_B(V')$ and at $\mathbf{D}_B(V)$. Let $d = \dim_F V$, $d' = \dim_F V'$, $d'' = \dim_F V''$, by (1), we have

$$\dim_E \mathbf{D}_B(V) = d, \quad \dim_E \mathbf{D}_B(V') \leq d', \quad \dim_E \mathbf{D}_B(V'') \leq d'',$$

but $d = d' + d''$, so we have equalities everywhere, and (3.11) is also exact at $\mathbf{D}_B(V'')$. Thus the functor $\mathbf{D}_B$ restricted to $\mathbf{Rep}_F^B(G)$ is exact, and is also faithful since $\mathbf{D}_B(V) \neq 0$ if $V \neq 0$.

Now we prove the second part of the assertion (2). (iii) is trivial. For (i), we have a commutative diagram

$$\begin{tikzcd}
(B \otimes_F V_1) \otimes_B (B \otimes_F V_2) \arrow[r, equal, "\Sigma"] & B \otimes_F (V_1 \otimes_F V_2) \\
\mathbf{D}_B(V_1) \otimes_E \mathbf{D}_B(V_2) \arrow[u, hook] \arrow[r, dashed, "\sigma"] & \mathbf{D}_B(V_1 \otimes_F V_2) \arrow[u]
\end{tikzcd}$$

where the map σ is induced by Σ. From the diagram σ is clearly injective. On the other hand, since V_1 and V_2 are admissible, then

$$\dim_E \mathbf{D}_B(V_1) \otimes_E \mathbf{D}_B(V_2) = \dim_B(B \otimes_F (V_1 \otimes_F V_2)) \geq \dim_E \mathbf{D}_B(V_1 \otimes_F V_2),$$

hence σ is in fact an isomorphism.

At last for (ii), assume V is B-admissible, we need to prove that V^* is B-admissible and $\mathbf{D}_B(V^*) \simeq \mathbf{D}_B(V)^*$.

The case $\dim_F V = 1$ is easy, since in this case $V = Fv$, $\mathbf{D}_B(V) = E\cdot(b\otimes v)$ for some $b \in B$, and $V^* = Fv^*$, $\mathbf{D}_B(V^*) = E \cdot (b^{-1} \otimes v^*)$.

If $\dim_F V = d \geq 2$, we use the isomorphism

$$(\bigwedge\nolimits_F^{d-1} V) \otimes (\det V)^* \cong V^*.$$

Note that $\bigwedge_F^{d-1} V$ is admissible since it is a quotient of $\bigotimes_F^{d-1} V$, and $(\det V)^*$ is admissible since $\det V$ is admissible of dimension 1, so V^* must also be admissible.

Consider the B-linear map

$$\Xi : B \otimes_F V^* \to (B \otimes_F V)^*, \ b \otimes f \mapsto (b_2 \otimes v \mapsto bb_2 f(v)),$$

where the dual in the right hand side is B-dual. The map Ξ is an isomorphism commuting with the G-action. Suppose $f \in \mathbf{D}_B(V^*)$ and $t \in B \otimes_F V$, then for $g \in G$, $g \circ f(t) = g(f(g^{-1}(t))) = f(t)$. If moreover $t \in D_B(V)$, then $g(f(t)) = f(t)$ and hence $f(t) \in E$. Therefore we get an induced homomorphism $\tau : D_B(V^*) \to D_B(V)^*$, which is injective. Since both $D_B(V)$ and $D_B(V^*)$ have the same dimension as E-vector spaces, τ must be an isomorphism.

3.2 Mod p Galois representations of fields of characteristic $p > 0$

In this section, we assume that E is a field of characteristic $p > 0$. We fix a separable closure E^s of E and set $G = G_E = \mathrm{Gal}(E^s/E)$. Let $\sigma = (\lambda \mapsto \lambda^p)$ be the absolute Frobenius of E.

3.2.1 Étale φ-modules over E.

Definition 3.15. *A* φ-module *over E is an E-vector space M together with a map $\varphi : M \to M$ which is semi-linear with respect to the absolute Frobenius σ, i.e.,*

$$\varphi(x + y) = \varphi(x) + \varphi(y), \quad \text{for all } x, y \in M; \tag{3.12}$$
$$\varphi(\lambda x) = \sigma(\lambda)\varphi(x) = \lambda^p \varphi(x), \quad \text{for all } \lambda \in E, \ x \in M. \tag{3.13}$$

If M is an E-vector space, let $M_\varphi = E\,{}_\sigma\!\otimes_E M$, where E is viewed as an E-module by the Frobenius $\sigma : E \to E$, which means for $\lambda, \mu \in E$ and $x \in M$,

$$\lambda(\mu \otimes x) = \lambda\mu \otimes x, \qquad \lambda \otimes \mu x = \mu^p \lambda \otimes x. \tag{3.14}$$

Then M_φ is again an E-vector space, and if $\{e_1, \cdots, e_d, \cdots\}$ is a basis of M over E, then $\{1 \otimes e_1, \cdots, 1 \otimes e_d, \cdots\}$ is a basis of M_φ over E. Hence we have

$$\dim_E M_\varphi = \dim_E M.$$

Our main observation is

Lemma 3.16. *If M is any E-vector space, giving a semi-linear map $\varphi : M \to M$ is equivalent to giving a linear map*

$$\begin{aligned} \varPhi : \quad M_\varphi &\longrightarrow M \\ \lambda \otimes x &\longmapsto \lambda\varphi(x). \end{aligned} \tag{3.15}$$

If M is a φ-module of finite dimension d, suppose $\{e_1, \cdots, e_d\}$ is a basis of M over E, and assume

$$\varphi e_j = \sum_{i=1}^{d} a_{ij} e_i,$$

then $\varPhi(1 \otimes e_j) = \sum_{i=1}^{d} a_{ij} e_i$. As $\varPhi : M_\varphi \to M$ is an E-linear map between E-vector spaces with the same finite dimension, then we have

Proposition 3.17. *If M is a φ-module of finite dimension d, then*

$$\begin{aligned} \varPhi \text{ is an isomorphism} &\Longleftrightarrow \varPhi \text{ is injective} \Longleftrightarrow \varPhi \text{ is surjective} \\ &\Longleftrightarrow M = E \cdot \varphi(M) \Longleftrightarrow A = (a_{ij}) \in \mathrm{GL}_d(E). \end{aligned} \tag{3.16}$$

Definition 3.18. *A φ-module M over E is called* étale *if $\varPhi : M_\varphi \to M$ is an isomorphism and if $\dim_E M$ is finite.*

Let $\mathscr{M}_\varphi^{\text{ét}}(E)$ be the category of étale φ-modules over E with the morphisms being the E-linear maps which commute with φ.

Proposition 3.19. *The category $\mathscr{M}_\varphi^{\text{ét}}(E)$ is an abelian category.*

Proof. Let $E[\varphi]$ be the non-commutative (if $E \neq \mathbb{F}_p$) ring generated by E and an element φ with the relation $\varphi\lambda = \lambda^p\varphi$, for every $\lambda \in E$. The category of φ-modules over E is nothing but the category of left $E[\varphi]$-modules. This is an abelian category.

To prove the proposition, it is enough to check that, if $\eta : M_1 \to M_2$ is a morphism of étale φ-modules over E, the kernel M' and the cokernel M'' of η in the category of φ-modules over E are étale.

In fact, the horizontal lines of the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & M'_\varphi \arrow[r] \arrow[d, "\varPhi'"] & (M_1)_\varphi \arrow[r] \arrow[d, "\varPhi_1"] & (M_2)_\varphi \arrow[r] \arrow[d, "\varPhi_2"] & (M'')_\varphi \arrow[r] \arrow[d, "\varPhi''"] & 0 \\ 0 \arrow[r] & M' \arrow[r] & M_1 \arrow[r] & M_2 \arrow[r] & M'' \arrow[r] & 0 \end{tikzcd}$$

are exact. By definition, $\varPhi_1$ and $\varPhi_2$ are isomorphisms, so $\varPhi'$ is injective and $\varPhi''$ is surjective. By comparing the dimensions, both $\varPhi'$ and $\varPhi''$ are isomorphisms, hence $\operatorname{Ker}\eta$ and $\operatorname{Coker}\eta$ are étale.

The category $\mathscr{M}_\varphi^{\text{ét}}(E)$ possesses the following Tannakian structure:

(a) Tensor product. If M_1, M_2 are two étale φ-modules over E, let $M_1 \otimes M_2 = M_1 \otimes_E M_2$, viewed as a φ-module by assigning

$$\varphi(x_1 \otimes x_2) = \varphi(x_1) \otimes \varphi(x_2).$$

One can easily check that $M_1 \otimes M_2 \in \mathscr{M}_\varphi^{\text{ét}}(E)$.

(b) Unit: E is an étale φ-module and for every étale φ-module M,

$$M \otimes E = E \otimes M = M.$$

(c) Dual. If M is an étale φ-module, assume that $\Phi : M_\varphi \xrightarrow{\sim} M$ is the corresponding isomorphism to φ. Set $M^* = \mathscr{L}_E(M, E)$, We have

$${}^t\Phi : M^* \xrightarrow{\sim} (M_\varphi)^* \cong (M^*)_\varphi,$$

where the second isomorphism is the canonical isomorphism since E is a flat E-module. Then

$${}^t\Phi^{-1} : (M^*)_\varphi \xrightarrow{\sim} M^* \tag{3.17}$$

gives a φ-module structure on M^*. Moreover, if $\{e_1, \cdots, e_d\}$ is a basis of M, and $\{e_1^*, \cdots, e_d^*\}$ is the dual basis of M^*, then

$$\varphi(e_j) = \sum a_{ij} e_i, \quad \varphi(e_j^*) = \sum b_{ij} e_i^*$$

with $A = (a_{ij})$ and $B = (b_{ij})$ satisfying $B = {}^tA^{-1}$.

3.2.2 The functor M.

Recall that a *mod p representation* of G is a finite dimensional $\mathbb{F}_p$-vector space V together with a linear and continuous action of G. Denote by $\mathbf{Rep}_{\mathbb{F}_p}(G)$ the category of all mod p representations of G.

We know that G acts continuously on E^s equipped with the discrete topology and $\mathbb{F}_p \subset (E^s)^G = E$, hence E^s is $(\mathbb{F}_p, G)$-regular. Let V be any mod p representation of G. By Hilbert's Theorem 90, the E^s-representation $E^s \otimes_{\mathbb{F}_p} V$ is trivial, thus V is always E^s-admissible. Set

$$\mathbf{M}(V) = \mathbf{D}_{E^s}(V) = (E^s \otimes_{\mathbb{F}_p} V)^G, \tag{3.18}$$

then $\dim_E \mathbf{M}(V) = \dim_{\mathbb{F}_p} V$, and

$$\alpha_V : E^s \otimes_E \mathbf{M}(V) \longrightarrow E^s \otimes_{\mathbb{F}_p} V$$

is an isomorphism.

On E^s, we have the absolute Frobenius $\sigma(x) = x^p$, which commutes with the action of G:

$$\sigma(g(x)) = g(\sigma(x)), \quad \text{for all } g \in G,\ x \in E^s$$

We define the Frobenius φ on $E^s \otimes_{\mathbb{F}_p} V$ as follows:

$$\varphi(\lambda \otimes v) = \lambda^p \otimes v = \sigma(\lambda) \otimes v.$$

For all $x \in E^s \otimes_{\mathbb{F}_p} V$, we have

$$\varphi(g(x)) = g(\varphi(x)), \quad \text{for all } g \in G,$$

which implies that if x belongs to $\mathbf{M}(V)$, so does $\varphi(x)$. We still denote by φ the restriction of φ on $\mathbf{M}(V)$, then we get

$$\varphi : \mathbf{M}(V) \longrightarrow \mathbf{M}(V).$$

Proposition 3.20. *If V is a mod p representation of G of dimension d, then the map*

$$\alpha_V : E^s \otimes_E \mathbf{M}(V) \to E^s \otimes_{\mathbb{F}_p} V$$

is an isomorphism, $\mathbf{M}(V)$ is an étale φ-module over E and $\dim_E \mathbf{M}(V) = d$.

Proof. We have already known that

$$\alpha_V : E^s \otimes_E \mathbf{M}(V) \to E^s \otimes_{\mathbb{F}_p} V$$

is an isomorphism and this implies $\dim_E \mathbf{M}(V) = d$.

Suppose $\{v_1, \cdots, v_d\}$ is a basis of V over $\mathbb{F}_p$ and by abuse of notations, write $v_i = 1 \otimes v_i$. Suppose $\{e_1, \cdots, e_d\}$ is a basis of $\mathbf{M}(V)$ over E. Then

$$e_j = \sum_{i=1}^{d} b_{ij} v_i, \quad \text{for } B = (b_{ij}) \in \mathrm{GL}_d(E^s).$$

Hence

$$\varphi(e_j) = \sum_{i=1}^{d} b_{ij}^p v_i = \sum_{i=1}^{d} a_{ij} e_i.$$

Then $A = (a_{ij}) = B^{-1}\varphi(B)$, and

$$\det A = (\det B)^{-1} \det(\varphi(B)) = (\det B)^{p-1} \neq 0.$$

This implies that $\mathbf{M}(V)$ is étale.

From Proposition 3.20, we thus get an additive functor

$$\mathbf{M} : \mathbf{Rep}_{\mathbb{F}_p}(G) \to \mathscr{M}_{\varphi}^{\text{ét}}(E). \tag{3.19}$$

3.2.3 The quasi-inverse functor V.

We now define a functor

$$\mathbf{V} : \mathscr{M}_{\varphi}^{\text{ét}}(E) \longrightarrow \mathbf{Rep}_{\mathbb{F}_p}(G). \tag{3.20}$$

Let M be any étale φ-module over E. We view $E^s \otimes_E M$ as a φ-module via

$$\varphi(\lambda \otimes x) = \lambda^p \otimes \varphi(x)$$

and define a G-action on it by

$$g(\lambda \otimes x) = g(\lambda) \otimes x, \quad \text{for } g \in G.$$

One can check that this action commutes with φ. Set

$$\mathbf{V}(M) = \{y \in E^s \otimes_E M \mid \varphi(y) = y\} = (E^s \otimes_E M)_{\varphi=1}\,, \tag{3.21}$$

which is a sub $\mathbb{F}_p$-vector space stable under G.

Lemma 3.21. *The natural map*

$$\begin{array}{rcl} \alpha_M : E^s \otimes_{F_p} \mathbf{V}(M) & \longrightarrow & E^s \otimes_E M \\ \lambda \otimes v & \longmapsto & \lambda v \end{array} \tag{3.22}$$

is injective and therefore $\dim_{\mathbb{F}_p} \mathbf{V}(M) \leq \dim_E M$.

Proof. We need to prove that if $v_1, \cdots, v_h \in \mathbf{V}(M)$ are linearly independent over $\mathbb{F}_p$, then they are also linearly independent over E^s. We use induction on h.

The case $h = 1$ is trivial.

Assume that $h \geq 2$, and that there exist $\lambda_1, \cdots, \lambda_h \in E^s$, not all zero, such that $\sum_{i=1}^{h} \lambda_i v_i = 0$. We may assume $\lambda_h = -1$, then we have $v_h = \sum_{i=1}^{h-1} \lambda_i v_i$. Since $\varphi(v_i) = v_i$, we have

$$v_h = \sum_{i=1}^{h-1} \lambda_i^p v_i,$$

which implies $\lambda_i^p = \lambda_i$ by induction, therefore $\lambda_i \in \mathbb{F}_p$.

Theorem 3.22. *The functor*

$$\mathbf{M} : \mathbf{Rep}_{\mathbb{F}_p}(G) \longrightarrow \mathscr{M}_{\varphi}^{\text{ét}}(E)$$

is an equivalence of Tannakian categories *and*

$$\mathbf{V} : \mathscr{M}_{\varphi}^{\text{ét}}(E) \longrightarrow \mathbf{Rep}_{\mathbb{F}_p}(G)$$

is a quasi-inverse functor of $\mathbf{M}$.

Proof. Let V be any mod p representation of G, then

$$\alpha_V : E^s \otimes_E \mathbf{M}(V) \xrightarrow{\sim} E^s \otimes_{F_p} V$$

is an isomorphism of E^s-vector spaces, compatible with the Frobenius and with the action of G. We use α_V to identify these two spaces. Then

$$\mathbf{V}(\mathbf{M}(V)) = \{y \in E^s \otimes_{F_p} V \mid \varphi(y) = y\}.$$

Let $\{v_1, \cdots, v_d\}$ be a basis of V. If

$$y = \sum_{i=1}^{d} \lambda_i \otimes v_i = \sum_{i=1}^{d} \lambda_i v_i \in E^s \otimes V,$$

we get $\varphi(y) = \sum \lambda_i^p v_i$, therefore

$$\varphi(y) = y \Longleftrightarrow \lambda_i \in \mathbb{F}_p \Longleftrightarrow y \in V.$$

We thus have $\mathbf{V}(\mathbf{M}(V)) = V$, in particular $\mathbf{V}(M) \neq 0$ if $M \neq 0$. A formal consequence of this fact is that $\mathbf{M}$ is an exact and fully faithful functor, inducing an equivalence of categories between $\mathbf{Rep}_{\mathbb{F}_p}(G)$ and its essential image (i.e., the full subcategory of $\mathscr{M}_{\varphi}^{\text{ét}}(E)$ consisting of those M which are isomorphic to an $\mathbf{M}(V)$).

We now need to show that if M is an étale φ-module over E, then there exists V such that

$$M \cong \mathbf{M}(V).$$

We take $V = \mathbf{V}(M)$, and prove that $M \cong \mathbf{M}(\mathbf{V}(M))$.

Note that

$$\begin{aligned}\mathbf{V}(M) =& \{v \in E^s \otimes_E M \mid \varphi(v) = v\}\\ =& \{v \in \mathscr{L}_E(M^*, E^s) \mid \varphi v = v\varphi\}.\end{aligned}$$

Let $\{e_1^*, \cdots, e_d^*\}$ be a basis of M^*, and suppose $\varphi(e_j^*) = \sum b_{ij} e_i^*$, then giving v is equivalent to giving $x_i = v(e_i^*) \in E^s$, for $1 \leq i \leq d$. From

$$\varphi(v(e_j^*)) = v(\varphi(e_j^*)),$$

we have

$$x_j^p = v\Big(\sum_{i=1}^{d} b_{ij} e_i^*\Big) = \sum_{i=1}^{d} b_{ij} x_i.$$

Thus

$$\mathbf{V}(M) = \Big\{(x_1, \cdots, x_d) \in (E^s)^d \,\Big|\, x_j^p = \sum_{i=1}^{d} b_{ij} x_i, \forall j = 1, ..., d\Big\}.$$

Let $R = E[X_1, \cdots, X_d]/(X_j^p - \sum_{i=1}^{d} b_{ij} X_i)_{1 \leq j \leq d}$, we have

$$\mathbf{V}(M) = \mathrm{Hom}_{E-\text{algebra}}(R, E^s). \tag{3.23}$$

Lemma 3.23. *Let p be a prime number, E be a field of characteristic p, E^s be a separable closure of E. Let $B = (b_{ij}) \in \mathrm{GL}_d(E)$ and $b_1, \cdots, b_d \in E$. Let*

$$R = E[X_1, \cdots, X_d]/(X_j^p - \sum_{i=1}^{d} b_{ij}X_i - b_j)_{1 \leq j \leq d}.$$

Then the set $\mathrm{Hom}_{E-\mathrm{algebra}}(R, E^s)$ has exactly p^d elements.

Let us first finish the proof of the theorem. By the lemma, $\mathbf{V}(M)$ has p^d elements, which implies that $\dim_{\mathbb{F}_p} \mathbf{V}(M) = d$. As the natural map

$$\alpha_M : E^s \otimes_{\mathbb{F}_p} \mathbf{V}(M) \longrightarrow E^s \otimes_E M$$

is injective, this is an isomorphism, and one can check that

$$\mathbf{M}(\mathbf{V}(M)) \cong M.$$

Moreover this is a Tannakian isomorphism: we have proven the following isomorphisms

- $\mathbf{M}(V_1 \otimes V_2) = \mathbf{M}(V_1) \otimes \mathbf{M}(V_2)$,
- $\mathbf{M}(V^*) = \mathbf{M}(V)^*$,
- $\mathbf{M}(\mathbb{F}_p) = E$,

and one can easily check that these isomorphisms are compatible with Frobenius. Also we have the isomorphisms

- $\mathbf{V}(M_1 \otimes M_2) = \mathbf{V}(M_1) \otimes \mathbf{V}(M_2)$;
- $\mathbf{V}(M^*) = \mathbf{V}(M)^*$;
- $\mathbf{V}(E) = \mathbb{F}_p$,

and these isomorphisms are compatible with the action of G.

Proof of Lemma 3.23. Denote by x_i the image of X_i in R for every $i = 1, \cdots, d$. We proceed the proof in three steps.

(1) First we show that $\dim_E R = p^d$. It is enough to check that $\{x_1^{t_1} x_2^{t_2} \cdots t_d^{i_d}\}$ with $0 \leq t_i \leq p-1$ form a basis of R over E. For $m = 0, 1, \ldots, d$, set

$$R_m = E[X_1, \cdots, X_d]/(X_j^p - \sum_{i=1}^{d} b_{ij}X_i - b_j)_{1 \leq j \leq m}.$$

Then, for $m > 0$, R_m is the quotient of R_{m-1} by the ideal generated by the image of $X_m^p - \sum_{i=1}^{d} b_{im}X_i - b_m$. By induction on m, we see that R_m is a free $E[X_{m+1}, X_{m+2}, \ldots, X_d]$-module with the images of $\{X_1^{t_1} X_2^{t_2} \ldots X_m^{t_m}\}$ with $0 \leq t_i \leq p-1$ as a basis.

(2) Then we prove that R is an étale E-algebra. This is equivalent to $\Omega^1_{R/E} = 0$. But $\Omega^1_{R/E}$ is generated by $dx_1, \cdots, dx_d$. From $x_j^p = \sum_{i=1}^{d} b_{ij}x_i + b_j$, we have

$$0 = px_j^{p-1}dx_j = \sum_{i=1}^{d} b_{ij}dx_j,$$

hence $dx_j = 0$, since (b_{ij}) is invertible in $\mathrm{GL}_d(E)$.

(3) As R is étale over E, it has the form $E_1 \times \cdots \times E_r$ (see, e.g. [Mil80], [FK88] or Illusie's course note at Tsinghua University) where the E_k's are finite separable extensions of E. Set $n_k = [E_k : E]$, then $p^d = \dim_E R = \sum_{k=1}^{r} n_k$. On the other hand, we have

$$\mathrm{Hom}_{E-\mathrm{algebra}}(R, E^s) = \coprod_k \mathrm{Hom}_{E-\mathrm{algebra}}(E_k, E^s),$$

and for any k, there are exactly n_k E-embeddings of E_k into E^s. Therefore the set $\mathrm{Hom}_{E-\mathrm{algebra}}(E, E^s)$ has p^d elements.

Remark 3.24. Suppose $d \geq 1$, $A \in \mathrm{GL}_d(E)$, we associate A with an E-vector space $M_A = E^d$, and equip it with a semi-linear map $\varphi : M_A \to M_A$ defined by

$$\varphi(\lambda e_j) = \lambda^p \sum_{i=1}^{d} a_{ij}e_i$$

where $\{e_1, \cdots, e_d\}$ is the canonical basis of M_A. Then for any $A \in \mathrm{GL}_d(E)$, we obtain a mod p representation $\mathbf{V}(M_A)$ of G of dimension d.

On the other hand, if V is any mod p representation of G of dimension d, then there exists $A \in \mathrm{GL}_d(E)$ such that $V \cong \mathbf{V}(M_A)$. This is because $\mathbf{M}(V)$ is an étale φ-module, then there is an $A \in \mathrm{GL}_d(E)$ associated with $\mathbf{M}(V)$, and $\mathbf{M}(V) \cong M_A$. Thus $V \cong \mathbf{V}(M_A)$.

Moreover, if $A, B \in \mathrm{GL}_d(E)$, then

$$\mathbf{V}(M_A) \cong \mathbf{V}(M_B) \Leftrightarrow \text{there exists } P \in \mathrm{GL}_d(E), \text{ such that } B = P^{-1}A\varphi(P).$$

Hence, if we define an equivalence relation on $\mathrm{GL}_d(E)$ by

$$A \sim B \Leftrightarrow \text{there exists } P \in \mathrm{GL}_d(E), \text{ such that } B = P^{-1}A\varphi(P),$$

then we get a bijection between the set of equivalences classes on $\mathrm{GL}_d(E)$ and the set of isomorphism classes of mod p representations of G of dimension d.

3.3 p-adic Galois representations of fields of characteristic $p > 0$

As in the previous section, let E be a field of characteristic $p > 0$, E^s a fixed separable closure of E and $G = \mathrm{Gal}(E^s/E)$. Let $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ (resp. $\mathbf{Rep}_{\mathbb{Z}_p}(G)$) be the category of p-adic representations (resp. of $\mathbb{Z}_p$-representations) of G.

3.3.1 Étale φ-modules over $\mathcal{E}$.

From §1.2.4, we let $\mathcal{O}_{\mathcal{E}}$ be the Cohen ring $\mathcal{C}(E)$ of E and $\mathcal{E}$ be the field of fractions of $\mathcal{O}_{\mathcal{E}}$. Then

$$\mathcal{O}_{\mathcal{E}} = \varprojlim_{n\in\mathbb{N}} \mathcal{O}_{\mathcal{E}}/p^n\mathcal{O}_{\mathcal{E}}$$

and $\mathcal{O}_{\mathcal{E}}/p\mathcal{O}_{\mathcal{E}} = E$, $\mathcal{E} = \mathcal{O}_{\mathcal{E}}[\frac{1}{p}]$.

The field $\mathcal{E}$ is of characteristic 0, with a complete discrete valuation, whose residue field is E and whose maximal ideal is generated by p. Moreover, if $\mathcal{E}'$ is another field with the same property, there is a continuous local homomorphism $\iota : \mathcal{E} \to \mathcal{E}'$ of valuation fields inducing the identity on E and ι is always an isomorphism. If E is perfect, ι is unique and $\mathcal{O}_{\mathcal{E}}$ may be identified with the ring $W(E)$ of Witt vectors with coefficients in E. In general, $\mathcal{O}_{\mathcal{E}}$ may be identified with a subring of $W(E)$.

We can always provide $\mathcal{E}$ with a Frobenius φ which is a continuous endomorphism sending $\mathcal{O}_{\mathcal{E}}$ into itself and inducing the absolute Frobenius $x \mapsto x^p$ on E. Again φ is unique whenever E is perfect.

For the rest of this section, we fix a choice of $\mathcal{E}$ and φ.

Definition 3.25. (i) *A* φ-module *over $\mathcal{O}_{\mathcal{E}}$ is an $\mathcal{O}_{\mathcal{E}}$-module M equipped with a semi-linear map $\varphi : M \to M$, that is:*

$$\varphi(x + y) = \varphi(x) + \varphi(y)$$

$$\varphi(\lambda x) = \varphi(\lambda)\varphi(x)$$

for $x, y \in M$, $\lambda \in \mathcal{O}_{\mathcal{E}}$.

(ii) *A φ-module over $\mathcal{E}$ is an $\mathcal{E}$-vector space D equipped with a semi-linear map $\varphi : D \to D$.*

Remark 3.26. A φ-module over $\mathcal{O}_{\mathcal{E}}$ killed by p is just a φ-module over E.

Set

$$M_\varphi = \mathcal{O}_{\mathcal{E}}\ {}_\varphi\!\otimes_{\mathcal{O}_{\mathcal{E}}} M,$$

which means for $\lambda, \mu \in \mathcal{O}_{\mathcal{E}}$, $m \in M$, the module structure on M_φ is given by

$$\lambda \otimes \mu m = \lambda\varphi(\mu) \otimes m, \quad \lambda(\mu \otimes m) = \lambda\mu \otimes m. \tag{3.24}$$

As in the case of φ-modules, giving a semi-linear map $\varphi : M \to M$ is equivalent to giving an $\mathcal{O}_{\mathcal{E}}$-linear map $\Phi : M_\varphi \to M$. Similarly if we set $D_\varphi = \mathcal{E}\ {}_\varphi\!\otimes_{\mathcal{E}} D$, then a semi-linear map $\varphi : D \to D$ is equivalent to a linear map $\Phi : D_\varphi \to D$.

Definition 3.27. (i) *A φ-module over $\mathcal{O}_{\mathcal{E}}$ is* étale *if M is an $\mathcal{O}_{\mathcal{E}}$-module of finite type and $\Phi : M_\varphi \to M$ is an isomorphism.*

(ii) *A φ-module D over $\mathcal{E}$ is étale if $\dim_{\mathcal{E}} D < \infty$ and if there exists an $\mathcal{O}_{\mathcal{E}}$-lattice M of D which is stable under φ, such that M is an étale φ-module over $\mathcal{O}_{\mathcal{E}}$.*

Remark 3.28. If D is an étale φ-module over $\mathcal{E}$ and M the associated étale lattice. If $\{e_1, \cdots, e_d\}$ is a basis of M over $\mathcal{O}_{\mathcal{E}}$, then it is also a basis of D over $\mathcal{E}$, and

$$\varphi e_j = \sum_{i=1}^{d} a_{ij} e_i, \quad (a_{ij}) \in \mathrm{GL}_d(\mathcal{O}_{\mathcal{E}}).$$

It is easy to check that

Proposition 3.29. *If M is an $\mathcal{O}_{\mathcal{E}}$-module of finite type with an action of φ, then M is étale if and only if M/pM is étale as an E-module.*

By Propositions 3.19 and 3.29, then

Proposition 3.30. *The category $\mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{O}_{\mathcal{E}})$ (resp. $\mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{E})$) of étale φ-modules over $\mathcal{O}_{\mathcal{E}}$ (resp. $\mathcal{E}$) is abelian.*

We want to construct equivalences of categories:

$$\mathbf{D} : \mathbf{Rep}_{\mathbb{Q}_p}(G) \to \mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{E})$$

and

$$\mathbf{M} : \mathbf{Rep}_{\mathbb{Z}_p}(G) \to \mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{O}_{\mathcal{E}}).$$

3.3.2 The field $\widehat{\mathcal{E}^{\mathrm{ur}}}$.

Let $\mathcal{F}$ be a finite extension of $\mathcal{E}$, $\mathcal{O}_{\mathcal{F}}$ be the ring of integers of $\mathcal{F}$. We say $\mathcal{F}/\mathcal{E}$ is *unramified* if

(a) p is a generator of the maximal ideal of $\mathcal{O}_{\mathcal{F}}$;
(b) $F = \mathcal{O}_{\mathcal{F}}/p$ is a separable extension of E.

For any homomorphism $f : E \to F$ of fields of characteristic p, by Theorem 1.51, the functoriality of Cohen rings tells us that there is a local homomorphism (unique up to isomorphism) $\mathcal{C}(E) \to \mathcal{C}(F)$ which induces f on the residue fields.

For any finite separable extension F of E, the inclusion $E \hookrightarrow F$ induces a local homomorphism $\mathcal{C}(E) \to \mathcal{C}(F)$, and through this homomorphism we identify $\mathcal{C}(E)$ with a subring of $\mathcal{C}(F)$. Then there is a *unique* unramified extension $\mathcal{F} = \operatorname{Frac} \mathcal{C}(F)$ of $\mathcal{E}$ whose residue field is F (here *unique* means that if $\mathcal{F}$, $\mathcal{F}'$ are two such extensions, then there exists a unique isomorphism $\mathcal{F} \to \mathcal{F}'$ which induces the identity map on $\mathcal{E}$ and on F), and moreover there exists a unique endomorphism $\varphi' : \mathcal{F} \to \mathcal{F}$ such that φ' maps $\mathcal{C}(F)$ to itself, $\varphi'|_{\mathcal{E}} = \varphi$ and induces the absolute Frobenius map $\lambda \mapsto \lambda^p$ on F. We write $\mathcal{F} = \mathcal{E}_F$ and still denote φ' as φ.

Again by Theorem 1.51, if F and F' are two separable extensions of E, then a morphism

$$f : F \to F', f|_E = \mathrm{Id} \text{ induces uniquely } f : \mathcal{E}_F \to \mathcal{E}_{F'}, f|_{\mathcal{E}} = \mathrm{Id}$$

and f commutes with the Frobenius map φ. In particular, if F/E is Galois, then $\mathcal{E}_F/\mathcal{E}$ is also Galois with Galois group

$$\mathrm{Gal}(\mathcal{E}_F/\mathcal{E}) = \mathrm{Gal}(F/E)$$

and the action of $\mathrm{Gal}(F/E)$ commutes with φ.

Let E^s be a separable closure of E, then

$$E^s = \bigcup_{F \in S} F$$

where S denotes the set of finite extensions of E contained in E^s. If $F, F' \in S$ and $F \subset F'$, then $\mathcal{E}_F \subset \mathcal{E}_{F'}$, we set

$$\mathcal{E}^{\mathrm{ur}} := \varinjlim_{F \in S} \mathcal{E}_F. \tag{3.25}$$

Then $\mathcal{E}^{\mathrm{ur}}/\mathcal{E}$ is a Galois extension with $\mathrm{Gal}(\mathcal{E}^{\mathrm{ur}}/\mathcal{E}) = G$. Let $\widehat{\mathcal{E}^{\mathrm{ur}}}$ be the p-adic completion of $\mathcal{E}^{\mathrm{ur}}$, and $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$ be its ring of integers. Then $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$ is a local ring, E^s is its residue field and

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} = \varprojlim \mathcal{O}_{\mathcal{E}^{\mathrm{ur}}}/p^n\mathcal{O}_{\mathcal{E}^{\mathrm{ur}}}. \tag{3.26}$$

We have the endomorphism φ on $\mathcal{E}^{\mathrm{ur}}$ such that $\varphi(\mathcal{O}_{\mathcal{E}^{\mathrm{ur}}}) \subset \mathcal{O}_{\mathcal{E}^{\mathrm{ur}}}$. The action of φ extends by continuity to an action on $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$ and $\widehat{\mathcal{E}^{\mathrm{ur}}}$. Similarly we have the action of G on $\mathcal{E}^{\mathrm{ur}}$, $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$ and $\widehat{\mathcal{E}^{\mathrm{ur}}}$. Moreover the action of φ commutes with the action of G. We have the following important facts:

Proposition 3.31. (1) $(\widehat{\mathcal{E}^{\mathrm{ur}}})^G = \mathcal{E}$, $(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}})^G = \mathcal{O}_{\mathcal{E}}$.

(2) $(\widehat{\mathcal{E}^{\mathrm{ur}}})_{\varphi=1} = \mathbb{Q}_p$, $(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}})_{\varphi=1} = \mathbb{Z}_p$.

Proof. (1) follows by the construction above, or is a consequence of Ax-Sen-Tate's Lemma in next chapter.

For (2), we can regard all the rings above as subrings of $W(E^s)$. such that the inclusion $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \hookrightarrow W(E^s)$ is G- and φ-compatible. Since $W(E^s)_{\varphi=1} = \mathbb{Z}_p$, (2) follows immediately.

3.3.3 $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$- and $\mathbb{Z}_p$-representations.

Proposition 3.32. *For any $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$-representation X of G, the natural map*

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} X^G \to X$$

is an isomorphism.

Proof. We prove the isomorphism in two steps.

(1) Assume there exists $n \geq 1$ such that X is killed by p^n. We prove the proposition in this case by induction on n.

For $n = 1$, X is an E^s-representation of G and this has been proved in Proposition 3.8.

Assume $n \geq 2$. Let X' be the kernel of the multiplication by p on X and $X'' = X/X'$. We get a short exact sequence

$$0 \to X' \to X \to X'' \to 0$$

where X' is killed by p and X'' is killed by p^{n-1}. Also we have a long exact sequence

$$0 \to X'^G \to X^G \to X''^G \to H^1_{\mathrm{cont}}(G, X').$$

Since X' is killed by p, it is just an E^s-representation of G, hence it is trivial (cf. Proposition 3.8), i.e. $X' \cong (E^s)^d$ with the natural action of G. So

$$H^1_{\mathrm{cont}}(G, X') = H^1(G, X') \cong (H^1(G, E^s))^d = 0.$$

Then we have the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} X'^G & \longrightarrow & \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} X^G & \longrightarrow & \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} X''^G & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & X' & \longrightarrow & X & \longrightarrow & X'' & \longrightarrow & 0.
\end{array}$$

By induction, the middle map is an isomorphism.

(2) Since $X = \varprojlim_{n \in \mathbb{N}} X/p^n$, the general case follows by passing to the limits.

Let T be a $\mathbb{Z}_p$-representation of G, then $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T$ is a φ-module over $\mathcal{O}_{\mathcal{E}}$, with φ- and G-action by

$$\varphi(\lambda \otimes t) = \varphi(\lambda) \otimes t, \quad g(\lambda \otimes t) = g(\lambda) \otimes g(t)$$

for any $g \in G$, $\lambda \in \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$ and $t \in T$. Let

$$\mathbf{M}(T) = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T)^G, \tag{3.27}$$

then by Proposition 3.32,

$$\alpha_T : \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} \mathbf{M}(T) \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T \tag{3.28}$$

is an isomorphism, which implies that $\mathbf{M}(T)$ is an $\mathcal{O}_{\mathcal{E}}$-module of finite type, and moreover $\mathbf{M}(T)$ is étale. Indeed, from the exact sequence $0 \to pT \to T \to T/pT \to 0$, one gets the isomorphism $\mathbf{M}(T)/p\mathbf{M}(T) \xrightarrow{\sim} \mathbf{M}(T/pT)$ as $H^1(G, \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T) = 0$ by Proposition 3.32. Thus $\mathbf{M}(T)$ is étale if and only if $\mathbf{M}(T/pT)$ is étale as a φ-module over E, which was proven in Proposition 3.20.

Let M be an étale φ-module over $\mathcal{O}_{\mathcal{E}}$, and let φ and G act on $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M$ through $g(\lambda \otimes x) = g(\lambda) \otimes x$ and $\varphi(\lambda \otimes x) = \varphi(\lambda) \otimes \varphi(x)$ for any $g \in G$, $\lambda \in \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$ and $x \in M$. Let

$$\mathbf{T}(M) = \{y \in \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M \mid \varphi(y) = y\} = \big(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M\big)_{\varphi=1}. \tag{3.29}$$

Proposition 3.33. *For any étale φ-module M over $\mathcal{O}_{\mathcal{E}}$, the natural map*

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} \mathbf{T}(M) \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M$$

is an isomorphism.

Proof. (1) We first prove the case when M is killed by p^n, for a fixed $n \geq 1$ by induction on n. For $n = 1$, this is the result for étale φ-modules over E. Assume $n \geq 2$. Consider the exact sequence:

$$0 \to M' \to M \to M'' \to 0,$$

where M' is the kernel of the multiplication by p in M. Then we have an exact sequence

$$0 \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M' \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M'' \to 0,$$

Let $X' = \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M'$, $X = \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M$, $X'' = \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M'$, then $X'_{\varphi=1} = \mathbf{T}(M')$, $X_{\varphi=1} = \mathbf{T}(M)$, $X''_{\varphi=1} = \mathbf{T}(M'')$. If the sequence

$$0 \to X'_{\varphi=1} \to X_{\varphi=1} \to X''_{\varphi=1} \to 0$$

is exact, then we can apply the same proof as the one for the previous proposition. So consider the exact sequence:

$$0 \to X'_{\varphi=1} \to X_{\varphi=1} \to X''_{\varphi=1} \xrightarrow{\delta} X'/(\varphi-1)X',$$

where if $x \in X_{\varphi=1}$, y is the image of x in $X''_{\varphi=1}$, then $\delta(y)$ is the image of $(\varphi-1)(x)$. It is enough to check that $X'/(\varphi-1)X' = 0$. As M' is killed by p, $X' = E^s \otimes_E M' \xrightarrow{\sim} (E^s)^d$, as an E^s-vector space with a Frobenius. Then $X'/(\varphi-1)X' \xrightarrow{\sim} (E^s/(\varphi-1)E^s)^d$. For any $b \in E^s$, there exist $a \in E^s$, such that a is a root of the polynomial $X^p - X - b$, so $b = a^p - a = (\varphi-1)a \in (\varphi-1)E^s$.

(2) The general case follows by passing to the limits.

The following result is a straightforward consequence of the two previous results and extends the analogous result in Theorem 3.22 for mod-p representations.

Theorem 3.34. *The functor*

$$\mathbf{M} : \mathbf{Rep}_{\mathbb{Z}_p}(G) \to \mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{O}_{\mathcal{E}}), \quad T \mapsto \mathbf{M}(T)$$

is an equivalence of categories and

$$\mathbf{T} : \mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{O}_{\mathcal{E}}) \to \mathbf{Rep}_{\mathbb{Z}_p}(G), \quad M \mapsto \mathbf{T}(M)$$

is a quasi-inverse functor of $\mathbf{M}$.

Proof. Identify $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M(T)$ with $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T$ through (3.28), then

$$\begin{aligned}\mathbf{T}(\mathbf{M}(T)) =&(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} \mathbf{M}(T))_{\varphi=1} = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T)_{\varphi=1}\\ =&(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}})_{\varphi=1} \otimes_{\mathbb{Z}_p} T = T,\end{aligned}$$

and

$$\begin{aligned}\mathbf{M}(\mathbf{T}(M)) =&(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} \mathbf{T}(M))^G \cong (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M)^G\\ =&\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}^G \otimes_{\mathcal{O}_{\mathcal{E}}} M = M.\end{aligned}$$

The theorem is proved.

3.3.4 p-adic representations.

If V is a p-adic representation of G, D is an étale φ-module over $\mathcal{E}$, let

$$\mathbf{D}(V) = (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V)^G,$$

$$\mathbf{V}(D) = (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} D)_{\varphi=1},$$

Theorem 3.35. (1) *For any p-adic representation V of G, $\mathbf{D}(V)$ is an étale φ-module over $\mathcal{E}$, and the natural map:*

$$\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} \mathbf{D}(V) \to \widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V$$

is an isomorphism.

(2) *For any étale φ-module D over $\mathcal{E}$, $\mathbf{V}(D)$ is a p-adic representation of G and the natural map*

$$\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} \mathbf{V}(D) \to \widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} D$$

is an isomorphism.

(3) *The functor*

$$\mathbf{D} : \mathbf{Rep}_{\mathbb{Q}_p}(G) \to \mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{E})$$

is an equivalence of categories, and

$$\mathbf{V} : \mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{E}) \to \mathbf{Rep}_{\mathbb{Q}_p}(G)$$

is a quasi-inverse functor of $\mathbf{D}$.

Proof. The proof is a formal consequence of what we did in §3.3.3 and of the following two facts:

(i) For any p-adic representation V of G, there exists a $\mathbb{Z}_p$-lattice T stable under G, $V = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$. Thus

$$\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T)[1/p], \quad \mathbf{D}(V) = \mathbf{M}(T)[1/p] = \mathcal{E} \otimes_{\mathcal{O}_{\mathcal{E}}} \mathbf{M}(T).$$

(ii) For any étale φ-module D over $\mathcal{E}$, there exists an $\mathcal{O}_{\mathcal{E}}$-lattice M stable under φ, which is an étale φ-module over $\mathcal{O}_{\mathcal{E}}$, $D=\mathcal{E}\otimes_{\mathcal{O}_{\mathcal{E}}} M$. Thus

$$\widehat{\mathcal{E}^{\mathrm{ur}}}\otimes_{\mathcal{E}} D=(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}\otimes_{\mathcal{O}_{\mathcal{E}}} M)[1/p],\quad \mathbf{V}(D)=\mathbf{T}(M)[1/p]=\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\mathbf{T}(M).$$

Remark 3.36. The category $\mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{E})$ has a natural structure of a Tannakian category, i.e. one may define tensor products, dual objects and the unit object satisfying suitable properties. For instance, if D_1, D_2 are étale φ-modules over $\mathcal{E}$, their tensor product $D_1\otimes D_2$ is $D_1\otimes_{\mathcal{E}} D_2$ with action of φ: $\varphi(x_1\otimes x_2)=\varphi(x_1)\otimes\varphi(x_2)$. Then the functor $\mathbf{D}$ is a tensor functor, i.e. we have natural isomorphisms

$$\mathbf{D}(V_1)\otimes\mathbf{D}(V_2)\to\mathbf{D}(V_1\otimes V_2) \text{ and } \mathbf{D}(V^*)\to\mathbf{D}(V)^*.$$

Similarly, we have a notion of tensor product in the category $\mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{O}_{\mathcal{E}})$, two notions of duality (one for free $\mathcal{O}_{\mathcal{E}}$-modules, the other for p-torsion modules) and similar natural isomorphisms.

3.3.5 Down to earth meaning of the equivalence of categories.

For any $d\geq 1$, $A\in \mathrm{GL}_d(\mathcal{O}_{\mathcal{E}})$, let $M_A=\mathcal{O}_{\mathcal{E}}^d$ as an $\mathcal{O}_{\mathcal{E}}$-module, let $\{e_1,\cdots,e_d\}$ be the canonical basis of M_A. Set $\varphi(e_j)=\sum\limits_{i=1}^{d}a_{ij}e_i$. Then M_A is an étale φ-module over $\mathcal{O}_{\mathcal{E}}$ and $T_A=\mathbf{T}(M_A)$ is a $\mathbb{Z}_p$-representation of G. Furthermore, $V_A=\mathbb{Q}_p\otimes_{\mathbb{Z}_p} T_A=\mathbf{V}(D_A)$ is a p-adic representation of G with $D_A=\mathcal{E}^d$ as an $\mathcal{E}$-vector space with the same φ.

On the other hand, for any p-adic representation V of G of dimension d, there exists $A\in\mathrm{GL}_d(\mathcal{O}_{\mathcal{E}})$, such that $V\cong V_A$. Given $A,B\in\mathrm{GL}_d(\mathcal{O}_{\mathcal{E}})$, T_A is isomorphic to T_B if and only if there exists $P\in\mathrm{GL}_d(\mathcal{O}_{\mathcal{E}})$, such that $B=P^{-1}A\varphi(P)$. V_A is isomorphic to V_B if and only if there exists $P\in\mathrm{GL}_d(\mathcal{E})$ such that $B=P^{-1}A\varphi(P)$.

Hence, if we define the equivalence relation on $GL_d(\mathcal{O}_{\mathcal{E}})$ by

$$A\sim B\Leftrightarrow \text{there exists } P\in\mathrm{GL}_d(\mathcal{E}),\ \text{such that } B=P^{-1}A\varphi(P),$$

we get a bijection between the set of equivalence classes and the set of isomorphism classes of p-adic representations of G of dimension d.

Remark 3.37. If A is in $\mathrm{GL}_d(\mathcal{O}_{\mathcal{E}})$ and $P\in\mathrm{GL}_d(\mathcal{O}_{\mathcal{E}})$, then $P^{-1}A\varphi(P)\in\mathrm{GL}_d(\mathcal{O}_{\mathcal{E}})$. But if $P\in\mathrm{GL}_d(\mathcal{E})$, then $P^{-1}A\varphi(P)$ may or may not be in $\mathrm{GL}_d(\mathcal{O}_{\mathcal{E}})$.

4

C-representations and Methods of Sen

4.1 The field C and its invariant subfields

In this section, let K be a complete nonarchimedean field, K^s be a separable closure of K, $\overline{K}$ be an algebraic closure of K containing K^s. Let $C = \widehat{K^s}$, the completion of K^s.

4.1.1 C is algebraically closed.

Lemma 4.1 (Krasner's Lemma). *Let F be a complete nonarchimedean field, and E be a closed subfield of F. Suppose $\alpha, \beta \in F$ and α separable over E, such that $|\beta - \alpha| < |\alpha' - \alpha|$ for all conjugates α' of α over E distinct from α, then $\alpha \in E(\beta)$.*

Proof. Let $E' = E(\beta)$, $\gamma = \beta - \alpha$. Then $E'(\gamma) = E'(\alpha)$, and $E'(\gamma)/E'$ is separable. We want to prove that $E'(\gamma) = E'$. It suffices to prove that there is no conjugate γ' of γ over E' distinct from γ. Let $\gamma' = \beta - \alpha'$ be such a conjugate, then $|\gamma'| = |\gamma|$. It follows that $|\gamma' - \gamma| \leq |\gamma| = |\beta - \alpha|$. On the other hand, $|\gamma' - \gamma| = |\alpha' - \alpha| > |\beta - \alpha|$ which leads to a contradiction.

Theorem 4.2. *The field $C = \widehat{K^s}$, the completion of K^s, is an algebraically closed field, and hence $C = \widehat{K^s} = \widehat{\overline{K}}$.*

Proof. It suffices to show

(i) If $\operatorname{char} K = p$, then for any $a \in C$, there exists $\alpha \in C$, such that $\alpha^p = a$.
(ii) C is separably closed.

Proof of (i): Choose $\pi \in \mathfrak{m}_K$, $\pi \neq 0$. Choose $v = v_\pi$, i.e., $v(\pi) = 1$. Then

$$\mathcal{O}_{K^s} = \{a \in K^s \mid v(a) \geq 0\}, \quad \mathcal{O}_C = \varprojlim \mathcal{O}_{K^s}/\pi^n \mathcal{O}_{K^s}$$

and $C = \mathcal{O}_C[1/\pi]$. Thus $\pi^{mp} a \in \mathcal{O}_C$ for $m \gg 0$, and we may assume $a \in \mathcal{O}_C$. Choose a sequence $(a_n)_{n\in\mathbb{N}}$ of elements of $\mathcal{O}_{K^s}$, such that $a \equiv a_n \bmod \pi^n$. Let

$$P_n(X) = X^p - \pi^n X - a_n \in K^s[X],$$

then $P_n(X)$ is separable since $P_n'(X) = -\pi^n \neq 0$. Let α_n be a root of P_n in K^s, then $\alpha_n \in \mathcal{O}_{K^s}$ and

$$\alpha_{n+1}^p - \alpha_n^p = \pi^{n+1}\alpha_{n+1} - \pi^n \alpha_n + a_{n+1} - a_n.$$

Therefore $v(\alpha_{n+1}^p - \alpha_n^p) \geq n$ and $v(\alpha_{n+1} - \alpha_n) \geq n/p$ since $(\alpha_{n+1} - \alpha_n)^p = \alpha_{n+1}^p - \alpha_n^p$. As a consequence $(\alpha_n)_{n\in\mathbb{N}}$ converges in $\mathcal{O}_C$. Call α the limit of (α_n), then $\alpha^p = \lim\limits_{n\to+\infty} \alpha_n^p = a$ since $v(\alpha_n^p - a) = v(\pi^n\alpha_n + a_n - a) \geq n$.

Proof of (ii): Let

$$P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_{d-1}X^{d-1} + X^d$$

be an arbitrary separable polynomial in $C[X]$. We need to prove $P(X)$ has a root in C. We may assume $a_i \in \mathcal{O}_C$. Let C' be the splitting field of P over C, let $r = \max v(\alpha_i - \alpha_j)$, where α_i and α_j are distinct roots of P in C'. Choose $b_i \in K^s$ such that $v(b_i - a_i) > rd$, and let

$$P_1 = b_0 + b_1 X + b_2 X^2 + \cdots + b_{d-1}X^{d-1} + X^d \in K^s[X].$$

We know, because of part (i), that C contains $\overline{K}$, hence there exists $\beta \in C$, such that $P_1(\beta) = 0$. Choose $\alpha \in C'$, a root of P, such that $|\beta - \alpha'| \geq |\beta - \alpha|$ for any root $\alpha' \in C'$ of P. Since $P(\beta) = P(\beta) - P_1(\beta)$, and $v(\beta) \geq 0$, we have $v(P(\beta)) > rd$. On the other hand,

$$P(\beta) = \prod_{i=1}^{d} (\beta - \alpha_i),$$

thus

$$v(P(\beta)) = \sum_{i=1}^{d} v(\beta - \alpha_i) > rd.$$

It follows that $v(\beta - \alpha) > r$. By Krasner's Lemma, we get $\alpha \in C(\beta) = C$.

4.1.2 Ax-Sen's Lemma.

Let E be an algebraic extension of K. For any element α contained in some separable extension of E, set

$$\Delta_E(\alpha) := \min\{v(\alpha' - \alpha)\}, \tag{4.1}$$

where α' runs through conjugates of α over E. Then

$$\Delta_E(\alpha) = +\infty \text{ if and only if } \alpha \in E. \tag{4.2}$$

Ax-Sen's Lemma means that if all the conjugates α' are close to α, then α is close to an element of E.

Proposition 4.3 (Ax-Sen's Lemma, Characteristic 0 case). *Let K, E, α be as above, Assume* $\operatorname{char} K = 0$, *then there exists $a \in E$ such that*

$$v(\alpha - a) > \Delta_E(\alpha) - \frac{p}{(p-1)^2} v(p). \tag{4.3}$$

Remark 4.4. (a) If $\alpha \in E$, we take $a = \alpha$ and assume (4.3) holds in this case.

(b) If choose $v = v_p$, then $v_p(\alpha - a) > \Delta_E(\alpha) - \frac{p}{(p-1)^2}$, it seems like that we have an absolute constant, however $\Delta_E(\alpha)$ also varies.

We shall follow the proof of Ax ([Ax70]).

Lemma 4.5. *Let $R(X) \in \overline{E}[X]$ be a monic polynomial of degree $d \geq 2$ over $\overline{E}$, the algebraic closure of E. Suppose for any root λ of R in $\overline{E}$, $v(\lambda) \geq r$. For $m \in \mathbb{N}$, $0 < m < d$, let $R^{(m)}(X)$ be the m-th derivative of $R(X)$. Then there exists a root $\mu \in \overline{E}$ of $R^{(m)}(X)$, such that*

$$v(\mu) \geq r - \frac{1}{d-m} v(\binom{d}{m}).$$

Proof. Write

$$R(X) = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_d) = \sum_{i=0}^{d} b_i X^i,$$

then $b_i \in \mathbb{Z}[\lambda_1, \cdots, \lambda_d]$ is homogeneous of degree $d - i$. If follows that $v(b_i) \geq (d-i)r$. Write

$$\frac{1}{m!} R^{(m)}(X) = \sum_{i=m}^{d} \binom{i}{m} b_i X^{i-m} = \binom{d}{m}(X - \mu_1)(X - \mu_2) \cdots (X - \mu_{d-m}),$$

then $b_m = \binom{d}{m}(-1)^{d-m}\mu_1\mu_2 \cdots \mu_{d-m}$, and

$$\sum_{i=1}^{d-m} v(\mu_i) = v(b_m) - v(\binom{d}{m}) \geq (d-m)r - v(\binom{d}{m}).$$

Hence there exists i, such that

$$v(\mu_i) \geq r - \frac{1}{d-m} v(\binom{d}{m}).$$

The lemma is proved.

Proof (Proof of Proposition 4.3). For any $d \geq 1$, let

$$\varepsilon(d) = \sum_{i \in \mathbb{Z}_+,\ p^i \leq d} \frac{1}{p^i - p^{i-1}}.$$

Then $\varepsilon(d) = 0$ if and only if $d < p$. We want to show that if $[E(\alpha) : E] = d$, then there exists $a \in E$, such that

$$v(\alpha - a) > \Delta_E(\alpha) - \varepsilon(d)v(p).$$

This implies the proposition, since $\varepsilon(d) \leq \varepsilon(d+1)$ and $\lim\limits_{d\to+\infty} \varepsilon(d) = \frac{p}{(p-1)^2}$.

We proceed by induction on d. It is easy to check for $d = 1$. Now we assume $d \geq 2$. Let $P(X)$ be the monic minimal polynomial of α over E. Let $R(X) = P(X + \alpha)$, then for $m \in \mathbb{N}$,

$$R^{(m)}(X) = P^{(m)}(X + \alpha).$$

If d is not a power of p, write $d = p^s n$, with n prime to p, and $n \geq 2$. Otherwise write $d = p^s p$, $s \in \mathbb{N}$. We take $m = p^s$.

The roots of $R(X)$ are of the form $\alpha' - \alpha$ for α' a conjugate of α. Set $r = \Delta_E(\alpha)$, and choose μ as in Lemma 4.5. Write $\beta = \mu + \alpha$. Then

$$v(\beta - \alpha) \geq r - \frac{1}{d-m} v(\binom{d}{m}).$$

As $P^{(m)}(\beta) = 0$ and $P^{(m)}(X) \in E[X]$ is of degree $d - m$, β is algebraic over E of degree no higher than $d - m$. Then either $\beta \in E$, we choose $a = \beta$; or $\beta \notin E$, and we choose $a \in E$ such that $v(\beta - a) \geq \Delta_E(\beta) - \varepsilon(d-m)v(p)$, whose existence is guaranteed by induction. We need to check that $v(\alpha - a) > r - \varepsilon(d)$.

Case 1: $d = mn = p^s n$ ($n \geq 2$ prime to p). It is easy to verify $v(\binom{d}{m}) = v(\binom{p^s n}{p^s}) = 0$, so $v(\mu) = v(\beta - \alpha) \geq r$. If β' is a conjugate of β, $\beta' = \alpha' + \mu'$, then

$$v(\beta' - \beta) = v(\alpha' - \alpha + \mu' - \mu) \geq r,$$

which implies $\Delta_E(\beta) \geq r$. Hence $v(\beta - a) \geq r - \varepsilon(d - p^s)v(p)$, and

$$v(\alpha - a) \geq \min\{v(\alpha - \beta), v(\beta - a)\} \geq r - \varepsilon(d)v(p).$$

Case 2: $d = mp = p^s p$. Then $v(\binom{d}{m}) = v(\binom{p^{s+1}}{p^s}) = v(p)$, and $v(\mu) \geq r - \frac{1}{p^{s+1} - p^s} v(p)$. Let β' be any conjugate of β, $\beta' = \mu' + \alpha'$, then

$$v(\beta' - \beta) = v(\mu' - \mu + \alpha' - \alpha) \geq r - \frac{1}{p^{s+1} - p^s} v(p),$$

which implies $\Delta_E(\beta) \geq r - \frac{1}{p^{s+1} - p^s} v(p)$. Then

$$v(\beta - a) \geq r - \frac{1}{p^{s+1} - p^s} v(p) - \varepsilon(p^{s+1} - p^s)v(p) = r - \varepsilon(p^{s+1})v(p).$$

Hence $v(\alpha - a) = v(\alpha - \beta + \beta - a) \geq r - \varepsilon(d)v(p)$.

Proposition 4.6 (Ax-Sen's Lemma, Characteristic > 0 case). *Assume K, E, α as above. Assume K is a perfect field of characteristic $p > 0$. Then for any $\varepsilon > 0$, there exists $a \in E$, such that $v(\alpha - a) \geq \Delta_E(\alpha) - \varepsilon$.*

Proof. Let $L = E(\alpha)$, then L/E is separable. Therefore there exists $c \in L$ such that $\mathrm{Tr}_{L/E}(c) = 1$. For r sufficiently large, $v(c^{p^{-r}}) > -\varepsilon$. Let $c' = c^{p^{-r}}$, then $\mathrm{Tr}_{L/E}(c')^{p^r} = \mathrm{Tr}_{L/E}(c) = 1$. Replacing c by c', we may assume $v(c) > -\varepsilon$. Let

$$S = \{\sigma \mid \sigma : L \hookrightarrow \overline{E} \text{ is an } E\text{-embedding}\},$$

and let

$$a = \mathrm{Tr}_{L/E}(c\alpha) = \sum_{\sigma\in S} \sigma(c\alpha) = \sum_{\sigma\in S} \sigma(c)\sigma(\alpha) \in E.$$

As $\sum_{\sigma\in S} \sigma(c)\alpha = \mathrm{Tr}_{L/E}(c)\alpha = \alpha$,

$$v(\alpha - a) = v(\sum_{\sigma\in S} \sigma(c)(\alpha - \sigma(\alpha))) \geq \min\{v(\sigma(c)(\alpha - \sigma(\alpha)))\} \geq \Delta_E(\alpha) - \varepsilon.$$

This completes the proof.

We give an application of Ax-Sen's Lemma. We first give a definition:

Definition 4.7. *If F is a field of characteristic $p > 0$, we let*

$$F^{\mathrm{rad}} := \{x \in \overline{F} \mid \text{there exists } n, \text{ such that } x^{p^n} \in F\}$$

be the perfect closure *of F, which is also denoted as F^{perf}.*

Back to our case. For K a complete nonarchimedean field, the action of G_K extends by continuity to $C = \widehat{K^s} = \widehat{\overline{K}}$. Let H be any closed subgroup of G_K, $L = (K^s)^H$, and $H = \mathrm{Gal}(K^s/L)$. A natural question arises:

Question 4.8. What is C^H?

Certainly $C^H \supseteq L$ and by continuity $C^H \supseteq \widehat{L}$. Moreover, if $\mathrm{char}\, K = p$, then $L^{\mathrm{rad}} \subset \overline{K} \subset C$ and H acts trivially on L^{rad}. Indeed, for any $x \in L^{\mathrm{rad}}$, there exists $n \in \mathbb{N}$, such that $x^{p^n} = a \in L$, then for any $g \in H$, $(g(x))^{p^n} = x^{p^n}$, which implies $g(x) = x$. Hence $\widehat{L^{\mathrm{rad}}} \subset C^H$.

Proposition 4.9. *For any close subgroup H of G_K, let $L = (K^s)^H$, then*

$$C^H = \begin{cases} \widehat{L}, & \text{if } \mathrm{char}\, K = 0, \\ \widehat{L^{\mathrm{rad}}}, & \text{if } \mathrm{char}\, K = p. \end{cases} \tag{4.4}$$

In particular,

$$C^{G_K} = \begin{cases} \widehat{K} = K, & \text{if } \mathrm{char}\, K = 0, \\ \widehat{K^{\mathrm{rad}}}, & \text{if } \mathrm{char}\, K = p. \end{cases} \tag{4.5}$$

Proof. If $\mathrm{char}\, K = p$, we have a diagram:

$$\begin{array}{ccccccc} K^s & \subset (K^{\mathrm{rad}})^s = \overline{K} & \subset & (\widehat{K^{\mathrm{rad}}})^s = \overline{\widehat{K^{\mathrm{rad}}}} \subset & C \\ {\scriptstyle G_K}\Big| & {\scriptstyle G_K}\Big| & & {\scriptstyle G_K}\Big| & \\ K & \subset \quad K^{\mathrm{rad}} & \subset & \widehat{K^{\mathrm{rad}}} & \end{array}$$

with $\widehat{K^{\mathrm{rad}}}$ perfect. This allows us to replace K by $\widehat{K^{\mathrm{rad}}}$, thus we may assume that K is perfect, in which case $\widehat{L^{\mathrm{rad}}} = \widehat{L}$. The proposition is reduced to show the claim $C^H = \widehat{L}$.

If $\mathrm{char}\, K = p$, we choose any $\varepsilon > 0$. If $\mathrm{char}\, K = 0$, we choose $\varepsilon = \frac{p}{(p-1)^2} v(p)$. For any $\alpha \in C^H$, we want to prove that $\alpha \in \widehat{L}$. We choose a sequence of elements $\alpha_n \in \overline{K}$ such that $v(\alpha - \alpha_n) \geq n$, it follows that

$$v(g(\alpha_n) - \alpha_n) \geq \min\{v(g(\alpha_n - \alpha)), v(\alpha_n - \alpha)\} \geq n$$

for any $g \in H$. Hence $\Delta_L(\alpha_n) \geq n$, which implies that there exists $a_n \in L$, such that $v(\alpha_n - a_n) \geq n - \varepsilon$, and $\lim\limits_{n\to+\infty} a_n = \alpha \in \widehat{L}$.

4.2 Study of $\overline{K}$- and $\overline{P}$-representations of G_K

4.2.1 A summary of notations and basic results

From now on, if without further notice, we shall fix the following notations.

(i) Let K be a p-adic field, $\mathcal{O}_K$ be its ring of integers, $\mathfrak{m}_K$ be the maximal ideal of $\mathcal{O}_K$, $k = \mathcal{O}_K/\mathfrak{m}_K$ be the residue field which is perfect of characteristic p, v_K be the normalized valuation of K, and $e_K = v_K(p)$ be the absolute ramification index of K.

(ii) Let $W = W(k)$ be the ring of Witt vectors of k and $K_0 = \mathrm{Frac}\, W = W[1/p]$ be its field of fractions.

(iii) Let $\overline{K}$ be a fixed algebraic closure of K. Let $C = \widehat{\overline{K}} = \widehat{K^s}$ be the p-adic completion of $\overline{K}$ which is also algebraically closed. Let v be the unique valuation of C such that $v(p) = 1$, in other words, $v = \frac{1}{e_K} v_K$.

(iv) Let $P_0 = W(\bar{k})[\frac{1}{p}] = \widehat{K_0^{\mathrm{ur}}}$ and $P = P_0 K = \widehat{K^{\mathrm{ur}}}$.

(v) For any subfield L of C,
   (a) let $\mathcal{O}_L = \{x \in L \mid v(x) \geq 0\}$ be the ring of integers, $\mathfrak{m}_L = \{x \in L \mid v(x) > 0\}$ the maximal ideal and $k_L = \mathcal{O}_L/\mathfrak{m}_L$ the residue field of L;
   (b) let $\widehat{L}$ is the p-adic completion of L in C, which means

$$\mathcal{O}_{\widehat{L}} = \varprojlim_{n\geq 1} \mathcal{O}_L/p^n\mathcal{O}_L, \quad \widehat{L} = \mathcal{O}_{\widehat{L}}[\frac{1}{p}] \quad \text{and} \quad k_{\widehat{L}} = k_L.$$

(vi) If L is a finite extension of K_0 inside $\overline{K}$, let $L_0 = W(k_L)[\frac{1}{p}]$.

We know that

(A) K/K_0 is totally ramified of degree e_K, $\mathcal{O}_K$ is a free W-module of rank e_K: if π_K is a uniformizer of K, then $\{1, \pi_K, \cdots, \pi_K^{e_K-1}\}$ is a basis of $\mathcal{O}_K$ over W as well as K over K_0.
(B) P_0 and K are linearly disjoint over K_0 and $P = P_0K$.
(C) Let σ be the absolute Frobenius map on K_0, then

$$\sigma(a) = a^p \pmod{pW} \quad \text{if } a \in W. \tag{4.6}$$

(D) If $K_0 \subseteq L \subseteq \overline{K}$, then

$$C^{G_L} = \widehat{L} \text{ which is } L \text{ if and only if } [L : K_0] < +\infty. \tag{4.7}$$

(E) Let $G_k = \mathrm{Gal}(\bar{k}/k)$, I_K be the inertia subgroup of G_K, then one has an exact sequence

$$1 \to I_K \to G_K \to G_k \to 1.$$

Moreover, $\mathrm{Gal}(\overline{P}/P) = I_K$ where $\overline{P}$ is the algebraic closure of P inside C.

Definition 4.10. *For any finite extension L of K_0, denote*

$$L^{\mathrm{cyc}} := L(\mu_{p^\infty}) = \bigcup_{n\in\mathbb{N}} L(\mu_{p^n}) = LK_0^{\mathrm{cyc}}$$

the subfield of $\overline{K}$ obtained by adjoining to L all p^n-th roots of unity, and denote

$$H_L := \mathrm{Gal}(\overline{K}/L^{\mathrm{cyc}}), \ \boldsymbol{\Gamma}_L := \mathrm{Gal}(L^{\mathrm{cyc}}/L).$$

By Kummer theory, then the cyclotomic character χ is the homomorphism

$$\chi : G_L \to \boldsymbol{\Gamma}_L \hookrightarrow \mathbb{Z}_p^\times$$

with $H_L = \mathrm{Ker}\,(\chi)$, and $\mathrm{Im}(\chi)$ a subgroup of $\mathbb{Z}_p^\times$ of finite index and they are equal if $L = L_0$. Thus we regard $\boldsymbol{\Gamma}_L$ as an open subgroup of $\mathbb{Z}_p^\times$. Moreover, the following result is well-known:

Lemma 4.11. *There exists a constant $n = n(L) \in \mathbb{N}$ such that*

(1) *$L^{\mathrm{cyc}}/L(\mu_{p^n})$ is totally ramified and hence $k_L^c := k_{L^{\mathrm{cyc}}}$ is a finite extension of k_L;*
(2) *for any $m \geq n$, $L(\mu_{p^n})$ and $L_0(\mu_{p^m})$ are linearly disjoint over $L_0(\mu_{p^n})$, and hence*

$$\mathrm{Gal}(L(\mu_{p^n})/L_0(\mu_{p^n})) = \cdots = \mathrm{Gal}(L(\mu_{p^m})/L_0(\mu_{p^m})) = \mathrm{Gal}(L^{\mathrm{cyc}}/L_0^{\mathrm{cyc}}).$$

If moreover $L = L_0$, then one can take $n(L_0) = 0$.

By the canonical isomorphism $\mathbb{Z}_p^\times = \mathbb{F}_p^\times \times (1+p\mathbb{Z}_p)$ (or $\mathbb{F}_2 \times (1+4\mathbb{Z}_2)$ if $p=2$), one can decompose

$$\mathbf{\Gamma}_L = \varDelta_L \times \varGamma_L$$

where $\varDelta_L$ is a subgroup of $\mathbb{F}_p^\times$ if $p \neq 2$ or $\mathbb{F}_2$ if $p=2$, and $\varGamma_L \cong \mathbb{Z}_p$. Then $L_\infty := (L^{\mathrm{cyc}})^{\varDelta_L}/L$ is the cyclotomic $\mathbb{Z}_p$ extension of L, which is almost totally ramified (i.e. totally ramified after some finite extension of L). Let $\mathbf{H}_L := \mathrm{Gal}(\overline{K}/L_\infty)$.

In conclusion, we have Fig. 4.1.

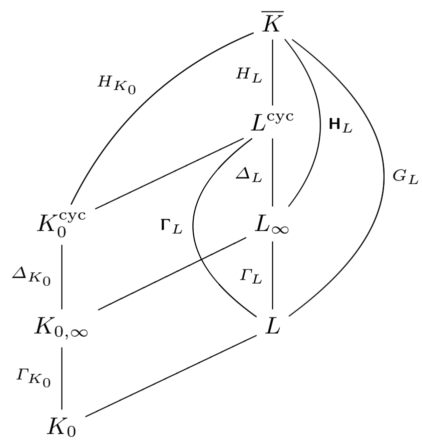


Fig. 4.1. Galois extensions of K and K_0

4.2.2 $\overline{K}$- and $\overline{P}$-admissible representations.

Note that $\overline{K}$ is a topological field on which G_K acts continuously. Recall a *$\overline{K}$-representation* X of G_K is a $\overline{K}$-vector space of finite dimension together with a continuous and semi-linear action of G_K.

For X a $\overline{K}$-representation, the map

$$\alpha_X : \overline{K} \otimes_K X^{G_K} \to X$$

is always injective. X is *trivial* if α_X is an isomorphism.

Proposition 4.12. *X is trivial if and only if the action of G_K is discrete.*

Proof. The sufficiency is clear because of Hilbert Theorem 90. Conversely if X is trivial, there is a basis $\{e_1, \cdots, e_d\}$ of X over $\overline{K}$, consisting of elements of X^{G_K}. For any $x = \sum_{i=1}^{d} \lambda_i e_i \in X$, we want to prove $G_x = \{g \in G|\ g(x) = x\}$ is an open subgroup of G. By the choice of e_i's, $g(x) = \sum_{i=1}^{d} g(\lambda_i)e_i$, therefore

$$G_x = \bigcap_{i=1}^{d} \{g \in G \mid g(\lambda_i) = \lambda_i\} := \bigcap_{i=1}^{d} G_{\lambda_i},$$

each $\lambda_i \in \overline{K}$ is algebraic over K, so G_{λ_i} is open, and the result follows.

Recall for a p-adic representation V of G_K, V is called $\overline{K}$*-admissible* if $\overline{K} \otimes_{\mathbb{Q}_p} V$ is trivial as a $\overline{K}$-representation.

Let $\{v_1, \cdots, v_d\}$ be a basis of V over $\mathbb{Q}_p$. We still write $v_i = 1 \otimes v_i$ when viewed as elements of $\overline{K} \otimes_{\mathbb{Q}_p} V$, then $\{v_1, \cdots, v_d\}$ is a basis of $\overline{K} \otimes_{\mathbb{Q}_p} V$ over $\overline{K}$. By Proposition 4.12, that V is $\overline{K}$-admissible is equivalent to that $G_{v_i} = \{g \in G \mid g(v_i) = v_i\}$ is an open subgroup of G for all $1 \leq i \leq d$, and it is also equivalent to that the kernel of

$$\rho : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_p}(V),$$

which is nothing but $\bigcap_{i=1}^{d} G_{v_i}$, is an open subgroup. We thus get

Proposition 4.13. *A p-adic representation V of G_K is $\overline{K}$-admissible if and only if the action of G_K is discrete.*

We can do a little further. Recall K^{ur} is the maximal unramified extension of K contained in $\overline{K}$, $P = \widehat{K^{\mathrm{ur}}}$ the completion in C, and $\overline{P}$ the algebraic closure of P in C. Clearly $\overline{P}$ is stable under G_K, and $\mathrm{Gal}(\overline{P}/P) = I_K$.

Proposition 4.14. (1) *A $\overline{P}$-representation X of G_K is trivial if and only if the action of I_K on X is discrete.*

(2) *A p-adic representation V of G_K is $\overline{P}$-admissible if and only if the action of I_K on V is discrete.*

Remark 4.15. By the preceding two propositions, if V is a p-adic representation of G_K, and $\rho : G_K \to \mathrm{Aut}_{\mathbb{Q}_p}(V)$ the corresponding homomorphism, then

$$\begin{aligned} V \text{ is } \overline{K}\text{-admissible} &\Longleftrightarrow \mathrm{Ker}\,\rho \text{ is open in } G_K, \\ V \text{ is } \overline{P}\text{-admissible} &\Longleftrightarrow \mathrm{Ker}\,\rho \cap I_K \text{ is open in } I_K. \end{aligned} \tag{4.8}$$

Proof. Obviously (2) is a consequence of (1), so we only need to prove (1).

The condition is necessary since if X is a $\overline{P}$-representation of G_K, then X is trivial if and only if $X \cong \overline{P}^d$ with the natural action of G_K.

We have to prove it is sufficient. Suppose X is a $\overline{P}$-representation of G_K of dimension d with discrete action of I_K. We know that $\overline{P}^{I_K} = P$, and

$$\overline{P} \otimes_P X^{I_K} \longrightarrow X$$

is an isomorphism by Hilbert Theorem 90. Set $Y = X^{I_K}$, because $G_K/I_K = G_k$, Y is a P-representation of G_k. If $P \otimes_K Y^{G_k} \to Y$ is an isomorphism, since $X^{G_K} = Y^{G_k}$, $\overline{P} \otimes_K X^{G_K} \to X$ is also an isomorphism. Thus it is enough to prove that any P-representation Y of G_k is trivial, i.e., to prove that $P \otimes_K Y^{G_k} \to Y$ is an isomorphism.

But we know that any P_0-representation of G_k is trivial by Proposition 3.32: we let

$$E = k,\ \mathcal{O}_{\mathcal{E}} = W,\ \mathcal{E} = K_0,\ \mathcal{E}^{\mathrm{ur}} = K_0^{\mathrm{ur}},$$

then $\widehat{\mathcal{E}^{\mathrm{ur}}} = P_0$ and any $\widehat{\mathcal{E}^{\mathrm{ur}}}$-representation of G_E is trivial. Note that $P = K \otimes_{K_0} P_0$ and $[P : P_0] = e_K$, any P-representation Y of dimension d of G_k can be viewed as a P_0-representation of dimension $e_K d$, and

$$P \otimes_K Y^{G_k} = P_0 \otimes_{K_0} Y^{G_k} \xrightarrow{\sim} Y.$$

The result is proven.

4.3 Classification of C-representations

In this section we write G for G_K. The goal of this section is to classify C-representations of K. To do so, by Hilbert's Theorem 90, one should study the cohomology group $H^1_{\mathrm{cont}}(G, \mathrm{GL}_d(C))$. Let K_∞/K be a totally ramified $\mathbb{Z}_p$-extension with Galois group $\varGamma \cong \mathbb{Z}_p$. Sen reduces the study of $H^1_{\mathrm{cont}}(G, \mathrm{GL}_d(C))$ to the study of $H^1_{\mathrm{cont}}(\varGamma, \mathrm{GL}_d(\widehat{K}_\infty))$ by the almost étale descent technique and then to the study of $H^1_{\mathrm{cont}}(\varGamma, \mathrm{GL}_d(K_\infty))$ by the decompletion technique. This section is devoted to Sen's method.

We fix an arbitrary totally ramified $\mathbb{Z}_p$-extension K_∞ of K contained in $\overline{K}$, though one may always take the cyclotomic $\mathbb{Z}_p$-extension of K as an example, which is totally ramified over a finite extension of K.

Let $H = G_{K_\infty} = \mathrm{Gal}(\overline{K}/K_\infty)$. Let $\varGamma = \varGamma_0 = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Let $\varGamma_m = \varGamma^{p^m}$ and $K_m = K_\infty^{\varGamma_m}$ the subfield of K_∞ fixed by $\varGamma_m$. Let γ be a topological generator of $\varGamma$ and $\gamma_m = \gamma^{p^m}$, which is a topological generator of $\varGamma_m$.

For a matrix $M = (m_{ij}) \in M_{r\times s}(C)$, we let $v(M) = \min v(m_{ij})$.

4.3.1 Almost étale descent.

Lemma 4.16. *Let H_0 be an open subgroup of H and U be a continuous cocycle of H_0 with values in $\mathrm{GL}_d(C)$ such that $v(U_\sigma - 1) \geq a$ for a constant $a > 0$ for all $\sigma \in H_0$. Then there exists a matrix $M \in \mathrm{GL}_d(C)$, $v(M-1) \geq a/2$, such that*

$$v(M^{-1}U_\sigma\sigma(M) - 1) \geq a + 1, \quad \textit{for all } \sigma \in H_0.$$

Proof. We are imitating the proof of Hilbert's Theorem 90 (Theorem 1.114).

Fix an open normal subgroup H_1 of H_0 such that $v(U_\sigma - 1) \geq a + 1 + a/2$ for $\sigma \in H_1$, which is possible by continuity. By Corollary 1.96, we can find $\alpha \in C^{H_1}$ such that

$$v(\alpha) \geqslant -a/2, \qquad \sum_{\tau \in H_0/H_1} \tau(\alpha) = 1.$$

Let $S \subset H_0$ be a set of representatives of H_0/H_1, denote

$$M_S = \sum_{\sigma \in S} \sigma(\alpha) U_\sigma,$$

we have $M_S - 1 = \sum_{\sigma \in S} \sigma(\alpha)(U_\sigma - 1)$. Hence $v(M_S - 1) \geqslant a/2$ and moreover the sequence

$$M_S^{-1} = \sum_{n=0}^{+\infty} (1 - M_S)^n$$

converges, and $M_S \in \mathrm{GL}_d(C)$. We also see that $v(M_S) = v(M_S^{-1}) = 0$. We claim that M_S is the matrix we need.

If $\tau \in H_1$, then $U_{\sigma\tau} - U_\sigma = U_\sigma(\sigma(U_\tau) - 1)$. If $S' \subset H_0$ is another set of representatives of H_0/H_1, then for any $\sigma' \in S'$, there exist a unique $\sigma \in S$ and $\tau_\sigma \in H_1$ such that $\sigma' = \sigma\tau_\sigma$, so we get

$$M_S - M_{S'} = \sum_{\sigma \in S} \sigma(\alpha)(U_\sigma - U_{\sigma\tau_\sigma}) = \sum_{\sigma \in S} \sigma(\alpha) U_\sigma (1 - \sigma(U_{\tau_\sigma})),$$

and

$$v(M_S - M_{S'}) \geqslant a + 1 + a/2 - a/2 = a + 1.$$

For any $\tau \in H_0$,

$$U_\tau \tau(M_S) = \sum_{\sigma \in S} \tau\sigma(\alpha) U_\tau \tau(U_\sigma) = M_{\tau S}.$$

Then

$$M_S^{-1} U_\tau \tau(M_S) = 1 + M_S^{-1}(M_{\tau S} - M_S),$$

with $v(M_S^{-1}(M_{\tau S} - M_S)) \geq a + 1$. The claim is proved.

Corollary 4.17. *Under the same hypotheses as the above lemma, there exists $M \in \mathrm{GL}_d(C)$ such that*

$$v(M - 1) \geq a/2, \ M^{-1} U_\sigma \sigma(M) = 1, \ \textit{for all } \sigma \in H_0.$$

Proof. Suppose M_1 is the matrix constructed for U_σ and a, for i a positive integer, repeat the lemma and suppose M_i is the matrix constructed for $(M_1 \cdots M_{i-1})^{-1} U_\sigma (M_1 \cdots M_{i-1})$ and $a + i$. Now we just need to take $M = M_1 M_2 \cdots$, which converges by construction.

Proposition 4.18. $H^1_{\mathrm{cont}}(H, \mathrm{GL}_d(C)) = 1$.

Proof. We need to show that any given cocycle U on H with values in $\mathrm{GL}_d(C)$ is trivial. Pick $a > 0$, by continuity, we can choose an open normal subgroup H_0 of H such that $v(U_\sigma - 1) > a$ for any $\sigma \in H_0$. By Corollary 4.17, the restriction of U on H_0 is trivial. By the inflation-restriction sequence

$$1 \to H^1_{\mathrm{cont}}(H/H_0, \mathrm{GL}_d(C^{H_0})) \to H^1_{\mathrm{cont}}(H, \mathrm{GL}_d(C)) \to H^1_{\mathrm{cont}}(H_0, \mathrm{GL}_d(C)),$$

since H/H_0 is finite, by Hilbert Theorem 90, $H^1_{\mathrm{cont}}(H/H_0, \mathrm{GL}_d(C^{H_0}))$ is trivial, as a consequence, U is also trivial.

Proposition 4.19. *The inflation map gives a bijection*

$$j : H^1_{\mathrm{cont}}(\varGamma, \mathrm{GL}_d(\widehat{K}_\infty)) \xrightarrow{\sim} H^1_{\mathrm{cont}}(G, \mathrm{GL}_d(C)). \tag{4.9}$$

Proof. Consider the exact inflation-restriction sequence

$$1 \to H^1_{\mathrm{cont}}(\varGamma, \mathrm{GL}_d(C^H)) \to H^1_{\mathrm{cont}}(G, \mathrm{GL}_d(C)) \to H^1_{\mathrm{cont}}(H, \mathrm{GL}_d(C)),$$

the last term is trivial by the previous Proposition, and $\widehat{K}_\infty = C^H$ by Ax-Sen's Lemma, hence follows the result.

4.3.2 Decompletion.

Recall for the totally ramified $\mathbb{Z}_p$-extension K_∞/K, in §1.4.2, we defined Tate's normalized trace map $R_r(x) : \widehat{K}_\infty \to K_r$ for every $r \in \mathbb{N}$. By Corollary 1.99 and Proposition 1.104, there exist positive constants c_1, c_2 independent of r, such that

$$v(R_r(x)) \geq v(x) - c_1, \quad x \in \widehat{K}_\infty; \tag{4.10}$$

$$v((\gamma_r - 1)^{-1}x) \geq v(x) - c_2, \quad x \in X_r = \{x \in \widehat{K}_\infty \mid R_r(x) = 0\}. \tag{4.11}$$

Lemma 4.20. *Given $\delta > 0$, $b \geq 2c_1 + 2c_2 + \delta$, $b' \geq b$. Given $r \geq 0$. Suppose $U = 1 + U_1 + U_2$ with*

$$U_1 \in \mathrm{M}_d(K_r), v(U_1) \geq b - c_1 - c_2$$
$$U_2 \in \mathrm{M}_d(\widehat{K}_\infty), v(U_2) \geq b' \geq b.$$

Then there exists $M \in \mathrm{GL}_d(\widehat{K}_\infty), v(M-1) \geq b - c - d$ such that

$$M^{-1}U\gamma_r(M) = 1 + V_1 + V_2,$$

with

$$V_1 \in \mathrm{M}_d(K_r),\ v(V_1) \geq b - c_1 - c_2,$$
$$V_2 \in \mathrm{M}_d(\widehat{K}_\infty),\ v(V_2) \geq b' + \delta.$$

Proof. One has $U_2 = R_r(U_2) + (1-\gamma_r)V$ such that

$$v(R_r(U_2)) \geq v(U_2) - c_1, \quad v(V) \geq v(U_2) - c_1 - c_2.$$

Thus,

$$\begin{aligned}(1+V)^{-1}U\gamma_r(1+V) &= (1 - V + V^2 - \cdots)(1 + U_1 + U_2)(1+\gamma_r(V)) \\ &= 1 + U_1 + R_r(U_2) + (\text{terms of degree} \geq 2).\end{aligned}$$

Let $V_1 = U_1 + R_r(U_2) \in \mathrm{M}_d(K_r)$ and W be the terms of degree ≥ 2. Thus $v(W) \geq b + b' - 2c_1 - 2c_2 \geq b' + \delta$. We can just take $M = 1 + V$ and $V_2 = W$.

Corollary 4.21. *Keep the same hypotheses as in Lemma 4.20. Then there exists $M \in \mathrm{GL}_d(\widehat{K}_\infty)$, $v(M-1) \geq b - c_1 - c_2$ such that $M^{-1}U\gamma_r(M) \in \mathrm{GL}_d(K_r)$.*

Proof. Repeat the lemma ($b \mapsto b + \delta \mapsto b + 2\delta \mapsto \cdots$), and take the limit.

Lemma 4.22. *Suppose $B \in M_{d\times s}(\widehat{K}_\infty)$ is a matrix of d rows and s columns with entries in $\widehat{K}_\infty$. If there exist $V_1 \in \mathrm{GL}_d(K_i)$ and $V_2 \in \mathrm{GL}_s(K_i)$ such that for some $r \geq i$,*

$$v(V_1 - 1) > c_2, \quad v(V_2 - 1) > c_2, \quad \gamma_r(B) = V_1 B V_2,$$

then $B \in M_{d\times s}(K_i)$.

Proof. Take $T = B - R_i(B)$. It suffices to show that $T = 0$. Note that T has entries in $X_i = (1 - R_i)\widehat{K}_\infty$, and R_i is K_i-linear and commutes with γ_r, thus,

$$\gamma_r(T) - T = V_1 T V_2 - T = (V_1 - 1)TV_2 + V_1 T(V_2 - 1) - (V_1 - 1)T(V_2 - 1).$$

Hence, $v(\gamma_r(T) - T) > v(T) + c_2$. By Proposition 1.104, this implies $v(T) = +\infty$, i.e. $T = 0$.

Proposition 4.23. *The inclusion $\mathrm{GL}_d(K_\infty) \hookrightarrow \mathrm{GL}_d(\widehat{K}_\infty)$ induces a bijection*

$$i : H^1_{\mathrm{cont}}(\varGamma, \mathrm{GL}_d(K_\infty)) \xrightarrow{\sim} H^1_{\mathrm{cont}}(\varGamma, \mathrm{GL}_d(\widehat{K}_\infty)).$$

Moreover, for any continuous cocycle $\sigma \to U_\sigma$ in $Z^1_{\mathrm{cont}}(\varGamma, \mathrm{GL}_d(\widehat{K}_\infty))$, if $v(U_\sigma - 1) > 2c_1 + 2c_2$ for $\sigma \in \varGamma_r$, then there exists $M \in \mathrm{GL}_d(\widehat{K}_\infty)$, $v(M-1) > c_1 + c_2$ such that

$$\sigma \longmapsto U'_\sigma = M^{-1}U_\sigma \sigma(M)$$

satisfies $U'_\sigma \in \mathrm{GL}_d(K_r)$.

Proof. We first prove the injectivity of i. Suppose U, U' are cocycles of $\varGamma$ in $\mathrm{GL}_d(K_\infty)$ which become cohomologous in $\mathrm{GL}_d(\widehat{K}_\infty)$, that is, there is an $M \in \mathrm{GL}_d(\widehat{K}_\infty)$ such that $M^{-1}U_\sigma\sigma(M) = U'_\sigma$ for all $\sigma \in \varGamma$. In particular, $\gamma_r(M) = U_{\gamma_r}^{-1} M U'_{\gamma_r}$. Pick r large enough such that U_{γ_r} and U'_{γ_r} satisfy the conditions in Lemma 4.22, then $M \in \mathrm{GL}_d(K_r)$. Thus U and U' are cohomologous in $\mathrm{GL}_d(K_\infty)$, and the injectivity is proved.

We now prove the surjectivity. Given U, a cocycle of Γ in $\mathrm{GL}_d(\widehat{K}_\infty)$, by continuity there exists one r such that for all $\sigma \in \Gamma_r$, we have $v(U_\sigma - 1) > 2c_1 + 2c_2$. By Corollary 4.21, there exists $M \in \mathrm{GL}_d(\widehat{K}_\infty)$, $v(M-1) > c_1 + c_2$ such that $U'_{\gamma_r} = M^{-1}U_{\gamma_r}\gamma_r(M) \in \mathrm{GL}_d(K_r)$.

Put $U'_\sigma = M^{-1}U_\sigma\sigma(M)$ for all $\sigma \in \Gamma$. For any such σ we have

$$U'_\sigma\sigma(U'_{\gamma_r}) = U'_{\sigma\gamma_r} = U'_{\gamma_r\sigma} = U'_{\gamma_r}\gamma_r(U'_\sigma),$$

which implies that $\gamma_r(U'_\sigma) = U'^{-1}_{\gamma_r}U'_\sigma\sigma(U'_{\gamma_r})$. Apply Lemma 4.22 with $V_1 = U'^{-1}_{\gamma_r}, V_2 = \sigma(U'_{\gamma_r})$, then $U'_\sigma \in \mathrm{GL}_d(K_r)$.

The last part follows from the proof of surjectivity.

Theorem 4.24. *the map*

$$\eta : H^1_{\mathrm{cont}}(\Gamma, \mathrm{GL}_d(K_\infty)) \longrightarrow H^1_{\mathrm{cont}}(G, \mathrm{GL}_d(C))$$

induced by $G \to \Gamma$ *and* $\mathrm{GL}_d(K_\infty) \hookrightarrow \mathrm{GL}_d(C)$ *is a bijection.*

4.3.3 Study of C-representations.

By Proposition 3.7, if L/K is a Galois extension, we know that there is a one-to-one correspondence between the elements of $H^1_{\mathrm{cont}}(\mathrm{Gal}(L/K), \mathrm{GL}_d(L))$ and the isomorphism classes of L-representations of dimension d of $\mathrm{Gal}(L/K)$. Thus we can reformulate the results in the previous subsections in the language of C-representations.

Let W be a C-representation of G of dimension d. Let

$$\widehat{W}_\infty := W^H = \{\omega \mid \omega \in W,\ \sigma(\omega) = \omega \text{ for all } \sigma \in H\}. \tag{4.12}$$

Since $C^H = \widehat{K}_\infty$, $\widehat{W}_\infty$ is a $\widehat{K}_\infty$-vector space with an action of Γ. Moreover,

Theorem 4.25. *The natural map*

$$C \otimes_{\widehat{K}_\infty} \widehat{W}_\infty \longrightarrow W$$

is an isomorphism.

Proof. This is a reformulation of Proposition 4.18.

Theorem 4.26. *There exists* $r \in \mathbb{N}$ *and a* K_r*-representation* W_r *of dimension* d *of* Γ, *such that*

$$\widehat{K}_\infty \otimes_{K_r} W_r \xrightarrow{\sim} \widehat{W}_\infty.$$

Proof. This is a reformulation of Proposition 4.23. Let $\{e_1, \cdots, e_d\}$ be a basis of $\widehat{W}_\infty$, the associated cocycle $\sigma \to U_\sigma$ in $H^1_{\mathrm{cont}}(\Gamma, \mathrm{GL}_d(\widehat{K}_\infty))$ is cohomologous to a cocycle with values in $\mathrm{GL}_d(K_r)$ for r sufficiently large. Thus there exists a basis $\{e'_1, \cdots, e'_d\}$ of $\widehat{W}_\infty$, such that $W_r = K_re'_1 \oplus \cdots \oplus K_re'_d$ is invariant by Γ_r.

From now on, we identify $\widehat{K}_\infty \otimes_{K_r} W_r$ with $\widehat{W}_\infty$ and W_r with $1 \otimes W_r$ in $\widehat{W}_\infty$.

Definition 4.27. *A vector $\omega \in \widehat{W}_\infty$ is called K-finite if its translate by Γ generates a K-vector space of finite dimension. Let*

$$W_\infty := \{w \in \widehat{W}_\infty \mid w \text{ is } K\text{-finite}\}. \tag{4.13}$$

By definition, one sees easily that W_∞ is a K_∞-subspace of $\widehat{W}_\infty$ on which Γ acts. Clearly $K_\infty \otimes_{K_r} W_r$ is a subset of W_∞.

Proposition 4.28. *One has $K_\infty \otimes_{K_r} W_r = W_\infty$, and hence $\widehat{K}_\infty \otimes_{K_\infty} W_\infty \cong \widehat{W}_\infty$.*

Proof. It suffice to show that $W_\infty \subset K_\infty \otimes_{K_r} W_r$.

Suppose $\{e_1, \cdots, e_d\}$ is a basis of W_r, then it is also a basis of $\widehat{W}_\infty$. For an element $\omega = \sum c_i e_i$ of W_∞, let X be the finite K-vector space generated by $\Gamma\omega$. Suppose $\{\omega_1, \cdots, \omega_s\}$ is a basis of X. Then one can write

$$(\omega_1, \cdots, \omega_s) = (e_1, \cdots, e_d)B$$

with $B \in M_{d\times s}(\widehat{W}_\infty)$. Suppose

$$\gamma_r(\omega_1, \cdots, \omega_s) = (\omega_1, \cdots, \omega_s)V_2$$

and

$$\gamma_r(e_1, \cdots, e_d) = (e_1, \cdots, e_d)V_1,$$

then $\gamma_r(B) = V_1^{-1}BV_2$. Choose r big enough such that Lemma 4.22 holds, then B has entries in K_∞ and hence $\omega \in K_\infty \otimes_{K_r} W_r$.

Remark 4.29. The set W_r depends on the choice of basis and is not canonical, but W_∞ is canonical.

4.3.4 Sen's operator Θ.

Suppose W is a C-representation of G of dimension d, and W_r and W_∞ are given as in the previous subsection. By Proposition 4.23, there is a basis $\{e_1, \cdots, e_d\}$ of W_r (over K_r) which is also a basis of W_∞ (over K_∞) and of W (over C). We fix this basis and let $\sigma \in \Gamma \mapsto U_\sigma \in \mathrm{GL}_d(K_\infty)$ be the corresponding cocycle. Then $\rho(\gamma_r) = U_{\gamma_r} \in \mathrm{GL}_d(K_r)$ satisfies $v(U_{\gamma_r} - 1) > c_1 + c_2$. Thus for any $\sigma \in \Gamma_r$, $v(U_\sigma - 1) > c_1 + c_2$ and

$$\log U_\sigma := \sum_{k\geq 1} (-1)^{k-1} \frac{(U_\sigma - 1)^k}{k} \tag{4.14}$$

converges to a matrix in $M_d(K_r)$.

Definition 4.30. *For $\sigma \in \Gamma$, let $\log \sigma = \log_\gamma \sigma$ be the unique $a \in \mathbb{Z}_p$ such that $\sigma = \gamma^a$. For $g \in G$, let $\log g := \log g_\Gamma$.*

If $\sigma \in \Gamma_r$, write $\sigma = \gamma_r^a$, then $\log(\sigma) = a \log(\gamma_r) = p^r a$, and $U_\sigma = U_{\gamma_r}^a$, hence

$$\frac{\log U_\sigma}{\log(\sigma)} = \frac{\log U_{\gamma_r}}{\log(\gamma_r)}. \tag{4.15}$$

Definition 4.31. *The* operator $\Theta = \Theta_W$ of Sen *associated to the C-representation W is the endomorphism of W_r whose matrix under the basis $\{e_1, \cdots, e_d\}$ is given by*

$$\Theta = \frac{\log U_{\gamma_r}}{\log(\gamma_r)} = \frac{\log U_\sigma}{\log(\sigma)}, \tag{4.16}$$

for any $\sigma \in \Gamma_r$. We use the same name for the endomorphisms extending by linearity to W_∞ and W.

Remark 4.32. If K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension, then

$$\log \circ \chi : \Gamma_K \hookrightarrow \mathrm{Gal}(K^{\mathrm{cyc}}/K) \hookrightarrow \mathbb{Z}_p^\times \to \mathbb{Z}_p$$

maps Γ_K to some open subgroup $p^c\mathbb{Z}_p$ of $\mathbb{Z}_p$, then $\log \chi(\sigma) = p^c \log(\sigma)$. If replacing $\log(\sigma)$ by $\log \chi(\sigma)$ appeared in the definition of Θ and the formulas in the following, then everything still works.

Theorem 4.33. *Sen's operator Θ is the unique K_∞-linear endomorphism of W_∞ such that, for every $\omega \in W_\infty$, there is an open subgroup Γ_ω of Γ satisfying*

$$\sigma(\omega) = \exp\Big(\log(\sigma)\Theta\Big)(\omega), \quad \textit{for all } \sigma \in \Gamma_\omega. \tag{4.17}$$

Proof. For $\omega = \lambda_1 e_1 + \cdots \lambda_d e_d \in W_\infty$ such that $\lambda_i \in K_\infty$, then $\Gamma_\omega = \Gamma_r \cap \Gamma_{\lambda_1} \cap \cdots \cap \Gamma_{\lambda_d}$ is an open normal subgroup of Γ. Then for any $\sigma \in \Gamma_\omega \subset \Gamma_r$, we have

$$\exp\Big(\log(\sigma)\Theta\Big) = \exp\log U_\sigma = U_\sigma.$$

Thus

$$\sigma(\omega) = \exp\Big(\log(\sigma)\Theta\Big)(\omega), \quad \text{for all } \sigma \in \Gamma_\omega.$$

To prove the uniqueness, if (4.17) holds, let $\sigma \in \Gamma_r \cap \Gamma_{e_1} \cap \cdots \cap \Gamma_{e_d}$, write $\sigma = \gamma_r^a$. For $\omega \in W_r$, on one hand, the action of σ on ω is given by U_σ under the basis $\{e_1, \cdots, e_d\}$; on the other hand, it is given by $\exp\Big(\log(\sigma)\Theta\Big)(\omega)$, so

$$U_{\gamma_r}^a = U_\sigma = \exp\Big(\log(\sigma)\Theta\Big),$$

hence

$$\Theta = \frac{a \log U_{\gamma_r}}{\log(\sigma)} = \frac{\log U_{\gamma_r}}{\log(\gamma_r)}.$$

This gives the uniqueness.

By the above theorem, Sen's operator Θ on W_∞ (and on W) does not depend on the choice of r and W_r. Moreover, by (4.17), one has

Corollary 4.34. *For $\omega \in W_\infty$,*

$$\Theta(\omega) = \frac{1}{\log(\sigma)} \lim_{\substack{t\to 0\\ p\text{-}adically}} \frac{\sigma^t(\omega)-\omega}{t} = \lim_{\substack{t\to 0\\ p\text{-}adically}} \frac{\gamma^t(\omega)-\omega}{t}. \tag{4.18}$$

Thus Γ commutes with Θ *on W_∞, and G* commutes with Θ *on W.*

Corollary 4.35. *For $\omega \in W_\infty$, $\Theta(\omega) = 0$ if and only if the Γ-orbit of ω is* finite*, equivalently, the stabilizer of ω is an open subgroup of Γ.*

Proof. This follows easily from (4.17) and (4.18).

Corollary 4.36. *Suppose W and W' are two C-representations of G.*

(1) $\Theta_{W\oplus W'} = \Theta_W \oplus \Theta_{W'}$.
(2) $\Theta_{W\otimes W'} = \Theta_W \otimes 1 + 1 \otimes \Theta_{W'}$.
(3) $\Theta_{\mathrm{Hom}(W,W')} = (f \mapsto f\circ\Theta_W - \Theta_{W'}\circ f)$.
(4) *If W' is a sub-representation of W, then $\Theta_{W'} = \Theta_W|_{W'}$.*

Proof. (1), (2) and (4) could be easily seen from definition or by (4.18).

For (3), use the Taylor expansion at $t=0$:

$$\begin{aligned}\sigma^t f(\sigma^{-t}\omega) - f(w) &= (1+t\log(\sigma))f((1-t\log(\sigma))\omega) + O(t^2)f(\omega) - f(\omega)\\ &= t\log(\sigma)f(\omega) - tf(\log(\sigma)\omega) + O(t^2)f(\omega),\end{aligned}$$

then use (4.18) to conclude.

Example 4.37. Suppose K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension and assume $\log\circ\chi = \log$. Let $W = Ce$ be the C-representation of dimension 1 such that $e \neq 0$ and $\sigma(e) = \chi(\sigma)^i e$ for all $\sigma \in G$ (in this case W is called *of Hodge-Tate type of dimension* 1 *and weight i in § 6.1*). Then $e \in W_\infty$, and $\gamma^t(e) = \chi(\gamma)^{it}e$. From this we have $(\gamma^t(e)-e)/t \to \log\chi(\gamma)ie = ie$. Therefore the operator Θ is nothing but the *multiplication* by i map. This example shows that K-finite elements can have infinite γ-orbits.

Proposition 4.38. *There exists a basis of W_∞ with respect to which the matrix of Θ has coefficients in K.*

Proof. For any $\sigma \in \Gamma$, we know $\sigma\Theta = \Theta\sigma$ in W_∞, thus $U_\sigma\sigma(\mathit{\Theta}) = \mathit{\Theta}U_\sigma$ and hence $\mathit{\Theta}$ and $\sigma(\mathit{\Theta})$ are similar to each other. Thus all invariant factors of $\mathit{\Theta}$ are inside K. By linear algebra, $\mathit{\Theta}$ is similar to a matrix with coefficients in K and we have the proposition.

Remark 4.39. Since locally U_σ is determined by Θ, the K-vector space generated by the basis given above is stable under the action of an open subgroup of Γ.

Theorem 4.40. *The kernel of Θ is the C-subspace of W generated by the elements invariant under G, i.e.* $\operatorname{Ker}\Theta = C \otimes_K W^G$.

Proof. Obviously every elements invariant under G is killed by Θ. Now let X be the kernel of Θ. It remains to show that X is generated by elements fixed by G. Since Θ and G commute, X is stable under G and thus is a C-representation. Therefore we can talk about X_∞. Since $C \otimes_{K_\infty} X_\infty = X$ and Θ is extended to X by linearity, it is enough to find a K_∞-basis $\{e_1, \cdots, e_m\}$ of X_∞ such that the e_i's are fixed by Γ. If $\omega \in X_\infty$, then the Γ-orbit of ω is finite by Corollary 4.35, therefore the action of Γ on X_∞ is continuous for the *discrete* topology of X_∞. So by Hilbert's Theorem 90, there exists a basis of $\{e_1, \cdots, e_m\}$ of X_∞ fixed by Γ.

Theorem 4.40 has a very important consequence.

Corollary 4.41. *Suppose V is a p-adic representation of K. Then V is C-admissible if and only if the corresponding Sen operator of $C \otimes_{\mathbb{Q}_p} V$ is identically zero.*

Next result implies that a C-representation W is determined by its Sen operator:

Theorem 4.42. *Let W^1 and W^2 be two C-representations, and Θ^1 and Θ^2 be the corresponding operators. For W^1 and W^2 to be isomorphic it is necessary and sufficient that Θ^1 and Θ^2 should be similar.*

Proof. Let $W = \operatorname{Hom}_C(W^1, W^2)$ with the usual action of G and let Θ be its Sen operator. The G-representations W^1 and W^2 are isomorphic means that there is a C-vector space isomorphism $F : W^1 \to W^2$ such that

$$\sigma \circ F = F \circ \sigma$$

for all $\sigma \in G$, so $F \in W^G$. The operators Θ^1 and Θ^2 are similar means that there is an isomorphism $f : W^1 \to W^2$ as C-vector spaces such that

$$\Theta^2 \circ f = f \circ \Theta^1,$$

that is $f \in \operatorname{Ker}\Theta$ by Corollary 4.36(3). By Theorem 4.40, $W^G \otimes_K C = \operatorname{Ker}\Theta$, we see that the necessity is obvious.

For sufficiency, it amounts to that given an isomorphism $f \in W^G \otimes_K C$, we can find an isomorphism $F \in W^G$.

Choose a K-basis $\{f_1, \cdots, f_m\}$ of W^G. The existence of the isomorphism f shows that there are scalars $c_1, \cdots, c_m \in C$ such that

$$\det(c_1 \bar{f}_1 + \cdots + c_m \bar{f}_m) \neq 0,$$

where $\bar{f}_i$ is the matrix of f_i with respect to some fixed bases of W^1 and W^2. In particular the polynomial $\det(t_1 \bar{f}_1 + \cdots + t_m \bar{f}_m)$ in the indeterminates

$t_1, \cdots, t_m$ cannot be identically zero. Since the field K is infinite, there exist elements $\lambda_i \in K$ such that

$$\det(\lambda_1 \bar{f}_1 + \cdots + \lambda_m \bar{f}_m) \neq 0.$$

The homomorphism $F = \lambda_1 f_1 + \cdots + \lambda_m f_m$ then has the required property.

4.3.5 C-admissible representations.

Suppose V is a p-adic Galois representation of K and ρ is the associated homomorphism. We need the following result of Sen whose proof will be given in the next section:

Proposition 4.43. *If k is algebraically closed, $\Theta = 0$ if and only if $\rho(G_K)$ is finite. In general, $\Theta = 0$ if and only if $\rho(I_K)$ is finite.*

Along with Corollary 4.41, this immediately gives

Proposition 4.44. *A p-adic representation V of G_K is C-admissible if and only if the action of I_K on V is discrete, i.e. V is $\overline{P}$-admissible.*

Recall that if V is a 1-dimensional p-adic representation of K, then $V = \mathbb{Q}_p(\eta)$ with $\eta : G_K \to \mathbb{Z}_p^\times$ a continuous homomorphism. The following famous result of Tate is the special case of Proposition 4.44 in dimension 1:

Corollary 4.45. *$\mathbb{Q}_p(\eta)$ is C-admissible if and only if $\eta(I_K)$ is finite, i.e., for $C(\eta) = C \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(\eta)$,*

$$C(\eta)^{G_K} \begin{cases} = 0, & \text{if } \eta(I_K) \text{ is not finite,} \\ \cong K, & \text{if } \eta(I_K) \text{ is finite.} \end{cases} \tag{4.19}$$

We give another proof of this result without using Proposition 4.43.

Proof. On one hand, if $\eta(I_K)$ is finite, then $\mathbb{Q}_p(\eta)$ is $\overline{P}$-admissible, hence must be C-admissible.

On the other hand, suppose $\eta(I_K)$ is infinite. Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension and then there exists n such that K_∞/K_n is totally ramified. By Sen's method, to show $C(\eta)^{G_K} = 0$, we only need to show $K_\infty(\eta)^{\Gamma_K} = 0$. As $\eta(I_K)$ is infinite, $\eta(\gamma)$ is not a root of unity and $K_\infty(\eta)^{\Gamma_K} = 0$ is a consequence of Proposition 1.104(3).

We end the study of C-representations with a result about the Galois cohomology of the i-th Tate twist $C(i) = Ct^i$ with G_K-action by $g(t^i) = \chi^i(g)t^i$ where χ is the cyclotomic character.

Proposition 4.46. *One has*

(1) *$H^n(G_K, C(i)) = 0$ for $i \neq 0$ or $n \geq 2$;*

(2) $H^0(G_K, C) = K$, *and* $H^1(G_K, C)$ *is a* 1*-dimensional* K*-vector space generated by* $\log\chi = (G_K \xrightarrow{\chi} \mathbb{Z}_p^\times \xrightarrow{\log} \mathbb{Z}_p) \in H^1(G_K, K_0)$.

Proof. For the case $n = 0$, this is just Corollary 4.45.

Let K_∞/K be the cyclotomic $\mathbb{Z}_p$-extension, $\mathbf{H}_K = \mathrm{Gal}(\overline{K}/K_\infty)$ and $\Gamma_K = \mathrm{Gal}(K_\infty/K) = \overline{\langle\gamma\rangle} \cong \mathbb{Z}_p$. We claim that $H^n(\mathbf{H}_K, C(i)) = 0$ for $n > 0$. Indeed, for any finite Galois extension L/K_∞, let $\alpha \in L$ such that $\mathrm{Tr}_{L/K_\infty}(\alpha) = 1$ and let $c \in H^n(L/K_\infty, C(i)^{G_L})$. Set

$$c'(g_1, \cdots, g_{n-1}) = \sum_{h \in \mathrm{Gal}(L/K_\infty)} g_1 g_2 \cdots g_{n-1} h(\alpha) c(g_1, \cdots, g_{n-1}, h),$$

then $dc' = c$. Thus $H^n(\mathbf{H}_K, C(i)) = 0$ by passing to the limit.

For $n = 1$, using the inflation and restriction exact sequence

$$0 \longrightarrow H^1(\Gamma_K, C(i)^{\mathbf{H}_K}) \xrightarrow{\inf} H^1(G_K, C(i)) \xrightarrow{\mathrm{res}} H^1(\mathbf{H}_K, C(i))^{\Gamma_K}.$$

Then the inflation map is actually an isomorphism. We have $C(i)^{\mathbf{H}_K} = \widehat{K}_\infty(i)$. Now $\widehat{K}_\infty = K_m \oplus X_m$ where X_m is the set of all elements whose normalized trace in K_m is 0 by Proposition 1.104. Let m be large enough such that $v_K(\chi(\gamma_m) - 1) > d$, then $\chi(\gamma_m)^i\gamma_m - 1$ is invertible in X_m by Proposition 1.104. We have

$$H^1(\Gamma_{K_m}, \widehat{K}_\infty(i)) = \frac{\widehat{K}_\infty}{\chi^i(\gamma_m)\gamma_m - 1} = \frac{K_m \oplus X_m}{\chi^i(\gamma_m)\gamma_m - 1} = \frac{K_m}{\chi^i(\gamma_m)\gamma_m - 1}.$$

Thus

$$H^1(\Gamma_{K_m}, \widehat{K}_\infty(i)) = \begin{cases} K_m, & \text{if } i = 0; \\ 0, & \text{if } i \neq 0. \end{cases}$$

Since $\widehat{K}_\infty(i)$ is a K-vector space, in particular, $\#\,\mathrm{Gal}(K_m/K)$ is invertible, we have

$$H^j(\mathrm{Gal}(K_m/K), \widehat{K}_\infty(i)^{\mathbf{\Gamma}_{K_m}}) = 0, \quad \text{for } j > 0.$$

By inflation-restriction again, $H^1(\Gamma_K, \widehat{K}_\infty(i)) = 0$ for $i \neq 0$ and for $i = 0$,

$$K = H^1(\Gamma_K, \widehat{K}_\infty) = H^1(\Gamma_K, K) = \mathrm{Hom}(\Gamma_K, K) = K \cdot \log\chi,$$

the last equality is because $\Gamma_K \cong \mathbb{Z}_p$ is pro-cyclic.

For $n \geq 2$, $H^n(\mathbf{H}_K, C(i)) = 0$. Then just use the exact sequence

$$1 \longrightarrow \mathbf{H}_K \longrightarrow G_K \longrightarrow \Gamma_K \longrightarrow 1$$

and the Hochschild-Serre spectral sequence to conclude, noting that the cohomological dimension of Γ_K is 1.

4.4 Sen's operator Θ and the Lie algebra of $\rho(G)$.

The main objective of this section is to show Proposition 4.43. The readers can skip this section if assuming the result.

4.4.1 Main Theorem.

Given a $\mathbb{Q}_p$-representation V of G_K, let $\rho : G_K \to \mathrm{Aut}_{\mathbb{Q}_p} V$ be the corresponding homomorphism. Let $W = C \otimes_{\mathbb{Q}_p} V$. Then some connection between the Lie group $\rho(G)$ and the operator Θ of W is expected. When the residue field k of K is algebraically closed, the connection is given by the following theorem of Sen:

Theorem 4.47. *Suppose the residue field k of K is algebraically closed. Then the Lie algebra $\mathfrak{g}$ of $\rho(G)$ is the smallest of the $\mathbb{Q}_p$-subspaces S of $\mathrm{End}_{\mathbb{Q}_p} V$ such that $\Theta \in C \otimes_{\mathbb{Q}_p} S$.*

Proof. Suppose $\dim_{\mathbb{Q}_p} V = d$. Choose a $\mathbb{Q}_p$-basis $\{e_1, \cdots, e_d\}$ of V and let U_σ be the matrix of $\rho(\sigma)$ with respect to the e_i's.

Assume K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension and we use $\log \circ \chi$ for log in the definition of Θ. Let $\{e_1', \cdots, e_d'\}$ be a basis of W_∞ such that the K-subspace generated by the e_i''s is stable under an open subgroup Γ_m of Γ (by Proposition 4.38, such a basis exists). If U' is the cocycle corresponding to the e_i''s, it follows that $U_\sigma' \in \mathrm{GL}_d(K)$ for $\sigma \in \Gamma_m$. Suppose $(e_1, \cdots, e_d) = (e_1', \cdots e_d')M$ for $M \in \mathrm{GL}_d(K_\infty)$. One then has $M^{-1}U_\sigma'\sigma(M) = U_\sigma$ for all $\sigma \in G$.

Let $\mathit{\Theta}$ be the matrix of Θ with respect to the $\{e_1', \cdots, e_d'\}$. Put $A = M^{-1}\mathit{\Theta} M$, then A is the matrix of Θ with respect to $\{e_1, \cdots, e_d\}$. For σ close to 1 in Γ one knows that $U_\sigma' = \exp(\log\chi(\sigma)\mathit{\Theta})$, and our assumptions imply that $\mathit{\Theta}$ has entries in K.

By duality the theorem is nothing but the assertion that a $\mathbb{Q}_p$-linear form f vanishes on $\mathfrak{g} \iff$ the C-extension of f vanishes on Θ. By the local homeomorphism between a Lie group and its Lie algebra, $\mathfrak{g}$ is the $\mathbb{Q}_p$-subspace of $\mathrm{End}_{\mathbb{Q}_p} V$ generated by the logarithms of the elements in any small enough neighborhood of 1 in $\rho(G)$, for example the one given by $U_\sigma \equiv 1 (\bmod p^m)$ for $m \geqq 2$. Thus it suffices to prove, for any $m \geqq 2$:

Claim: $f(A) = 0 \iff f(\log U_\sigma) = 0 \quad \text{for all } U_\sigma \equiv 1(\bmod p^m)$.

Let

$$G_n = \{\sigma \in G \mid U_\sigma \equiv I \text{ and } \log\chi(\sigma)\mathit{\Theta} \equiv 0(\bmod p^n)\},\ n \geq 2. \tag{4.20}$$

Let

$$G_\infty = \bigcap_{n=2}^{\infty} G_n = \{\sigma \in G \mid U_\sigma = I \text{ and } \chi(\sigma) = 1\}. \tag{4.21}$$

Let $\overset{\vee}{G} = G_2/G_\infty$ and $\overset{\vee}{G}_m = G_m/G_\infty$ for $m \geqq 2$. Then $\overset{\vee}{G}$ is a p-adic Lie group and $\{\overset{\vee}{G}_m\}$ is a Lie filtration of it. Let L be the fixed field of G_∞ in $\overline{K}$, by Proposition 4.9, the fixed field of G_∞ in C is $\widehat{L}$, the completion of L. It is clear that for $\sigma \in G_\infty$ we have $M^{-1}\sigma(M) = I$, it follows that M has entries in $\widehat{L}$, hence A also has entries in $\widehat{L}$. From now on we work within $\widehat{L}$, and σ will be a (variable) element of $\overset{\vee}{G}$.

Assume n_0 is an integer large enough such that $n > n_0$ implies the formula

$$U'_\sigma = \exp(\Theta \, \log \chi(\sigma)) \qquad \text{for all } \sigma \in \overset{\vee}{G}_n. \tag{4.22}$$

The statement of our theorem remains unchanged if we multiply M by a power of p. We may therefore suppose that M has integral entries. After multiplying f by a power of p we may assume that f is "integral", i.e., takes integral values on integral matrices.

For $n > n_0$, $\sigma \in \overset{\vee}{G}_n$, $U'_\sigma \equiv I \bmod p^n$, the equation

$$MU_\sigma = U'_\sigma \sigma(M) \tag{4.23}$$

shows then that $\sigma(M) \equiv M(\bmod p^n)$ for $\sigma \in \overset{\vee}{G}_n$. By Ax-Sen's lemma (Proposition 4.3) it follows that for each n there is a matrix $M_n \in \mathrm{GL}_d(\widehat{L})$ such that

$$M_n \equiv M(\bmod \ p^{n-1}), \text{ and } \sigma(M_n) = M_n \text{ for } \sigma \in \overset{\vee}{G}_n. \tag{4.24}$$

Now suppose $\sigma \in \overset{\vee}{G}_n$, with $n \geqq 2$. We then have

$$U_\sigma \equiv I + \log U_\sigma, \text{ and } U'_\sigma \equiv I + \log U'_\sigma = I + \log \chi(\sigma) \cdot \Theta \quad (\bmod p^{2n}).$$

Substituting these congruences in (4.23) we get

$$M + M \log U_\sigma \equiv \sigma(M) + \log \chi(\sigma) \cdot \Theta \sigma(M)(\bmod p^{2n}).$$

Since $\log U_\sigma$ and $\log \chi(\sigma)$ are divisible by p^n we have by (4.24):

$$M + M_n \log U_\sigma \equiv \sigma(M) + \log \chi(\sigma) \cdot \Theta M_n(\bmod p^{2n-1}). \tag{4.25}$$

Let r_1 and r_2 be integers such that $p^{r_1-1}M^{-1}$ and $p^{r_2}\Theta$ have integral entries. Let $n > r := 2r_1 + r_2 - 1$. Then M_n is invertible and $p^{r_1-1}M_n^{-1}$ is integral. Multiplying (4.25) on the left by $p^{r_1-1}M_n^{-1}$ and dividing by p^{r_1-1} we get

$$C_n + \log U_\sigma \equiv \sigma(C_n) + \log \chi(\sigma) \cdot M_n^{-1}\Theta M_n \quad (\bmod p^{2n-r_1}) \tag{4.26}$$

where $C_n = M_n^{-1}M \equiv I(\bmod p^{n-r_1})$. Write $A_n = M_n^{-1}\Theta M_n$, then it is fixed by $\overset{\vee}{G}_n$ and

$$\begin{aligned} A_n - A =& M_n^{-1}\Theta M_n - M^{-1}\Theta M = (M_n^{-1} - M^{-1})\Theta M_n + M^{-1}\Theta(M_n - M) \\ =& (M_n^{-1}M - I)M^{-1}\Theta M_n + M^{-1}\Theta(M_n - M) \equiv 0 \bmod p^{n-r}. \end{aligned}$$

We get
$$\log\chi(\sigma)A_n \equiv \log\chi(\sigma)A(\bmod p^{2n-r}).$$

Hence
$$(\sigma - 1)C_n \equiv \log U_\sigma - \log\chi(\sigma)\cdot A_n(\bmod p^{2n-r_1}).$$

Applying f to the above equation, note that f is an extension of some linear form on $M_d(\mathbb{Q}_p)$, we get

$$(\sigma - 1)f(C_n) \equiv f(\log U_\sigma) - \log\chi(\sigma)\cdot f(A_n)(\bmod p^{2n-r_1})$$

and hence

$$(\sigma - 1)f(C_n) \equiv f(\log U_\sigma) - \log\chi(\sigma)\cdot f(A)(\bmod p^{2n-r}). \tag{4.27}$$

We need the following important lemma, whose proof will be given in next subsection.

Lemma 4.48. *Let $G = \mathrm{Gal}(L/K)$ be a p-adic Lie group, $\{G(n)\}$ be a p-adic Lie filtration on it. Suppose for some n there is a continuous function $\lambda : G(n) \to \mathbb{Q}_p$ and an element x in the completion of L such that*

$$\lambda(\sigma) \equiv (\sigma - 1)x(\bmod p^m),\ \textit{for all } \sigma \in G(n)$$

and some $m \in \mathbb{Z}$. Then there exists a constant c such that

$$\lambda(\sigma) \equiv 0(\bmod p^{m-c-1}),\ \textit{for all } \sigma \in G(n).$$

Suppose $f(A) = 0$. By (4.27) and Lemma 4.48, we conclude that $f(\log U_\sigma) \equiv 0(\bmod p^{2n-r-c-1})$ for any $\sigma \in \check{G}_n$, where c is the constant of the lemma (which depends only on $\check{G}$). Since $\sigma^{p^{n-2}} \in \check{G}_n$ and $\log U_{\sigma^{p^{n-2}}} = p^{n-2}\log U_\sigma$ for any $\sigma \in \check{G}$. We conclude that $f(\log U_\sigma) \equiv 0(\bmod\ p^{n-r-c+1})$ for all $\sigma \in \check{G}$, hence $f(\log U_\sigma) = 0$ as desired, since n was arbitrary.

Suppose $f(\log U_\sigma) = 0$ for all $\sigma \in \check{G}$: We wish to show $f(A) = 0$. Suppose not, then $f(A_n) \neq 0$ and has constant ordinal for large n, dividing (4.27) by $f(A)$ and using Lemma 4.48, we obtain

$$\log\chi(\sigma) \equiv 0(\bmod p^{2n-r-c-1-s})$$

for large n and all $\sigma \in \check{G}_n$, where s is a constant with $p^s f(A)^{-1}$ integral. Analogous argument as above shows that $\log\chi(\sigma) = 0$ for all $\sigma \in \check{G}$. This is a contradiction since, as is well known, χ is a non-trivial representation with infinite image. This concludes the proof of the main theorem.

By this theorem, we can prove Proposition 4.43:

Proof. First suppose k is algebraically closed. By the theorem $\Theta = 0 \Leftrightarrow \mathfrak{g} = 0$. So we only need to show $\mathfrak{g} = 0 \Leftrightarrow \rho(G)$ is finite.

The sufficiency is obvious. For the necessity, $\mathfrak{g} = 0$ implies that $\rho(G)$ has a trivial open subgroup which in turn implies that $\rho(G)$ is finite.

In general one just needs to replace G by the inertia subgroup I_K and K by the completion of K^{ur}, then the assertion follows from the algebraically closed case.

4.4.2 Application of Sen's filtration Theorem.

We assume k is algebraically closed. We need to use the notation in § 1.4.

Lemma 4.49. *Let L/K be finite cyclic of p-power degree with Galois group $A = \mathrm{Gal}(L/K)$. Suppose $v_A > e_A(r+1/(p-1))$ for some integer $r \geq 0$. Then p^r divides the different $\mathfrak{D}_{L/K}$.*

Proof. Let $p^n = [L : K]$, and for $0 \leq i \leq n$, let $A_{(i)}$ be the subgroup of order p^i in A, so $A = A_{(n)} \supset A_{(n-1)} \supset \cdots \supset A_{(1)} \supset A_{(0)} = 1$. Let $v_i = v_{A/A_{(i)}}$. From Corollary 1.87, we get by induction on j:

$$v_j = v_A - je_A > \left(r - j + \frac{1}{p-1}\right)e_A, \quad \text{for } 0 \leq j \leq r.$$

By Herbrand's theorem, we have

$$A^v = A_{(j)}, \text{ for } v_j < v \leq v_{j-1}, \ 1 \leq j \leq r.$$

Then

$$\begin{aligned}
v_p(\mathfrak{D}_{L/K}) =& \frac{1}{e_A}\int_{-1}^{\infty}(1 - |A^v|^{-1})dv \\
\geq& \frac{1}{e_A}\Big(\int_{-1}^{v_r}(1 - |A^v|^{-1})dv + \sum_{j=1}^{r}(1 - \frac{1}{p^j})e_A\Big) \\
\geq& \frac{1}{e_A}\Big((1 - p^{-r})\frac{1}{p-1}e_A + re_A - e_A \cdot \sum_{j=1}^{r}\frac{1}{p^j}\Big) \\
\geq& r.
\end{aligned}$$

Hence p^r divides the different $\mathfrak{D}_{L/K}$.

Proposition 4.50. *Suppose $G = \mathrm{Gal}(L/K)$ is a p-adic Lie group and that $\{G(n)\}$ is the Lie filtration of G. Let K_n be the fixed field of $G(n)$. Then there is a constant c independent of n such that for every finite cyclic extension E/K_n such that $E \subset L$, the different $\mathfrak{D}_{E/K_n}$ is divisible by $p^{-c}[E : K_n]$.*

Proof. Put $u_n = u_{G/G(n)}, v_n = v_{G/G(n)}$, and $e_n = e_{G(n)}$. From Proposition 1.91, we know that there exists a constant a such that

$$v_n = a + ne \quad \text{for } n \text{ large.}$$

By the filtration theorem (Theorem 1.92), we can find an integer b large enough such that

$$G^{a+ne} \supset G(n+b)$$

for n large.

Let E/K_n be cyclic of degree p^s and n large. Let $\mathrm{Gal}(E/K_n) = G(n)/H = A$. We have $G(n+s-1) = G(n)^{p^{s-1}} \not\subseteq H$ because $A^{p^{s-1}} \neq 1$. Thus, if $G(n)^y \supset G(n+s-1)$, then $u_A \geq y$, because $A^y = G(n)^y H/H \neq 1$.

By Proposition 1.90, we have, for $t > 0$, with the above choice of a and b:

$$G(n)^{u_n + te_n} = G^{v_n + te} = G^{a+(n+t)e} \supset G(n+t+b).$$

If $s > b+1$, put $t = s-b-1$, then we get $v_A \geq y$ as above, with

$$y = u_n + (s-b-1)e_n > (s-b-3+1/(p-1))e_n.$$

So if $s \geq b+3$, then $p^{s-b-3} = p^{-(b+3)}[E : K_n]$ divides $\mathfrak{D}_{E/K_n}$ by Lemma 4.49. The same is trivially true if $s < b+3$. Thus $c = b+3$ works for large n (say $n \geq n_1$) and $c = n_1 + b + 3$ works for all n.

Corollary 4.51. $\mathrm{Tr}_{E/K_n}(\mathcal{O}_E) \subset p^{-c}[E : K_n]\mathcal{O}_{K_n}$.

Proof. Let $[K : K_n] = p^s$. The proposition states that $\mathfrak{D}_{E/K_n} \subset p^{s-c}\mathcal{O}_E$, hence $\mathcal{O}_E \subset p^{s-c}\mathfrak{D}^{-1}_{E/K_n}$. On taking the trace the corollary follows.

We now come to the proof of Lemma 4.48:

Proof (Proof of Lemma 4.48). Multiplying λ and x by p^{-m} we may assume $m = 0$. Let $\bar{\lambda} : G(n) \to \mathbb{Q}_p/\mathbb{Z}_p$ be the function $\bar{\lambda}(\sigma) = \lambda(\sigma) + \mathbb{Z}_p$. Following $\bar{\lambda}$ by the inclusion $\mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow L/\mathcal{O}_L$, we see that $\bar{\lambda}$ is a 1-coboundary, hence a 1-cocycle, and thus a homomorphism, because $G(n)$ acts trivially on $\mathbb{Q}_p/\mathbb{Z}_p$.

Let $H = \mathrm{Ker}\,\bar{\lambda}$ and E be the fixed field of H. For $\sigma \in H$ we have $(\sigma - 1)x \in \widehat{\mathcal{O}}_L$, by Ax-Sen's Lemma, there exists an element $y \in E$ such that $y \equiv x(\bmod\ p^{-1})$. Then

$$\lambda(\sigma) \equiv (\sigma - 1)x \equiv (\sigma - 1)y \pmod{p^{-1}}, \text{ for } \sigma \in G(n).$$

Select $\sigma_0 \in G_n$, such that $\sigma_0 H$ generates $G(n)/H$. Let

$$\lambda(\sigma_0) = (\sigma_0 - 1)y + p^{-1}z.$$

Then $z \in \mathcal{O}_E$. Taking the trace from E to K_n, we find, using the Corollary 4.51, that

$$[E : K_n]\lambda(\sigma_0) \in p^{-c-1}[E : K_n]\mathcal{O}_{K_n},$$

i.e. $\lambda(\sigma_0) \equiv 0(\bmod p^{-c-1})$ and hence $\lambda(\sigma) \equiv 0(\bmod\ p^{-c-1})$ for all $\sigma \in G(n)$, as was to be shown.

5

The ring R and its structure

5.1 The ring R and its basic properties

5.1.1 The R-construction.

If A is a commutative ring of characteristic p, the *absolute Frobenius map* is the ring homomorphism

$$\varphi : A \to A, \qquad a \mapsto a^p.$$

Recall that A is perfect (resp. reduced) if φ is an isomorphism (resp. a monomorphism).

Definition 5.1. *Assume A is a commutative ring of characteristic p, set*

$$R(A) := \varprojlim_{n \in \mathbb{N}} A_n, \tag{5.1}$$

where $A_n = A$ and the transition map is φ. Then an element $x \in R(A)$ is a sequence $x = (x_n)_{n\in\mathbb{N}}$ satisfying $x_n \in A$ and $x_{n+1}^p = x_n$.

Proposition 5.2. *The ring $R(A)$ is a perfect ring of characteristic p.*

Proof. Since the transition map φ is a ring homomorphism, $R(A)$ must be a ring of characteristic p.

For any $x = (x_n)_{n\in\mathbb{N}}$, let $y = (x_{n+1})_{n\in\mathbb{N}}$, then $x = y^p$. If $x^p = 0$, then $x_{n+1}^p = x_n = 0$ for any $n \geq 0$, hence $x = 0$. Thus $R(A)$ is perfect.

For any n, let θ_n be the projection map

$$\theta_n : R(A) \longrightarrow A, \quad (x_n)_{n\in\mathbb{N}} \longmapsto x_n. \tag{5.2}$$

We have

(a) If A is perfect, then each θ_n is an isomorphism; if A is reduced, then θ_0 (hence θ_n) is injective and the image

$$\theta_0(R(A)) = \bigcap_{n\geq 0} \varphi^n(A). \tag{5.3}$$

(b) If A is a topological ring, then $R(A)$ is endowed with the topology of the inverse limit, i.e., the weakest topology such that θ_n is continuous for all n. In particular, one can endow A with the discrete topology and study the induced topology on $R(A)$.

Now let A be a ring which is separated and complete for the p-adic topology, that is, the canonical map $A \to \varprojlim_{n\in\mathbb{N}} A/p^n A$ is an isomorphism. We consider the ring $R(A/pA)$.

Proposition 5.3. *There exists a bijection between $R(A/pA)$ and the set*

$$R(A) := \varprojlim_{x\mapsto x^p} A = \{(x^{(n)})_{n\in\mathbb{N}} \mid x^{(n)} \in A,\ (x^{(n+1)})^p = x^{(n)}\}. \tag{5.4}$$

Proof. Take $x \in R(A/pA)$, that is,

$$x = (x_n)_{n\in\mathbb{N}},\ x_n \in A/pA \text{ and } x_{n+1}^p = x_n.$$

For any n, choose a lifting of x_n in A, say $\widehat{x}_n$, we have

$$\widehat{x}_{n+1}^p \equiv \widehat{x}_n \bmod pA.$$

Note that for $m \in \mathbb{N}$, $m \geq 1$, if $\alpha \equiv \beta \bmod p^m A$, then

$$\alpha^p \equiv \beta^p \bmod p^{m+1} A.$$

Thus for $n, m \in \mathbb{N}$, we have

$$\widehat{x}_{n+m+1}^{p^{m+1}} \equiv \widehat{x}_{n+m}^{p^m} \bmod p^{m+1} A.$$

Hence for every n, $\lim_{m\to+\infty} \widehat{x}_{n+m}^{p^m}$ exists in A, and the limit is independent of the choice of the liftings. We denote

$$x^{(n)} = \lim_{m\to+\infty} \widehat{x}_{n+m}^{p^m}.$$

Then $x^{(n)}$ is a lifting of x_n, $(x^{(n+1)})^p = x^{(n)}$ and $x \mapsto (x^{(n)})_{n\in\mathbb{N}}$ defines a map

$$R(A/pA) \longrightarrow R(A).$$

On the other hand the reduction modulo p from A to A/pA naturally induces the map $R(A) \to R(A/pA)$, $(x^{(n)})_{n\in\mathbb{N}} \mapsto (x^{(n)} \bmod pA)_{n\in\mathbb{N}}$. One can easily check that the two maps are inverse to each other.

From now on, for a ring A which is separated and complete for the p-adic topology, we shall use the above bijection to identify $R(A)$ with $R(A/pA)$. Thus $R(A)$ inherits a ring structure via this identification, and any element $x \in R(A)$ can be written in two ways

$$x = (x_n)_{n\in\mathbb{N}} = (x^{(n)})_{n\in\mathbb{N}},\ x_n \in A/pA,\ x^{(n)} \in A. \tag{5.5}$$

If $x = (x^{(n)})$, $y = (y^{(n)}) \in R(A)$, then

$$(xy)^{(n)} = (x^{(n)}y^{(n)}), \tag{5.6}$$

and

$$(x+y)^{(n)} = \lim_{m\to+\infty}(x^{(n+m)} + y^{(n+m)})^{p^m}. \tag{5.7}$$

5.1.2 Basic properties of the ring *R*.

The most important case in practice for $R(A)$ is that $A = \mathcal{O}_{\widehat{L}}$ with L being a subfield of $\overline{K}$ containing K_0 and its completion $\widehat{L}$ by the p-adic valuation. Identify $\mathcal{O}_L/p\mathcal{O}_L = \mathcal{O}_{\widehat{L}}/p\mathcal{O}_{\widehat{L}}$, then

$$R(\mathcal{O}_{\widehat{L}}) = R(\mathcal{O}_L/p\mathcal{O}_L) = \{x = (x^{(n)})_{n\in\mathbb{N}} \mid x^{(n)} \in \mathcal{O}_{\widehat{L}},\ (x^{(n+1)})^p = x^{(n)}\}.$$

In particular,

Definition 5.4. *The ring* $R := R(\mathcal{O}_C) = R(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})$.

Theorem 5.5. *The ring R is a complete valuation ring perfect of characteristic p with the valuation $v = v_R$ defined by*

$$v_R(x) = v(x) := v(x^{(0)})$$

where $v = v_p$ is the valuation on C normalized by $v(p) = 1$, its residue field is $\bar{k}$, and its fraction field $\mathrm{Fr}\,R = R(C)$ *is a complete nonarchimedean perfect field of characteristic p.*

Furthermore, R is equipped with a natural continuous action of G_{K_0} given by

$$g(x) := (gx^{(n)})_n.$$

Proof. We have $v(R) = \mathbb{Q}_{\geq 0} \cup \{+\infty\}$ as the map $R \to \mathcal{O}_C,\ x \mapsto x^{(0)}$ is onto. We also obviously have

$$v(x) = +\infty \Leftrightarrow x^{(0)} = 0 \Leftrightarrow x = 0,$$

and

$$v(xy) = v(x) + v(y).$$

To see that v is a valuation, we just need to verify $v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in R$.

We may assume $x,\ y \neq 0$, then $x^{(0)}, y^{(0)} \neq 0$. Since $v(x) = v(x^{(0)}) = p^n v(x^{(n)})$, there exists n such that $v(x^{(n)}) < 1$, $v(y^{(n)}) < 1$. By definition, $(x+y)^{(n)} \equiv x^{(n)} + y^{(n)} \pmod p$, so

$$\begin{aligned} v((x+y)^{(n)}) &\geq \min\{v(x^{(n)}), v(y^{(n)}), 1\} \\ &\geq \min\{v(x^{(n)}), v(y^{(n)})\}, \end{aligned}$$

it follows that $v(x+y) \geq \min\{v(x), v(y)\}$.

Since

$$v(x) \geq p^n \Leftrightarrow v(x^{(n)}) \geq 1 \Leftrightarrow x_n = 0,$$

we have

$$\{x \in R \mid v(x) \geq p^n\} = \operatorname{Ker}(\theta_n : R \to \mathcal{O}_C/p\mathcal{O}_C).$$

So the topology defined by the valuation is nothing but the inverse limit topology, and therefore is complete.

Because R is a valuation ring, R is a domain and thus we may consider $\operatorname{Fr} R$, the fraction field of R. Then

$$\operatorname{Fr} R = R(C) = \{x = (x^{(n)})_{n\in\mathbb{N}} \mid x^{(n)} \in C, (x^{(n+1)})^p = x^{(n)}\}.$$

The valuation v extends to the fraction field $\operatorname{Fr} R$ by the same formula $v(x) = v(x^{(0)})$. $\operatorname{Fr} R$ is a complete nonarchimedean perfect field of characteristic $p > 0$ with the ring of integers

$$R = \{x \in \operatorname{Fr} R \mid v(x) \geq 0\}$$

whose maximal ideal is $\mathfrak{m}_R = \{x \in \operatorname{Fr} R \mid v(x) > 0\}$.

For the residue field $R/\mathfrak{m}_R$, one can check that the map

$$R \xrightarrow{\theta_0} \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}} \longrightarrow \bar{k}$$

is onto and its kernel is $\mathfrak{m}_R$, so the residue field of R is $\bar{k}$.

Finally the continuity of Galois action is clear.

Because $\bar{k}$ is perfect and R is complete, there exists a unique section $s : \bar{k} \to R$ of the map $R \to \bar{k}$, which is a homomorphism of rings.

Proposition 5.6. *The section s is given by*

$$a \in \bar{k} \longrightarrow ([a^{p^{-n}}])_{n\in\mathbb{N}}$$

where $[a^{p^{-n}}] = (a^{p^{-n}}, 0, 0, \cdots) \in \mathcal{O}_{\widehat{K}_0^{\mathrm{ur}}}$ *is the Teichmüller representative of* $a^{p^{-n}}$.

Proof. One can check easily $([a^{p^{-(n+1)}}])^p = [a^{p^{-n}}]$ for every $n \in \mathbb{N}$, thus $([a^{p^{-n}}])_{n\in\mathbb{N}}$ is an element $\tilde{a}$ in R, and $\theta_0(\tilde{a}) = [a]$ whose reduction $\bmod p$ is just a. We just need to check $a \mapsto \tilde{a}$ is a homomorphism, which is obvious.

Proposition 5.7. $\mathrm{Fr}\, R$ *is an algebraically closed field.*

Proof. As $\mathrm{Fr}\, R$ is perfect, it suffices to prove that it is separably closed, which means that if a monic polynomial $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0 \in R[X]$ is separable, then $P(X)$ must have a root in R.

Since P is separable, there exist U_0, $V_0 \in \mathrm{Fr}\, R[X]$ such that

$$U_0 P + V_0 P' = 1.$$

Choose $\pi \in R$, such that $v(\pi) = 1$(for example, take $\pi = (p^{(n)})_{n\in\mathbb{N}}$, $p^{(0)} = p$), then we can find $m \geq 0$, such that

$$U = \pi^m U_0 \in R[X], \quad V = \pi^m V_0 \in R[X],$$

and $UP + VP' = \pi^m$.

Claim: For any $n \in \mathbb{N}$, there exists $x \in R$, such that $v(P(x)) \geq p^n$.

For a fixed n, consider $\theta_n : R \twoheadrightarrow \mathcal{O}_{\overline{K}}/p$, recall

$$\mathrm{Ker}\, \theta_n = \{y \in R \mid v(y) \geq p^n\},$$

we just need to find $x \in R$ such that $\theta_n(P(x)) = 0$. Let

$$Q(X) = X^d + \cdots + \alpha_1 X + \alpha_0 \in \mathcal{O}_{\overline{K}}[X],$$

where α_i is a lifting of $\theta_n(a_i)$. Since $\overline{K}$ is algebraic closed, let $u \in \mathcal{O}_{\overline{K}}$ be a root of $Q(X)$, and $\bar{u}$ be its image in $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$, then any $x \in R$ such that $\theta_n(x) = \bar{u}$ satisfies $\theta_n(P(x)) = 0$. This proves the claim.

Take $n_0 = 2m + 1$, we want to construct a sequence $(x_n)_{n\geq n_0}$ of R such that

$$v(x_{n+1} - x_n) \geq n - m, \quad \text{and} \quad P(x_n) \in \pi^n R,$$

then $\lim\limits_{n\to+\infty} x_n$ exists, and it will be a root of $P(X)$.

We construct (x_n) inductively. We first use the above claim to construct x_{n_0}. Assume x_n has already been constructed. Put

$$P^{[j]} = \frac{1}{j!} P^{(j)}(X) = \sum_{i\geq j} \binom{i}{j} a_i X^{i-j},$$

then

$$P(X + Y) = P(X) + YP'(X) + \sum_{j\geq 2} Y^j P^{[j]}(X).$$

Write $x_{n+1} = x_n + y$, then

$$P(x_{n+1}) = P(x_n) + yP'(x_n) + \sum_{j\geq 2} y^j P^{[j]}(x_n). \tag{5.8}$$

If $v(y) \geq n-m$, then $v(y^j P^{[j]}(x_n)) \geq 2(n-m) \geq n+1$ for $j \geq 2$, so we only need to find some y such that

$$v(y) \geq n-m, \quad \text{and} \quad v(P(x_n) + yP'(x_n)) \geq n+1.$$

By construction, $v(U(x_n)P(x_n)) \geq n > m$, so

$$v\big(V(x_n)P'(x_n)\big) = v\big(\pi^m - U(x_n)P(x_n)\big) = m,$$

which implies that $v(P'(x_n)) \leq m$. Take $y = -\frac{P(x_n)}{P'(x_n)}$, then $v(y) \geq n-m$, and we get x_{n+1} as required.

5.1.3 Fr $R^\times$ and its subgroups.

Recall that the group $C^\times$ has the following subgroups:

(i) $U_C = \mathcal{O}_C^\times = \mathcal{O}_C - \mathfrak{m}_C := \{x \in C \mid v(x) = 0\}$ is the unit group of $\mathcal{O}_C$;
(ii) $U_C^+ = 1 + \mathfrak{m}_C := \{x \in C \mid v(x-1) > 0\} \subseteq U_C$;
(iii) $U_C^1 = 1 + p\mathcal{O}_C := \{x \in C \mid v(x-1) \geq 1\} \subseteq U_C^+$.

Then

(a) the sequence $0 \to U_C \to C^\times \xrightarrow{v} \mathbb{Q} \to 0$ is exact;
(b) the exact sequence $1 \to U_C^+ \to U_C \to \bar{k}^\times \to 1$ and the Teichmüller map $\bar{k}^\times \to U_C$ induce an isomorphism $U_C = \bar{k}^\times \times U_C^+$;
(c) for any $a \in U_C^+$, there exists $n \in \mathbb{N}$ such that $a^{p^n} \in U_C^1$;
(d) U_C^1 is separated and complete by the p-adic topology.

Similarly, we define subgroups of Fr $R^\times$:

(i) $U_R = R^\times = R - \mathfrak{m}_R := \{x \in R \mid v(x) = 0\}$ = the unit group of R;
(ii) $U_R^+ = 1 + \mathfrak{m}_R := \{x \in R \mid v(x-1) > 0\} \subseteq U_R$;
(iii) $U_R^1 := \{x \in R \mid v(x-1) \geq 1\} \subseteq U_R^+$.

Proposition 5.8. *The map*

$$\mathrm{Hom}(\mathbb{Z}[1/p], C^\times) \to \mathrm{Fr}\, R^\times, \;\; f \mapsto (f(p^{-n}))_{n\in\mathbb{N}}$$

is a canonical isomorphism of $\mathbb{Z}[G_{K_0}]$-modules. Moreover, identifying these two groups through this isomorphism, then

(1) $U_R = \mathrm{Hom}(\mathbb{Z}[1/p], \mathcal{O}_C^\times) = \bar{k}^\times \times U_R^+$*;*
(2) $U_R^1 \xrightarrow{\sim} \varprojlim_{n\in\mathbb{N}} U_R^1/(U_R^1)^{p^n}$ *is a torsion free $\mathbb{Z}_p$-module and* $U_R^+ = \mathrm{Hom}(\mathbb{Z}[1/p], U_C^+) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U_R^1$.

Proof. If f is a homomorphism from $\mathbb{Z}[1/p]$ to $C^\times$, write $x^{(n)} = f(p^{-n})$, then $(x^{(n+1)})^p = x^{(n)}$, so $x = (x^{(n)})_{n\in\mathbb{N}} \in (\mathrm{Fr}\, R)^\times$. Conversely, if $x = (x^{(n)})_{n\in\mathbb{N}} \in (\mathrm{Fr}\, R)^\times$, let $f(p^{-n}) = x^{(n)}$, then we get a homomorphism $f : \mathbb{Z}[1/p] \to C^\times$. It is clear this correspondence is G_{K_0}-compatible.

For $x \in R$, $x \in U_R \Leftrightarrow x^{(0)} \in U_C$, thus we get

$$\begin{aligned} U_R &= \mathrm{Hom}(\mathbb{Z}[1/p], \mathcal{O}_C^\times) = \mathrm{Hom}(\mathbb{Z}[1/p], \bar{k}^\times \times U_C^+) \\ &= \mathrm{Hom}(\mathbb{Z}[1/p], \bar{k}^\times) \times \mathrm{Hom}(\mathbb{Z}[1/p], U_C^+). \end{aligned}$$

In $\bar{k}$, any element has exactly one p-th root, so $\mathrm{Hom}(\mathbb{Z}[1/p], \bar{k}^\times) = \bar{k}^\times$. Similarly we have

$$U_R^+ = \{x \in R \mid x^{(n)} \in U_C^+\} = \mathrm{Hom}(\mathbb{Z}[1/p], U_C^+),$$

therefore we get the factorization

$$U_R = \bar{k}^\times \times U_R^+.$$

Since $(U_R^1)^{p^n} = \{x \in U_R^1 \mid v(x-1) \geq p^n\}$, the map

$$U_R^1 \xrightarrow{\sim} \varprojlim_{n \in \mathbb{N}} U_R^1/(U_R^1)^{p^n}$$

is an isomorphism of topological groups. Thus we may consider U_R^1 as a $\mathbb{Z}_p$-module which is certainly torsion free. For $x \in U_R^+$, $v(x-1) > 0$, then $v(x^{p^n} - 1) = p^n v(x-1) \geq 1$ for n large enough. Conversely, any element $x \in U_R^1$ has a unique p^n-th root in U_R^+. We get

$$\begin{aligned} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U_R^1 &\longrightarrow U_R^+ \\ p^{-n} \otimes u &\longmapsto u^{p^{-n}} \end{aligned}$$

is an isomorphism.

5.2 The action of Galois groups on R

As seen in the previous section, let $W = W(k)$, $K_0 = \mathrm{Frac}\, W$, then the group $G_{K_0} = \mathrm{Gal}(\overline{K}/K_0)$ acts on R and $\mathrm{Fr}\, R$ continuously via

$$g(x^{(n)})_{n \in \mathbb{N}} = (gx^{(n)})_{n \in \mathbb{N}}.$$

5.2.1 Elements invariant by closed subgroups of G_{K_0}.

Proposition 5.9. *Let L be an extension of K_0 contained in $\overline{K}$ and let $H = \mathrm{Gal}(\overline{K}/L)$. Then*

$$R^H = R(\mathcal{O}_L/p\mathcal{O}_L), \quad (\mathrm{Fr}\, R)^H = \mathrm{Frac}(R(\mathcal{O}_L/p\mathcal{O}_L)).$$

The residue field of R^H is $k_L = \bar{k}^H$, the residue field of L.

Proof. Assume $x \in R^H$(resp. $\mathrm{Fr}\, R^H$). Write

$$x = (x^{(n)})_{n\in\mathbb{N}},\ x^{(n)} \in \mathcal{O}_C(\text{resp. } C).$$

For $h \in H$, $h(x) = (h(x^{(n)}))_{n\in\mathbb{N}}$. Hence

$$x \in R^H(\text{resp. } \mathrm{Fr}\, R^H) \Longleftrightarrow x^{(n)} \in (\mathcal{O}_C)^H(\text{resp. } C^H),\ \text{for all } n \in N,$$

then the first assertion follows from the fact

$$C^H = \widehat{L}, \quad (\mathcal{O}_C)^H = \mathcal{O}_{C^H} = \mathcal{O}_{\widehat{L}} = \varinjlim_n \mathcal{O}_L/p^n\mathcal{O}_L.$$

The map $\bar{k} \hookrightarrow R \twoheadrightarrow \bar{k}$ induces the map $k_L \hookrightarrow R^H \twoheadrightarrow k_L$, and the composition map is nothing but the identity map, so the residue field of R^H is k_L.

Proposition 5.10. *If $v(L^\times)$ is discrete, then*

$$R(\mathcal{O}_L/p\mathcal{O}_L) = R^H = k_L.$$

This is the case if L is a finite extension of K_0.

Proof. From the proof of the previous proposition, we know $k_L \subset R^H = R(\mathcal{O}_L/p\mathcal{O}_L)$, it remains to show that

$$x = (x^{(n)})_{n\in\mathbb{N}} \in R^H,\ v(x) > 0 \Longrightarrow x = 0.$$

We have $v(x^{(n)}) = p^{-n}v(x^{(0)})$, but $v(\widehat{L}^\times) = v(L^\times)$ is discrete, so $v(x) = v(x^{(0)}) = +\infty$, which means that $x = 0$.

5.2.2 $R(K_0^{\mathrm{cyc}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}})$, ε and π.

We denote ε and π the following two elements inside R:

(i) $\varepsilon = (1, \varepsilon^{(1)}, \cdots)$ such that $\varepsilon^{(0)} = 1$ and $\varepsilon^{(1)} \neq 1$;
(ii) $\pi = \varepsilon - 1$.

Thus $\varepsilon^{(n)}$ is a primitive p^n-th root of unity in $\overline{K}$ satisfying the compatibility condition $(\varepsilon^{(n+1)})^p = \varepsilon^{(n)}$. Thus

$$L^{\mathrm{cyc}} = \bigcup_{n\in\mathbb{N}} L(\varepsilon^{(n)}).$$

Lemma 5.11. *The element $\varepsilon = (\varepsilon^{(n)})_{n\in\mathbb{N}}$ and π are elements in $R(\mathcal{O}_{K_0^{\mathrm{cyc}}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}})$, $v(\pi) = \frac{p}{p-1} > 1$ and $\varepsilon \in U_R^1$. Moreover, for $g \in G_{K_0}$,*

$$g(\varepsilon) = \varepsilon^{\chi(g)}, \qquad g(\pi) = (1+\pi)^{\chi(g)} - 1, \tag{5.9}$$

thus $\varepsilon^{\mathbb{Z}_p} \cong \mathbb{Z}_p(1)$ as G_{K_0}-modules.

Proof. Note that $\pi^{(0)} = \lim\limits_{m\to+\infty}(\varepsilon^{(m)}-1)^{p^m}$. Since $\varepsilon^{(0)}-1=0$, and $v(\varepsilon^{(m)}-1) = \frac{1}{(p-1)p^{m-1}}$ for $m \geq 1$, we have $v(\pi) = v(\pi^{(0)}) = \frac{p}{p-1} > 1$. Thus the element $\varepsilon = (\varepsilon^{(n)})_{n\in\mathbb{N}}$ is a unit of $R(\mathcal{O}_{K_0^{\mathrm{cyc}}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}})$ and belongs to U_R^1. The rest is clear.

Set $H = H_{K_0} = \mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}})$. Then $R^H = R(\mathcal{O}_{K_0^{\mathrm{cyc}}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}})$ whose residue field is k by Proposition 5.9. Since $\pi \in R^H$ and $v(\pi) = v_p(\pi^{(0)}) = \frac{p}{p-1} > 1$, the residue field $k \subset R^H$, and R^H is complete, we have

$$k[[\pi]] \subset R^H \text{ and } k((\pi)) \subset (\mathrm{Fr}\, R)^H.$$

If $x = (x^{(n)})_{n\in\mathbb{N}} \in R^H$ and $x = y^p$, then $y = (x^{(n+1)})_{n\in\mathbb{N}} \in R^H$, hence R^H and $(\mathrm{Fr}\, R)^H$ are both perfect and complete, we have

$$\widehat{k[[\pi]]^{\mathrm{rad}}} \subset R^H, \quad \widehat{k((\pi))^{\mathrm{rad}}} \subset (\mathrm{Fr}\, R)^H.$$

Theorem 5.12. *For $H = H_{K_0} = \mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}})$, we have*

$$\widehat{k[[\pi]]^{\mathrm{rad}}} = R^H, \quad \widehat{k((\pi))^{\mathrm{rad}}} = (\mathrm{Fr}\, R)^H.$$

Moreover, for $m \in \mathbb{N}$, the projection map

$$\theta_m : R \to O_{\overline{K}}/pO_{\overline{K}},\ \theta_m((x_n)_{n\in N}) = x_m$$

has image

$$\theta_m(R^H) = \mathcal{O}_{K_0^{\mathrm{cyc}}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}}.$$

Proof. Set $E_0 = k((\pi))$, $F = E_0^{\mathrm{rad}}$, $L = K_0^{\mathrm{cyc}} = \bigcup\limits_{n\geq 1} K_0(\varepsilon^{(n)})$. It suffices to check that $\mathcal{O}_{\widehat{F}}$ is dense in R^H, or even that $\mathcal{O}_F$ is dense in R^H. Since R^H is the inverse limit of $\mathcal{O}_L/p\mathcal{O}_L$, both assertions follow from

$$\theta_m(\mathcal{O}_F) = \mathcal{O}_L/p\mathcal{O}_L \quad \text{for all } m \in \mathbb{N}.$$

So it suffices to show that $\mathcal{O}_L/p\mathcal{O}_L \subset \theta_m(\mathcal{O}_F)$, for all m.

Set $\varpi_n = \varepsilon^{(n)} - 1$, then

$$\mathcal{O}_{K_0}[\varepsilon^{(n)}] = W[\varpi_n], \quad \mathcal{O}_L = \bigcup_{n=0}^{\infty} W[\varpi_n].$$

Write $\pi = (\pi_n)_{n\in\mathbb{N}}$. Then $\pi_n = \varepsilon_n - 1$ is also the image of ϖ_n in $\mathcal{O}_L/p\mathcal{O}_L$, thus $\mathcal{O}_L/p\mathcal{O}_L$ is a k-algebra generated as a k-algebra by π_n's. Since $k \subset \mathcal{O}_{E_0}$, we are reduced to prove

$$\pi_n \in \theta_m(\mathcal{O}_F) = \theta_m(k[[\pi]]^{\mathrm{rad}}), \quad \text{for all } m, n \in \mathbb{N}.$$

For all $s \in \mathbb{Z}$, $\pi^{p^{-s}} \in k[[\pi]]^{\mathrm{rad}}$, and

$$\begin{aligned}\pi^{p^{-s}} &= \varepsilon^{p^{-s}} - 1 = (\varepsilon^{(n+s)})_{n\in\mathbb{N}} - 1 \\ &= (\varepsilon_{n+s} - 1)_{n\in\mathbb{N}},\end{aligned}$$

where $\varepsilon^{(n)} = 1$ if $n < 0$. Since $\varepsilon_{n+s} - 1 = \pi_{n+s}$ for $n + s \geq 0$, let $s = n - m$, we get

$$\pi_n = \theta_m(\pi^{p^{m-n}}) \in \theta_m(k[[\pi]]^{\mathrm{rad}}).$$

This completes the proof.

5.2.3 A fundamental theorem.

Theorem 5.13. *Let E_0^s be the separable closure of $E_0 = k((\pi))$ in $\operatorname{Fr} R$, then E_0^s is dense in $\operatorname{Fr} R$, and is stable under G_{K_0}. Moreover, for any $g \in \operatorname{Gal}(\overline{K}/K_0^{\mathrm{cyc}})$,*

$$g|_{E_0^s} \in \operatorname{Gal}(E_0^s/E_0),$$

and the map $\operatorname{Gal}(\overline{K}/K_0^{\mathrm{cyc}}) \to \operatorname{Gal}(E_0^s/E_0)$, $g \mapsto g|_{E_0^s}$ is an isomorphism.

Proof. Let us first show that E_0^s is dense in $\operatorname{Fr} R$. As E_0^s is separably closed, $\widehat{E_0^s}$ is algebraically closed. Let $\overline{E}_0$ be the algebraic closure of E_0 in $\operatorname{Fr} R$. It is enough to check that $\overline{E}_0$ is dense in $\operatorname{Fr} R$. In other words, we need to prove that $\mathcal{O}_{\overline{E}_0}$ is dense in R. As R is the inverse limit of $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$, it is enough to show that

$$\theta_m(\mathcal{O}_{\overline{E}_0}) = \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}, \quad \text{for all } m \in \mathbb{N}.$$

As $\overline{E}_0$ is algebraically closed, it suffices to show that

$$\theta_0(\mathcal{O}_{\overline{E}_0}) = \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}.$$

Since $\mathcal{O}_{\overline{K}} = \varinjlim_{\substack{[L:K]<+\infty \\ L/K_0 \text{ Galois}}} \mathcal{O}_L$, it is enough to check that for any finite Galois extension L of K_0,

$$\mathcal{O}_L/p\mathcal{O}_L \subset \theta_0(\mathcal{O}_{\overline{E}_0}). \tag{5.10}$$

Let $K_{0,n} = K_0(\varepsilon^{(n)})$ and $L_n = K_{0,n}L$, then $L_n/K_{0,n}$ is Galois with Galois group $J_n = \operatorname{Gal}(L_n/K_{0,n})$ and for n large, we have $J_n = J_{n+1} = \cdots := J$. Since $\bar{k} \subset \mathcal{O}_{\overline{E}_0}$, replacing K_0 by a finite unramified extension, we may assume $L_n/K_{0,n}$ is totally ramified for any n.

Let ν_n be a generator of the maximal ideal of $\mathcal{O}_{L_n}$, then $\mathcal{O}_{L_n} = \mathcal{O}_{K_{0,n}}[\nu_n]$ since $L_n/K_{0,n}$ is totally ramified. Since $\theta_0(\mathcal{O}_{\overline{E}_0}) \supset \mathcal{O}_{K_{0,n}}/p\mathcal{O}_{K_{0,n}}$, to prove (5.10), it is enough to check that there exists n such that $\bar{\nu}_n \in \theta_0(\mathcal{O}_{\overline{E}_0})$, where $\bar{\nu}_n$ is the image of ν_n in $\mathcal{O}_{L_n}/p\mathcal{O}_{L_n}$.

Let $P_n(X) \in K_{0,n}[X]$ be the minimal polynomial of ν_n, which is an Eisenstein polynomial. When n is sufficiently large, P_n is of degree $d = |J|$. Write $P_n(X) = \prod_{g\in J}(X - g(\nu_n))$. We need the following lemma:

Lemma 5.14. *For any $g \in J$, $g \neq 1$, we have $v(g(\nu_n) - \nu_n) \to 0$ as $n \to +\infty$.*

Proof (Proof of the Lemma). This follows immediately from (1.53) and the proof of Proposition 1.95.

We will see that the lemma implies (5.10). Choose n such that $v(g(\nu_n) - \nu_n) < 1/d$ for all $g \neq 1$. Let $\overline{P_n}(X) \in \mathcal{O}_{K_{0,n}}[X]/p\mathcal{O}_{K_{0,n}}[X]$ be the polynomial $P_n(X) \pmod p$, We choose $Q(X) \in \mathcal{O}_{\overline{E}_0}[X]$, monic of degree d, a lifting of $\overline{P_n}$. Let x be a root of $Q(X)$. Write $\beta = \theta_0(x)$. Suppose $b \in \mathcal{O}_{\overline{K}}$ is a lifting of β, then there exists $g_0 \in J$ such that $v(b - g_0\nu_n) \geq v(b - g\nu_n)$ for all $g \in J$. Note that

$$P_n(b) = \prod_{g\in J}(b - g\nu_n), \quad \text{and} \quad v(P_n(b)) \geq 1,$$

then

$$v(g_0^{-1}b - \nu_n) = v(b_n - g_0\nu_n) \geq \frac{1}{d} > v(\nu_n - g(\nu_n)), \quad \text{for all } g \in J\backslash\{1\}.$$

By Krasner's Lemma, $\nu_n \in K_{0,n}(g_0^{-1}b)$, moreover, $\bar{\nu}_n \in \theta_0(\mathcal{O}_{\overline{E}_0})$. This proves (5.10) and the first part of the theorem.

For any $a \in E_0^s$, let $P(x) = \sum\limits_{i=0}^{d} \lambda_i X^i \in E_0[X]$ be a separable polynomial such that $P(a) = 0$. Then for any $g \in G_{K_0}$, $g(a)$ is a root of $g(P) = \sum\limits_{i=0}^{d} g(\lambda_i)X^i$. To prove $g(a) \in E_0^s$, it is enough to show $g(E_0) = E_0$, which follows from the fact

$$g(\pi) = (1+\pi)^{\chi(g)} - 1.$$

Moreover, for any $g \in \mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}})$, then $g(a)$ is a root of P. Thus for $g \in \mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}})$, $g|_{E_0^s} \in \mathrm{Gal}(E_0^s/E_0)$, in other words, we get a homomorphism

$$\mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}}) \longrightarrow \mathrm{Gal}(E_0^s/E_0).$$

We need to prove this homomorphism is an isomorphism.

Injectivity: g is in the kernel means that $g(a) = a$ for all $a \in E_0^s$, then $g(a) = a$ for all $a \in \mathrm{Fr}\, R$ because E_0^s is dense in $\mathrm{Fr}\, R$ and the action of g is continuous.

Let $a \in \mathrm{Fr}\, R$, then $a = (a^{(n)})_{n\in\mathbb{N}}$ with $a^{(n)} \in C$, and $(a^{(n+1)})^p = a^{(n)}$. $g(a) = a$ implies that $g(a^{(0)}) = a^{(0)}$, but the map $\theta_0 : \mathrm{Fr}\, R \to C$ is surjective, so g acts trivially on C, hence also on $\overline{K}$, we get $g = 1$.

Surjectivity: We identify $H = \mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}})$ with a closed subgroup of $\mathrm{Gal}(E_0^s/E_0)$ by injectivity. If the above map is not onto, we have

$$E_0 \subsetneq F = (E_0^s)^H \subset (\mathrm{Fr}\, R)^H = \widehat{E_0^{\mathrm{rad}}},$$

that is, F is a separable proper extension of E_0 contained in $\widehat{E_0^{\mathrm{rad}}}$. To finish the proof, we just need to prove the following lemma.

Lemma 5.15. *Let E be a complete field of characteristic $p > 0$. There is no nontrivial separable extension F of E contained in $\widehat{E^{\mathrm{rad}}}$.*

Proof. Otherwise, we could find a nontrivial finite separable extension E' of E contained in $\widehat{E^{\mathrm{rad}}}$. There are $d = [E' : E] > 1$ distinct E-embeddings $\sigma_1, \cdots, \sigma_d$ of E' to E^s. We can extend each σ_i to $E'^{\,\mathrm{rad}}$ in the natural way, that is, by setting $\sigma_i(a) = \sigma_i(a^{p^n})^{p^{-n}}$. This map is continuous, hence it can be extended to $\widehat{E'^{\,\mathrm{rad}}} = \widehat{E^{\mathrm{rad}}}$. But σ_i acts as the identity map on E^{rad}, so it acts as the identity map on $\widehat{E^{\mathrm{rad}}}$. This is a contradiction.

5.2.4 Fields in the *E*-series.

From now on, let $E_0 := k((\pi))$ and E_0^s be the separable closure of E_0 inside $\mathrm{Fr}\, R$.

Definition 5.16. *Set*

$$E^+ := \mathcal{O}_{E^s} \subset E = \mathrm{Frac}(E^+) := E_0^s, \tag{5.11}$$

$$\widetilde{E}^+ := R \subset \widetilde{E} = \mathrm{Fr}\, R. \tag{5.12}$$

Moreover, if L is a finite extension of K_0 inside $\overline{K}$, set

$$E_L^+ := (E^+)^{H_L}, \qquad E_L := E^{H_L}, \tag{5.13}$$

$$\widetilde{E}_L^+ := (\widetilde{E}^+)^{H_L}, \qquad E_L := \widetilde{E}^{H_L}. \tag{5.14}$$

Remark 5.17. The notion $^+$ means the ring of integer and $^\sim$ means the completion.

We can describe E_L and $\widetilde{E}_L$ explicitly.

Proposition 5.18. *For L a finite extension of K_0, let $n(L)$ be given by Lemma 4.11 and k_L^{c} be the residue field of L^{cyc}. Then*

$$E_L^+ = \{(x_n) \in R \mid x_n \in \mathcal{O}_{L(\varepsilon^{(n)})}/p,\ x_{n+1}^p = x_n \text{ for } n \geq n(L)\}, \tag{5.15}$$

$$\widetilde{E}_L^+ = R(\mathcal{O}_{L^{\mathrm{cyc}}}/p\mathcal{O}_{L^{\mathrm{cyc}}}) = \{(x_n) \mid x_n \in \mathcal{O}_{L^{\mathrm{cyc}}}/p,\ x_{n+1}^p = x_n\}, \tag{5.16}$$

and

$$E_L = E_L^+[\frac{1}{\overline{\pi}_L}] = k_L^{\mathrm{c}}((\overline{\pi}_L)),\ \widetilde{E}_L = \widetilde{E}_L^+[\frac{1}{\overline{\pi}_L}] = k_L^{\mathrm{c}}\widehat{((\overline{\pi}_L))}^{\mathrm{rad}}. \tag{5.17}$$

where $\overline{\pi}_L$ is any uniformizer of E_L.

Proof. By Proposition 5.9,

$$\widetilde{E}_L^+ = R(\mathcal{O}_{L^{\mathrm{cyc}}}/p) = \{(x_n) \mid x_n \in \mathcal{O}_{L^{\mathrm{cyc}}}/p,\ x_{n+1}^p = x_n\}.$$

By Theorem 5.13, $\widetilde{E}_L = \widehat{E_L^{\mathrm{rad}}}$. Thus the residue field of E_L is also k_L^c and $E_L = k_L^c((\pi_L))$, $\widetilde{E}_L = k_L^c\widehat{((\overline{\pi}_L))^{\mathrm{rad}}}$. E_L is the subfield of $\widetilde{E}_L$ such that $E_L^{H_{K_0}/H_L} = E_0$.

If $L = W(k_L^c)[\frac{1}{p}]$, let $n(L) = 0$, then $E_L^+ = k_L^c[[\pi]]$ and $E_L = k_L^c((\pi))$. One can easily check that (5.15) holds and $E_L = E_L^+[\frac{1}{\pi}]$.

In general, write $L_0 = W(k_L^c)[\frac{1}{p}]$. Then $E_L = E_{L_0}(\overline{\pi}_L)$. For $n \geq n(L)$, $\mathrm{Gal}(L(\varepsilon^{(n)})/L_0(\varepsilon^{(n)})) = \cdots = H_{L_0}/H_K := J$. Let

$$X = \{(x_n) \in R \mid x_n \in \mathcal{O}_{L(\varepsilon^{(n)})}/p,\ x_{n+1}^p = x_n \text{ for } n \geq n(L)\}.$$

Then $X^J = k_L^c[[\pi]] = E_{L_0}^+$, and $(\mathrm{Frac}\, X)^J = E_{L_0}$. If $\overline{\pi}_L \in X$, then $\mathrm{Frac}\, X = X[\frac{1}{\overline{\pi}_L}]$, the subfield of J-invariant elements of which is E_{L_0}, hence $\mathrm{Frac}\, X = E_L$ and $X = E_L^+$. We are reduced to show the existence of one uniformizer $\overline{\pi}_L$ of E_L in X.

For $n \geq n(L)$, we let $L(\varepsilon^{(n)}) = L_0(\varepsilon^{(n)})[\nu_n]$. We choose ν_n coherently such that $N_{L(\varepsilon^{(n+1)})/L(\varepsilon^{(n)})}(\nu_{n+1}) = \nu_n$. Then one can check the element $x = (x_n)_{n\in\mathbb{N}} \in X$ such that $x_n = \bar{\nu}_n$ is a uniformizer of E_L.

Note that $\mathbf{\Gamma}_{K_0} = G_{K_0}/H_{K_0}$ acts on E_0, then G_{K_0} acts on E and hence $\mathbf{\Gamma}_L$ acts on E_L. Set

$$\mathbf{E}_L = E^{\mathbf{H}_L} = E_L^{\Delta_L}, \tag{5.18}$$

then $\mathbf{E}_L/E_L$ is a Galois extension with Galois group $\mathrm{Gal}(\mathbf{E}_L/E_L) = \Delta_L$. Set $\mathbf{E}_0 := \mathbf{E}_{K_0}$.

Lemma 5.19. (1) *If $p \neq 2$, set*

$$\overline{\pi}_0 := \sum_{a\in\mathbb{F}_p} \varepsilon^{[a]}, \tag{5.19}$$

where $[a] \in \mathbb{Z}_p$ is the Teichmüller representative of a, then

(i) $\overline{\pi}_0 \in \mathbf{E}_0$ *and* $\overline{\pi}_0 = \pi^{p-1}\lambda$ *with* $\lambda \equiv 1 \bmod \pi$.
(ii) $\mathbf{E}_0 = k((\overline{\pi}_0))$.

(2) *If $p = 2$, set $\overline{\pi}_0 := \pi + \pi^{-1}$. Then $\mathbf{E}_0 == k((\overline{\pi}_0))$.*

Proof. Exercise.

In conclusion, we have Fig. 5.1.

5.3 Basic theory of (φ, Γ)-modules

5.3.1 The field $W(\mathrm{Fr}\, R)[\frac{1}{p}]$ and its subrings.

Consider the Witt vectors of R and $\mathrm{Fr}\, R$, we have the following rings:

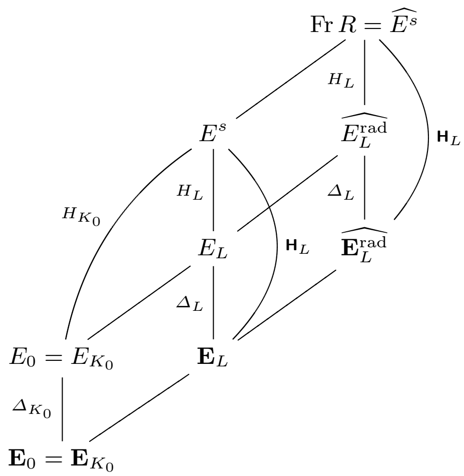


Fig. 5.1. Galois extensions of E and E_0

$$W(R) \subset W(R)[\frac{1}{p}] \subset W(\mathrm{Fr}\, R)[\frac{1}{p}],$$
$$W(R) \subset W(\mathrm{Fr}\, R) \subset W(\mathrm{Fr}\, R)[\frac{1}{p}].$$

Note that the ring $W(\mathrm{Fr}\, R)$ is a complete discrete valuation ring whose maximal ideal is generated by p and residue field is the algebraically closed field $\mathrm{Fr}\, R$, $W(\mathrm{Fr}\, R)[\frac{1}{p}]$ is the field of fractions of $W(\mathrm{Fr}\, R)$, and $W(R)[\frac{1}{p}]$ is a subring of $W(\mathrm{Fr}\, R)[\frac{1}{p}]$. The ring $W := W(k) \subset W(R)$.

The Galois group G_{K_0} (and therefore G_K) acts naturally on $W(\mathrm{Fr}\, R)$ and $W(\mathrm{Fr}\, R))[\frac{1}{p}]$. Denote by φ the Frobenius map on $W(\mathrm{Fr}\, R)[\frac{1}{p}]$ and on $W(\mathrm{Fr}\, R))[\frac{1}{p}]$. Then φ commutes with the action of G_{K_0}: $\varphi(ga) = g\varphi(a)$ for any $g \in G_{K_0}$ and $a \in \widetilde{B}$. Moreover, $W(R)$ and $W(R)[\frac{1}{p}]$ is stable under φ- and G_{K_0}-actions.

We know that $E_0 = k((\pi)) \subset \mathrm{Fr}\, R$ and $k[[\pi]] \subset R$. Let $[\varepsilon] = (\varepsilon, 0, 0, \cdots) \in W(R)$ be the Teichmüller representative of ε. Set

$$\boldsymbol{\pi} = [\varepsilon] - 1 \in W(R). \tag{5.20}$$

Then $\boldsymbol{\pi} = (\pi, *, *, \cdots)$ is a lifting of π. By the isomorphism

$$W(R) = \varprojlim W_n(R) = \varprojlim W(R)/p^n W(R)$$

where $W_n(R) = \{(a_0, \cdots, a_{n-1}) \mid a_i \in R\}$ is a topological ring induced by the valuation topology of R, the natural topology of $W(R)$ is nothing but the $(p, \boldsymbol{\pi})$-topology. The series

$$\sum_{n=0}^{\infty} \lambda_n \boldsymbol{\pi}^n, \quad \lambda_n \in W,\ n \in \mathbb{N},$$

converges in $W(R)$, which gives a continuous embedding

$$W[[\boldsymbol{\pi}]] \hookrightarrow W(R).$$

We identify $W[[\boldsymbol{\pi}]]$ with a closed subring of $W(R)$.

The element $\boldsymbol{\pi}$ is invertible in $W(\mathrm{Fr}\, R)$, hence

$$W((\boldsymbol{\pi})) = W[[\boldsymbol{\pi}]][\frac{1}{\boldsymbol{\pi}}] \subset W(\mathrm{Fr}\, R)$$

whose elements are of the form

$$\sum_{n=-\infty}^{+\infty} \lambda_n \boldsymbol{\pi}^n : \ \lambda_n \in W,\ \lambda_n = 0 \text{ for } n \ll 0.$$

Since $W(\mathrm{Fr}\, R)$ is complete, this inclusion extends by continuity to

$$\mathcal{O}_{\mathcal{E}_0} := \left\{ \sum_{n=-\infty}^{+\infty} \lambda_n \boldsymbol{\pi}^n |\ \lambda_n \in W,\ \lambda_n \to 0 \text{ when } n \to -\infty \right\}, \tag{5.21}$$

the p-adic completion of $W((\boldsymbol{\pi}))$.

Note that $\mathcal{O}_{\mathcal{E}_0}$ is a complete discrete valuation ring, whose maximal ideal is generated by p and whose residue field is E_0, thus is the Cohen ring of E_0. Let $\mathcal{E}_0 = \mathcal{O}_{\mathcal{E}_0}[\frac{1}{p}]$ be its fraction field, then $\mathcal{E}_0 \subset \widetilde{B}$.

Note that $\mathcal{O}_{\mathcal{E}_0}$ and $\mathcal{E}_0$ are both stable under φ and G_{K_0}. Moreover

$$\varphi([\varepsilon]) = (\varepsilon^p, 0, \cdots) = [\varepsilon]^p, \text{ and } \varphi(\boldsymbol{\pi}) = (1+\boldsymbol{\pi})^p - 1. \tag{5.22}$$

The group G_{K_0} acts through $\boldsymbol{\Gamma}_{K_0}$: for $g \in G_{K_0}$,

$$g([\varepsilon]) = (\varepsilon^{\chi(g)}, 0, \cdots) = [\varepsilon]^{\chi(g)},$$

therefore

$$g(\boldsymbol{\pi}) = (1+\boldsymbol{\pi})^{\chi(g)} - 1. \tag{5.23}$$

Let

$$\pi_0 = -p + \sum_{a \in \mathbb{F}_p} [\varepsilon]^{[a]} \text{ (or } [\varepsilon] + [\varepsilon^{-1}] - 2 \text{ if } p = 2),$$

then $\boldsymbol{\mathcal{E}}_0 = \mathcal{E}_0^{\Delta_{K_0}}$, whose ring of integers is just the p-adic completion of $W((\pi_0))$ and the Cohen ring of $\mathbf{E}_0 = k((\overline{\pi}_0))$.

Proposition 5.20. *For any finite extension F of E_0 contained in $E^s = E_0^s$, there is a unique finite extension $\mathcal{E}_F$ of $\mathcal{E}_0$ contained in $\widetilde{B}$ which is unramified and whose residue field is F.*

Proof. By general theory on unramified extensions, we can assume $F = E_0(a)$ is a simple separable extension, and $P(X) \in E_0[X]$ is the minimal polynomial of a over E_0. Choose $Q(X) \in \mathcal{O}_{\mathcal{E}_0}[X]$ to be a monic polynomial lifting of P. By Hensel's lemma, there exists a unique $\alpha \in \widetilde{B}$ such that $Q(\alpha) = 0$ and the image of α in $\mathrm{Fr}\, R$ is a, then $\mathcal{E}_F = \mathcal{E}_0(\alpha)$ is what we required.

By the above proposition,

$$\mathcal{E}_0^{\mathrm{ur}} = \bigcup_F \mathcal{E}_F \subset \widetilde{B}, \tag{5.24}$$

where F runs through all finite separable extension of E_0 contained in E^s. Let $\widehat{\mathcal{E}_0^{\mathrm{ur}}}$ be the p-adic completion of $\mathcal{E}_0^{\mathrm{ur}}$ in $\widetilde{B}$, then $\widehat{\mathcal{E}_0^{\mathrm{ur}}}$ is a discrete valuation field whose residue field is E^s and whose maximal ideal is generated by p.

We have

$$\mathrm{Gal}(\mathcal{E}_0^{\mathrm{ur}}/\mathcal{E}_0) = \mathrm{Gal}(E_0^s/E_0) = H_{K_0}, \quad \mathrm{Gal}(\mathcal{E}_0^{\mathrm{ur}}/\boldsymbol{\mathcal{E}}_0) = \mathrm{Gal}(E_0^s/\mathbf{E}_0) = \mathsf{H}_{K_0}.$$

Set

$$(\mathcal{E}_0^{\mathrm{ur}})^{H_K} = \mathcal{E}_K := \mathcal{E}, \quad (\mathcal{E}_0^{\mathrm{ur}})^{\mathsf{H}_K} = \boldsymbol{\mathcal{E}}_K := \boldsymbol{\mathcal{E}}, \tag{5.25}$$

then $\mathcal{E}$ (resp. $\boldsymbol{\mathcal{E}}$) is again a complete discrete valuation field whose residue field is E (resp. $\mathbf{E}$) and whose maximal ideal is generated by p, and $\mathcal{E}_0^{\mathrm{ur}}/\mathcal{E}$ (resp. $\mathcal{E}_0^{\mathrm{ur}}/\boldsymbol{\mathcal{E}}$) is a Galois extension with the Galois group $\mathrm{Gal}(\mathcal{E}_0^{\mathrm{ur}}/\mathcal{E}) = H_K$ (resp. $\mathbf{H}_K$). Set

$$\mathcal{E}^{\mathrm{ur}} = \mathcal{E}_0^{\mathrm{ur}}, \quad \widehat{\mathcal{E}^{\mathrm{ur}}} = \widehat{\mathcal{E}_0^{\mathrm{ur}}}.$$

It is easy to check that $\mathcal{E}$ (resp. $\boldsymbol{\mathcal{E}}$) is stable under φ, and also stable under G_K, which acts through $\mathbf{\Gamma}_K$ (resp. Γ_K).

Replacing E and $\mathbf{E}$ by E_L and $\mathbf{E}_L$ for L a finite extension of K_0, one gets the corresponding $\mathcal{E}_L$ and $\boldsymbol{\mathcal{E}}_L$, whose residue fields are E_L and $\mathbf{E}_L$ respectively.

We have Fig.5.2 .

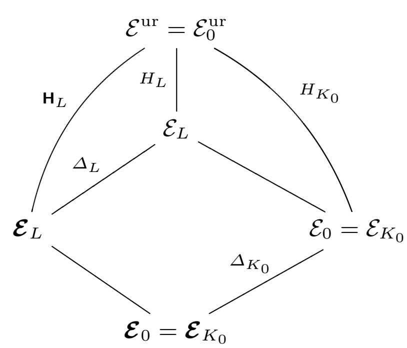


Fig. 5.2. Galois extensions of $\mathcal{E}$ and $\mathcal{E}_0$.

5.3.2 Basic theory of (φ, Γ)-modules.

Suppose T is a $\mathbb{Z}_p$-representation of $H_K = \mathrm{Gal}(\overline{K}/K^{\mathrm{cyc}})$ which equals $\mathrm{Gal}(E^s/E) = \mathrm{Gal}(\mathcal{E}^{\mathrm{ur}}/\mathcal{E})$, then

$$\mathbf{M}(T) = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T)^{H_K} \tag{5.26}$$

is an étale φ-module over $\mathcal{O}_{\mathcal{E}}$. By Theorem 3.34, $\mathbf{M}$ defines an equivalence of categories from $\mathbf{Rep}_{\mathbb{Z}_p}(H_K)$, the category of $\mathbb{Z}_p$-representations of H_K to $\mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{O}_{\mathcal{E}})$, the category of étale φ-modules over $\mathcal{O}_{\mathcal{E}}$, with a quasi-inverse functor given by

$$\mathbf{T} : M \longmapsto (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M)_{\varphi=1}. \tag{5.27}$$

If instead, suppose V is a p-adic Galois representation of H_K. Then by Theorem 3.35,

$$\mathbf{D} : V \longmapsto (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V)^{H_K} \tag{5.28}$$

defines an equivalence of categories from $\mathbf{Rep}_{\mathbb{Q}_p}(H_K)$, the category of p-adic representations of H_K to $\mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{E})$, the category of étale φ-modules over $\mathcal{E}$, with a quasi-inverse functor given by

$$\mathbf{V} : D \longmapsto (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} D)_{\varphi=1}. \tag{5.29}$$

Now assume V is a $\mathbb{Z}_p$ or p-adic Galois representation of G_K, set

$$\mathbf{D}(V) := (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} V)^{H_K} \text{ or } \mathbf{D}(V) := (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V)^{H_K}. \tag{5.30}$$

Definition 5.21. *A (φ, Γ)-module D over $\mathcal{O}_{\mathcal{E}}$ (resp. $\mathcal{E}$) is a φ-module over $\mathcal{O}_{\mathcal{E}}$ (resp. $\mathcal{E}$) together with an action of $\mathbf{\Gamma}_K$ which is semi-linear, and commutes with φ. D is called* étale *if it is an étale φ-module and the action of $\mathbf{\Gamma}_K$ is continuous.*

If V is a $\mathbb{Z}_p$ or p-adic representation of G_K, $\mathbf{D}(V)$ is an étale (φ, Γ)-module. Moreover, by Theorems 3.34 and 3.35, we have

Theorem 5.22. $\mathbf{D}$ *induces an equivalence of categories between $\mathbf{Rep}_{\mathbb{Z}_p}(G_K)$ (resp. $\mathbf{Rep}_{\mathbb{Q}_p}(G_K)$), the category of $\mathbb{Z}_p$ (resp. p-adic) representations of G_K and $\mathscr{M}_{\varphi,\Gamma}^{\text{ét}}(\mathcal{O}_{\mathcal{E}})$ (resp. $\mathscr{M}_{\varphi,\Gamma}^{\text{ét}}(\mathcal{E})$), the category of étale (φ, Γ)-modules over $\mathcal{O}_{\mathcal{E}}$ (resp. $\mathcal{E}$), with a quasi-inverse functor*

$$\mathbf{V}(D) = \left(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} D\right)_{\varphi=1} \quad (\textit{resp. } \left(\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} D\right)_{\varphi=1}) \tag{5.31}$$

and G_K acting on $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} D$ and $\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} D$ by

$$g(\lambda \otimes d) = g(\lambda) \otimes \bar{g}(d)$$

where $\bar{g}$ is the image of $g \in G_K$ in $\mathbf{\Gamma}_K$. Actually, this is an equivalence of Tannakian categories.

Remark 5.23. To be more precise, (φ, Γ)-modules in the above definition are actually $(\varphi, \mathbf{\Gamma}_K)$-modules. If set

$$\mathbf{D}'(V) := (\widehat{\mathcal{E}_0^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V)^{\mathsf{H}_K}, \tag{5.32}$$

then $\mathbf{D}'(V)$ is an étale (φ, Γ_K)-module over $\boldsymbol{\mathcal{E}} = (\mathcal{E}^{\mathrm{ur}})^{\mathsf{H}_K}$, and

$$\mathbf{D}'(V) = (\mathbf{D}(V))^{\Delta_K}, \quad \Delta_K = \mathrm{Gal}(\mathcal{E}/\boldsymbol{\mathcal{E}}).$$

However, by Hilbert's Theorem 90, the map

$$\mathcal{E} \otimes_{\boldsymbol{\mathcal{E}}} \mathbf{D}'(V) \xrightarrow{\sim} \mathbf{D}(V)$$

is an isomorphism. Thus both $\mathscr{M}^{\text{ét}}_{\varphi,\mathbf{\Gamma}}(\boldsymbol{\mathcal{E}})$ and $\mathscr{M}^{\text{ét}}_{\varphi,\Gamma}(\mathcal{E})$ are equivalence of categories with $\mathbf{Rep}_{\mathbb{Q}_p}(G_K)$. For $\mathbb{Z}_p$-representations, the corresponding result is also true.

Example 5.24. If $K = K_0 = W(k)[\frac{1}{p}]$, $W = W(k)$, then $\mathcal{E} = \mathcal{E}_0 = \widehat{W((\boldsymbol{\pi}))}[\frac{1}{p}]$. If $V = \mathbb{Z}_p$, then $\mathbf{D}(V) = \mathcal{O}_{\mathcal{E}_0} = \widehat{W((\boldsymbol{\pi}))}$ with the (φ, Γ)-action given by

$$\varphi(\boldsymbol{\pi}) = (1+\boldsymbol{\pi})^p - 1, \quad g(\boldsymbol{\pi}) = (1+\boldsymbol{\pi})^{\chi(g)} - 1. \tag{5.33}$$

Remark 5.25. We give some remarks about a (φ, Γ)-module D of dimension d over $\mathcal{E}$. Let $(e_1, \cdots, e_d)$ be a basis of D, then

$$\varphi(e_j) = \sum_{i=1}^d a_{ij} e_i.$$

To give φ is equivalent to giving a matrix $A = (a_{ij}) \in \mathrm{GL}_d(\mathcal{E})$. If $\mathbf{\Gamma}_K$ is pro-cyclic (i.e. if $p \neq 2$ or $\boldsymbol{\mu}_4 \subset K$), let γ_0 be a topological generator of $\mathbf{\Gamma}_K$,

$$\gamma_0(e_j) = \sum_{i=1}^d b_{ij} e_i.$$

To give the action of γ_0 is equivalent to giving a matrix $B = (b_{ij}) \in \mathrm{GL}_d(\mathcal{E})$. Moreover, we may choose the basis such that $A, B \in \mathrm{GL}_d(\mathcal{O}_{\mathcal{E}})$.

Exercise 5.26. (1) Find the necessary and sufficient conditions on D such that the action of γ_0 can be extended to an action of Γ_K.

(2) Find formulas relying A and B equivalent to the requirement that φ and Γ commute.

(3) Given (A_1, B_1), (A_2, B_2) two pairs of matrices in $\mathrm{GL}_d(\mathcal{E})$ satisfying the required conditions. Find a necessary and sufficient condition such that the associated representations are isomorphic.

For the theory of (φ, Γ)-modules, the operator ψ is extremely important.

Lemma 5.27. (1) $\{1, \varepsilon, \cdots, \varepsilon^{p-1}\}$ *is a basis of* E_0 *over* $\varphi(E_0)$*;*

(2) $\{1, \varepsilon, \cdots, \varepsilon^{p-1}\}$ *is a basis of* E_K *over* $\varphi(E_K)$*;*

(3) $\{1, \varepsilon, \cdots, \varepsilon^{p-1}\}$ *is a basis of* E^s *over* $\varphi(E^s)$*;*

(4) $\{1, [\varepsilon], \cdots, [\varepsilon]^{p-1}\}$ *is a basis of* $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$ *over* $\varphi(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}})$.

Proof. (1) Since $E_0 = k((\pi))$ with $\pi = \varepsilon - 1$, we have $\varphi(E_0) = k((\pi^p))$;

(2) Use the following diagram of fields, note that E_K/E_0 is separable but $E_0/\varphi(E_0)$ is purely inseparable:

$$\begin{tikzcd} E_0 \arrow[r, dash] \arrow[d, dash] & E_K \arrow[d, dash] \\ \varphi(E_0) \arrow[r, dash] & \varphi(E_K) \end{tikzcd}$$

We note the statement is still true if replacing K by any finite extension L over K_0.

(3) Because $E^s = \bigcup_L E_L$.

(4) To show that

$$(x_0, x_1, \cdots, x_{p-1}) \in \mathcal{O}^p_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \overset{\sim}{\longmapsto} \sum_{i=0}^{p-1} [\varepsilon]^i \varphi(x_i) \in \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$$

is a bijection, by the completeness of $\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$, it suffices to check it $\bmod p$, which is nothing but (3).

Definition 5.28. *The operator* $\psi : \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$ *is an additive defined by*

$$\psi(\sum_{i=0}^{p-1} [\varepsilon]^i \varphi(x_i)) = x_0. \tag{5.34}$$

Proposition 5.29. *The followings are true:*

(1) $\psi\varphi = \mathrm{Id}$*;*
(2) ψ *commutes with* G_{K_0}.

Proof. (1) The first statement is obvious.

(2) Note that

$$g(\sum_{i=0}^{p-1} [\varepsilon]^i \varphi(x_i)) = \sum_{i=0}^{p-1} [\varepsilon]^{i\chi(g)} \varphi(g(x_i)).$$

If for $1 \leq i \leq p-1$, write $i\chi(g) = i_g + pj_g$ with $1 \leq i_g \leq p-1$, then

$$\psi(\sum_{i=0}^{p-1} [\varepsilon]^{i\chi(g)} \varphi(g(x_i))) = \psi(\varphi(g(x_0)) + \sum_{i=1}^{p-1} [\varepsilon]^{i_g} \varphi([\varepsilon]^{j_g} g(x_i))) = g(x_0).$$

Corollary 5.30. (1) *If V is a $\mathbb{Z}_p$-representation of G_K, there exists a unique additive operator $\psi : \mathbf{D}(V) \to \mathbf{D}(V)$ such that*

$$\psi(\varphi(a)x) = a\psi(x), \quad \psi(a\varphi(x)) = \psi(a)x \tag{5.35}$$

if $a \in \mathcal{O}_{\mathcal{E}_K}, x \in \mathbf{D}(V)$ and moreover ψ commute with $\mathbf{\Gamma}_K$.

(2) *If D is an étale (φ, Γ)-module over $\mathcal{O}_{\mathcal{E}_K}$ or $\mathcal{E}_K$, there exists a unique additive operator $\psi : D \to D$ satisfying* (5.35)*. Moreover, for any $x \in D$,*

$$x = \sum_{i=0}^{p^n-1} [\varepsilon]^i \varphi^n(x_i) \tag{5.36}$$

where $x_i = \psi^n([\varepsilon]^{-i}x)$.

Proof. (1) The uniqueness follows from $\mathcal{O}_{\mathcal{E}} \otimes_{\varphi(\mathcal{O}_{\mathcal{E}})} \varphi(D) = D$. For the existence, first define ψ on $\mathcal{O}_{\mathcal{E}} \otimes V \supset \mathbf{D}(V)$ by $\psi(a \otimes v) = \psi(a)v$. $\mathbf{D}(V)$ is stable under ψ because ψ commutes with H_K, ψ commutes with Γ_K^c because ψ commutes with G_{K_0}.

(2) Since $D = \mathbf{D}(\mathbf{V}(D))$, we have the existence and uniqueness of ψ. (5.36) follows by induction on n.

Remark 5.31. From the proof, we can define an operator ψ satisfying (5.35) but not the commutativity of the action of Γ_K^c for any étale φ-module D.

Example 5.32. For $\mathcal{O}_{\mathcal{E}_0} \supset \mathcal{O}_{\mathcal{E}_0}^+ = W[[\boldsymbol{\pi}]]$, $[\varepsilon] = 1 + \boldsymbol{\pi}$, let $x = F(\boldsymbol{\pi}) \in \mathcal{O}_{\mathcal{E}_0}^+$, then $\varphi(x) = F((1+\boldsymbol{\pi})^p - 1)$. Write

$$F(\boldsymbol{\pi}) = \sum_{i=0}^{p-1} (1+\pi)^i F_i((1+\boldsymbol{\pi})^p - 1),$$

then $\psi(F(\boldsymbol{\pi})) = F_0(\boldsymbol{\pi})$. It is easy to see if $F(\boldsymbol{\pi})$ belongs to $W[[\boldsymbol{\pi}]]$, $F_i(\boldsymbol{\pi})$ belongs to $W[[\boldsymbol{\pi}]]$ for all i. Hence $\psi(\mathcal{O}_{\mathcal{E}_0}^+) \subset \mathcal{O}_{\mathcal{E}_0}^+ = W[[\boldsymbol{\pi}]]$. Consequently, ψ is continuous on $\mathcal{E}_0$ for the natural topology (the $(p, \boldsymbol{\pi})$-topology).

Moreover, we have:

$$\begin{aligned}\varphi(\psi(F)) =& F_0((1+\boldsymbol{\pi})^p - 1) = \frac{1}{p} \sum_{z^p=1} \sum_{i=0}^{p-1} (z(1+\boldsymbol{\pi}))^i F_i((z(1+\boldsymbol{\pi}))^p - 1) \\ =& \frac{1}{p} \sum_{z^p=1} F(z(1+\boldsymbol{\pi}) - 1).\end{aligned}$$

Proposition 5.33. *If D is an étale φ-module over $\mathcal{O}_{\mathcal{E}_0}$, then ψ is continuous for the weak topology. Thus ψ is continuous for any an étale φ-module D over $\mathcal{O}_{\mathcal{E}}$ in the weak topology.*

Proof. For the first part, choose $e_1, e_2, \cdots, e_d$ in D, such that

$$D = \bigoplus (\mathcal{O}_{\mathcal{E}_0}/p^{n_i})e_i, \quad n_i \in \mathbb{N} \cup \{\infty\}.$$

Since D is étale, we have $D = \bigoplus (\mathcal{O}_{\mathcal{E}_0}/p^{n_i})\varphi(e_i)$. Then we have the following diagram:

$$\begin{tikzcd} D \arrow[r, "\psi"] \arrow[d, "\wr"] & D \arrow[d, "\wr"] \\ \bigoplus (\mathcal{O}_{\mathcal{E}_0}/p^{n_i})\varphi(e_i) \arrow[r] & \bigoplus (\mathcal{O}_{\mathcal{E}_0}/p^{n_i})e_i \end{tikzcd}$$

$$\sum x_i \varphi(e_i) \longmapsto \sum \psi(x_i)e_i$$

Now since $x \mapsto \psi(x)$ is continuous in $\mathcal{O}_{\mathcal{E}_0}$, the map ψ is continuous in D.

The second part follows from the fact that $\mathcal{O}_{\mathcal{E}}$ is a free module of $\mathcal{O}_{\mathcal{E}_0}$ of finite rank, and an étale φ-module over $\mathcal{O}_{\mathcal{E}}$ is also étale over $\mathcal{O}_{\mathcal{E}_0}$.

6

Hodge-Tate and de Rham representations

6.1 The ring B_{HT} and Hodge-Tate representations

We recall the Tate module $\mathbb{Z}_p(1) = T_p(\mathbb{G}_m) \cong \mathbb{Z}_p \cdot t$ of the multiplicative group is a free $\mathbb{Z}_p$ of rank 1, with G_K-action via the cyclotomic character χ:

$$g(t) = \chi(g)t, \qquad \chi : G_K \to \mathbb{Z}_p^*.$$

For $i \in \mathbb{Z}$, the Tate twist $\mathbb{Z}_p(i) = \mathbb{Z}_p t^i$ is the free $\mathbb{Z}_p$-module with G_K-action through χ^i. Moreover, for a $\mathbb{Z}_p$-module M and $i \in \mathbb{Z}$, the *i-th Tate twist* of M is $M(i) = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(i)$. Then

$$M \to M(i), \quad x \mapsto x \otimes t^i$$

is an isomorphism of $\mathbb{Z}_p$-modules. Moreover, if G_K acts on M, it acts on $M(i)$ through

$$g(x \otimes u) = gx \otimes gu = \chi^i(g) gx \otimes u.$$

One sees immediately the above isomorphism in general does not commute with the action of G_K.

Recall $C = \widehat{\overline{K}}$.

Definition 6.1. *The ring of periods of Hodge-Tate, the* Hodge-Tate ring B_{HT} *is defined to be*

$$B_{\mathrm{HT}} = \bigoplus_{i \in \mathbb{Z}} C(i) = C[t, \frac{1}{t}]$$

where the element $c \otimes t^i \in C(i) = C \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(i)$ is denoted as ct^i, equipped with a multiplicative structure by

$$ct^i \cdot c' t^j = cc' t^{i+j}.$$

We have

$$B_{\mathrm{HT}} \subset \widehat{B_{\mathrm{HT}}} = C((t)) = \{ \sum_{i=-\infty}^{+\infty} c_i t^i, c_i = 0, \text{if } i \ll 0. \}$$

Proposition 6.2. *The ring B_{HT} is $(\mathbb{Q}_p, G_K)$-regular, which means that*

(1) *B_{HT} is a domain;*
(2) $(\mathrm{Frac}\, B_{\mathrm{HT}})^{G_K} = B_{\mathrm{HT}}^{G_K} = K$;
(3) *For every $b \in B_{\mathrm{HT}}, b \neq 0$ such that $g(b) \in \mathbb{Q}_p b$, for all $g \in G_K$, then b is invertible.*

Proof. (1) is trivial.

(2) Note that $B_{\mathrm{HT}} \subset \mathrm{Frac}\, B_{\mathrm{HT}} \subset \widehat{B_{\mathrm{HT}}}$, it suffices to show that $(\widehat{B_{\mathrm{HT}}})^{G_K} = K$.

Let $b = \sum\limits_{i \in \mathbb{Z}} c_i t^i,\ c_i \in C$, then for $g \in G_K$,

$$g(b) = \sum g(c_i)\chi^i(g)t^i.$$

For all $g \in G_K$, $g(b) = b$, it is necessary and sufficient that each $c_i t^i$ is fixed by G_K, i.e., $c_i t^i \in C(i)^{G_K}$. By Corollary 4.45, we have $C^{G_K} = K$ and $C(i)^{G_K} = 0$ if $i \neq 0$. This completes the proof of (2).

(3) Assume $0 \neq b = \sum c_i t^i \in B_{\mathrm{HT}}$ such that

$$g(b) = \eta(g)b,\ \eta(g) \in \mathbb{Q}_p,\ \text{for all } g \in G_K.$$

Then $g(c_i)\chi^i(g) = \eta(g)c_i$ for all $i \in \mathbb{Z}$ and $g \in G_K$. Hence

$$g(c_i) = (\eta\chi^{-i})(g)c_i.$$

For all i such that $c_i \neq 0$, then $\mathbb{Q}_p c_i$ is a one-dimensional sub $\mathbb{Q}_p$-vector space of C stable under G_K. Thus the one-dimensional representation associated to the character $\eta\chi^{-i}$ is C-admissible. This means that, by Tate's Theorem (Corollary 4.45), for all i such that $c_i \neq 0$ the action of I_K through $\eta\chi^{-i}$ is finite, which can be true for at most one i. Thus there exists $i_0 \in \mathbb{Z}$ such that $b = c_{i_0} t^{i_0}$ with $c_{i_0} \neq 0$, hence b is invertible in B_{HT}.

Definition 6.3. *A p-adic representation V of G_K is called* Hodge-Tate *if it is B_{HT}-admissible.*

Let V be any p-adic representation, define

$$\mathbf{D}_{\mathrm{HT}}(V) := (B_{\mathrm{HT}} \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

By Theorem 3.14 and Proposition 6.2, we have

Proposition 6.4. *For any p-adic representation V, the canonical map*

$$\alpha_{\mathrm{HT}}(V) : B_{\mathrm{HT}} \otimes_K \mathbf{D}_{\mathrm{HT}}(V) \longrightarrow B_{\mathrm{HT}} \otimes_{\mathbb{Q}_p} V$$

is injective and $\dim_K \mathbf{D}_{\mathrm{HT}}(V) \leqslant \dim_{\mathbb{Q}_p} V$. V is Hodge-Tate if and only if the equality

$$\dim_K \mathbf{D}_{\mathrm{HT}}(V) = \dim_{\mathbb{Q}_p} V$$

holds.

Proposition 6.5. *For a p-adic representation V to be Hodge-Tate, it is necessary and sufficient that Sen's operator Θ of the C-representation $W = C\otimes_{\mathbb{Q}_p} V$ is semi-simple and that its eigenvalues belong to $\mathbb{Z}$.*

Proof. If V is Hodge-Tate, then

$$W_i = (C(i) \otimes_{\mathbb{Q}_p} V)^{G_K}(-i) \otimes_K C$$

is a subspace of W and $W = \oplus W_i$. One sees that the operator Θ_{W_i} is just the multiplication-by-i map (cf Example 4.37). Therefore the condition is necessary.

To show this is also sufficient, since Θ is semi-simple, we can decompose W into the eigenspaces W_i of Θ, where Θ is the multiplication-by-i map on W_i. Then $\Theta = 0$ on $W_i(-i)$ and by Theorem 4.40, we have

$$W_i(-i) = C \otimes_K (W_i(-i))^{G_K}.$$

Therefore

$$\dim_K \mathbf{D}_{\mathrm{HT}}(V) \geq \sum_i \dim_K (W_i(-i))^{G_K} = \sum_i \dim_C W_i = \dim_{\mathbb{Q}_p} V$$

and V is Hodge-Tate.

For a p-adic representation V, $\mathbf{D}_{\mathrm{HT}}(V)$ is actually a graded K-vector space

$$\mathbf{D}_{\mathrm{HT}}(V) = \bigoplus_{i\in\mathbb{Z}} \mathrm{gr}^i\, \mathbf{D}_{\mathrm{HT}}(V),$$

where $\mathrm{gr}^i\, \mathbf{D}_{\mathrm{HT}}(V) = (C(i) \otimes_{\mathbb{Q}_p} V)^{G_K}$.

Definition 6.6. *The* Hodge-Tate numbers *of a p-adic representation V of G_K are those*

$$h_i := \dim_K (C(-i) \otimes V)^{G_K} \neq 0$$

for $i \in \mathbb{Z}$

Example 6.7. Let E be an elliptic curve over K, then $V_p(E) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(E)$ is a 2-dimensional Hodge-Tate representation, and

$$\dim(C \otimes_{\mathbb{Q}_p} V_p(E))^{G_K} = \dim(C(-1) \otimes_{\mathbb{Q}_p} V_p(E))^{G_K} = 1.$$

Thus the Hodge-Tate numbers are $h_0 = 1$ and $h_1 = 1$.

Let V be a p-adic representation of G_K, define

$$\mathrm{gr}^i\, \mathbf{D}^*_{\mathrm{HT}}(V) = (\mathscr{L}_{\mathbb{Q}_p}(V, C(i)))^{G_K},$$

then

$$\mathrm{gr}^i\, \mathbf{D}^*_{\mathrm{HT}}(V) \simeq \mathrm{gr}^{-i}\, \mathbf{D}_{\mathrm{HT}}(V^*)$$

as K-vector spaces.

Exercise 6.8. A p-adic representation V of G_K is $\widehat{B_{\mathrm{HT}}}$-admissible if and only if it is B_{HT}-admissible.

6.2 The field B_{dR} and de Rham representations

In this section, we shall define the ring B_{dR}^+ and its fraction field, the field of p-adic periods B_{dR} such that

$$W(R) \subset W(R)[\frac{1}{p}] \subset B_{\mathrm{dR}}^+ \subset B_{\mathrm{dR}}.$$

6.2.1 The homomorphism θ.

Let $a = (a_0, a_1, \cdots, a_m, \cdots) \in W(R)$, where $a_m \in R$. Recall that one can write a_m in two ways: either

$$a_m = (a_m^{(r)})_{r\in\mathbb{N}},\ a_m^{(r)} \in \mathcal{O}_C,\ (a_m^{(r+1)})^p = a_m^{(r)};$$

or

$$a_m = (a_{m,r}),\ a_{m,r} \in \mathcal{O}_{\overline{K}}/p,\ a_{m,r+1}^p = a_{m,r}.$$

Then $a \mapsto (a_{0,n}, a_{1,n}, \cdots, a_{n-1,n})$ gives a natural map $W(R) \to W_n(\mathcal{O}_{\overline{K}}/p)$. For every $n \in \mathbb{N}$, the following diagram is commutative:

$$\begin{tikzcd} & W_{n+1}(\mathcal{O}_{\overline{K}}/p) \arrow[d, "f_n"] \\ W(R) \arrow[ur] \arrow[r] & W_n(\mathcal{O}_{\overline{K}}/p) \end{tikzcd}$$

where $f_n((x_0, x_1, \cdots, x_n)) = (x_0^p, \cdots, x_{n-1}^p)$. It is easy to check the natural map

$$W(R) = \varprojlim_{f_n} W_n(\mathcal{O}_{\overline{K}}/p) \tag{6.1}$$

is an isomorphism. Moreover, It is also a homeomorphism if the right hand side is equipped with the inverse limit topology of the discrete topology.

Note that $\mathcal{O}_{\overline{K}}/p = \mathcal{O}_C/p$. We have a surjective map

$$W_{n+1}(\mathcal{O}_C) \to W_n(\mathcal{O}_{\overline{K}}/p), \quad (a_0, \cdots, a_n) \mapsto (\bar{a}_0, \cdots, \bar{a}_{n-1}).$$

Let I be its kernel, then

$$I = \{(pb_0, pb_1, \cdots, pb_{n-1}, a_n) \mid b_i, a_n \in \mathcal{O}_C\}.$$

Recall $w_{n+1} : W_{n+1}(\mathcal{O}_C) \to \mathcal{O}_C$ is the map which sends $(a_0, a_1, \cdots, a_n)$ to $a_0^{p^n} + pa_1^{p^{n-1}} + \cdots + p^n a_n$. Composite w_{n+1} with the quotient map $\mathcal{O}_C \to \mathcal{O}_C/p^n$, then we get a natural map $W_{n+1}(\mathcal{O}_C) \to \mathcal{O}_C/p^n$. Since

$$w_{n+1}(pb_0, \cdots, pb_{n-1}, a_n) = (pb_0)^{p^n} + \cdots + p^{n-1}(pb_{n-1})^p + p^n a_n \in p^n\mathcal{O}_C,$$

there is a unique homomorphism

$$\theta_n : W_n(\mathcal{O}_{\overline{K}}/p) \to \mathcal{O}_C/p^n, \quad (\bar{a}_0, \bar{a}_1, \cdots, \bar{a}_{n-1}) \mapsto \sum_{i=0}^{n-1} p^i \overline{a_i^{p^{n-i}}} \tag{6.2}$$

such that the following diagram

$$\begin{tikzcd} W_{n+1}(\mathcal{O}_C) \arrow[r, "w_{n+1}"] \arrow[d] & \mathcal{O}_C \arrow[d] \\ W_n(\mathcal{O}_{\overline{K}}/p) \arrow[r, "\theta_n"] & \mathcal{O}_C/p^n = \mathcal{O}_{\overline{K}}/p^n \end{tikzcd}$$

is commutative. Furthermore, we have a commutative diagram:

$$\begin{tikzcd} W_{n+1}(\mathcal{O}_{\overline{K}}/p) \arrow[r, "\theta_{n+1}"] \arrow[d, "f_n"] & \mathcal{O}_C/p^{n+1} \arrow[d] \\ W_n(\mathcal{O}_{\overline{K}}/p) \arrow[r, "\theta_n"] & \mathcal{O}_C/p^n \end{tikzcd}$$

Thus it induces a homomorphisms of rings

$$\theta : W(R) \longrightarrow \mathcal{O}_C. \tag{6.3}$$

Lemma 6.9. *If $x = (x_0, x_1, \cdots, x_n, \cdots) \in W(R)$ for $x_n \in R$ and $x_n = (x_n^{(m)})_{m\in\mathbb{N}}$, $x_n^{(m)} \in \mathcal{O}_C$, then*

$$\theta(x) = \sum_{n=0}^{+\infty} p^n x_n^{(n)}. \tag{6.4}$$

Thus θ is a homomorphism of W-algebras which commutes with the action of G_{K_0}.

Proof. For $x = (x_0, x_1, \cdots)$, the image of x in $W_n(\mathcal{O}_{\overline{K}}/p)$ is $(x_{0,n}, x_{1,n}, \cdots, x_{n-1,n})$. We can pick $x_i^{(n)} \in \mathcal{O}_C$ as a lifting of $x_{i,n}$, then

$$\theta_n(x_{0,n}, \cdots, x_{n-1,n}) = \sum_{i=0}^{n-1} p^i \overline{(x_i^{(n)})^{p^{n-i}}} = \sum_{i=0}^{n-1} p^i \overline{x_i^{(i)}}$$

since $(x_i^{(n)})^{p^r} = x_i^{(n-r)}$. Passing to the limit we have the lemma.

Remark 6.10. If write $x \in W(R)$ as $x = \sum_n p^n [x_n]$ where $x_n \in R$ and $[x_n]$ is its Teichmüller representative, then

$$\theta(x) = \sum_{n=0}^{+\infty} p^n x_n^{(0)}. \tag{6.5}$$

Proposition 6.11. *The homomorphism θ is surjective.*

Proof. For any $a \in \mathcal{O}_C$, there exists $x \in R$ such that $x^{(0)} = a$. Let $[x] = (x, 0, 0, \cdots)$, then $\theta([x]) = x^{(0)} = a$.

Choose $\varpi \in R$ such that $\varpi^{(0)} = -p$. Set

$$\xi := [\varpi] + p = (\varpi, 1, 0, \cdots) \in W(R). \tag{6.6}$$

By Lemma 6.9, $\theta(\xi) = \varpi^{(0)} + p = 0$.

Proposition 6.12. *The kernel of θ,* $\operatorname{Ker}\theta$ *is the principal ideal generated by ξ. Moreover, $\bigcap(\operatorname{Ker}\theta)^n = 0$.*

Proof. For the first assertion, it is enough to check that $\operatorname{Ker}\theta \subset (\xi, p)$, because $\mathcal{O}_C$ has no p-torsion and $W(R)$ is p-adically separated and complete. In other words, if $x \in \operatorname{Ker}\theta$ and $x = \xi y_0 + p x_1$, then $\theta(x) = p\theta(x_1)$, hence $x_1 \in \operatorname{Ker}\theta$. We may construct inductively a sequence (x_n) in $\operatorname{Ker}\theta$ by the relation $x_{n-1} = \xi y_{n-1} + p x_n$, then $x = \xi(\sum p^n y_n)$ is a multiple of ξ.

Now assume $x = (x_0, x_1, \cdots, x_n, \cdots) \in \operatorname{Ker}\theta$, then

$$0 = \theta(x) = x_0^{(0)} + p \sum_{n=1}^{\infty} p^{n-1} x_n^{(n)},$$

Thus $v(x_0^{(0)}) \geqslant 1 = v_p(p)$, so $v(x_0) \geqslant 1 = v(\varpi)$. Hence there exists $b_0 \in R$ such that $x_0 = b_0\varpi$. Let $b = [b_0]$, then

$$\begin{aligned} x - b\xi =& (x_0, x_1, \cdots) - (b, 0, \cdots)(\varpi, 1, 0, \cdots) \\ =& (x_0 - b_0\varpi, \cdots) = (0, y_1, y_2, \cdots) \\ =& p(y_1', y_2', \cdots) \in pW(R), \end{aligned}$$

where $(y_i')^p = y_i$. Hence $\operatorname{Ker}\theta \subset (\xi, p)$.

For the second assertion, if $x = (x_0, \cdots) \in (\operatorname{Ker}\theta)^n$ for all $n \in \mathbb{N}$, then $v_R(x_0) \geq v_R(\varpi^n) = n$. Hence $x_0 = 0$ and $x = py \in pW(R)$. Then $p\theta(y) = \theta(x) = 0$ and $y \in \operatorname{Ker}\theta$. Replacing x by x/ξ^n, we see that $y/\xi^n \in \operatorname{Ker}\theta$ for all n and thus $y \in \bigcap(\operatorname{Ker}\theta)^n$. Repeat this process, then $x = py = p(pz) = \cdots = 0$.

6.2.2 B_{dR}^+ and B_{dR}.

Note that $K_0 = \operatorname{Frac} W = W\left[\frac{1}{p}\right]$, then

$$W(R)\left[\frac{1}{p}\right] = K_0 \otimes_W W(R).$$

We use the injection $x \mapsto 1 \otimes x$ to identify $W(R)$ with a subring of $W(R)\left[\frac{1}{p}\right]$, then

$$W(R)\big[\frac{1}{p}\big] = \bigcup_{n=0}^{\infty} W(R)p^{-n} = \varinjlim_{n\in\mathbb{N}} W(R)p^{-n}$$

with the natural inductive topology. The G_{K_0}-equivariant homomorphism $\theta : W(R) \twoheadrightarrow \mathcal{O}_C$ extends to a G_{K_0}-equivariant homomorphism of K_0-algebras

$$\theta : W(R)\big[\frac{1}{p}\big] \to C, \quad \sum_{n\geq n_0\in\mathbb{Z}} p^n[x_n] \mapsto \sum_{n\geq n_0\in\mathbb{Z}} p^n x_n^{(0)}, \tag{6.7}$$

which again is surjective and continuous, and whose kernel is the principal ideal generated by ξ. Then $\operatorname{Ker}\theta$ is a maximal ideal of $W(R)\big[\frac{1}{p}\big]$ whose associated quotient field is C. We still have $\bigcap_n (\operatorname{Ker}\theta)^n = 0$.

Definition 6.13. (i) *The ring B_{dR}^+ is the $(\operatorname{Ker}\theta)$-adic completion of $W(R)\big[\frac{1}{p}\big]$, which means*

$$B_{\mathrm{dR}}^+ := \varprojlim_{n\in\mathbb{N}} W(R)\big[\frac{1}{p}\big]/(\operatorname{Ker}\theta)^n = \varprojlim_{n\in\mathbb{N}} W(R)\big[\frac{1}{p}\big]/(\xi)^n. \tag{6.8}$$

(ii) *The field of p-adic periods B_{dR} is the fractional field of B_{dR}^+, i.e.,*

$$B_{\mathrm{dR}} := \operatorname{Frac} B_{\mathrm{dR}}^+ = B_{\mathrm{dR}}^+\big[\frac{1}{\xi}\big]. \tag{6.9}$$

By definition,

Lemma 6.14. *B_{dR}^+ is a complete discrete valuation ring whose residue field is C, equipped with a continuous G_{K_0}-action, and B_{dR} is its valuation field.*

Definition 6.15. *For $i \in \mathbb{Z}$, let $\operatorname{Fil}^i B_{\mathrm{dR}}$ be the free B_{dR}^+-module generated by ξ^i. The filtration on B_{dR} is the decreasing exhaustive and separated filtration*

$$\cdots \supset \operatorname{Fil}^i B_{\mathrm{dR}} = B_{\mathrm{dR}}^+\xi^i \supset \operatorname{Fil}^{i+1} B_{\mathrm{dR}} \supset \cdots . \tag{6.10}$$

Note that $\operatorname{Fil}^0 B_{\mathrm{dR}} = B_{\mathrm{dR}}^+$ and if $i \geq 0$, $\operatorname{Fil}^i B_{\mathrm{dR}} = \mathfrak{m}^i_{B_{\mathrm{dR}}^+}$ is the i-th power of the maximal ideal of B_{dR}^+. The corresponding valuation v_{dR} on B_{dR} is also given by the filtration: $v_{\mathrm{dR}}(0) = +\infty$ and for $0 \neq x \in B_{\mathrm{dR}}$,

$$v_{\mathrm{dR}}(x) = i, \text{ if } x \in \operatorname{Fil}^i B_{\mathrm{dR}} \text{ but } x \notin \operatorname{Fil}^{i+1} B_{\mathrm{dR}}. \tag{6.11}$$

Remark 6.16. One must *be careful* for the topology on B_{dR}^+. There are at least two different topologies on B_{dR}^+ that we shall consider in the book.

(a) the topology as a discrete valuation ring;
(b) the induced topology by the inverse limit, with the topology on each component $W(R)\big[\frac{1}{p}\big]/(\operatorname{Ker}\theta)^n$ being the induced quotient topology of $W(R)\big[\frac{1}{p}\big]$.

We call (b) the *canonical topology* or the *natural topology* of B_{dR}^{+}. The topology (a) is stronger than (b). Actually for the topology in (a) the residue field C is endowed with the discrete topology; for the topology in (b), the induced topology on C is the natural topology by p-adic valuation.

Since $\bigcap\limits_{n=1}^{\infty} \xi^n W(R)\left[\frac{1}{p}\right] = 0$, there is an injection

$$W(R)\left[\frac{1}{p}\right] \hookrightarrow B_{\mathrm{dR}}^{+}.$$

We use this to identify $W(R)$ and $W(R)\left[\frac{1}{p}\right]$ with subrings of B_{dR}^{+}. In particular, $K_0 = W\left[\frac{1}{p}\right]$ is a subfield of B_{dR}^{+}. For any monic irreducible polynomial $P(X) \in K_0[X]$, under the map

$$K_0 \hookrightarrow B_{\mathrm{dR}}^{+} \xrightarrow{\theta} C,$$

$P(X) \in C[X]$ has distinct roots in C, hence $P(X) \in B_{\mathrm{dR}}^{+}[X]$ has distinct roots in B_{dR}^{+} by Hensel's Lemma. In this way, we see that

Lemma 6.17. *$\overline{K}$ is naturally a subfield of B_{dR}^{+} preserving the Galois action, and $\overline{K} \cap \mathrm{Fil}^1 B_{\mathrm{dR}} = 0$.*

Remark 6.18. We can also see the inclusion of $\overline{K} \subset B_{\mathrm{dR}}^{+}$ in the following way. Let L be any totally ramified finite extension of K_0 inside $\overline{K}$ and π_L be a uniformizer of L. Set $W_L(R) = L \otimes_W W(R)$ (hence $W_{K_0}(R) = W(R)\left[\frac{1}{p}\right]$). Then any element $x \in W_L(R)$ can be uniquely written as $\sum_{n \geq n_0} \pi_L^n [x_n]$ with $x_n \in R$. The surjective homomorphism $\theta : W_{K_0}(R) \twoheadrightarrow C$ can be extended naturally to

$$\theta : W_L(R) \twoheadrightarrow C, \ \sum_{n \geq n_0} \pi_L^n [x_n] \mapsto \sum_{n \geq n_0} \pi_L^n x_n^{(0)}, \tag{6.12}$$

whose kernel is again a principal ideal (but not generated by ξ). Moreover, we have a commutative diagram

$$\begin{tikzcd} W_{K_0}(R) \arrow[r, "\theta"] \arrow[d, "\mathrm{incl}"'] & C \arrow[d, "\mathrm{Id}"'] \\ W_L(R) \arrow[r, "\theta"] & C \end{tikzcd}$$

Set

$$B_{\mathrm{dR},L}^{+} = \varprojlim_{n \in \mathbb{N}} W_L(R)/(\mathrm{Ker}\,\theta)^n. \tag{6.13}$$

Then the inclusion $W_{K_0}(R) \hookrightarrow W_L(R)$ induces the inclusion $B_{\mathrm{dR}}^{+} \hookrightarrow B_{\mathrm{dR},L}^{+}$. However, since both are complete discrete valuation rings with the same residue field C, the inclusion is actually an isomorphism. Moreover, this isomorphism is compatible with the G_{K_0}-action. By this way, we identify B_{dR}^+ with $B_{\mathrm{dR},L}^+$ and hence $\overline{K} \subset B_{\mathrm{dR}}^+$.

Furthermore, let K and L be two p-adic local fields. Let $\overline{K}$ and $\overline{L}$ be algebraic closures of K and L respectively. Given a continuous homomorphism $h : \overline{K} \to \overline{L}$, then there is a canonical homomorphism $B_{\mathrm{dR}}(h) : B_{\mathrm{dR}}^+(K) \to B_{\mathrm{dR}}^+(L)$ such that $B_{\mathrm{dR}}(h)$ is an isomorphism if and only if h induces an isomorphism of the completions of $\overline{K}$ and $\overline{L}$. Through this, we see that B_{dR} *depends only on C not on K.*

By Theorem 1.23, we have the following important fact:

Proposition 6.19. *There exists a section $s : C \to B_{\mathrm{dR}}^+$ which is a homomorphism of rings such that $\theta(s(c)) = c$ for all $c \in C$.*

However, the section s is not unique. Moreover, one can prove that

Exercise 6.20. (1) There is no section $s : C \to B_{\mathrm{dR}}^+$ which is continuous in the natural topology.

(2) There is no section $s : C \to B_{\mathrm{dR}}^+$ which commutes with the action of G_K.

In the following remark, we list some main properties of B_{dR}.

Remark 6.21. (a) Note that $\bar{k}$ is the residue field of $\overline{K}$, as well as the residue field of R, and $\bar{k} \subset R$ (see Proposition 5.6). Thus $W(\bar{k}) \subset W(R)$. Then

$$P_0 = W(\bar{k})[\frac{1}{p}] = \widehat{K_0^{\mathrm{ur}}} \subset W(R)\big[\frac{1}{p}\big]$$

and θ is a homomorphism of P_0-algebras. Let $\overline{P} = P_0\overline{K}$ which is an algebraic closure of P_0, then

$$\overline{P} \subset B_{\mathrm{dR}}^+$$

and θ is also a homomorphism of $\overline{P}$-algebras.

(b) A theorem by Colmez (cf. appendix of [Fon94a]) claims that $\overline{K}$ is dense in B_{dR}^+ with a quite complicated topology in $\overline{K}$ induced by the natural topology of B_{dR}^+. However it is not dense in B_{dR}.

(c) The Frobenius map $\varphi : W(R)\big[\frac{1}{p}\big] \to W(R)\big[\frac{1}{p}\big]$ is not extendable to a continuous map $\varphi : B_{\mathrm{dR}}^+ \to B_{\mathrm{dR}}^+$. Indeed, $\theta([\varpi^{1/p}] + p) \neq 0$, thus $[\varpi^{1/p}] + p$ is invertible in B_{dR}^+. But if φ were a natural extension of the Frobenius map, on one hand $\varphi(1/([\varpi^{1/p}] + p))$ should still be invertible in B_{dR}^+, on the other hand one should have $\varphi(1/([\varpi^{1/p}] + p)) = 1/\xi \notin B_{\mathrm{dR}}^+$.

6.2.3 The element t.

Recall $\varepsilon \in R$ is the element given by $\varepsilon^{(0)} = 1$ and $\varepsilon^{(1)} \neq 1$, then $\boldsymbol{\pi} = [\varepsilon] - 1 \in W(R)$ and

$$\theta([\varepsilon]-1)=\varepsilon^{(0)}-1=0.$$

Thus $[\varepsilon]-1\in \operatorname{Ker}\theta=\operatorname{Fil}^1 B_{\mathrm{dR}}$. Then $(-1)^{n+1}\frac{([\varepsilon]-1)^n}{n}\in W(R)[\frac{1}{p}]\xi^n$ and

$$\log[\varepsilon]=\sum_{n=1}^{\infty}(-1)^{n+1}\frac{([\varepsilon]-1)^n}{n}\in B_{\mathrm{dR}}^+. \tag{6.14}$$

We call the above element $t=\log[\varepsilon]$.

Proposition 6.22. *The element*

$$t\in \operatorname{Fil}^1 B_{\mathrm{dR}} \text{ and } t\notin \operatorname{Fil}^2 B_{\mathrm{dR}}.$$

In other words, t generates the maximal ideal of B_{dR}^+.

Proof. That $t\in \operatorname{Fil}^1 B_{\mathrm{dR}}$ is because

$$\frac{([\varepsilon]-1)^n}{n}\in \operatorname{Fil}^1 B_{\mathrm{dR}} \text{ for all } n\geq 1.$$

Since

$$\frac{([\varepsilon]-1)^n}{n}\in \operatorname{Fil}^2 B_{\mathrm{dR}} \text{ if } n\geq 2,$$

to prove that $t\notin \operatorname{Fil}^2 B_{\mathrm{dR}}$, it is enough to check that

$$[\varepsilon]-1\notin \operatorname{Fil}^2 B_{\mathrm{dR}}.$$

Since $[\varepsilon]-1\in\operatorname{Ker}\theta$, write $[\varepsilon]-1=\lambda\xi$ with $\lambda\in W(R)$, then

$$[\varepsilon]-1\notin \operatorname{Fil}^2 B_{\mathrm{dR}}\Longleftrightarrow \theta(\lambda)\neq 0\Longleftrightarrow \lambda\notin W(R)\xi.$$

It is enough to check that $[\varepsilon]-1\notin W(R)\xi^2$. Assume the contrary and let $[\varepsilon]-1=\lambda\xi^2$ with $\lambda\in W(R)$. Write $\lambda=(\lambda_0,\lambda_1,\lambda_2,\cdots)$. Since

$$\xi=(\varpi,1,0,0,\cdots),\quad \xi^2=(\varpi^2,\cdots),$$

we have $\lambda\xi^2=(\lambda_0\varpi^2,\cdots)$. But

$$[\varepsilon]-1=(\varepsilon,0,0,\cdots)-(1,0,0,\cdots)=(\varepsilon-1,\cdots),$$

hence $\varepsilon-1=\lambda_0\varpi^2$ and

$$v(\varepsilon-1)\geqslant 2.$$

We have computed that $v(\varepsilon-1)=\frac{p}{p-1}$ (see Lemma 5.11), which is less than 2 if $p\neq 2$, we get a contradiction. If $p=2$, just compute the next term, we will get a contradiction too.

Remark 6.23. We should point out that our t is the *p-adic analogue of* $2\pi i\in\mathbb{C}$. Although $\exp(t)=[\varepsilon]\neq 1$ in B_{dR}^+, $\theta([\varepsilon])=1$ in $C=\mathbb{C}_p$.

Recall by Lemma 5.11), the multiplicative module $\varepsilon^{\mathbb{Z}_p}$ is isomorphic to the Tate module $T_p(\mathbb{G}_m) = \mathbb{Z}_p(1)$ as G_{K_0}-modules. By the relation

$$\log([\varepsilon^\lambda]) = \log([\varepsilon]^\lambda) = \lambda \log([\varepsilon]) = \lambda t,$$

the Tate module $\mathbb{Z}_p(1)$ can be realized as $\mathbb{Z}_p t \subset B_{\mathrm{dR}}^+$: for any $g \in G_{K_0}$, $g(t) = \chi(g)t$ where χ is the cyclotomic character. Moreover, we have

$$\begin{aligned} \operatorname{Fil}^i B_{\mathrm{dR}} &= B_{\mathrm{dR}}^+ t^i = B_{\mathrm{dR}}^+(i), \\ B_{\mathrm{dR}} &= B_{\mathrm{dR}}^+[\frac{1}{t}] = B_{\mathrm{dR}}^+[\frac{1}{\xi}], \end{aligned}$$

thus

$$\begin{aligned} \operatorname{gr} B_{\mathrm{dR}} &= \bigoplus_{i\in\mathbb{Z}} \operatorname{gr}^i B_{\mathrm{dR}} = \bigoplus_{i\in\mathbb{Z}} \operatorname{Fil}^i B_{\mathrm{dR}} / \operatorname{Fil}^{i+1} B_{\mathrm{dR}} \\ &= \bigoplus_{i\in\mathbb{Z}} B_{\mathrm{dR}}^+(i)/tB_{\mathrm{dR}}^+(i) = \bigoplus_{i\in\mathbb{Z}} C(i). \end{aligned}$$

Hence

Proposition 6.24. $\operatorname{gr} B_{\mathrm{dR}} = B_{\mathrm{HT}} = C[t, \frac{1}{t}] \subset \widehat{B_{\mathrm{HT}}} = C((t))$.

Remark 6.25. If we choose a section $s : C \to B_{\mathrm{dR}}^+$ which is a homomorphism of rings and use it to identify C with a subfield of B_{dR}^+, then $B_{\mathrm{dR}} \simeq C((t))$. This is not the right way since s is not continuous. Note there is no such an isomorphism which is compatible with the action of G_K.

6.2.4 de Rham representations and filtered *K*-vector spaces.

Proposition 6.26. $B_{\mathrm{dR}}^{G_K} = K$.

Proof. Since $K \subset \overline{K} \subset B_{\mathrm{dR}}^+ \subset B_{\mathrm{dR}}$, we have

$$K \subset \overline{K}^{G_K} \subset \cdots \subset B_{\mathrm{dR}}^{G_K}.$$

Let $0 \neq b \in B_{\mathrm{dR}}^{G_K}$, we are asked to show that $b \in K$. For such a b, there exists an $i \in \mathbb{Z}$ such that $b \in \operatorname{Fil}^i B_{\mathrm{dR}}$ but $b \notin \operatorname{Fil}^{i+1} B_{\mathrm{dR}}$. Denote by $\bar{b}$ the image of b in $\operatorname{gr}^i B_{\mathrm{dR}} = C(i)$, then $\bar{b} \neq 0$ and $\bar{b} \in C(i)^{G_K}$. Recall that

$$C(i)^{G_K} = \begin{cases} 0, & i \neq 0, \\ K, & i = 0, \end{cases}$$

then $i = 0$ and $\bar{b} \in K \subseteq B_{\mathrm{dR}}^+$. Now $b - \bar{b} \in B_{\mathrm{dR}}^{G_K}$ and $b - \bar{b} \in (\operatorname{Fil}^i B_{\mathrm{dR}})^{G_K}$ for some $i \geq 1$, hence $b - \bar{b} = 0$.

Note that B_{dR} is a field containing K, therefore containing $\mathbb{Q}_p$, and is equipped with an action of G_K. It is $(\mathbb{Q}_p, G_K)$-regular since it is a field. For a p-adic representation V of G_K, set

$$\mathbf{D}_{\mathrm{dR}}(V) := (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K}. \tag{6.15}$$

Then the map

$$\alpha_{\mathrm{dR}}(V) : B_{\mathrm{dR}} \otimes_K \mathbf{D}_{\mathrm{dR}}(V) \longrightarrow B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$$

is injective.

Definition 6.27. *A p-adic representation V of G_K is called* de Rham *if it is B_{dR}-admissible, i.e., if $\alpha_{\mathrm{dR}}(V)$ is an isomorphism.*

The category of p-adic Galois representations of K which are de Rham is denoted by $\mathbf{Rep}^{\mathrm{dR}}_{\mathbb{Q}_p}(G_K)$.

We immediately see that

Lemma 6.28. *V is a de Rham representation if and only if $\dim_K \mathbf{D}_{\mathrm{dR}}(V) = \dim_{\mathbb{Q}_p}(V)$.*

Definition 6.29. *The category of filtered K-vector spaces, denoted by $\mathbf{Fil}_K$, is the category such that*

(i) *an object of $\mathbf{Fil}_K$ is a finite dimensional K-vector space D equipped with a decreasing filtration indexed by $\mathbb{Z}$ which is exhaustive and separated, i.e.,*
   - $\mathrm{Fil}^i D$ *are sub K-vector spaces of D,*
   - $\mathrm{Fil}^{i+1} D \subset \mathrm{Fil}^i D$,
   - $\mathrm{Fil}^i D = 0$ *for $i \gg 0$, and* $\mathrm{Fil}^i D = D$ *for $i \ll 0$.*

(ii) *a morphism*

$$\eta : D_1 \to D_2$$

between two objects of $\mathbf{Fil}_K$ is a K-linear map such that

$$\eta(\mathrm{Fil}^i D_1) \subset \mathrm{Fil}^i D_2 \text{ for all } i \in \mathbb{Z}.$$

For D an object in $\mathbf{Fil}_K$, set

$$\mathrm{gr}^i D := \mathrm{Fil}^i D / \mathrm{Fil}^{i+1} D, \qquad \mathrm{gr}\, D := \bigoplus_{i\in\mathbb{Z}} \mathrm{gr}^i D. \tag{6.16}$$

The category $\mathbf{Fil}_K$ of filtered K-vector spaces is an additive category with kernels and cokernels. In fact, let $\eta : D_1 \to D_2$ be a morphism of $\mathbf{Fil}_K$, then

(a) $\mathrm{Ker}\,\eta$ is the kernel of η as a K-linear map, with the filtration $\mathrm{Fil}^i(\mathrm{Ker}\,\eta) = \mathrm{Ker}\,\eta \cap \mathrm{Fil}^i D_1$,

(b) $\mathrm{Coker}\,\eta$ is the cokernel of η a K-linear map, with the filtration $\mathrm{Fil}^i(\mathrm{Coker}\,\eta) = \mathrm{Im}(\mathrm{Fil}^i D_2)$.

However, the induced map $\mathrm{coIm}(\eta) \to \mathrm{Im}(\eta)$, even though is an isomorphism of K-vector spaces, but is not always filtration-preserving, hence not a morphism between filtered K-vector spaces.

Definition 6.30. *A morphism $\eta : D_1 \to D_2$ is called* strict or strictly compatible with the filtration *if for all $i \in \mathbb{Z}$,*

$$\eta(\mathrm{Fil}^i D_1) = \mathrm{Fil}^i D_2 \cap \mathrm{Im}\, \eta.$$

Proposition 6.31. *A morphism η of $\mathbf{Fil}_K$ is strict if and only if the induced map from the coimage of η to the image of η is an isomorphism.*

Proof. Exercise.

By abstract nonsense, $\mathbf{Fil}_K$ thus becomes an exact category with the following definition of short exact sequence:

Definition 6.32. *A short exact sequence in $\mathbf{Fil}_K$ is a sequence*

$$0 \longrightarrow D' \xrightarrow{\alpha} D \xrightarrow{\beta} D'' \longrightarrow 0$$

such that:

(i) *α and β are strict morphisms;*
(ii) *α is injective, β is surjective and*

$$\alpha(D') = \{x \in D \mid \beta(x) = 0\}.$$

The category $\mathbf{Fil}_K$ is equipped with tensor product, unit and dual:

(a) If D_1 and D_2 are two objects in $\mathbf{Fil}_K$, $D_1 \otimes D_2$ is defined as
  - $D_1 \otimes D_2 = D_1 \otimes_K D_2$ as K-vector spaces;
  - $\mathrm{Fil}^i(D_1 \otimes D_2) = \sum_{i_1+i_2=i} \mathrm{Fil}^{i_1} D_1 \otimes_K \mathrm{Fil}^{i_2} D_2$.

(b) The unit object is $D = K$ with

$$\mathrm{Fil}^i K = \begin{cases} K, & i \leq 0, \\ 0, & i > 0. \end{cases}$$

(c) If D is an object in $\mathbf{Fil}_K$, its dual D^* is defined as
  - $D^* = \mathscr{L}_K(D, K)$ as a K-vector space;
  - $\mathrm{Fil}^i D^* = (\mathrm{Fil}^{-i+1} D)^{\perp} = \{f : D \to K \mid f(x) = 0, \text{ for all } x \in \mathrm{Fil}^{-i+1} D\}$.

If V is any p-adic representation of G_K, then $\mathbf{D}_{\mathrm{dR}}(V)$ is a filtered K-vector space, with

$$\mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(V) := (\mathrm{Fil}^i B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K}. \tag{6.17}$$

For the short exact sequence

$$0 \to \mathrm{Fil}^{i+1} B_{\mathrm{dR}} \to \mathrm{Fil}^i B_{\mathrm{dR}} \to C(i) \to 0,$$

if tensoring with V we get

$$0 \to \mathrm{Fil}^{i+1} B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V \to \mathrm{Fil}^i B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V \to C(i) \otimes_{\mathbb{Q}_p} V \to 0.$$

Take the G_K-invariant, we get

$$0 \to \mathrm{Fil}^{i+1} \mathbf{D}_{\mathrm{dR}}(V) \to \mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(V) \to (C(i) \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

Thus

$$\mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V) = \mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(V)/\mathrm{Fil}^{i+1} \mathbf{D}_{\mathrm{dR}}(V) \hookrightarrow (C(i) \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

Hence,

$$\mathrm{gr}\, \mathbf{D}_{\mathrm{dR}}(V) = \bigoplus_{i \in \mathbb{Z}} \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V) \hookrightarrow \bigoplus_{i \in \mathbb{Z}} (C(i) \otimes_{\mathbb{Q}_p} V)^{G_K} = \mathbf{D}_{\mathrm{HT}}(V).$$

As a consequence, we have

Proposition 6.33. *If a p-adic representation V is de Rham, then V is Hodge-Tate and*

$$\mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V) = (C(i) \otimes_{\mathbb{Q}_p} V)^{G_K}, \qquad \mathrm{gr}\, \mathbf{D}_{\mathrm{dR}}(V) = \mathbf{D}_{\mathrm{HT}}(V). \tag{6.18}$$

Theorem 6.34. *The functor $\mathbf{D}_{\mathrm{dR}} : \mathbf{Rep}_{\mathbb{Q}_p}^{\mathrm{dR}}(G_K) \to \mathbf{Fil}_K$ is an exact, faithful and tensor functor.*

Proof. One needs to show that

(i) For an exact sequence $0 \to V' \to V \to V'' \to 0$ of de Rham representations, then

$$0 \to \mathbf{D}_{\mathrm{dR}}(V') \to \mathbf{D}_{\mathrm{dR}}(V) \to \mathbf{D}_{\mathrm{dR}}(V'') \to 0$$

is a short exact sequence of filtered K-vector spaces.

(ii) If V_1, V_2 are de Rham representations, then

$$\mathbf{D}_{\mathrm{dR}}(V_1) \otimes \mathbf{D}_{\mathrm{dR}}(V_2) \xrightarrow{\sim} \mathbf{D}_{\mathrm{dR}}(V_1 \otimes V_2)$$

is an isomorphism of filtered K-vector spaces.

(iii) If V is de Rham, then $V^* = \mathscr{L}_{\mathbb{Q}_p}(V, \mathbb{Q}_p)$ and

$$\mathbf{D}_{\mathrm{dR}}(V^*) \cong (\mathbf{D}_{\mathrm{dR}}(V))^*$$

as filtered K-vector spaces.

By Theorem 3.14, (i)-(iii) all hold in the category of K-vector spaces. We just need to check the filtration. We identify $\mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V)$ with $(C(i) \otimes_{\mathbb{Q}_p} V)^{G_K}$ by Proposition 6.33.

For (i), tensoring $C(i)$ to the exact sequence $0 \to V' \to V \to V'' \to 0$ and then taking the G_K-invariants, we have an exact sequence as K-vector spaces:

$$0 \to \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V') \to \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}} \to \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V'').$$

In particular, $\dim \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V) \geq \dim \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V') + \dim \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V'')$ for all $i \in \mathbb{Z}$. The equality $\dim \mathbf{D}_{\mathrm{dR}}(V) = \dim \mathbf{D}_{\mathrm{dR}}(V') + \dim \mathbf{D}_{\mathrm{dR}}(V'')$ then means $\dim \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V) = \dim \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V') + \dim \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V'')$ for all $i \in \mathbb{Z}$. Thus

$$0 \to \mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(V') \to \mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(V) \to \mathbf{D}_{\mathrm{dR}} D_{\mathrm{dR}}(V'') \to 0$$

are all exact sequences as K-vector spaces. This implies (i).

For (ii), the map

$$\begin{aligned} \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V_1) \otimes_K \mathrm{gr}^j \mathbf{D}_{\mathrm{dR}}(V_2) &\longrightarrow \mathrm{gr}^{i+j} \mathbf{D}_{\mathrm{dR}}(V_1 \otimes V_2), \\ c_1 v_1 t^i \otimes c_2 v_2 t^j &\longmapsto c_1 c_1 (v_1 \otimes v_2) t^{i+j} \end{aligned}$$

is an injection, which gives the injection

$$\mathrm{gr}^i(\mathbf{D}_{\mathrm{dR}}(V_1) \otimes \mathbf{D}_{\mathrm{dR}}(V_2)) \hookrightarrow \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V_1 \otimes V_2)$$

for all $i \in \mathbb{Z}$. Taking into account of the equality $\dim_K \mathbf{D}_{\mathrm{dR}}(V_1) \otimes \mathbf{D}_{\mathrm{dR}}(V_2) = \dim_K \mathbf{D}_{\mathrm{dR}}(V_1 \otimes V_2)$, we find that the above injection must be an isomorphism as K-vector spaces for every $i \in \mathbb{Z}$. This gives the proof of (ii).

(iii) follows from

$$\begin{aligned} \mathbf{D}_{\mathrm{dR}}(V^*) =& (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} \mathrm{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p))^{G_K} \cong \mathrm{Hom}_{B_{\mathrm{dR}}}(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V, B_{\mathrm{dR}})^{G_K} \\ &\cong \mathrm{Hom}_K((B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K}, K) = \mathbf{D}_{\mathrm{dR}}(V)^*. \end{aligned}$$

Proposition 6.35. *Suppose $i < j \in \mathbb{Z} \cup \{\pm\infty\}$, then if $i \geq 1$ or $j \leq 0$,*

$$H^1(G_K, t^i B_{\mathrm{dR}}^+ / t^j B_{\mathrm{dR}}^+) = 0;$$

if $i \leq 0$ and $j > 0$, then $x \mapsto x \cup \log \chi$ gives an isomorphism

$$H^0(G_K, t^i B_{\mathrm{dR}}^+ / t^j B_{\mathrm{dR}}^+) (\simeq K) \xrightarrow{\sim} H^1(G_K, t^i B_{\mathrm{dR}}^+ / t^j B_{\mathrm{dR}}^+).$$

Proof. For the case i, j finite, let $n = j - i$, we prove it by induction. For $n = 1$, $t^i B_{\mathrm{dR}}^+ / t^{i+1} B_{\mathrm{dR}}^+ \simeq C(i)$, this follows from Proposition 4.46. For general n, we just use the long exact sequence in continuous cohomology attached to the exact sequence

$$0 \longrightarrow C(i+n) \longrightarrow t^i B_{\mathrm{dR}}^+ / t^{n+i+1} B_{\mathrm{dR}}^+ \longrightarrow t^i B_{\mathrm{dR}}^+ / t^{i+n} B_{\mathrm{dR}}^+ \longrightarrow 0$$

to conclude.

By passage to the limit, we obtain the general case.

Proposition 6.36. (1) *There exists a p-adic representation V of G_K which is a nontrivial extension of $\mathbb{Q}_p(1)$ by $\mathbb{Q}_p$, i.e. there exists a non-split exact sequence of p-adic representations*

$$0 \to \mathbb{Q}_p \to V \to \mathbb{Q}_p(1) \to 0.$$

(2) *Such a representation V is a Hodge-Tate representation.*
(3) *Such a representation V is not a de Rham representation.*

Proof. (1) It is enough to prove the case $K = \mathbb{Q}_p$ (the general case is by base change $\mathbb{Q}_p \to K$). In this case $\mathrm{Ext}^1(\mathbb{Q}_p(1), \mathbb{Q}_p) = H^1_{\mathrm{cont}}(\mathbb{Q}_p, \mathbb{Q}_p(-1)) \neq 0$ (by Tate's duality, it is isomorphic to $H^0_{\mathrm{cont}}(\mathbb{Q}_p, \mathbb{Q}_p) = \mathbb{Q}_p$) and hence is nontrivial. Thus there must exist a nontrivial extension of $\mathbb{Q}_p(1)$ by $\mathbb{Q}_p$.

(2) By tensoring $C(i)$ for $i \in \mathbb{Z}$, we have an exact sequence

$$0 \to C(i) \to C(i) \otimes_{\mathbb{Q}_p} V \to C(i+1) \to 0.$$

This induces a long exact sequence by taking the G_K-invariants

$$0 \to C(i)^{G_K} \to (C(i) \otimes_{\mathbb{Q}_p} V)^{G_K} \to C(i+1)^{G_K} \to H^1(G_K, C(i)).$$

By Proposition 4.46,

(i) if $i \neq 0, -1$, $C(i)^{G_K} = C(i+1)^{G_K} = 0$, then $(V \otimes_{\mathbb{Q}_p} C(i))^{G_K} = 0$;
(ii) if $i = 0$, $C^{G_K} = K$, then $C(1)^{G_K} = 0$ and $(V \otimes_{\mathbb{Q}_p} C)^{G_K} = K$;
(iii) if $i = -1$, $C(-1)^{G_K} = 0$, $C^{G_K} = K$ and $H^1(G_K, C(-1)) = 0$, hence $(C(-1) \otimes_{\mathbb{Q}_p} V)^{G_K} = K$.

As a consequence V is Hodge-Tate.

(3) is not so easy! We shall prove it in Corollary 9.30.

Remark 6.37. Any extension of $\mathbb{Q}_p$ by $\mathbb{Q}_p(1)$ is de Rham. Indeed, by the exact sequence $0 \to \mathbb{Q}_p(1) \to V \to \mathbb{Q}_p \to 0$, the functor $(B^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} -)^{G_K}$ induces a long exact sequence

$$0 \to (tB^+_{\mathrm{dR}})^{G_K} = 0 \to (B^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K} \to K \to H^1(G_K, tB^+_{\mathrm{dR}}).$$

By Proposition 6.35, $H^1(G_K, tB^+_{\mathrm{dR}}) = 0$. Hence $\mathbf{D}_{\mathrm{dR}}(V) \to (B^+_{\mathrm{dR}} \otimes V)^{G_K} \to K = \mathbf{D}_{\mathrm{dR}}(\mathbb{Q}_p)$ is surjective. Thus $\dim_K \mathbf{D}_{\mathrm{dR}}(V) = 2$ and V is de Rham.

6.2.5 A digression.

Let E be any field of characteristic 0 and X a projective (or even proper) smooth algebraic variety over E. One has the de Rham complex

$$\Omega^\bullet_{X/E} : \ \mathcal{O}_{X/E} \to \Omega^1_{X/E} \to \Omega^2_{X/E} \to \cdots .$$

For $m \in \mathbb{N}$, the de Rham cohomology group $H^m_{\mathrm{dR}}(X/E)$ is defined to be $\mathbb{H}^m(\Omega^\bullet_{X/E})$, the m-th hyper cohomology of $\Omega^\bullet_{X/E}$, which is a finite dimensional E-vector space equipped with the Hodge filtration.

Given an embedding $\sigma : E \hookrightarrow \mathbb{C}$, then $X(\mathbb{C})$ is an analytic manifold. The singular cohomology $H^m(X(\mathbb{C}), \mathbb{Q})$ is defined to be the dual of $H_m(X(\mathbb{C}), \mathbb{Q})$ which is a finite dimensional $\mathbb{Q}$-vector space. The Comparison Theorem of Hodge theory claims that there exists a canonical isomorphism (classical Hodge structure)

$$\mathbb{C} \otimes_{\mathbb{Q}} H^m(X(\mathbb{C}), \mathbb{Q}) \simeq \mathbb{C} \otimes_E H^m_{\mathrm{dR}}(X/E).$$

We now consider the p-adic analogue. Assume $E = K$ is a p-adic field and ℓ is a prime number. Then for each $m \in \mathbb{N}$, the étale cohomology group $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_\ell)$ is an ℓ-adic representation of G_K which is potentially semi-stable if $\ell \neq p$. When $\ell = p$, we have

Theorem 6.38 (Tsuji [Tsu99], Faltings [Fal89]). *The p-adic representation $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is a de Rham representation and there is a canonical isomorphism of filtered K-vector spaces:*

$$\mathbf{D}_{\mathrm{dR}}(H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)) \simeq H^m_{\mathrm{dR}}(X/K),$$

and the identification

$$B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) = B_{\mathrm{dR}} \otimes_K H^m_{\mathrm{dR}}(X/K)$$

gives rise to the notion of p-adic Hodge structure.

Let ℓ be a prime number. Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. For p a prime number, let $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and I_p be the inertia group. Choose an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, then $I_p \subset G_p \hookrightarrow G_{\mathbb{Q}}$.

Definition 6.39. *An ℓ-adic representation V of $G_{\mathbb{Q}}$ is called* geometric *if*

(i) *V is* unramified *away from finitely many p's, i.e., let $\rho : G_{\mathbb{Q}} \to Aut_{\mathbb{Q}_l}(V)$ be the representation, then $\rho(I_p) = 1$ except finite many p's.*
(ii) *The representation is de Rham at $p = \ell$.*

Conjecture 6.40 (Fontaine-Mazur [FM95]). Geometric representations are exactly *the representations coming from algebraic geometry.*

7

B_{cris} and its properties

7.1 The ring of crystalline periods B_{cris}

7.1.1 Definition of B_{cris}.

Recall the θ-map:

$$\begin{tikzcd} W(R) \arrow[r, "\theta"] \arrow[d, hook] & \mathcal{O}_C \arrow[d, hook] \\ W(R)[\frac{1}{p}] \arrow[r, "\theta"] & C, \end{tikzcd}$$

we know $\operatorname{Ker}\theta = (\xi)$ where $\xi = [\varpi] + p = (\varpi, 1, 0, \cdots)$, $\varpi \in R$ such that $\varpi^{(0)} = -p$.

Definition 7.1. *The module A^0_{cris} is defined to be the* divided power envelope *of $W(R)$ with respect to* $\operatorname{Ker}\theta$*, that is, by adding all elements $\gamma_n(a) := \frac{a^n}{n!}$ for $a \in \operatorname{Ker}\theta$ and $n \in \mathbb{N}$.*

By definition, A^0_{cris} is the sub-$W(R)$-module of $W(R)\big[\frac{1}{p}\big]$ generated by the elements $\gamma_n(\xi) = \frac{\xi^n}{n!}, n \in \mathbb{N}$, i.e.,

$$A^0_{\mathrm{cris}} = \Big\{\sum_{n=0}^{N} a_n\gamma_n(\xi),\ N < +\infty,\ a_n \in W(R)\Big\} \subset W(R))\big[\frac{1}{p}\big]. \tag{7.1}$$

Moreover, it possesses a ring structure since

$$\gamma_m(\xi)\cdot\gamma_n(\xi) = \binom{m+n}{n}\frac{\xi^{m+n}}{(m+n)!} = \binom{m+n}{n}\gamma_{m+n}(\xi). \tag{7.2}$$

Note that $\gamma_n(\xi) \in W(R)[\xi/p]$, then A^0_{cris} is a subring of $W(R)[\xi/p]$. The completion of $W(R)[\xi/p]$ by $\operatorname{Ker}\theta$ is $W(R)[[\xi/p]]$, the ring of power series of ξ/p over $W(R)$, which is a subring of B^+_{dR}.

Lemma 7.2. *The ring $W(R)[[\xi/p]]$ is separated and complete by the p-adic topology, i.e., the natural map*

$$W(R)[[\xi/p]] \longrightarrow \varprojlim_n W(R)[[\xi/p]]/p^n W(R)[[\xi/p]]$$

is an isomorphism.

Proof. Write $S = W(R)[[\xi/p]]$. We first show that S is separated, i.e., $\bigcap p^n S = 0$. Suppose $x \in p^n S$ for all $n \in \mathbb{N}$. For every n, write

$$x = p^n \sum_i a_{i,n} \left(\frac{\xi}{p}\right)^i, \ a_{i,n} \in W(R).$$

Then $\theta(x) = p^n \theta(a_{0,n})$, which implies $\theta(x) = 0$ and in turn implies that $\theta(a_{0,n}) = 0$. Then $a_{0,n} = \xi b_{0,n}$ with $b_{0,n} \in W(R)$. Hence $x = \xi x_1$ with

$$x_1 = p^{n-1}\Big((pb_{0,n} + a_{1,n}) + \sum_{i\geq 2} a_{i,n} \left(\frac{\xi}{p}\right)^{i-1}\Big) \in p^{n-1}S.$$

By induction we have $x \in \xi^n S$ for all $n \in \mathbb{N}$. By Proposition 6.12, we have $x = 0$.

For completeness, suppose $y = (y_n)_{n\in\mathbb{N}} \in \varprojlim_n S/p^n S$, and suppose x_n is a lifting of y_n in S. We can write

$$x_{n+1} - x_n = \sum_{i\geq 0} p^n a_{i,n} \left(\frac{\xi}{p}\right)^i, \ a_{i,n} \in W(R).$$

Then $\sum_n p^n a_{i,n}$ converges to some $a_i \in W(R)$ and $x = \sum_i a_i(\xi/p)^i + x_0$ maps to y. This finishes the proof of the lemma.

Definition 7.3. *The ring A_{cris} is defined to be $\varprojlim_{n\in\mathbb{N}} A^0_{\mathrm{cris}}/p^n A^0_{\mathrm{cris}}$.*

The ring B^+_{cris} is defined to be $A_{\mathrm{cris}}\left[\frac{1}{p}\right]$.

By Lemma 7.2, A^0_{cris} is p-adically separated and $A^0_{\mathrm{cris}} \to A_{\mathrm{cris}}$ is injective. Moreover, the inclusion $A^0_{\mathrm{cris}} \subset W(R)[[\xi/p]]$ induces the injection of

$$A_{\mathrm{cris}} \subset W(R)[[\xi/p]] \subset B^+_{\mathrm{dR}}, \text{ and } B^+_{\mathrm{cris}} \subset B^+_{\mathrm{dR}}.$$

We have

$$\begin{tikzcd}
A^0_{\mathrm{cris}} \arrow[r, hook] \arrow[d, hook] & A_{\mathrm{cris}} \arrow[r, hook] \arrow[dr, hook] & B^+_{\mathrm{cris}} \arrow[d, hook] \\
W(R)[\frac{1}{p}] \arrow[rr, hook] & & B^+_{\mathrm{dR}}
\end{tikzcd}$$

and

$$A_{\mathrm{cris}} = \Big\{\sum_{n=0}^{+\infty} a_n\gamma_n(\xi),\ a_n \to 0 \ p\text{-adically in } W(R)\Big\} \subset B_{\mathrm{dR}}^+, \tag{7.3}$$

$$B_{\mathrm{cris}}^+ = \Big\{\sum_{n=0}^{+\infty} a_n\gamma_n(\xi),\ a_n \to 0 \ p\text{-adically in } W(R)[\frac{1}{p}]\Big\} \subset B_{\mathrm{dR}}^+. \tag{7.4}$$

However, one has to keep in mind that the expression of an element $\alpha \in A_{\mathrm{cris}}$ (resp. B_{cris}^+) in the above form is not unique.

Note that the ring homomorphism $\theta : W(R) \to \mathcal{O}_C$ extends naturally to A_{cris}^0 and A_{cris}, which is also the restriction of the theta map on B_{dR}^+.

Proposition 7.4. *The kernel*

$$\mathrm{Ker}\,(\theta : A_{\mathrm{cris}} \to \mathcal{O}_C)$$

is a divided power ideal, *which means that, if $a \in A_{\mathrm{cris}}$ such that $\theta(a) = 0$, then for all $m \in \mathbb{N}, m \geq 1$, $\frac{a^m}{m!} (\in B_{\mathrm{cris}}^+)$ is again in A_{cris} and $\theta(\frac{a^m}{m!}) = 0$.*

Proof. If $a = \sum a_n\gamma_n(\xi) \in A_{\mathrm{cris}}^0$, then

$$\frac{a^m}{m!} = \sum_{\text{sum of } i_n = m} \prod_n a_n \frac{\xi^{ni_n}}{(n!)^{i_n}(i_n)!}.$$

We claim that $\frac{(ni)!}{(n!)^i i!} \in \mathbb{N}$ for $n \geq 1$ and $i \in \mathbb{N}$. This fact is trivially true for $i = 0$. If $ni > 0$, $\frac{(ni)!}{(n!)^i i!}$ can be interpreted combinatorially as the number of choices to put ni balls into i unlabeled boxes. Thus

$$\frac{a^m}{m!} = \sum_{\text{sum of } i_n = m} \prod_n a_n \cdot \frac{(ni_n)!}{(n!)^{i_n}(i_n)!} \cdot \gamma_{ni_n}(\xi) \in A_{\mathrm{cris}}^0$$

and $\theta(\frac{a^m}{m!}) = 0$.

The case for $a \in A_{\mathrm{cris}}$ follows by continuity.

Proposition 7.5. *For the map*

$$\bar{\theta} : A_{\mathrm{cris}} \xrightarrow{\theta} \mathcal{O}_C \to \mathcal{O}_C/p = \mathcal{O}_{\overline{K}}/p.$$

its kernel $\mathrm{Ker}\,(\bar{\theta}) = (\mathrm{Ker}\,\theta, p)$ *is also a divided power ideal, i.e. if $a \in \mathrm{Ker}\,(\bar{\theta})$, then for all $m \in \mathbb{N}$, $m \geq 1$, $\frac{a^m}{m!} \in A_{\mathrm{cris}}$ and $\bar{\theta}(\frac{a^m}{m!}) = 0$.*

Proof. This is an easy exercise, noting that p divides $\frac{p^m}{m!}$ in $\mathbb{Z}_p$.

Recall that

$$t = \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{([\varepsilon]-1)^n}{n} \in B_{\mathrm{dR}}^+.$$

Proposition 7.6. *One has* $t \in A_{\mathrm{cris}}$ *and* $t^{p-1} \in pA_{\mathrm{cris}}$.

Proof. Since $[\varepsilon]-1 = b\xi$, $b \in W(R)$, $\frac{([\varepsilon]-1)^n}{n} = (n-1)!b^n\gamma_n(\xi)$ and $(n-1)! \to 0$ p-adically, we have $t \in A_{\mathrm{cris}}$.

To show $t^{p-1} \in pA_{\mathrm{cris}}$, we just need to show that $([\varepsilon]-1)^{p-1} \in pA_{\mathrm{cris}}$. Note that $[\varepsilon]-1 = (\varepsilon - 1, *, \cdots)$, and

$$(\varepsilon - 1)^{(n)} = \lim_{m \to +\infty} (\zeta_{p^{n+m}} - 1)^{p^m}$$

where $\zeta_{p^n} = \varepsilon^{(n)}$ is a primitive p^n-th root of unity. Then $v((\varepsilon-1)^{(n)}) = \frac{1}{p^{n-1}(p-1)}$ and

$$(\varepsilon - 1)^{p-1} = (p^p, 1, \cdots) \times \text{unit} = \varpi^p \cdot \mathit{unit}.$$

Then

$$([\varepsilon]-1)^{p-1} \equiv [\varpi^p] \cdot (*) = (\xi - p)^p \cdot (*) \equiv \xi^p \cdot (*) \bmod pA_{\mathrm{cris}},$$

but $\xi^p = p(p-1)!\gamma_p(\xi) \in pA_{\mathrm{cris}}$, we thus get the result.

Definition 7.7. *The* ring of crystalline periods B_{cris} *is defined to be the ring* $B^+_{\mathrm{cris}}[\frac{1}{t}] = A_{\mathrm{cris}}[\frac{1}{t}] = A_{\mathrm{cris}}[\frac{1}{p}, \frac{1}{t}]$.

We then have $B_{\mathrm{cris}} \subset B_{\mathrm{dR}}$.

7.1.2 Galois action on B_{cris}.

The rings A_{cris}, B^+_{cris} and B_{cris} are all stable under the action of G_K. Moreover, we have

Proposition 7.8. (1) *The map*

$$\iota : K \otimes_{K_0} B_{\mathrm{cris}} \to B_{\mathrm{dR}}, \ \lambda \otimes x \mapsto \lambda x$$

is injective.

(2) $B^{G_K}_{\mathrm{cris}} = K_0$.

Proof. (2) follows easily from (1). Indeed, since $B_{\mathrm{cris}} \supset W(R)[\frac{1}{p}]$,

$$B^{G_K}_{\mathrm{cris}} = L \supset (W(R)[\frac{1}{p}])^{G_K} = K_0,$$

where L is a K_0-algebra. If (1) is satisfied, then

$$K = B^{G_K}_{\mathrm{dR}} \supset (K \otimes_{K_0} B_{\mathrm{cris}})^{G_K} = K \otimes_{K_0} L$$

and thus $L = K_0$.

Write $A^0_{\mathrm{cris},\mathcal{O}_K} = \mathcal{O}_K \otimes_W A^0_{\mathrm{cris}} \subset W_{\mathcal{O}_K}(R)[\xi/p]$. Then by the same method in Lemma 7.2, suppose π_K is a uniformizer of K, then

$$A_{\mathrm{cris},\mathcal{O}_K} = \varprojlim_n A^0_{\mathrm{cris},\mathcal{O}_K}/\pi_K^n = \varprojlim_n A^0_{\mathrm{cris},\mathcal{O}_K}/p^n \subset B^+_{\mathrm{dR},K} = B^+_{\mathrm{dR}}$$

and consequently we have the inclusion ι.

7.1.3 Frobenius action φ on B_{cris}.

Recall on $W(R)$, we have a Frobenius map

$$\varphi((a_0, a_1, \cdots, a_n, \cdots)) = (a_0^p, a_1^p, \cdots, a_n^p, \cdots).$$

For all $b \in W(R)$, $\varphi(b) \equiv b^p \bmod p$, thus

$$\varphi(\xi) = \xi^p + p\eta = p(\eta + (p-1)!\gamma_p(\xi)), \ \eta \in W(R),$$

and $\varphi(\xi^m) = p^m(\eta + (p-1)!\gamma_p(\xi))^m$. Therefore we can define

$$\varphi(\gamma_m(\xi)) := \frac{p^m}{m!}(\eta + (p-1)!\gamma_p(\xi))^m \in W(R)[\gamma_p(\xi)] \subset A^0_{\mathrm{cris}}.$$

As a consequence,

$$\varphi(A^0_{\mathrm{cris}}) \subset A^0_{\mathrm{cris}}.$$

By continuity, we extend φ to A_{cris} and B^+_{cris}. Then

$$\varphi(t) = \log([\varepsilon^p]) = \log([\varepsilon]^p) = p\log([\varepsilon]) = pt,$$

hence $\varphi(t) = pt$. Consequently φ is extended to B_{cris} by setting $\varphi(\frac{1}{t}) = \frac{1}{pt}$.

The action of φ commutes with the action of G_K: for any $g \in G_K$, $b \in B_{\mathrm{cris}}$, $\varphi(gb) = g(\varphi b)$.

7.1.4 The logarithm map.

To define the logarithm maps on $C^\times$ and $(\mathrm{Fr}\, R)^\times$, we need a basic fact:

Lemma 7.9. *For any positive integer N, let c_N be the least common multiple of integers from 1 to N, i.e., $c_N = \prod\limits_{\ell \le N} \ell^{[\log_\ell N]}$. Then*

$$\begin{aligned}&\sum_{n=1}^{N}(-1)^{n-1}\frac{X^n}{n} + \sum_{n=1}^{N}(-1)^{n-1}\frac{Y^n}{n} \\ =&\sum_{n=1}^{N}(-1)^{n-1}\frac{(XY+X+Y)^n}{n} + \frac{1}{c_N}P_N(X,Y)\end{aligned} \tag{7.5}$$

where $P_N(X,Y) \in \mathbb{Z}[X,Y]$ is a sum of monomials of degree $\ge N+1$.

Proof. Exercise.

The construction of the classical p-adic logarithm

$$\log : C^\times \to C$$

satisfying the key fact

$$\log(xy) = \log x + \log y,$$

is processed in the following four steps:

(a) For $x \in U_C^1$ which means $v(x-1) \geq 1$, set

$$\log x := \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(x-1)^n}{n}. \tag{7.6}$$

Then Lemma 7.9 implies $\log(xy) = \log(x) + \log(y)$. This function is in fact a bijection from U_C^1 to $p\mathcal{O}_C$, whose inverse is the exponential function

$$\exp : p\mathcal{O}_C \to U_C^1,\ \exp(x) := \sum_{n=0}^{\infty} \frac{x^n}{n!}. \tag{7.7}$$

(b) For $x \in U_C^+ = 1 + \mathfrak{m}_C = \{x \in C \mid v(x-1) > 0\}$, we define $\log : U_C^+ \to C$ by (7.6). Moreover, there exists $m \in \mathbb{N}$ such that $v(x^{p^m} - 1) \geq 1$, then

$$\log x = \frac{1}{p^m} \log(x^{p^m}). \tag{7.8}$$

One can also define $\log x$ via this identity.

(c) For $a \in U_C = \mathcal{O}_C^\times$, by the canonical decomposition

$$a = [\bar{a}]x,$$

where $\bar{a} \in \bar{k}^\times, [\bar{a}] \in W(\bar{k})$ and $x \in U_C^+$, set

$$\log a := \log x. \tag{7.9}$$

(d) Finally for $x \in C^\times$, suppose $v(x) = \frac{r}{s}$ with $r, s \in \mathbb{Z}$ and $s \geq 1$, then $v(x^s) = r = v(p^r)$ and $\frac{x^s}{p^r} = y \in \mathcal{O}_C^\times$. By the relation

$$\log(\frac{x^s}{p^r}) = \log y = s \log x - r \log p,$$

to define $\log x$, it suffices to define $\log p$. In particular, if set $\log p := 0$, the corresponding logarithm, usually denoted as $\log_p$, is called the Iwasawa logarithm, which means

$$\log_p x := \frac{1}{s} \log_p y = \frac{1}{s} \log y. \tag{7.10}$$

From now on, the logarithm on $C^\times$ used will be the Iwasawa logarithm.

Exercise 7.10. If $x \in U_C^+$, then $\log x = 0$ if and only if $x \in \boldsymbol{\mu}_{p^\infty}(C) = \boldsymbol{\mu}_{p^\infty}(\overline{K})$.

Similarly, we define the logarithm map

$$\log : (\operatorname{Fr} R)^\times \to B_{\mathrm{dR}},\ x \mapsto \log[x]$$

as follows, with the key rule

$$\log[xy] = \log[x] + \log[y] \tag{7.11}$$

enforced. Recall that

$$\begin{aligned} U_R^+ &= 1 + \mathfrak{m}_R = \{x \in R \mid v(x-1) > 0\} \supset \\ U_R^1 &= \{x \in R \mid v(x-1) \geq 1\}. \end{aligned}$$

For any $x \in U_R^+$, there exists $m \in \mathbb{N}$, $m \geq 1$, such that $x^{p^m} \in U_R^1$. Choose $x \in U_R^1$, then the Teichmüller representative of x is $[x] = (x, 0, \cdots) \in W(R)$.

(1) For $x \in U_R^1$, set

$$\log[x] := \sum_{n=1}^{\infty} (-1)^{n-1} \frac{([x]-1)^n}{n} = ([x]-1) \sum_{n=0}^{\infty} (-1)^n \frac{([x]-1)^n}{n+1}. \tag{7.12}$$

This series converges in A_{cris}: one has

$$\theta([x]-1) = x^{(0)} - 1 \implies \bar{\theta}([x]-1) = 0,$$

hence $\gamma_n([x]-1) = \frac{([x]-1)^n}{n!} \in A_{\mathrm{cris}}$ and

$$\log[x] = \sum_{n=0}^{\infty} (-1)^{n-1} (n-1)!\, \gamma_n([x]-1)$$

converges since $(n-1)! \to 0$ when $n \to \infty$. We thus get

$$\log : U_R^1 \longrightarrow A_{\mathrm{cris}}, \quad x \longmapsto \log[x].$$

By Lemma 7.9, we know (7.11) is satisfied. We also see easily that $\log[x] = 0$ only if $x = 1$, thus the logarithm map is injective.

(2) For $x \in U_R^+$, suppose $m \gg 0$ such that $x^{p^m} \in U_R^1$, then the logarithm map on U_R^1 extends uniquely to B_{cris}^+ by

$$\log : \ U_R^+ \to B_{\mathrm{cris}}^+, \quad \log[x] := \frac{1}{p^m} \log[x^{p^m}]. \tag{7.13}$$

(7.11) implies that this definition is independent of the choice of m.

(3) For $a \in R^\times$, we define

$$\log[a] := \log[x] \tag{7.14}$$

by using the decomposition $R^\times = \bar{k}^\times \times U_R^+$, $a = a_0 x$ for $a_0 \in \bar{k}^\times$, $x \in U_R^+$.

(4) Finally, for any $x \in (\mathrm{Fr}\, R)^\times$, suppose $v(x) = \frac{r}{s}$, with $r, s \in \mathbb{Z}$ and $s \geq 1$. Recall $\varpi \in R$ is given by $\varpi^{(0)} = -p, v(\varpi) = 1$. Then $\frac{x^s}{\varpi^r} = y \in R^\times$. Hence the relation

$$\log\left[\frac{x^s}{\varpi^r}\right] = \log[y] = s\log[x] - r\log[\varpi],$$

implies that

$$\log[x] = \frac{1}{s}(r\log[\varpi] + \log[y]).$$

Thus in order to define $\log[x]$, it suffices to define $\log[\varpi]$.

Note that $\theta\left(\frac{[\varpi]}{-p} - 1\right) = \frac{-p}{-p} - 1 = 0$, then

$$\log\left(\frac{[\varpi]}{-p}\right) = \sum_{n=1}^{\infty}(-1)^{n-1}\frac{(\frac{[\varpi]}{-p}-1)^n}{n} = -\sum_{n=1}^{\infty}\frac{\xi^n}{np^n}$$

is a well defined element in B_{dR}^+. Set

$$\mathbf{u} = \log[\varpi] := \log\left(\frac{[\varpi]}{-p}\right) = -\sum_{n=1}^{\infty}\frac{\xi^n}{np^n} \in B_{\mathrm{dR}}^+. \tag{7.15}$$

Then we get the desired logarithm map

$$\log:\ (\operatorname{Fr} R)^\times \longrightarrow B_{\mathrm{dR}}^+, \quad x \longmapsto \log[x].$$

We note that the logarithm map commutes with G_K-action. Moreover, for $x \in (\operatorname{Fr} R)^\times$, if set $\varphi(\log[x]) = \log[\varphi(x)]$, then $\varphi(\log[x]) = p\log[x]$. In this way, φ extends to $\operatorname{Im}(\log:\ (\operatorname{Fr} R)^\times \to B_{\mathrm{dR}}^+)$.

Definition 7.11. *Set* $U := \operatorname{Im}(\log:\ U_R^+ \to B_{\mathrm{cris}}^+) \subset (B_{\mathrm{cris}}^+)^{\varphi=p}$.

Clearly $t = \log[\varepsilon] \in U$.

Lemma 7.12. *The kernel of* $\log: R^\times \to U \hookrightarrow B_{\mathrm{cris}}^+$ *is* $\bar{k}^\times$*, and the isomorphism* $\log: U_R^+ \cong U$ *induces the following commutative diagram with exact rows*

$$\begin{tikzcd}
0 \arrow[r] & \varepsilon^{\mathbb{Q}_p} \arrow[r] \arrow[d, "\cong"] & U_R^+ \arrow[r, "\log^{(0)}"] \arrow[d, "\cong"] & C \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{Q}_p t \arrow[r] \arrow[d, hook] & U \arrow[r, "\theta"] \arrow[d, hook] & C \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \operatorname{Fil}^1 B_{\mathrm{dR}} \arrow[r] & B_{\mathrm{dR}}^+ \arrow[r, "\theta"] & C \arrow[r] & 0
\end{tikzcd}$$

where $\log^{(0)}: U_R^+ \to C$ *is given by* $x \mapsto \log x^{(0)}$*. As a consequence,*

$$U \cap \operatorname{Fil}^1 B_{\mathrm{dR}} = \mathbb{Q}_p t = \mathbb{Q}_p(1), \qquad U + \operatorname{Fil}^1 B_{\mathrm{dR}} = B_{\mathrm{dR}}^+. \tag{7.16}$$

Proof. Clear.

Remark 7.13. We shall see in Theorem 7.28 that $U = \{u \in B_{\mathrm{cris}}^+ \mid \varphi u = pu\}$.

We need to know more about $\mathbf{u} = \log[\varpi]$. For every $g \in G_{K_0}$, $g\varpi = \varpi\varepsilon^{\eta(g)}$ where $\eta : G_{K_0} \to \mathbb{Z}_p^\times$ is a character of G_{K_0}, thus

$$g(\mathbf{u}) = \log([g\varpi]) = \mathbf{u} + \eta(g)t. \tag{7.17}$$

Proposition 7.14. *The element* $\mathbf{u}$ *is transcendental over* C_{cris}*, the field of fractions of* B_{cris}*.*

We need a lemma:

Lemma 7.15. $\mathbf{u}$ *is not contained in* C_{cris}*.*

Proof. Let $\beta = \xi/p$, then ξ and β are both inside $\mathrm{Fil}^1 B_{\mathrm{dR}}$ but not $\mathrm{Fil}^2 B_{\mathrm{dR}}$. Let $S = W(R)[[\beta]] \subset B_{\mathrm{dR}}^+$ be the subring of power series $\sum a_n\beta^n$ with coefficients $a_n \in W(R)$. For every $i \in \mathbb{N}$, let $\mathrm{Fil}^i S = S \cap \mathrm{Fil}^i B_{\mathrm{dR}}$, then $\mathrm{Fil}^i S$ is a principal ideal of S generated by β^i. We denote by

$$\theta^i : \mathrm{Fil}^i B_{\mathrm{dR}} \longrightarrow \mathcal{O}_C$$

the map $\beta^i\alpha \mapsto \theta(\alpha)$. Then $\theta^i(\mathrm{Fil}^i S) = \mathcal{O}_C$.

By construction, $A_{\mathrm{cris}} \subset S$ and hence $C_{\mathrm{cris}} = \mathrm{Frac}\, A_{\mathrm{cris}} \subset \mathrm{Frac}(S)$. We show that $\alpha\mathbf{u} \notin S$ for all $0 \neq \alpha \in S$, which is sufficient for the lemma.

By Lemma 7.2, S is separated by the p-adic topology, it suffices to show that if $r \in \mathbb{N}$ and $\alpha \in S - pS$, then $p^r\alpha\mathbf{u} \notin S$. Write $\alpha = \sum_n c_n\beta^n$ wth $c_n \in W(R)$. If for all n, $\theta(c_n) \in p\mathcal{O}_C$, then $c_n \in (p,\xi)W(R) \subseteq pS$ and $\alpha \in pS$, which is not possible. Thus there exists $i < +\infty$ such that $\theta(c_i) \notin p\mathcal{O}_C$ and $\theta(c_n) \in p\mathcal{O}_C$ for $n < i$. In other word, we may write

$$\alpha = p\sum_{n<i} b_n\beta^n + b_i\beta^i + \sum_{n>i} b_n\beta^n := A_1 + A_2 + A_3$$

with $b_n \in W(R)$ and $\theta(b_i) \notin p\mathcal{O}_C$. Suppose $j \in \mathbb{N}$ such that $j > r$ and $p^j > i$. Write

$$-p^{j-1}\mathbf{u} = \sum_{n\geq 1} \frac{p^{j-1}\beta^n}{n} = \sum_{n<p^j} \frac{p^{j-1}\beta^n}{n} + \frac{\beta^{p^j}}{p} + \sum_{n>p^j} \frac{p^{j-1}\beta^n}{n} := B_1 + B_2 + B_3.$$

We are reduced to show $-p^{j-1}\alpha\mathbf{u} \notin S$. Note that

(a) $B_1 \in S$ and hence $\alpha B_1 \in S$, also clearly $A_1B_2 \in S$;
(b) A_3B_3, A_3B_2 and A_2B_3 are all in $\mathrm{Fil}^{i+p^j+1} B_{\mathrm{dR}}$;
(c) For all n such that $p^j < n \leq p^j + i < 2p^j$, $\frac{p^{j-1}\beta^n}{n} \cdot A_1 \in S$, hence $A_1B_3 \in S + \mathrm{Fil}^{i+p^j+1} B_{\mathrm{dR}}$;
(d) $A_2B_2 = b_i\beta^{i+p^j}/p \in \mathrm{Fil}^{i+p^j} B_{\mathrm{dR}}$.

Thus if $-p^{j-1}\alpha\mathbf{u} \in S$, then

$$b_i\beta^{i+p^j}/p \in \mathrm{Fil}^{i+p^j} B_{\mathrm{dR}} \cap (S + \mathrm{Fil}^{i+p^j+1} B_{\mathrm{dR}}) = \mathrm{Fil}^{i+p^j} S + \mathrm{Fil}^{i+p^j+1} B_{\mathrm{dR}}.$$

Now on one hand, $\theta^{i+p^j}(b_i\beta^{i+p^j}/p) = \theta(b_i)/p \notin \mathcal{O}_C$; on the other hand,

$$\theta^{i+p^j}(\mathrm{Fil}^{i+p^j} S + \mathrm{Fil}^{i+p^j+1} B_{\mathrm{dR}}) = \mathcal{O}_C,$$

we have a contradiction.

Proof (Proof of Proposition 7.14). If $\mathbf{u}$ is not transcendental, suppose $c_0 + c_1X + \cdots + c_{d-1}X^{d-1} + X^d$ is the minimal polynomial of $\mathbf{u}$ in C_{cris}. By (7.17), for $g \in G_{K_0}$, $g\mathbf{u} = \mathbf{u} + \eta(g)t$. Since C_{cris} is stable by G_{K_0}, then

$$g(c_0) + \cdots + g(c_{d-1})(\mathbf{u} + \eta(g)t)^{d-1} + (\mathbf{u} + \eta(g)t)^d = 0.$$

By the uniqueness of the minimal polynomial, for every $g \in G_{K_0}$, one has $g(c_{d-1}) + d\cdot\eta(g)t = c_{d-1}$. Let $c = c_{d-1} + d\mathbf{u}$, then $g(c) = c$ and $c \in (B_{\mathrm{dR}})^{G_{K_0}} = K_0 \subset B_{\mathrm{cris}}$, thus $\mathbf{u} = d^{-1}(c - c_{d-1}) \in C_{\mathrm{cris}}$, which contradicts Lemma 7.15.

Corollary 7.16. *For the map* $\log : (\mathrm{Fr}\, R)^\times \to B_{\mathrm{dR}}^+$, *its kernel is* $\bar{k}^\times$ *and its image is* $U \oplus \mathbb{Q}_p\mathbf{u}$.

Proof. Exercise.

7.2 Interaction of Filtration and Frobenius on B_{cris}.

Definition 7.17. *Suppose* A *is a subring of* B_{dR} *(in particular,* $A = W(R)$, $W(R)[\frac{1}{p}]$, $W_K(R) = W(R)[\frac{1}{p}] \otimes_{K_0} K$, A_{cris}, B_{cris}^+, B_{cris}*).*

(i) *For every* $r \in \mathbb{Z}$, *set* $\mathrm{Fil}^r A := A \cap \mathrm{Fil}^r B_{\mathrm{dR}}$. *Denote by* $\theta : \mathrm{Fil}^0 A = A \cap B_{\mathrm{dR}}^+ \to C$ *the restriction of* $\theta : B_{\mathrm{dR}}^+ \to C$.
(ii) *If* A *is moreover a subring of* B_{cris} *stable by* φ, *set*

$$I^{[r]}A := \{a \in A \mid \varphi^n(A) \in \mathrm{Fil}^r A \text{ for } n \in \mathbb{N}\}. \tag{7.18}$$

By definition, if $I^{[0]}A = A$, i.e., $A \subseteq B_{\mathrm{dR}}^+$ (which is the case for $A = W(R)$, $W(R)[\frac{1}{p}]$, A_{cris} or B_{cris}^+), then $\{I^{[r]}A : r \in \mathbb{N}\}$ forms a decreasing sequence of ideals of A, which reveals the interaction between the filtration structure and the Frobenius action on A. We write $I^{[1]}A = IA$ in this case.

We shall study $I^{(r)}W(R)$ and $I^{(r)}A_{\mathrm{cris}}$ in this section.

7.2.1 The ideals $I^{(r)}W(R)$.

For $x \in R$, let $x' = x^{p^{-1}} = \varphi^{-1}(x)$. For $x \in W(R)$, let $x' = \varphi^{-1}(x)$, and let $\bar{x} \in R$ be the reduction of x modulo p. Then $\bar{\boldsymbol{\pi}} = \pi = \varepsilon - 1$. Set

$$\tau := \frac{\boldsymbol{\pi}}{\boldsymbol{\pi}'} = \frac{[\varepsilon]-1}{[\varepsilon']-1} = 1 + [\varepsilon'] + \cdots + [\varepsilon']^{p-1}. \tag{7.19}$$

Then we have $\theta(\tau) = \sum_{0 \le i \le p-1} (\varepsilon^{(1)})^i = 0$,

$$\bar{\tau} = 1 + \varepsilon' + \cdots + \varepsilon'^{p-1} = \frac{\varepsilon - 1}{\varepsilon' - 1},$$

and $v(\bar{\tau}) = \frac{p}{p-1} - \frac{1}{p-1} = 1$, hence τ is a generator of $\operatorname{Ker}\theta$.

Proposition 7.18. *Suppose $r \in \mathbb{N}$.*

(1) *The ideal $I^{[r]}W(R)$ is the principal ideal generated by $\boldsymbol{\pi}^r$. In particular, $I^{[r]}W(R)$ is the r-th power of $IW(R)$.*
(2) *For every element $a \in I^{[r]}W(R)$, a generates this ideal if and only if $v(\bar{a}) = \frac{rp}{p-1}$.*

We first show the case $r = 1$, which is the following lemma:

Lemma 7.19. (1) *The ideal $IW(R)$ is principal, generated by $\boldsymbol{\pi}$.*
(2) *For every element $a = (a_0, a_1, \cdots) \in IW(R)$, a generates the ideal $IW(R)$ if and only if $v(a_0) = \frac{p}{p-1}$. In this case, $v(a_n) = \frac{p}{p-1}$ for every $n \in \mathbb{N}$.*

Proof. For $a = (a_0, \cdots, a_n, \cdots) \in IW(R)$, let $\alpha_n = a_n^{n}$, then for every $m \in \mathbb{N}$,

$$\theta(\varphi^m a) = \sum_{n \ge 0} p^n \alpha_n^{p^m} = \alpha_0^{p^m} + \cdots + p^m \alpha_m^{p^m} + p^{m+1}\alpha_{m+1}^{p^m} + \cdots = 0. \tag{7.20}$$

We claim that for any pair $(r, m) \in \mathbb{N} \times \mathbb{N}$, one has $v(\alpha_m) \ge p^{-m}(1 + p^{-1} + \cdots + p^{-r})$. This can be shown by induction to the pair (r, m) ordered by the lexicographic order:

(a) If $r = m = 0$, $\theta(a) = \alpha_0 \pmod p$, thus $v(\alpha_0) \ge 1$.
(b) If $r = 0$, but $m \ne 0$, one has

$$0 = \theta(p^m a) = \sum_{n=0}^{m-1} p^n \alpha_n^{p^m} + p^m \alpha_m^{p^m} \pmod{p^{m+1}};$$

by induction hypothesis, for $0 \le n \le m-1$, $v(\alpha_n) \ge p^{-n}$, thus $v(p^n \alpha_n^{p^m}) \ge n + p^{m-n} \ge m+1$, hence $v(p^m \alpha_m^{p^m}) \ge m+1$ and $v(\alpha_m) \ge p^{-m}$.

(c) If $r \neq 0$, one has

$$0 = \theta(p^m a) = \sum_{n=0}^{m-1} p^n \alpha_n^{p^m} + p^m \alpha_m^{p^m} \sum_{n=m+1}^{\infty} p^n \alpha_n^{p^m};$$

by induction hypothesis,
- for $0 \leq n \leq m-1$, $v(\alpha_n) \geq p^{-n}(1+p^{-1}+\cdots p^{-r})$, thus

$$v(p^n \alpha_n^{p^m}) \geq n + p^{m-n}(1+\cdots p^{-r}) \geq m + (1+\cdots p^{-r});$$

- for $n \geq m+1$, $v(\alpha_n) \geq p^{-n}(1+\cdots p^{-r+1})$, thus

$$v(p^n \alpha_n^{p^m}) \geq n + p^{m-n}(1+\cdots p^{-r+1}) \geq m + (1+\cdots p^{-r});$$

one thus has $v(\alpha_m) \geq p^{-m}(1+\cdots+p^{-r})$.

By the claim, if $a \in IW(R)$, $v(\alpha_n) \geq p^n \cdot \frac{p}{p-1}$, thus $v(a_n) \geq \frac{p}{p-1}$. On the other hand, for any $n \in \mathbb{N}$, $\theta(\varphi^n \boldsymbol{\pi}) = \theta([\varepsilon]^{p^n} - 1) = 0$, thus $\boldsymbol{\pi} \in IW(R)$. As $v(\varepsilon - 1) = \frac{p}{p-1}$, the claim implies $IW(R) \subseteq (\boldsymbol{\pi}, p)$. But the set $(\mathcal{O}_C)^{\mathbb{N}}$ is p-torsion free, thus if $px \in IW(R)$, then $x \in IW(R)$. Hence $IW(R) = (\boldsymbol{\pi})$ and $v(a_0) = \frac{p}{p-1}$.

By induction to n, repeatedly applying (7.20) and the condition $v(a_n) \geq \frac{p}{p-1}$, we obtain $v(a_n) = \frac{p}{p-1}$.

Proof (Proof of the Proposition). Let $\mathrm{gr}^i W(R) = \mathrm{Fil}^i W(R)/\mathrm{Fil}^{i+1} W(R)$ and let θ^i be the projection from $\mathrm{Fil}^i W(R)$ to $\mathrm{gr}^i W(R)$. As $\mathrm{Fil}^i W(R)$ is the principal ideal generated by τ^i, $\mathrm{gr}^i W(R)$ is a free $\mathcal{O}_C$-module of rank 1 generated by $\theta^i(\tau^i) = \theta^1(\tau)^i$. Note that $\boldsymbol{\pi} = \boldsymbol{\pi}'\tau$, then

$$\varphi^n(\boldsymbol{\pi}) = \boldsymbol{\pi}' \tau^{1+\varphi+\cdots+\varphi^n} \text{ for every } n \in \mathbb{N}.$$

For $i \geq 1$, $\theta(\varphi^i(\tau)) = p$, hence $\theta^1(\varphi^n(\boldsymbol{\pi})) = p^n(\varepsilon^{(1)} - 1) \cdot \theta^1(\tau)$.

Proof of (1): The inclusion $\boldsymbol{\pi}^r W(R) \subseteq I^{[r]}$ is clear. We show $\boldsymbol{\pi}^r W(R) \supseteq I^{[r]}$ by induction. The case $r = 0$ is trivial. Suppose $r \geq 1$. If $a \in I^{(r)}W(R)$, by induction hypothesis, we can write $a = \boldsymbol{\pi}^{r-1} b$ with $b \in W(R)$. We know that $\theta^{r-1}(\varphi^n(a)) = 0$ for every $n \in \mathbb{N}$. But

$$\theta^{r-1}(\varphi^n(a)) = \theta(\varphi^n(b)) \cdot (\theta^1(\varphi^n(\boldsymbol{\pi})))^{r-1} = (p^n(\varepsilon^{(1)} - 1))^{r-1} \cdot \theta(\varphi^n(b)) \cdot \theta^1(\tau)^{r-1}.$$

Since $\theta^1(\tau)^{r-1}$ is a generator of $\mathrm{gr}^{r-1} W(R)$ and since $p^n(\varepsilon^{(1)} - 1) \neq 0$, one must have $\theta(\varphi^n(b)) = 0$ for every $n \in \mathbb{N}$, hence $b \in IW(R)$. By the precedent lemma, there exists $c \in W(R)$ such that $b = \boldsymbol{\pi} c$. Thus $a \in \boldsymbol{\pi}^r W(R)$.

Proof of (2): It follows immediately from that $v(\overline{\boldsymbol{\pi}^r}) = rv(\varepsilon - 1) = \frac{rp}{p-1}$, and that $x \in W(R)$ is a unit if and only if $\bar{x}$ is a unit in R, i.e. if $v(\bar{x}) = 0$.

7.2.2 A description of A_{cris}.

For $n \in \mathbb{N}$, write $n = r_n + (p-1)q_n$ with $r_n, q_n \in \mathbb{N}$ and $0 \le r_n < p-1$ and set

$$t^{\{n\}} := t^{r_n}\gamma_{q_n}(t^{p-1}/p) = (p^{q_n} \cdot q_n!)^{-1} \cdot t^n. \tag{7.21}$$

Note that

(a) if $p = 2$, $t^{\{n\}} = t^n/(2^n n!) = \gamma_n(t/2)$, and $t^{\{2n\}} = \gamma_{2n}(t/2) = \frac{1}{(2n-1)!!}\gamma_n(t^2/8)$;
(b) if $p > 2$, $t^{\{(p-1)n\}} = \gamma_n(t^{p-1}/p)$.

We have shown that $t^{p-1}/p \in A_{\mathrm{cris}}$, therefore $t^{\{n\}} \in A_{\mathrm{cris}}$. We denote

$$\Lambda_\varepsilon := \left\{ \sum_{n\in\mathbb{N}} a_n t^{\{n\}} \mid a_n \in W, \lim_{n\to\infty} a_n = 0 \right\} \subset K_0[[t]] \cap A_{\mathrm{cris}}, \tag{7.22}$$

$$\mathbf{O}_\varepsilon := W[[\boldsymbol{\pi}]]. \tag{7.23}$$

By the fact

$$\boldsymbol{\pi} = e^t - 1 = \sum_{n\ge1} \frac{t^n}{n!} = \sum_{n\ge1} \frac{p^{q_n} q_n!}{n!} t^{\{n\}} \in \Lambda_\varepsilon,$$

then

$$S_\varepsilon \subseteq \Lambda_\varepsilon \subseteq A_{\mathrm{cris}}$$

are sub-W-algebras of A_{cris} stable by the actions of φ and of G_{K_0} which factors through $\Gamma_{K_0} = \mathrm{Gal}(K_0^{\mathrm{cyc}}/K_0)$. We also see that

$$t = \log([\varepsilon]) = \boldsymbol{\pi} \cdot \sum_{n\ge0} (-1)^n \frac{\boldsymbol{\pi}^n}{n+1} = \boldsymbol{\pi} \cdot u,$$

where u is a unit in Λ_ε. Recall Δ_{K_0} is the torsion subgroup of Γ_{K_0}, set

$$\mathbf{O} := \mathbf{O}_\varepsilon^{\Delta_{K_0}} \subset \Lambda := \Lambda_\varepsilon^{\Delta_{K_0}}, \tag{7.24}$$

$$\pi_0 = -p + \sum_{a\in\mathbb{F}_p} [\varepsilon]^{[a]} = (p-1) \sum_{\substack{n\ge1\\ p-1\mid n}} \frac{t^n}{n!} \quad (\text{resp. } 2\sum_{\substack{n\ge1\\ 2\mid n}} \frac{t^n}{n!}) \in \mathbf{O}. \tag{7.25}$$

Lemma 7.20. *If $p \neq 2$, then*

$$\begin{aligned}\Lambda &= \left\{ \sum_{n\in\mathbb{N}} a_n \gamma_n(t^{p-1}/p) \mid a_n \in W, \lim_{n\to\infty} a_n = 0 \right\} \\ &= \left\{ \sum_{n\in\mathbb{N}} a_n \gamma_n(\pi_0/p) \mid a_n \in W, \lim_{n\to\infty} a_n = 0 \right\};\end{aligned}$$

if $p = 2$, then replacing t^{p-1}/p by $t^2/8$ and π_0/p by $\pi_0/8$. And

$$\mathbf{O} = W[[\pi_0]], \qquad \mathbf{O}_\varepsilon \otimes_{\mathbf{O}} \Lambda = \Lambda_\varepsilon.$$

Proof. Since the subfield of $K_0((t))$ fixed by Δ_{K_0} is $K_0((t^{p-1}))$ (resp. $K((t^2))$ if $p=2$), we get the first identity for Λ.

By computation $\pi_0 = \boldsymbol{\pi}^{p-1}w$ (resp. $\boldsymbol{\pi}^2 w$) for some unit $w \in \mathbf{O}^\times$. Thus $\mathbf{O} = W[[\boldsymbol{\pi}^{p-1}]] = W[[\pi_0]]$. Now by the relation $t = \boldsymbol{\pi}u$, we can replace t^{p-1}/p (resp. $t^2/8$) by π_0/p (resp. $\pi_0/8$) to get the second identity for Λ. One also sees the evident identification $\mathbf{O}_\varepsilon \otimes_{\mathbf{O}} \Lambda = \Lambda_\varepsilon$.

Proposition 7.21. (1) *The element π_0 is a generator of $I^{[p-1]}W(R)$ if $p \neq 2$ (resp. of $I^{[2]}W(R)$ if $p=2$).*
(2) *There exists a unit $u \in \mathbf{O}$ such that*

$$\varphi\pi_0 = u\pi_0(p+\pi_0)^{p-1} \text{ if } p \neq 2 \text{ (resp. } u\pi_0(p+\pi_0)^2 \text{ if } p=2).$$

Proof. We just show the case $p \neq 2$, the case $p=2$ is analogous.

Proof of (1): Let π_1 be the norm of $\boldsymbol{\pi}$ over the field extension $K_0((t))/K_0((t^{p-1}))$. Then

$$\pi_1 = \prod_{h \in \Delta_{K_0}} h(\boldsymbol{\pi}) = \prod_{a \in \mathbb{F}_p^\times} ([\varepsilon]^{[a]} - 1) \in \mathbf{O}.$$

By Proposition 7.18, since $[\varepsilon]^{[a]} - 1$ is a generator of $IW(R)$, π_1 is a generator of $I^{[p-1]}W(R)$. Since $\pi_1 = \boldsymbol{\pi}^{p-1}w$ for some unit $w \in \mathbf{O}$, $\mathbf{O} = W[[\boldsymbol{\pi}^{p-1}]] = W[[\pi_1]]$. We can write $\pi_0 = \sum_{m \geq 1} a_m \pi_1^m$ where $a_m \in W$ and a_1 is a unit. Moreover, since $a_0 = \theta(\pi_0) = 0$, π_0 generates the same ideal as π_1.

Proof of (2): Write $q = p + \pi_0 = \sum_{a \in \mathbb{F}_p} [\varepsilon]^{[a]}$ and $q' = \varphi^{-1}(q)$. By computation, q', like τ, is a generator of the kernel of the restriction of θ to $\mathbf{O}'_\varepsilon = \varphi^{-1}(\mathbf{O}_\varepsilon) = W[[\boldsymbol{\pi}']]$, thus

$$\boldsymbol{\pi} = \varphi(\boldsymbol{\pi}') = \boldsymbol{\pi}'\tau = u_1'\boldsymbol{\pi}'q'$$

with u_1' a unit in $\mathbf{O}'_\varepsilon$. Then $\varphi(\boldsymbol{\pi}) = u_1\boldsymbol{\pi}q$ and $\varphi(\boldsymbol{\pi}^{p-1}) = u_1^{p-1}\boldsymbol{\pi}^{p-1}q^{p-1}$. Since π_0 and $\boldsymbol{\pi}^{p-1}$ are two generators of $\mathbf{O}_\varepsilon \cap I^{[p-1]}W(R)$, $\varphi(\pi_0) = u\pi_0 q^{p-1}$ with u a unit in $\mathbf{O}_\varepsilon$. Now the uniqueness of u and the fact that $\mathbf{O} = \mathbf{O}_\varepsilon^{\Delta_{K_0}}$ imply that u and $u^{-1} \in \mathbf{O}$.

If A_0 is a commutative ring, A_1 and A_2 are two A_0 algebras such that A_1 and A_2 are separated and complete by the p-adic topology, we let $A_1 \widehat{\otimes}_{A_0} A_2$ be the separate completion of $A_1 \otimes_{A_0} A_2$ by the p-adic topology.

Theorem 7.22. *One has an isomorphism of $W(R)$-algebras*

$$\alpha: \quad W(R)\widehat{\otimes}_{\mathbf{O}}\Lambda \longrightarrow A_{\mathrm{cris}}$$

which is continuous by p-adic topology, given by

$$\alpha\left(\sum a_m \otimes \gamma_m(\frac{\pi_0}{p})\right) = \sum a_m \gamma_m(\frac{\pi_0}{p}).$$

The isomorphism α thus induces an isomorphism

$$\alpha_\varepsilon: \quad W(R)\widehat{\otimes}_{\mathbf{O}_\varepsilon}\Lambda_\varepsilon \longrightarrow A_{\mathrm{cris}}.$$

Proof. The isomorphism α_ε comes from

$$W(R)\widehat{\otimes}_{\mathbf{O}_\varepsilon}\Lambda_\varepsilon \cong W(R)\widehat{\otimes}_{\mathbf{O}_\varepsilon}\mathbf{O}_\varepsilon \otimes_{\mathbf{O}} \Lambda \cong W(R)\widehat{\otimes}_{\mathbf{O}}\Lambda$$

and the isomorphism α. We only consider the case $p \neq 2$ ($p = 2$ is analogous).

As q' is a generator of $\operatorname{Ker}\theta$ and $q'^p = p!\gamma_p(q') \in pA_{\mathrm{cris}}$, $\pi_0 = q - p \in pA_{\mathrm{cris}}$ and $\pi_0/p \in \mathrm{Fil}^1 A_{\mathrm{cris}}$. Thus the homomorphism α is well defined and continuous. We are left to show that α is an isomorphism. Since both the source and the target are rings separated and complete by p-adic topology without p-torsion, it suffices to show that α induces an isomorphism on reduction modulo p.

But $A_{\mathrm{cris}}/pA_{\mathrm{cris}} = A^0_{\mathrm{cris}}/pA^0_{\mathrm{cris}}$ is the divided power envelope of R relative to the ideal generated by $\overline{q'}$, thus it is the free module over $R/\overline{q'^p}$ with a basis consisting of the images of $\gamma_{pm}(q')$ or equivalently of $\gamma_m(\frac{q'^p}{p})$. By the previous proposition, $\varphi(\pi_0) = u\pi_0 q^{p-1}$, thus $\pi_0 = u'\pi_0' q'^{p-1} = u'(q'^p - pq'^{p-1})$, which implies that $R/\overline{q'^p} = R/\overline{\pi_0}$ and $A_{\mathrm{cris}}/pA_{\mathrm{cris}}$ is the free module over $R/\overline{\pi_0}$ with a basis consisting of the images of $\gamma_m(\frac{\pi_0}{p})$. It is clear this is also the case for the ring $W(R)\widehat{\otimes}_{\mathbf{O}}\Lambda$ modulo p.

7.2.3 Filtration of A_{cris} by $I^{[r]} = I^{[r]}A_{\mathrm{cris}}$.

Proposition 7.23. *For every $r \in \mathbb{N}$, write $I^{[r]} = I^{[r]}A_{\mathrm{cris}}$. Then if $r \geq 1$, $I^{[r]}$ is a divided power ideal of A_{cris} which is the associated sub-$W(R)$-module (and also an ideal) of A_{cris} generated by $t^{\{s\}}$ for $s \geq r$.*

Proof. Suppose $I(r)$ is the sub-$W(R)$-module generated by $t^{\{s\}}$ for $s \geq r$. It is clear that $I(r) \subseteq I^{[r]}$ and $I(r)$ is a divided power ideal.

It remains to show that $I^{[r]} \subseteq I(r)$. We show this by induction on r. The case $r = 0$ is trivial.

Suppose $r \geq 1$ and $a \in I^{[r]}$. The induction hypothesis allows us to write a as the form

$$a = \sum_{s \geq r-1} a_s t^{\{s\}}$$

where $a_s \in W(R)$ tends p-adically to 0. If $b = a_{r-1}$, we have $a = bt^{\{r-1\}} + a'$ where $a' \in I(r) \subseteq I^{[r]}$, thus $bt^{\{r-1\}} \in I^{[r]}$. But

$$\varphi^n(bt^{\{r-1\}}) = p^{(r-1)n} \cdot \varphi^n(b) \cdot t^{\{r-1\}} = c_{r,n} \cdot \varphi^n(b) \cdot t^{r-1}$$

where $c_{r,n}$ is a nonzero rational number. Since $t^{r-1} \in \mathrm{Fil}^{r-1} - \mathrm{Fil}^r$, one has $b \in I^{[1]} \cap W(R)$, which is the principal ideal generated by $\boldsymbol{\pi}$. Thus $bt^{\{r-1\}}$ belongs to an ideal of A_{cris} generated by $\boldsymbol{\pi}t^{\{r-1\}}$. But in A_{cris}, t and $\boldsymbol{\pi}$ generate the same ideal as $t = \boldsymbol{\pi} \times (\text{unit})$, hence $bt^{\{r-1\}}$ belongs to an ideal generated by $t \cdot t^{\{r-1\}}$, which is contained in $I(r)$.

For every $r \in \mathbb{N}$, we let

$$A^r_{\mathrm{cris}} = A_{\mathrm{cris}}/I^{[r]}, \quad W^r(R) = W(R)/I^{[r]}W(R). \tag{7.26}$$

Proposition 7.24. *For every $r \in \mathbb{N}$, A^r_{cris} and $W^r(R)$ have no p-torsion. The natural map*

$$\iota^r: \quad W^r(R) \longrightarrow A^r_{\mathrm{cris}}$$

are injective, and its cokernel is p-torsion, annihilated by $p^m m!$ where m is the largest integer such that $(p-1)m < r$, i.e., $m = [\frac{r-1}{p-1}]$.

Proof. For every $r \in \mathbb{N}$, $A_{\mathrm{cris}}/\operatorname{Fil}^r A_{\mathrm{cris}}$ is torsion free. The kernel of the map

$$A_{\mathrm{cris}} \to (A_{\mathrm{cris}}/\operatorname{Fil}^r A_{\mathrm{cris}})^{\mathbb{N}}, \quad x \mapsto (\varphi^n x \bmod \operatorname{Fil}^r)_{n \in \mathbb{N}}$$

is nothing but $I^{[r]}$, thus

$$A^r_{\mathrm{cris}} \hookrightarrow (A_{\mathrm{cris}}/\operatorname{Fil}^r A_{\mathrm{cris}})^{\mathbb{N}}$$

is torsion free. As ι^r is injective by definition, $W^r(R)$ is also torsion free.

As a $W(R)$-module, A^r_{cris} is generated by the images of $\gamma_s(p^{-1}\pi_0)$ for $0 \leq (p-1)s < r$, since $p^s s! \gamma_s(p^{-1}\pi_0) \in W(R)$, and $v(p^s s!)$ is increasing, we have the proposition.

Proposition 7.25. *For $r \in \mathbb{N}$, let $\operatorname{Fil}^r_p A_{\mathrm{cris}} = \{x \in \operatorname{Fil}^r A_{\mathrm{cris}} \mid \varphi x \in p^r A_{\mathrm{cris}}\}$.*

(1) *The sequence*

$$0 \longrightarrow \mathbb{Z}_p t^{\{r\}} \longrightarrow \operatorname{Fil}^r_p A_{\mathrm{cris}} \xrightarrow{p^{-r}\varphi - 1} A_{\mathrm{cris}} \longrightarrow 0$$

is exact.

(2) *The ideal $\operatorname{Fil}^r_p A_{\mathrm{cris}}$ is the associated sub-$W(R)$-module of A_{cris} generated by $q'^j \gamma_n(p^{-1}t^{p-1})$, for $j + (p-1)n \geq r$.*

(3) *If m is the largest integer such that $(q-1)m < r$, then for every $x \in \operatorname{Fil}^r A_{\mathrm{cris}}$, $p^m m! x \in \operatorname{Fil}^r_p A_{\mathrm{cris}}$.*

Proof. Write $\nu = p^{-r}\varphi - 1$. It is clear that $\mathbb{Z}_p t^{\{r\}} \subseteq \operatorname{Ker} \nu$. Conversely, if $x \in \operatorname{Ker} \nu$, then $x \in I^{[r]}$ and can be written as

$$x = \sum_{s \geq r} a_s t^{\{s\}}, \ a_s \in W(R) \text{ tends to } 0 \ p\text{-adically}.$$

Note that for every $n \in \mathbb{N}$, $(p^{-r}\varphi)^n(x) \equiv \varphi^n(a_r)t^{\{r\}} \pmod{p^n A_{\mathrm{cris}}}$, thus $x = bt^{\{r\}}$ with $b \in W(R)$ and moreover, $\varphi(b) = b$, i.e. $b \in \mathbb{Z}_p$.

Let N be the associated sub-$W(R)$-module of A_{cris} generated by $q'^j\gamma_n(\frac{t^{p-1}}{p})$, for $j + (p-1)n \geq r$. If $j, n \in \mathbb{N}$, one has

$$\varphi(q'^j \gamma_n(\frac{t^{p-1}}{p})) = q^j p^{n(p-1)} \gamma_n(\frac{t^{p-1}}{p}) = p^{j+n(p-1)}(1 + \frac{\pi_0}{p})^j \gamma_n(\frac{t^{p-1}}{p}),$$

thus $N \subseteq \operatorname{Fil}^r_p A_{\mathrm{cris}}$.

Since $\mathbb{Z}_p t^{\{r\}} \subseteq N$, to prove the first two assertions, it suffices to show that for every $a \in A_{\mathrm{cris}}$, there exists $x \in N$ such that $\nu(x) = a$. Since N and A_{cris} are separated and complete by the p-adic topology, it suffices to show that for every $a \in A_{\mathrm{cris}}$, there exists $x \in N$, such that $\nu(x) \equiv a \pmod p$. If $a = \sum_{n > r/p-1} a_n \gamma_n(\frac{t^{p-1}}{p})$ with $a_n \in W(R)$, we can just take $x = -a$.

Thus it remains to check that for every $i \in \mathbb{N}$ such that $(p-1)i \leq r$ and for $b \in W(R)$, there exists $x \in N$ such that $\nu(x) - b\gamma_i(\frac{t^{p-1}}{p})$ is contained in the ideal M generated by p and $\gamma_n(p^{-1}t^{p-1})$ with $n > i$. It suffices to take $x = yq'^{r-(p-1)i}\gamma_i(\frac{t^{p-1}}{p})$ with $y \in W(R)$ the solution of the equation

$$\varphi y - q'^{r-(p-1)i} y = b.$$

Proof of (3): Suppose $x \in \mathrm{Fil}^r A_{\mathrm{cris}}$, then by Proposition 7.24, one can write

$$p^m m! x = y + z, \ y \in W(R), \ z \in I^{[r]}.$$

Since $z \in I^{[r]} \subseteq N$, one sees that $y \in \mathrm{Fil}^r W(R) = q'^r W(R) \subseteq N$.

Theorem 7.26. (1) *Suppose*

$$B'_{\mathrm{cris}} = \{x \in B_{\mathrm{cris}} \mid \varphi^n(x) \in \mathrm{Fil}^0 B_{\mathrm{cris}} \textit{ for all } n \in \mathbb{N}\}.$$

Then $\varphi(B'_{\mathrm{cris}}) \subseteq B^+_{\mathrm{cris}} \subseteq B'_{\mathrm{cris}}$ *if* $p \neq 2$ *and* $\varphi^2(B'_{\mathrm{cris}}) \subseteq B^+_{\mathrm{cris}} \subseteq B'_{\mathrm{cris}}$ *if* $p = 2$.

(2) *For every* $r \in \mathbb{N}$, *the sequence*

$$0 \longrightarrow \mathbb{Q}_p(r) \longrightarrow \mathrm{Fil}^r B^+_{\mathrm{cris}} \xrightarrow{p^{-r}\varphi - 1} B^+_{\mathrm{cris}} \longrightarrow 0$$

is exact.

(3) *For every* $r \in \mathbb{Z}$, *the sequence*

$$0 \longrightarrow \mathbb{Q}_p(r) \longrightarrow \mathrm{Fil}^r B_{\mathrm{cris}} \xrightarrow{p^{-r}\varphi - 1} B_{\mathrm{cris}} \longrightarrow 0$$

is exact.

Proof. For (1), $B^+_{\mathrm{cris}} \subseteq B'_{\mathrm{cris}}$ is trivial. Conversely, suppose $x \in B'_{\mathrm{cris}}$. There exist $r, j \in \mathbb{N}$ and $y \in A_{\mathrm{cris}}$ such that $x = t^{-r}p^{-j}y$. If $n \in \mathbb{N}$, $\varphi^n(x) = p^{-nr-j}t^{-r}\varphi^n(y)$, then $\varphi^n(y) \in \mathrm{Fil}^r A_{\mathrm{cris}}$ for all n, and thus $y \in I^{[r]}$. One can write $y = \sum\limits_{m \geq 0} a_m t^{\{m+r\}}$ with $a_m \in W(R)$ converging to 0 p-adically. One thus has

$$x = p^{-j} \sum_{m \geq 0} a_m t^{\{m+r\}-r} \text{ and } \varphi x = p^{-j-r} \sum_{m \geq 0} \varphi(a_m) p^{m+r} t^{\{m+r\}-r}.$$

By a simple calculation, $\varphi x = p^{-j-r} \sum\limits_{m \geq 0} c_m \varphi(a_m) t^m$, where c_m is a rational number satisfying

$$v(c_m) \geq (m+r)\left(1 - \frac{1}{p-1} - \frac{1}{(p-1)^2}\right).$$

If $p \neq 2$, it is a positive integer and $\varphi(x) \in p^{-j-r}W(R)[[t]] \subseteq p^{-j-r}A_{\mathrm{cris}} \subseteq B^+_{\mathrm{cris}}$. For $p = 2$, the proof is analogous.

The assertion (2) follows directly from Proposition 7.25.

For the proof of (3), by (2), for every integer i such that $r+i \geq 0$, one has an exact sequence

$$0 \longrightarrow \mathbb{Q}_p(r+i) \longrightarrow \mathrm{Fil}^{r+i} B^+_{\mathrm{cris}} \longrightarrow B^+_{\mathrm{cris}} \longrightarrow 0,$$

which, Tensoring by $\mathbb{Q}_p(-i)$, results the following exact sequence

$$0 \longrightarrow \mathbb{Q}_p(r) \longrightarrow t^{-i}\,\mathrm{Fil}^{r+i} B^+_{\mathrm{cris}} \longrightarrow t^{-i}B^+_{\mathrm{cris}} \longrightarrow 0.$$

The result follows by passing the above exact sequence to the limit.

7.3 The subrings B_e, ${}^hB_e$ and $B_{e,h}$ of B_{cris}

7.3.1 The ring B_e.

Definition 7.27. *For $h, d \in \mathbb{Z}$ and $h \geq 1$, set*

$$P_{h,d} = \{x \in B_{\mathrm{cris}} \mid \varphi x = p^d x\}, \qquad P^+_{h,d} = P_{h,d} \cap B^+_{\mathrm{cris}}.$$

In particular, set $B_e := P_{1,0} = B_{\mathrm{cris}}^{\varphi=1}$ and ${}^hB_e := P_{h,0} = B_{\mathrm{cris}}^{\varphi^h=1}$.

Let us first consider the case $h = 1$. Note that $B_e \supseteq \mathbb{Q}_p$ is a ring, and every $P_{1,d} = B_e t^d$ is a free B_e-module of rank 1. Recall U is the image of U_R^+ in B^+_{cris} under the logarithm map, hence $U \subset P^+_{1,1}$. Moreover, we have

Theorem 7.28. (1) $\mathrm{Fil}^0 B_e = \mathbb{Q}_p$*, and $P^+_{1,d} = 0$ for every $d < 0$.*

(2) *One has $U = P^+_{1,1}$, hence the sequence $0 \to \mathbb{Q}_p t \to P^+_{1,1} \xrightarrow{\theta} C \to 0$ is exact.*

(3) *Moreover, pick any $u \in U - \mathbb{Q}_p t$, then for $d > 0$,*

$$P^+_{1,d} = \{x = x_0 t^{d-1} + x_1 u t^{d-2} + \cdots + x_{d-1}u^{d-1} \mid x_0, \cdots, x_{d-1} \in U\}$$

and thus $P^+_{1,d}$ is generated by U.

(4) *The sequence*

$$0 \longrightarrow \mathbb{Q}_p \longrightarrow B_e \oplus B^+_{\mathrm{dR}} \longrightarrow B_{\mathrm{dR}} \longrightarrow 0 \qquad (7.27)$$

is exact.

Proof. (1) $\mathrm{Fil}^0 B_e = \mathbb{Q}_p$ is a special case of Theorem 7.26 (3). If $x \in P^+_{1,d}$, then $t^{-d} \in B_e \cap \mathrm{Fil}^{-d} B_{\mathrm{dR}}$, which is 0 if $d < 0$.

(2) Suppose $x \in P^+_{1,1}$, and suppose $u \in U$ such that $\theta(x) = \theta(u)$, then $x - u = tx_0$ with $x_0 \in B_e \cap B^+_{\mathrm{dR}} \subset \mathrm{Fil}^0 B_e = \mathbb{Q}_p$. Therefore $x \in U$ and (2) is proven.

(3) In general, for $x \in P^+_{1,d}$, suppose $\theta(x) = c$ and $\theta(u) = c_0$, we find $x_{d-1} \in U$ such that $\theta(x_{d-1}) = c/c_0^{d-1}$, then $\theta(x - x_{d-1}u^{d-1}) = 0$ and we may write $x - x_{d-1}u^{d-1} = ty$ with $y \in B^+_{\mathrm{dR}} \cap P_{1,d-1}$. Moreover, one can easily check that $\varphi^n(y) \in B^+_{\mathrm{dR}}$ for $n \in \mathbb{N}$. By Theorem 7.26(1), $y \in B^+_{\mathrm{cris}}$ and hence in $P^+_{1,d-1}$. We now proceed by induction.

(4) It is enough to show that $B_e + B^+_{\mathrm{dR}} = B_{\mathrm{dR}}$. We show by induction on $d > 0$ that $\mathrm{Fil}^{-d} B_{\mathrm{dR}} \subset B_e + B^+_{\mathrm{dR}}$. Suppose $\mathrm{Fil}^{-d+1} B_{\mathrm{dR}} \subset B_e + B^+_{\mathrm{dR}}$. Suppose $x = t^{-d}\lambda \in \mathrm{Fil}^{-d} B_{\mathrm{dR}}$ and $\theta(\lambda) = c \neq 0$. By (3), we can find $y \in P^+_{1,d}$, $\theta(y) = c$. Then $t^{-d}y \in B_e$ and

$$x - t^{-d}y = t^{-d}(\lambda - y) \in \mathrm{Fil}^{-d+1} B_{\mathrm{dR}},$$

and the claim is proven.

Remark 7.29. The exact sequence (7.27) is the so-called *fundamental exact sequence* of p-adic Hodge theory, which also has the form

$$0 \longrightarrow \mathbb{Q}_p \longrightarrow B_e \longrightarrow B_{\mathrm{dR}}/B^+_{\mathrm{dR}} \longrightarrow 0. \tag{7.28}$$

Moreover, for $x \in B_e$, we define

$$\deg_\infty(x) := \min\{d \in \mathbb{Z}, t^d x \in P^+_{1,d}\}. \tag{7.29}$$

Then the proof of the theorem implies that $\deg_\infty(x) = d$ if and only if $x \in \mathrm{Fil}^{-d} B^+_{\mathrm{dR}} - \mathrm{Fil}^{-d+1} B_{\mathrm{dR}}$. In this sense, $\deg_\infty(x) = -v_{\mathrm{dR}}(x)$ and B_{dR} is the completion of $\mathrm{Frac}\, B_e$ under the valuation v_{dR}.

7.3.2 Lubin-Tate representations and the ring $B_{e,h}$.

Lemma 7.30. *The map $P_0 \otimes_{\mathbb{Q}_p} B_e \to B_{\mathrm{cris}}$, $\lambda \otimes x \mapsto \lambda x$ is injective.*

Proof. Suppose $x = \sum_i \lambda_i \otimes x_i \mapsto 0$, $\lambda_i \in P_0$, $x_i \in B_e$, we need to show $x = 0$.

We use induction on the number of (non-zero) terms n in the summand of x. The case $n = 1$ is trivial. Now suppose $\sum_i \lambda_i x_i = 0$, then $\sum_i \varphi(\lambda_i)x_i = 0$. We may assume $\varphi(\lambda_j) \neq \lambda_j$ for some j (otherwise $\lambda_i \in \mathbb{Q}_p$ for all i and hence $x = 0$). Then the element

$$\sum_i (\varphi(\lambda_j)\lambda_i - \varphi(\lambda_i)\lambda_j) \otimes x_i \mapsto 0$$

has fewer terms in the summand. The inductive hypothesis implies that $\varphi(\lambda_j)\lambda_i - \varphi(\lambda_i)\lambda_j = 0$ for each i, i.e., $\lambda_i/\lambda_j \in \mathbb{Q}_p$. Hence $x = 0$.

From now on, we use the above injection to identify $P_0 \otimes_{\mathbb{Q}_p} B_e$ with a subring of B_{cris}. Let $\mathbb{Q}_{p^h} = W(\mathbb{F}_{p^h})[\frac{1}{p}] \subset P_0$ be the unique unramified extension of $\mathbb{Q}_p$ of degree h and let $\mathbb{Z}_{p^h} = W(\mathbb{F}_{p^h})$ be its ring of integers.

Proposition 7.31. *The injection above induces an isomorphism*

$$\iota_h : \ \mathbb{Q}_{p^h} \otimes_{\mathbb{Q}_p} B_e \to {}^h B_e, \quad a \otimes b \to ab.$$

In particular, $\mathrm{Fil}^0\, {}^h B_e = \mathbb{Q}_{p^h}$.

Proof. We need to find the inverse map. Suppose $e_0, e_1 = \varphi(e_0), \cdots, e_{h-1} = \varphi^{h-1}(e_0)$ is a normal basis of $\mathbb{Q}_{p^r}$ over $\mathbb{Q}_p$. Suppose $\{e_i^* \mid 1 \leq i \leq r\}$ is the dual basis defined by the trace map, then $\varphi(e_i^*) = e_{i-1}^*$, and the inverse map is just the map $x \mapsto \sum\limits_{i=0}^{h-1} e_i \otimes \rho_h(e_i^* x)$ where for $x \in {}^h B_e$, $\rho(x) = x + \varphi(x) + \cdots + \varphi^{h-1}(x) \in B_e$.

Definition 7.32. *For $h \in \mathbb{N}$, $h \geq 1$, set*

$$V_h := \{x \in B^+_{\mathrm{cris}} \ \mid \varphi^h(x) = px, \theta(x) = 0\} = P^+_{h,1} \cap \mathrm{Fil}^1 B_{\mathrm{dR}}.$$

Lemma 7.33. *If $V_h \neq 0$, then V_h is a 1-dimensional $\mathbb{Q}_{p^h}$-vector space and the map $V_h \to V_1$, $x \mapsto x\varphi(x) \cdots \varphi^{h-1}(x)$ is onto.*

Proof. We know $V_1 = \mathbb{Q}_p t$ by Theorem 7.28. Note that V_h is a $\mathbb{Q}_{p^h}$-vector space by definition. For any $0 \neq x \in V_h$, $0 \neq x\varphi(x) \cdots \varphi^{h-1}(x) = at \in V_1$ with $a \in Q_p^\times$. Since the norm map of $\mathbb{Q}_{p^h}$ to $\mathbb{Q}_p$ is onto, we can take $b \in \mathbb{Q}_{p^h}$ such that $b\varphi(b) \cdots \varphi^{h-1}(b) = a^{-1}$. Then the element $t_h = bx \in V_h$ satisfies $t_h \varphi(t_h) \cdots \varphi^{h-1}(t_h) = t$, hence the map is onto.

For any $0 \neq x \in V_h$, then $x \in B^+_{\mathrm{cris}}$ and hence $\varphi^i(x) \in B^+_{\mathrm{cris}} \subseteq B^+_{\mathrm{dR}}$. By the identity $x\varphi(x) \cdots \varphi^{h-1}(x) = at$ and the fact at is invertible in B_{cris}, x is also invertible in B_{cris}. This identity also implies $x \in \mathrm{Fil}^1 B_{\mathrm{dR}} - \mathrm{Fil}^2 B_{\mathrm{dR}}$ and $\varphi^i(x) \in \mathrm{Fil}^0 B_{\mathrm{dR}} - \mathrm{Fil}^1 B_{\mathrm{dR}}$ for all $1 \leq i < h$. In particular, we have $x/t_h \in B_{\mathrm{cris}}$ and

$$\varphi^i(x/t_h) \in B^+_{\mathrm{dR}} \cap B_{\mathrm{cris}} \quad \text{for } i \in \mathbb{N}.$$

By Theorem 7.26(1), $x/t_h \in B'_{\mathrm{cris}}$ and then $x/t_h = \varphi^h(x/t_h) \in B^+_{\mathrm{cris}}$. As a consequence $x/t_h \in (B^+_{\mathrm{cris}})^{\varphi^h=1} = \mathbb{Q}_{p^h}$ and $V_h = \mathbb{Q}_{p^h} t_h$.

We recall the functional equation lemma ([Haz78],§2.2 and §8) of formal groups.

Lemma 7.34 (Functional Equation Lemma). *Suppose A is a subring of the field K, I is an ideal of A, p is a prime number such that $p \in I$, q is a power of p and $s \in K$ such that $sI \subset A$. If $g(X) = \sum_{i=1}^\infty b_i X^i \in A[[X]]$ such that $b_1 = 1$, and $f_g(X) \in K[[X]]$ satisfies the functional equation*

$$f_g(X) = g(X) + s \cdot f_g(X^q), \tag{7.30}$$

Then $\Gamma_g(X,Y) = f_g^{-1}(f_g(X) + f_g(Y))$ defines a one dimensional commutative formal group law over A. Furthermore,

(1) *If* $\tilde{g}(X) = \sum_{i=1}^{\infty} \tilde{b}_i X^i$, *then* $f_{\tilde{g}}^{-1} f_g(X) \in A[[X]]$; *if moreover* $\tilde{b}_1 = 1$, *then* Γ_g *and* $\Gamma_{\tilde{g}}$ *are isomorphic over* A, *with the isomorphism given by* $f_{\tilde{g}}^{-1} f_g(X)$.
(2) *Suppose* K *is a local field,* $A = \mathcal{O}_K$ *the ring of valuation,* q *the cardinality of the residue field,* I *the maximal ideal of* $\mathcal{O}_K$ *and* $s = \pi$ *a uniformizer of* I. *Then* Γ_g *is a Lubin-Tate formal group law over* A *associated to* π.

Applying Lemma 7.34 to the case

$$q = p^h,\ K = \mathbb{Q}_q,\ A = \mathbb{Z}_q,\ I = p\mathbb{Z}_q,\ s = p \text{ and } g(X) = X,$$

then

$$l_\Gamma(X) := f_X(X) = \sum_{n\in\mathbb{N}} \frac{1}{p^n} X^{q^n} \in \mathbb{Q}_p[[X]], \tag{7.31}$$

$$\Gamma(X,Y) := l_\Gamma^{-1}(l_\Gamma(X) + l_\Gamma(Y)) \in \mathbb{Z}_p[[X,Y]] \tag{7.32}$$

defines a Lubin-Tate formal group law Γ over $\mathbb{Z}_q$ associated to the uniformizer p. By the theory of Lubin-Tate formal groups, $\mathbb{Z}_q$ is isomorphic to $\mathrm{End}(\Gamma)$ by $a \mapsto [a]_\Gamma(X)$ where

$$[a]_\Gamma(X) = l_\Gamma^{-1}(a l_\Gamma(X)) = aX + \text{ degree } \geq 2 \in \mathrm{End}(\Gamma).$$

Proposition 7.35. (1) *The map* $l_h : (\mathfrak{m}_R, \oplus_\Gamma) \to P_{h,1}^+$,

$$l_h(x) = \sum_{n\in\mathbb{Z}} p^{-n} [x]^{p^{nh}} \tag{7.33}$$

is an isomorphism, where $x \oplus_\Gamma y = \Gamma(x,y)$ *is the Lubin-Tate group law.*
(2) V_h *is* 1*-dimensional* $\mathbb{Q}_{p^h}$*-representation of* G_K *and the sequence*

$$0 \longrightarrow V_h \longrightarrow P_{h,1}^+ \xrightarrow{\theta} C \longrightarrow 0 \tag{7.34}$$

is exact. As a consequence, $\theta(P_{h,d}^+) = C$ *for every* $d \in \mathbb{N}$, $d \geq 1$.

Proof. We first check that $l_h(x)$ is a well defined element in $P_{h,1}^+$ for $x \in \mathfrak{m}_R$. Suppose $x = (x^{(n)})_{n\in\mathbb{N}} \in \mathfrak{m}_R$, we can certainly write it as $x = (x^{(n)})_{n\in\mathbb{Z}}$ by setting $x^{(n)} = (x^{(n+1)})^p$ for $n < 0$. There exist $n_0 \in \mathbb{Z}$ such that $x^{(n_0 h)} \in p\mathcal{O}_C$. For $u = x^{p^{n_0 h}}$, then $\frac{[u]^n}{n!} \in A_{\mathrm{cris}}$ for every $n \in \mathbb{N}$ and the series

$$\sum_{n=0}^{+\infty} p^{-n}[u^{p^{nh}}] = \sum_{n=0}^{+\infty} \frac{(p^{nh})!}{p^n} \cdot \frac{[u]^{p^{nh}}}{(p^{nh})!} \in A_{\mathrm{cris}}.$$

Thus

$$\sum_{n=n_0}^{+\infty} p^{-n}[x^{p^{nh}}] = p^{-n_0} \sum_{n=0}^{+\infty} p^{-n}[u^{p^{nh}}] \in B_{\mathrm{cris}}^+.$$

Since $\sum_{n=-\infty}^{-1} p^{-n}[u^{p^{nh}}]$ converges in $W(R)$,

$$\sum_{n=-\infty}^{n_0-1} p^{-n}[x^{p^{nh}}] = p^{-n_0} \sum_{n=-\infty}^{-1} p^{-n}[u^{p^{nh}}] \in B^+_{\mathrm{cris}}.$$

Therefore $l_h(x)$ is a well defined element in B^+_{cris}. It is easy to see that $\varphi^h(l_h(x)) = pl_h(x)$ and hence $l_h(x) \in P^+_{h,1}$.

Let $q = p^h$. We see that

$$l(x) = l_\Gamma([x]) + \sum_{n=0}^{\infty}[x^{q^{-n}}]p^n = \lim_{n\to+\infty} p^n l_\Gamma([x^{q^{-n}}]), \tag{7.35}$$

which implies l is a group homomorphism. Note that

$$\Gamma(\mathcal{O}_C) = \mathrm{Hom}_{\mathrm{cont.}\, E-\mathrm{alg}}(\mathbb{Z}_q[[X]], \mathcal{O}_C) = \mathfrak{m}_C$$

with the addition law $x \oplus_\Gamma y = \Gamma(x,y)$. Moreover, $\Gamma(\mathcal{O}_C)$ is a $\mathbb{Z}_q$-module via the action

$$a \cdot x = [a]_\Gamma(x).$$

For $x \in \mathfrak{m}_C$, $l_\Gamma(x) \in C$. Furthermore, by the method of Newton polygon, we know $l_\Gamma : \Gamma(\mathcal{O}_C) \to C$ is surjective and clearly $\Gamma_{\mathrm{tor}}(\mathcal{O}_C)$ is in the kernel. On the other hand, if $l_\Gamma(x) = 0$, then $l_\Gamma(a\cdot x) = 0$ for all $a \in \mathbb{Z}_q$. Pick a close to 0 such that $v(a\cdot x) > 2$, then compare the valuations of x^{q^n}/p^n, by $l_\Gamma(a\cdot x) = 0$, we must have $a \cdot x = 0$ and $x \in \Gamma_{\mathrm{tor}}(\mathcal{O}_C)$. Thus we have an exact sequence

$$0 \longrightarrow \Gamma_{\mathrm{tor}}(\mathcal{O}_C) \longrightarrow \Gamma(\mathcal{O}_C) \xrightarrow{l_\Gamma} C \longrightarrow 0$$

where $\Gamma_{\mathrm{tor}}(\mathcal{O}_C) \cong \mathbb{Q}_q/\mathbb{Z}_q$ by the Lubin-Tate theory.

Suppose $V(\Gamma) = \mathrm{Hom}_{\mathbb{Z}_q}(\mathbb{Q}_q, \Gamma(\mathcal{O}_C))$, then we have an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & V(\Gamma_{\mathrm{tor}}(\mathcal{O}_C)) \arrow[r] \arrow[d, equal] & V(\Gamma) \arrow[r, "\tau"] \arrow[d, equal] & C \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{Q}_q \arrow[r] & V(\Gamma) \arrow[r, "\tau"] & C \arrow[r] & 0.
\end{tikzcd}$$

An element in $V(\Gamma)$ is of the form $v = (v_n), v_n = v(p^{-n}) \in \mathfrak{m}_C$, such that $v_n = [p]_\Gamma(v_{n+1}) = v_{n+1}^q \bmod p$. The map τ is just

$$\tau(v) = l_\Gamma(v_0) = \pi^n l_\Gamma(v_n) \text{ for any } n \in \mathbb{N}.$$

Let $\tilde{v}_n = v_n \bmod p$ in $\mathcal{O}_C/p$, then $\tilde{v}_{n+1}^q = \tilde{v}_n^q$, and $\tilde{v} = (\tilde{v}_n)_{n\in\mathbb{N}} \in \mathfrak{m}_R = \Gamma(R)$. By this way, we can identify $V(\Gamma)$ and $\mathfrak{m}_R$, and the map τ is nothing but $\theta \circ l$:

$$\begin{aligned} V(\Gamma) = \mathfrak{m}_R &\longrightarrow C \\ x = (\tilde{v}_n) &\longmapsto \theta_C(l(x)). \end{aligned}$$

Thus $\theta : P_{h,1}^{+} \to C$ is surjective.

Since $B_{\mathrm{cris}}^{G_K} = K_0$, $(P_{h,1}^{+})^{G_K} = \{x \in K_0 \mid \varphi^h(x) = px\} = 0$, but $C^{G_K} \neq 0$, and since the map θ commutes with Galois action, θ can not be bijective. Therefore $V_h \neq 0$. By Lemma 7.33, $\dim_{\mathbb{Q}_q} V_h = 1$. The bijection of l_h in (1) then follows from the above exact sequence and this fact.

For $c \in C$, we can find $x, y \in P_{h,1}^{+}$ such that $\theta(x) = c$ and $\theta(y) = 1$, then $xy^{d-1} \in P_{h,d}^{+}$ and $\theta(xy^{d-1}) = c$. Hence $\theta(P_{h,d}^{+}) = C$.

For $r \geq 1$, if $x \in V_{hr}$, then $x\varphi^h(x)\cdots\varphi^{h(r-1)}(x) \in V_h$ and the map $V_{hr} \to V_h$, $x \mapsto x\varphi^h(x)\cdots\varphi^{h(r-1)}(x)$ is onto. Consequently, we can give the following definition:

Definition 7.36. *The* Lubin-Tate elements $\{t_h\}_{h\in\mathbb{N}}$ *is a compatible system of elements in* B_{cris}^{+} *such that* $V_h = \mathbb{Q}_{p^h} t_h$ *and*

(i) $\varphi^h(t_h) = pt_h$, $\theta(t_h) = 0$ *if* $h \neq 0$;
(ii) $t_0 = 1$ *and* $t_1 = t$;
(iii) *For* $r \geq 1$, $t_{hr}\varphi^h(t_{hr})\cdots\varphi^{h(r-1)}(t_{hr}) = t_h$.

By definition,

Proposition 7.37. *The Lubin-Tate elements* $\{t_h\}$ *satisfy the following properties*

(1) t_h *is invertible in* B_{cris}.
(2) *For* $h \geq 2$, $t_h \in \mathrm{Fil}^1 B_{\mathrm{dR}} - \mathrm{Fil}^2 B_{\mathrm{dR}}$ *is a uniformizing parameter of* $(B_{\mathrm{dR}}^{+}, v_{\mathrm{dR}})$, *and* $\varphi^n(t_h) \in \mathrm{Fil}^0 B_{\mathrm{dR}} - \mathrm{Fil}^1 B_{\mathrm{dR}}$ *for* $1 \leq n \leq h-1$.
(3) *For every* d, $P_{h,d} = {}^hB_e t_h^d$ *is a free* ${}^hB_e$*-module of rank* 1.

Definition 7.38. *For* $h \geq 1$, *set*

$$B_{e,h} = \{x \in B_{\mathrm{cris}}^{\varphi^h=1} \mid \exists\, d \in \mathbb{N} \text{ such that } xt_h^d \in B_{\mathrm{cris}}^{+}\}. \tag{7.36}$$

One can see easily that the definition of $B_{e,h}$ is independent of the choice of t_h. If $h = 1$, $B_{e,1}$ is nothing but B_e. By definition, $B_{e,h}$ is a subring of ${}^hB_e$. Moreover, since $\varphi^n(t_h)/t_h$ and $t/t_h^h \in B_{e,h}$,

$${}^hB_e = B_{e,h}[t_h^h/t] = B_{e,h}[(t_h/\varphi^n(t_h))_{1\leq n\leq h-1}] \tag{7.37}$$

is contained in the fraction field of $B_{e,h}$.

By the same method used in the proof of Theorem 7.28, we have

Proposition 7.39. *Suppose* $h \geq 1$ *is an integer, then*

(1) $P_{h,0}^{+} = \mathbb{Q}_{p^h}$ *and for every* $d < 0$, $P_{h,d}^{+} = 0$.
(2) *The sequence*

$$0 \longrightarrow \mathbb{Q}_{p^h} t_h \longrightarrow P_{h,1}^{+} \xrightarrow{\theta} C \longrightarrow 0$$

is exact.

(3) *Suppose* $u \in P^+_{h,1}$ *and* $u \notin \mathbb{Q}_{p^h} t_h$*, then for* $d > 0$*,*

$$P^+_{h,d} = \{a_0 t_h^{d-1} + a_1 u t_h^{d-2} + \cdots a_{d-1} u^{d-1} \mid a_i \in P^+_{h,1}\}. \tag{7.38}$$

(4) *The sequence*

$$0 \longrightarrow \mathbb{Q}_{p^h} \longrightarrow B_{e,h} \oplus B^+_{\mathrm{dR}} \longrightarrow B_{\mathrm{dR}} \longrightarrow 0 \tag{7.39}$$

is exact.

Remark 7.40. We call this sequence (7.39) the *fundamental exact sequence* of $B_{e,h}$.

7.4 The Fundamental Lemma of Colmez

7.4.1 The statement.

Recall $U = \{u \in B_{\text{cris}} \mid \varphi(u) = pu\} \cap B^+_{\mathrm{dR}} = P^+_{1,1}$. Set $B_2 = B^+_{\mathrm{dR}} / \operatorname{Fil}^2 B_{\mathrm{dR}}$. We have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Q}_p(1) \arrow[r] \arrow[d, "incl"'] & U \arrow[r, "\theta"] \arrow[d] & C \arrow[r] \arrow[d, "\mathrm{Id}"'] & 0 \\
0 \arrow[r] & C(1) \arrow[r] & B_2 \arrow[r, "\theta"] & C \arrow[r] & 0
\end{tikzcd}$$

where all rows are exact and all vertical arrows are injective.

Suppose h is an integer ≥ 2. Suppose $\lambda_1, \lambda_2, \ldots, \lambda_h \in C$ are not all zero. Set

$$Y := \{(u_1, u_2, \ldots, u_h) \in U^h \mid \exists c \in C \text{ such that for all } i, \theta(u_i) = c\lambda_i\}. \tag{7.40}$$

Suppose $b_1, b_2, \ldots, b_h \in B_2$, not all zero, such that $\sum_{i=1}^h \lambda_i \theta(b_i) = 0$. Then the map

$$\rho : Y \to B_2, \quad (u_1, \ldots, u_h) \mapsto \sum_{i=1}^h b_i u_i \tag{7.41}$$

has image in $C(1)$, as $\theta(\sum_{i=1}^h b_i u_i) = \sum \theta(b_i)\theta(u_i) = c \sum \theta(b_i)\lambda_i = 0$.

Theorem 7.41 (Fundamental Lemma). *Assume the above hypotheses. Then* $\operatorname{Im} \rho \subset C(1)$ *and*

(1) *either* $\operatorname{Im} \rho = \rho(\mathbb{Q}_p(1)^{h'})$ *and hence* $\dim_{\mathbb{Q}_p} \operatorname{Im} \rho \leq h$*,*
(2) *or* $\operatorname{Im} \rho = C(1)$ *and* $\dim_{\mathbb{Q}_p} \operatorname{Ker} \rho = h$*.*

The following proof is an improvement of the proof in the thesis of Plût [Plû09], written up by Yi Ouyang, Shenxing Zhang and Jinbang Yang. In particular, the proof of Proposition 7.42, Proposition 7.44 and Proposition 7.46 contains a great deal of ideas from [Plû09].

7.4.2 Technical preparation for the proof

Proposition 7.42. *Suppose $\mu_0, \dots, \mu_{h-1} \in C$ are not all zero. Let $\delta : P_{h,1}^+ \to C$ be defined by*

$$\delta(x) = \sum_{i=0}^{h-1} \mu_i \theta(\varphi^i x).$$

Then δ is onto and $\dim_{\mathbb{Q}_p} \operatorname{Ker} \delta = h$.

Proof. Throughout the proof we write $q = p^h$. Recall that the map

$$l_h : \mathfrak{m}_R \to P_{h,1}^+, \ x \mapsto \sum_{n \in \mathbb{Z}} p^{-n} [x]^{p^{nh}}$$

is bijective, to prove δ is surjective, it suffices to show that $\delta \circ l_h$ is surjective. We write $\delta = \delta \circ l_h$ for simplicity. Then

$$\delta(x) = \sum_{i=0}^{h-1} \mu_i \sum_{n \in \mathbb{Z}} p^{-n} x^{-(nh+i)}, \quad x = (x^{(n)})_{n \in \mathbb{Z}} \in \mathfrak{m}_R.$$

Note that the result is true for δ if and only if it is true for $\delta \circ \varphi^i$ for any one $i \in \mathbb{Z}$. Suppose $i \in \{0, \dots, h-1\}$ such that $v(\mu_i) + \frac{i}{h}$ is minimal, let

$$\mu_j' = \begin{cases} \mu_{i+j}\theta(p), & \text{if } 0 \le j \le h-i-1, \\ \mu_{i+j-h}, & \text{if } h-i \le j \le h-1; \end{cases}$$

then $\delta \circ \varphi^{h-i} = \sum_{j=0}^{h-1} \mu_j' \theta \circ \varphi^j$ such that

$$v(\mu_j') + \frac{j}{h} \ge v(\mu_i) + \frac{i}{h} + \frac{j}{h} - \frac{i+j-h}{h} = v(\mu_0')$$

holds for every j. Thus we may assume

$$\mu_0 = 1, \quad v(\mu_i) \ge -\frac{i}{h} \text{ for } 0 \le i \le h-1. \tag{7.42}$$

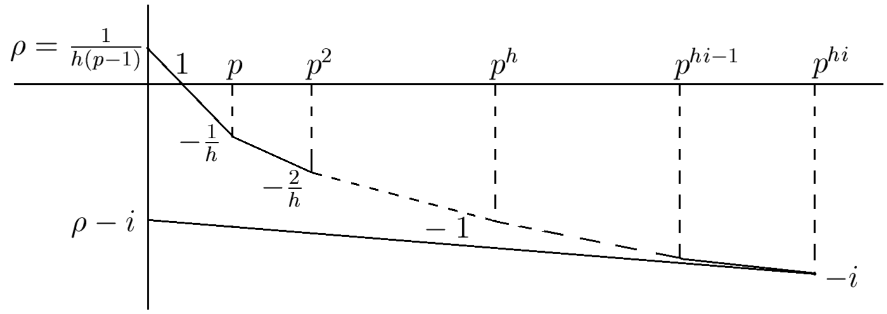
Define $\mu_{i+nh} = p^{-n}\mu_i$ for $n \in \mathbb{Z}$ and $0 \le i \le h-1$, then

$$\delta(x) = \sum_{i \in \mathbb{Z}} \mu_i x^{(-i)}.$$

Write $f_+(x) = \sum_{i \ge 0} \mu_i x^{p^i} \in C[[X]]$, then

$$f_+(x) = g(x) + \frac{1}{p} f_+(x^q), \text{ with } g(x) = x + \mu_1 x^p + \dots + \mu_{h-1} x^{p^{h-1}}.$$

For $n \in \mathbb{N}, x \in \mathfrak{m}_R$, set $\delta_n(x) = \sum_{i \ge -nh} \mu_i x^{(-i)}$, then



$$\delta_n(x^{q^n}) = p^n f_+(x^{(0)}), \text{ for all } n \in \mathbb{N}, \ x \in \mathfrak{m}_R.$$

Let $b \in \mathcal{O}_C$. By the Newton polygon method, the equation $f_+(x) = b$ has a solution of valuation equal to $v(b)$ if $v(b) \geq \rho := \frac{1}{h(p-1)}$ and has q^i solutions of valuation at least $q^{-i}\rho$ if $v(b) \geq \rho - i$.

For $b \in \mathcal{O}_C$, $v(b) \geq \rho$, we construct by recursion a sequence $(x_i)_{i \in \mathbb{N}}$ of $\mathcal{O}_C$ such that

(i) $f_+(x_i) = p^{-i}b$;
(ii) the limit $\lim_{j \to +\infty} x_{i+j}^{q^j}$ exists for every $i \in \mathbb{N}$.

Suppose x_i has been constructed, choose y such that $y^q = x_i$, then $f_+(y) = g(y) + p^{-i-1}b$ with $v(y) = \frac{1}{q}v(x_i) \geq 0$. We want to construct $x_{i+1} = y + z$, then

$$f_+(y+z) - f_+(y) = -g(y).$$

Note that

$$\begin{aligned} f_+(y+z) - f_+(y) &= \sum_{k \geq 0} \mu_k \sum_{j=1}^{p^k} \binom{p^k}{j} z^j y^{p^k - j} \\ &= \sum_{j \geq 1} z^j \sum_{p^k \geq j} \binom{p^k}{j} \mu_k y^{p^k - j} \\ &= \sum_{j \geq 1} \nu_j z^j := F(z). \end{aligned}$$

For $j = mp^e, (m,p) = 1$, note that $p^{k-e} \parallel \binom{p^k}{mp^e}$ and $v(\mu_k) \geq -\frac{k}{h}$, then $v(\nu_j) \geq -\frac{e}{h}$. If $m = 1$ and $e = nh$, then $v(\nu_{p^{nh}}) = -\frac{nh}{h} = -n$. Thus

$$\begin{aligned} v(g(y)) &\geq \min_{0 \leq j \leq h-1} (v(\mu_j) + p^j v(y)) \\ &= \min_{0 \leq j \leq h-1} (v(\mu_j) + \frac{p^j}{q} v(x_i)) > -1 + \frac{1}{h}. \end{aligned}$$

Then the Newton polygon of $F(z)+g(y)$ is above the segment connecting $(0,-1+\frac{1}{h})$ and $(q,-1)$, thus there exist exactly q roots z whose valuation is greater than $\frac{1}{qh}$. Choose one such z, let $x_{i+1}=y+z$, then $f_+(x_{i+1})=p^{-i-1}b$. By construction,

$$v(x_{i+j+1}^{q}-x_{i+j})=v((y+z)^q-y^q)\geq qv(z)>\frac{1}{h},$$
$$v(x_{i+j+1}^{q^{j+1}}-x_{i+j}^{q^j})\geq\frac{q^j}{h},$$

the sequence $(x_{i+j}^{q^j})_{j\in\mathbb{N}}$ is Cauchy and the limit exists. Let x_i' be its limits, then $(x_{i+1}')^q=x_i'$. We get an element $x\in\mathfrak{m}_R$ such that $x^{(ih)}=x_i'$ and

$$f_+(x_{i+j}^{q^j})=p^{-i}b-p^jg(x_{i+j})-\cdots-pg(x_{i+j}^{q^{j-1}}).$$

Since f_+ is continuous,

$$\begin{aligned}\delta_n(x)&=p^nf_+(x^{(nh)})=p^nf_+(x_n')\\&=b-\lim_{j\to+\infty}p^n(p^jg(x_{n+j})+\cdots+pg(x_{n+j}^{q^{j-1}}))\\&=b+\ (\text{valuation}\geq n\text{ terms}).\end{aligned}$$

Thus $\delta(x)=b$ and δ is surjective.

To compute $\operatorname{Ker}\delta$ in $P_{h,1}^+$, note that it is clearly a $\mathbb{Q}_p$-vector space, it suffices to show that $\Lambda/p\Lambda$ is of cardinality $q=p^h$ for a fixed lattice Λ of $\operatorname{Ker}\delta$. Let

$$\Lambda=\{x\in\operatorname{Ker}\delta\mid v(x)>1/h\},$$

then

$$p\Lambda=\{x\in\operatorname{Ker}\delta\mid v(x)>q/h\}.$$

We want to find $x_i\in\mathcal{O}_C(i\geq 1)$ such that $f_+(x_i)=0$ and $v(x_i-x^{(ih)})>1/h$. Let $z=x_i-x^{(ih)}$, then $f_+(x^{(ih)}+z)=0$, $f_+(x^{(ih)})+F(z)=0$ where $F(z)$ is the power series above with y replaced by $x^{(ih)}$. Note

$$\begin{aligned}f_+(x^{(ih)})&=\sum_{j\geq 0}\mu_j(x^{(ih)})^{p^j}=\sum_{j\geq 0}\mu_jx^{(ih-j)}\\&=\sum_{k\geq -ih}\mu_{ih+k}x^{(-k)}=p^{-i}\sum_{k\geq -ih}\mu_kx^{(-k)}\\&=-p^{-i}\sum_{k<-ih}\mu_kx^{(-k)},\end{aligned}$$

and if $k<-ih$,

$$v\left(\mu_kx^{(-k)}\right)\geq-\frac{k}{h}+p^kv(x)>-\frac{k}{h}+p^kc>i+\frac{1}{h},$$

thus $v(f_+(x^{(ih)})) > 1/h$ and there exists a solution z such that $v(z) > 1/h$.

From the construction of x_i, we have $x_0 = 0, x_i = \sum_{j=1}^{i} z_j^{q^{j-i}}$ and then $x^{(ih)} = \sum_{j=1}^{+\infty} z_j^{q^{j-i}}$. Since

$$v(x_i - x^{(ih)}) = v(z_{i+1}^q + z_{i+1}^{q^2} + \cdots) > \frac{1}{qh},$$

then $v(z_i) > \frac{1}{qh}$. Since

$$x^{(0)} = z_1^q + \sum_{j=2}^{+\infty} z_j^{q^j} \equiv z_1^q \bmod p\Lambda$$

and we have exactly $q-1$ different nonzero z_1 with $\frac{1}{h} \geq \frac{1}{(p-1)h} \geq v(z_1) > \frac{1}{qh}$, then $\Lambda/p\Lambda$ has exactly q elements.

Remark 7.43. If the μ_i's can be arranged such that $\mu_i \in \mathcal{O}_C$ for $0 \leq i \leq h-1$ and μ_0 is a unit in $\mathcal{O}_C$, then there is an easier proof for the above proposition. In this situation, applying Lemma 7.34, then $f(X) = l_\Gamma^{-1} \circ f_+(X) = \mu_0 X +$ higher terms $\in \mathcal{O}_C[[X]]$ and there is a commutative diagram of $\mathbb{Z}_q$-modules

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Ker}\ f_+ \arrow[r] \arrow[d, "f"'] & \mathfrak{m}_C \arrow[r, "\delta_+"] \arrow[d, "f"'] & C \arrow[r] \arrow[d, "\mathrm{Id}"'] & 0 \\
0 \arrow[r] & \mathrm{Ker}\ l_\Gamma \arrow[r] & \mathfrak{m}_C \arrow[r, "l_\Gamma"] & C \arrow[r] & 0
\end{tikzcd}$$

which is exact in the bottom row. Since $f : \mathfrak{m}_C \to \mathfrak{m}_C$ is an isomorphism, the first row is also exact, and $f : \mathrm{Ker}\ f_+ \cong \mathrm{Ker}\ l_\Gamma$. Now apply the functor $\mathrm{Hom}_{\mathbb{Z}_q}(\mathbb{Q}_q, -)$ to the diagram, by the fact that the induced map by f_+ on

$$\mathrm{Hom}_{\mathbb{Z}_q}(\mathbb{Q}_q, \mathfrak{m}_C) \cong \mathfrak{m}_R \to \mathrm{Hom}_{\mathbb{Z}_q}(\mathbb{Q}_q, C) = C$$

is just $\delta(x)$ and by the exact sequence

$$0 \to V_h \to \mathfrak{m}_R \xrightarrow{\theta \circ l} C \to 0$$

in Proposition 7.35, we obtain the proposition.

Proposition 7.44. *Suppose $\lambda_1, \ldots, \lambda_h \in \mathcal{O}_C$, whose images modulo $\mathfrak{m}_C$ are linearly independent over $\mathbb{F}_p$. Then*

$$\begin{aligned}
\eta : (P_{h,1}^+)^h &\longrightarrow C^h \\
(x_1, \ldots, x_h) &\longmapsto (\sum_{i=1}^{h} \lambda_i \theta(\varphi^r(x_i)))_{0 \leq r \leq h-1}
\end{aligned}$$

is surjective and its kernel is a $\mathbb{Q}_{p^h}$-vector space of dimension h.

Proof. Write $q = p^h$. Since $l_h : \mathfrak{m}_R \to P_{h,1}^+$ is a bijective, it suffices to show the map

$$f = \eta \circ l_h^h : \mathfrak{m}_R^h \longrightarrow C^h$$
$$(x_1, \ldots, x_h) \longmapsto (\sum_{i=1}^{h} \lambda_i \theta(\varphi^r(l_h(x_i))))_{r=0,\ldots,h-1}$$

is surjective. Let

$$S = \left\{(x_1, \ldots, x_h) \in \mathfrak{m}_R^h \mid v(x_i) \geq \frac{1}{q-1}\right\},$$
$$T = \left\{(x_1, \ldots, x_h) \in C^h \mid v(x_i) \geq \frac{p^{i-1}}{q-1}\right\}.$$

One can verify that $f(S) \subseteq T$. It suffices to show $f : S \to T$ is surjective and the kernel is a $\mathbb{Z}_{p^h}$-module of rank h.

Let H be the $\mathbb{Q}_{p^h}$-division algebra generated by ϑ where $\vartheta^h = p, \vartheta x = \varphi(x)\vartheta$ for any $x \in \mathbb{Q}_{p^h}$, then H acts as automorphisms on $(P_{h,1}^+)^h$ and $\mathfrak{m}_R^h$, with the action of ϑ being φ. Similarly, H acts as automorphisms on C^h, the action of ϑ is $\Theta(x_0, \ldots, x_{h-1}) = (x_1, \ldots, x_{h-1}, px_0)$. Then η is compatible with H-action, so is f, thus $\operatorname{Ker} f$ is an H-module.

Let $\mathcal{H}$ be the maximal order of H, then it is separated and complete for the p-adic topology, ϑ is a uniformizer of $\mathcal{H}$ and $\mathcal{H}/\vartheta\mathcal{H} = \mathbb{F}_{p^h}$. Moreover, S and T are sub-$\mathcal{H}$-modules of R^h and C^h respectively, $\vartheta(S) = \varphi(S)$ and $\vartheta(T) = \Theta T$. It suffices to show that

$$\bar{f} : S/\varphi(S) \to T/\Theta T$$

is surjective and the kernel is an $\mathbb{F}_q$-vector space of dimension 1.

Since $1 + \frac{1}{q-1} = \frac{p^h}{q-1}$,

$$\Theta T = \{(x_1, \ldots, x_h) \in C^h \mid v(x_i) \geq \frac{p^i}{q-1}\}.$$

For $x \in S,\ r = 0, \ldots, h-1$,

$$\theta \circ \varphi^r \circ l_h(x) = \sum_{n \in \mathbb{Z}} p^{-n} \theta([x^{p^{nh+r}}]) = \sum_{n \in \mathbb{Z}} p^{-n} (x^{(-nh-r)}).$$

Since $v_R(x) \geq \frac{1}{q-1}$,

$$v\left(p^{-n} x^{(-nh-r)}\right) = -n + p^{nh+r} v(x) \geq \frac{p^{nh+r}}{q-1} - n,$$

which is at least $\frac{p^{r+1}}{q-1}$ unless

– for $r = 0, n = -1$, the valuation $\geq 1 + \frac{q^{-1}}{q-1} (\geq \frac{p^{r+1}}{q-1}$ unless $p = q, r = h-1)$; $n = 0$, the valuation $\geq \frac{1}{q-1}$; $n = 1$, the valuation $\geq \frac{q}{q-1} - 1 = \frac{1}{q-1}$;

- for $1 \le r \le h-2, n = 0$, the valuation $\ge \frac{p^r}{q-1}$;
- for $r = h-1, n = 0$, the valuation $\ge \frac{p^{h-1}}{q-1}$; $n = -1$, the valuation $\ge 1 + \frac{p^{-1}}{q-1}$.

Then $\bar{f}(x_1, \dots, x_d)$ can be written as

$$\left(\sum_{i=1}^{h} \lambda_i([x_i] + \frac{1}{p}[x_i^{p^h}]), \sum_{i=1}^{h} \lambda_i[x_i^p], \dots, \sum_{i=1}^{h} \lambda_i[x_i^{p^{h-2}}], \sum_{i=1}^{h} \lambda_i(p[x_i^{1/p}] + [x_i]^{p^{h-1}})\right). \tag{7.43}$$

Suppose $\hat{\lambda}_i, \hat{p} \in R$ such that $\hat{\lambda}_i^{(0)} = \lambda_i$ and $\hat{p}^{(0)} = p$. The surjectivity of $\bar{f}$ can be reduced to show that the lifting equations

$$\begin{cases} \sum \hat{\lambda}_i(x_i + \frac{1}{\hat{p}} x_i^{p^h}) & = b_0, \\ \sum \hat{\lambda}_i x_i^{p^r} & = b_r, \quad r = 1, \dots, h-2, \\ \sum \hat{\lambda}_i(\hat{p} x_i^{\frac{1}{p}} + x_i^{p^{h-1}}) & = b_{h-1}, \end{cases} \tag{7.44}$$

for any $b_0, \dots, b_{h-1} \in R,\ v(b_r) \ge \frac{p^r}{q-1}$ has a solution $(x_1, \dots, x_h) \in S^h$. Let $\zeta \in R$ such that $\zeta^{p(q-1)} = \hat{p}$, then $S = (\zeta^p R)^h$. Let $x_i = (\zeta y_i)^p,\ y_i \in R$, then the above equations are reduced to

$$\begin{cases} \sum \hat{\lambda}_i(y_i^p + y_i^{p^{h+1}}) & = \zeta^{-p} b_0, \\ \sum \hat{\lambda}_i y_i^{p^{r+1}} & = \zeta^{-p^{r+1}} b_r, \quad r = 1, \dots, h-2, \\ \sum \hat{\lambda}_i(\zeta^{(p-1)(q-1)} y_i + y_i^{p^h}) & = \zeta^{-p^h} b_{h-1}. \end{cases} \tag{7.45}$$

Let $\mu_i = \hat{\lambda}_i^{p^{-h}}$, then we can linearize the equations to

$$\begin{cases} \sum \mu_i^{p^r} y_i & = c_r, \quad r = 1, \dots, h-2, \\ \sum \mu_i^{p^{h-1}}(y_i + y_i^{p^h}) & = c_{h-1}, \\ \sum \mu_i^{p^h}(\zeta^{(p-1)(q-1)} y_i + y_i^{p^h}) & = c_h, \end{cases} \tag{7.46}$$

for $c = (c_1, \dots, c_h) \in R^h$.

We need a lemma:

Lemma 7.45. *Suppose $X_i (i = 0, \cdots, n-1)$ are indeterminants over an integral domain of characteristic p, then*

$$\det(X_i^{p^j})_{i,j=0,\dots,n-1} = \prod_{a \in I}(\sum_{i=0}^{n-1} a_i X_i), \tag{7.47}$$

where $I \subset \mathbb{F}_p^n - \{0\}$ such that the first nonzero component a_i of $a \in I$ is 1.

Proof (Proof of Lemma 7.45). Assume $a_i = 1$, then replacing X_i in the matrix by $-\sum_{j \ne i} a_j X_j$, the determinant of the matrix is certainly 0, hence $\sum a_i X_i$ is a factor of $\det(X_i^{p^j})$. Now we just need to check that the degrees and leading coefficients in both sides of (7.47) agree with each other.

By Lemma 7.45, the matrix $(\mu_j^{p^i})_{1\le i,j\le h}$ is invertible in R since the λ_j's are linearly independent modulo $\mathfrak{m}_C$. Let

$$\sum \mu_i^{p^{-1}} y_i = c_{-1},\ \sum \mu_i y_i = c_0,$$

then

$$\begin{cases} \sum \mu_i^{p^{h-1}} y_i = c_{h-1} - c_{-1}^q, \\ \sum \mu_i^{p^h} y_i \quad = \zeta^{-(p-1)(q-1)}(c_h - c_0^q). \end{cases} \tag{7.48}$$

Let $A = (a_{ij})_{1\le i,j\le h}$ be the inverse of $(\mu_j^{p^{i-2}})_{1\le i,j\le h}$, then $a_{ij}\in R$ and

$$(y_1, y_2, \cdots, y_h) = (c_{-1}, c_0, \cdots, c_{h-1})A^T$$

is uniquely determined by (c_{-1}, c_0). Plug $y_i = \sum_{j=1}^h a_{ij} c_{j-2}$ into (7.48), then we get

$$\begin{cases} \sum_i \mu_i^{p^{h-1}} y_i = -\sum_j b_j c_{j-2} = c_{h-1} - c_{-1}^q, \\ \sum_i \mu_i^{p^h} y_i = -\sum_j b'_j c_{j-2} = \zeta^{-(p-1)(q-1)}(c_h - c_0^q), \end{cases} \tag{7.49}$$

where $b_i = -\sum_{j=1}^h \mu_j^{p^{h-1}} a_{ji}$ and $b'_i = -\sum_{j=1}^h \mu_j^{p^h} a_{ji} \in R$. Let

$$\alpha = b_3 c_1 + \cdots + b_h c_{h-2},\ \beta = b'_3 c_1 + \cdots + b'_h c_{h-2},\ \zeta' = \zeta^{(p-1)(q-1)},$$

then (7.46) is reduced to the following equations on c_0 and c_{-1}

$$\begin{cases} b_1 c_{-1} + b_2 c_0 + \alpha + c_{h-1} - c_{-1}^q = 0, \\ b'_1 c_{-1} + b'_2 c_0 + \beta + \frac{c_h - c_0^q}{\zeta'} \qquad = 0, \end{cases} \tag{7.50}$$

which in turn is reduced to the equation on c_0

$$((c_0^q - c_h) - \zeta'(b'_2 c_0 + \beta))^q - (\alpha + b_2 c_0) b_1'^q \zeta'^q + \frac{b_1}{b'_1}\left(b'_2 c_0 + \beta + \frac{c_h - c_0^q}{\zeta'}\right) b_1'^q \zeta'^q = 0. \tag{7.51}$$

The left hand side of the above equation is a monic polynomial of c_0 with coefficients in R, so all the roots c_0 are in R. We can work similarly for c_{-1}. Then there are q^2 compatible pairs $(c_0, c_{-1}) \in R^2$ and therefore q^2 distinct solutions $(y_1, \ldots, y_h) \in R^h$. Let Z_c denote the corresponding $(x_1, \ldots, x_h) \in S$.

It remains to prove that the kernel of $\bar f$ is 1-dimensional over $\mathbb{F}_{p^h}$. First we show that $\operatorname{Ker} \bar f = \overline{\operatorname{Ker} f}$. Let $\bar a \in \operatorname{Ker} \bar f, a \in S$, then $f(a) \in \Theta T$. By the fact that $f: S \to T$ is surjective, let $b \in S$ such that $f(a) = \Theta f(b) = f(\varphi b)$, then $f(a - \varphi b) = 0$, $a - \varphi b \in \operatorname{Ker} f$ and $\bar a \in \overline{\operatorname{Ker} f}$.

Since $\theta(b) = 0 \in \mathcal{O}_C$ for $y \in R$ if and only if $b = 0$, the kernel of $\bar f$ is $Z_0/\varphi(S)$. Thus we only need to show that $Z_0/\varphi(S)$ has q points. There is a short exact sequence of $\mathbb{F}_p$-vector spaces

$$0 \longrightarrow Z_0 \cap \varphi(S) \longrightarrow Z_0 \longrightarrow Z_0/\varphi(S) \longrightarrow 0,$$

thus it suffices to show that $Z_0 \cap \varphi(S)$ has exactly q distinct points. By $v(\zeta) = \frac{1}{p(q-1)}$, let $y_i = \zeta^{p-1} z_i$, then (7.46) is reduced to

$$\begin{cases} \sum \mu_i^{p^r} z_i & = 0, \quad r = 1, \ldots, h-2, \\ \sum \mu_i^{p^{h-1}} (z_i + \zeta^{(p-1)(q-1)} z_i^q) & = 0, \\ \sum \mu_i^{p^h} (z_i + z_i^q) & = 0. \end{cases} \tag{7.52}$$

We then have $c_0 = (\zeta' c_{-1}^q - b_1 c_{-1})/b_2$ and

$$\zeta' c_{-1}^{q^2} + ((-1)^q b_1^q - b_2^{q-1} b_2' \zeta') c_{-1}^q + (b_1 b_2' - b_2 b_1') b_2^{q-1} c_0 = 0.$$

Since

$$b_1 = \det(\mu_i^{p^{r-2}})_{i,r} = \prod_{a \in I} (\sum_{i=0}^{h-1} a_i \mu_i^{p^{-1}})$$

is a unit in R,

$$v((-1)^q b_1^q - b_2^{q-1} b_2' \zeta') = 0, \quad v((b_1 b_2' - b_2 b_1') b_2^{q-1}) \geq (q-1) v(b_2),$$

by Newton polygon method, there are exactly $q-1$ nonzero distinct c_{-1} such that $v(c_{-1}) \geq v(b_2)$. In this case $c_0 = (c_{-1}^q - b_1 c_{-1})/b_2 \in R$. Hence we have exactly q distinct solutions $(c_{-1}, c_0) \in R^2$ and then exactly q distinct solutions $(z_1, \ldots, z_h) \in R^h$, that is to say, $Z_0 \cap \varphi(S)$ has exactly q distinct points.

Proposition 7.46. *Assume $\lambda_1, \ldots, \lambda_h \in C$ are linearly independent over $\mathbb{Q}_p$, then*

$$\begin{aligned} \eta : (P_{h,1}^+)^h &\longrightarrow C^h \\ (x_1, \ldots, x_h) &\longmapsto (\sum_{i=1}^h \lambda_i \theta(\varphi^r(x_i)))_{0 \leq r \leq h-1} \end{aligned}$$

is surjective and the kernel is a $\mathbb{Q}_{p^h}$-vector space of dimension h.

For the proof, we first need two lemmas:

Lemma 7.47. *Suppose $s \geq 2$, $n_0 = 0 < n_1 < \cdots n_2 < \cdots < n_s = h$ are integers, and $0 \leq v_1 < v_2 < \cdots < v_s < 1$ and $v_0 = v_s - 1$. Suppose $\rho_1, \cdots \rho_s$ are defined by*

$$\begin{cases} \rho_j - \rho_{j+1} = p^{-n_j}(v_{j+1} - v_j), \quad (1 \leq j \leq s-1), \\ p^h \rho_s - \rho_1 = v_1 - v_s + 1. \end{cases} \tag{7.53}$$

Then for $1 \leq j \leq s-1$,

$$v_j + p^{n_{j-1}} \rho_j \cdot p = v_{j+1} + p^{n_j} \rho_{j+1}, \text{ and } v_1 + \rho_1 + 1 = v_s + p^h \rho_s. \tag{7.54}$$

For $1 \leq j, j' \leq s$ and $n_{j'-1} \leq r \leq n_{j'} - 1$,

(i) *if* $n \geq 2$ *or* $n \leq -2$,

$$v_j - n + p^{nh+r}\rho_j \geq v_{j'} + p^{r+1}\rho_{j'}; \tag{7.55}$$

(ii) *if* $n = 0$ *or* ± 1,

$$v_j - n + p^{nh+r}\rho_j \geq v_{j'} + p^{r}\rho_{j'}, \tag{7.56}$$

and the equality holds if and only if $j = j'$ *and* $n = 0$.

Proof. By direct calculation.

Lemma 7.48. *Suppose* $P_1, \cdots, P_n$ *are polynomials in* $R[X_1, \cdots, X_n]$ *defined by*

$$\begin{pmatrix} P_1 \\ \vdots \\ P_n \end{pmatrix} = -M_0 \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} + \begin{pmatrix} X_1^q \\ \vdots \\ X_n^q \end{pmatrix} - M_2 \begin{pmatrix} X_1^{q^2} \\ \vdots \\ X_n^{q^2} \end{pmatrix}, \tag{7.57}$$

where M_0, M_2 *are* $n \times n$ *matrices with entries in* $\mathfrak{m}_R$ *and* $\det M_0 \neq 0$. *Then for any* $(b_1, \cdots, b_n) \in R^n$, *the equations* $(P_1 = b_1, \cdots, P_n = b_n)$ *has* q^n *distinct solutions in* R^n.

Proof. For a matrix $A = (a_{ij})$, set $A^{(q)} = (a_{ij}^q)$ and $v(A) = \min\{v(a_{ij})\}$. Suppose $v(M_0)$ and $v(M_2) \geq c > 0$. Let $X = (X_1, \cdots, X_n)^T$ and $b = (b_1, \cdots, b_n)^T$, The equations $(P_1 = b_1, \cdots, P_n = b_n)$ is equivalent to

$$X^{(q)} = M_0 X + M_2 X^{(q^2)} + b. \tag{7.58}$$

Take q-th power in both side of (7.58) and then plug the resulting $X^{(q^2)}$ into (7.58), we get

$$\begin{aligned} X^{(q)} =& (M_0 + M_2 M_0^{(q)} M_0) X + M_2 M_0^{(q)} M_2 X^{(q^2)} \\ &+ M_2 M_2^{(q)} X^{(q^3)} + (M_2 M_0^{(q)} b + M_2 b^{(q)} b). \end{aligned}$$

By recursion, the solutions of the original equations satisfy

$$X^{(q)} = MX + b' \tag{7.59}$$

with $v(M) = v(M_0)$ and $\det(M) \neq 0$. The classical p-adic differential equation theory tells us that (7.59) has q^n distinct solutions.

On the other hand, from $X^{(q)} = MX + b$, Then

$$(I + M' M^{(q)}) X^{(q)} = MX + M' X^{(q^2)} + b - M' b^{(q)},$$

Given M_0 and M_2, by repeatedly using the relations

$$M = (I + M' M^{(q)}) M_0, \quad M' = (I + M' M^{(q)}) M_2,$$

we obtain M and M'. Then $X^{(q)} = MX + b$ implies that $X^{(q)} = M_0 X + M_2 X^{(q^2)} + b'$. This tells us that (7.57) has q^n solutions.

Proof (Proof of Proposition 7.46). Let V be the sub-$\mathbb{Q}_p$-vector space of C generated by $\lambda_1, \ldots, \lambda_h$. Let Λ be a lattice of V, then $\Lambda/(V \cap \mathfrak{m}_C \Lambda)$ is an $\overline{\mathbb{F}}_p$-vector space of dimension h, so we can choose the basis $(\lambda_1, \ldots, \lambda_h)$ of V such that there exist $0 \leq v_1 < \cdots < v_s < 1$ and integers $n_0 = 0 < \cdots < n_s = h$ such that $v(\lambda_i) = v_j$ for $n_{j-1}+1 \leq i \leq n_j$. Then the images of $\lambda_{n_{j-1}+1}, \ldots, \lambda_{n_j}$ are linearly independent modulo the ideal of $\mathcal{O}_C$ of valuation v_j. For $i = 1, \cdots, h$, let $m(i) = j$ if $v(\lambda_i) = v_j$, in particular $m(n_j) = j$. If $s = 1$, the results have already been proved in the previous proposition, thus we may assume $s \geq 2$.

Let $f = \eta \circ l_h^h : \mathfrak{m}_R^h \to C^h$. For elements in $S = \{(x_1, \ldots, x_h) \in m_R^h \mid v_R(x_i) \geq \rho_{m(i)}\}$, and for $r = 0, \ldots, h-1$,

$$\begin{aligned} &v(\sum_{i=1}^{h} \lambda_i \theta(\varphi^r(l_h(x_i)))) = v(\sum_{i=1}^{h} \sum_{n \in \mathbb{Z}} \lambda_i p^{-n} x_i^{(-nh-r)}) \\ \geq &\min_{1 \leq i \leq h} (v(\lambda_i) + p^{nh+r} v_R(x_i) - n) \\ \geq &v_{m(r+1)} + p^r \rho_{m(r+1)} \text{ (by Lemma 7.47).} \end{aligned}$$

Thus

$$f(S) \subseteq T = \{(x_0, \ldots, x_{h-1}) \in C^h \mid v(x_r) \geq v_{m(r+1)} + p^r \rho_{m(r+1)}\}.$$

As in the proof of the previous proposition, $(P_{h,1}^+)^h$, $\mathfrak{m}_R^h$ and C^h are H-modules and η is H-linear. Moreover, by (7.54),

$$\Theta T = \{(x_0, \ldots, x_{h-1}) \in C^h \mid v(x_r) \geq v_{m(r+1)} + p^{r+1} \rho_{m(r+1)}\}.$$

Consequently, we just need to show

$$\begin{aligned} \bar{f} : S/\varphi(S) &\longrightarrow T/\Theta T \\ (x_1, \ldots, x_h) &\longmapsto (\sum_{i=1}^{h} \sum_{n \in \mathbb{Z}} \lambda_i p^{-n} x_i^{(-nh-r)})_{0 \leq r \leq h-1} \end{aligned} \tag{7.60}$$

is surjective and the kernel is an $\mathbb{F}_q$-vector space of dimension 1.

By (7.55), if $n \geq 2$ or ≤ -2,

$$v(\lambda_i p^{-n} x_i^{(-nh-r)}) \geq v_{m(r+1)} + p^{r+1} \rho_{m(r+1)},$$

thus

$$\bar{f}(x_1, \ldots, x_h) = (\sum_{i=1}^{h} \sum_{n=-1}^{1} \lambda_i p^{-n} x_i^{(-nh-r)})_{0 \leq r \leq h-1}. \tag{7.61}$$

Let $\xi_1, \ldots, \xi_s \in R$ such that

$$\left(\frac{\xi_j^{(0)}}{\xi_{j+1}^{(0)}} \right)^{p^{n_j}} = \frac{\lambda_{n_{j+1}}}{\lambda_{n_j}} \quad \text{and} \quad \frac{(\xi_s^{(0)})^{p^h}}{\xi_1^{(0)}} = p \frac{\lambda_{n_1}}{\lambda_{n_s}}.$$

Then $v(\xi_j) = \rho_j$ and

$$\tau : \bigoplus_{j=1}^{s} (R/\xi_j^{p-1}R)^{n_j - n_{j-1}} \longrightarrow S/\varphi(S), \quad (y_i)_{1\le i\le h} \longmapsto (\xi_{m(i)} y_i) \tag{7.62}$$

is bijective. Let $x_i = \xi_{m(i)} y_i$.

For $n_{j-1}+1 \le i \le n_j$, let $\hat{\lambda}_i$ be an element in R such that $\theta(\hat{\lambda}_i) = \lambda_i$ and $\mu_i = \hat{\lambda}_i/\hat{\lambda}_{n_j}$, then $\mu_i \in R^\times$ and the images of $\mu_{n_{j-1}+1}, \dots, \mu_{n_j}$ are linearly independent over $\mathbb{F}_p$. Let $c_r = \hat{\lambda}_{n_{m(r+1)}}^{p^{h-r}} \xi_{m(r+1)}^q$,

$$Q_r = \sum_{i=1}^{h} \sum_{n=-1}^{1} \hat{\lambda}_i \hat{p}^{-n} X_i^{p^{nh+r}}, \tag{7.63}$$

and

$$P_r = c_r^{-1} Q_r(\xi_{m(1)}Y_1, \cdots, \xi_{m(h)}Y_h)^{p^{h-r}} \in R[Y_1, \cdots, Y_h]. \tag{7.64}$$

Then to show $\bar{f} \circ \tau$ is surjective, it suffices to show the equations $(P_0 = b_0, \dots, P_{h-1} = b_{h-1})$ has a solution in R^h for any $b \in R^h$. Note that P_r is of the form

$$P_r(Y_1, \cdots, Y_h) = \sum_{i=1}^{h} (a_{ir}Y_i + b_{ir}Y_i^q + c_{ir}Y_i^{q^2}) \tag{7.65}$$

with

$$a_{ir} = c_r^{-1}(\hat{\lambda}_i\hat{p})^{p^{h-r}} \xi_{m(i)}, \; b_{ir} = c_r^{-1}\hat{\lambda}_i^{p^{h-r}} \xi_{m(i)}^q, \; c_{ir} = c_r^{-1}(\hat{\lambda}_i\hat{p}^{-1})^{p^{h-r}} \xi_{m(i)}^{q^2}.$$

By (7.56), $v(a_{ir})$, $v(c_{ir}) > 0$, and $v(b_{ir}) \ge 0$ with $v_{br} = 0$ if and only if $m(i) = m(r+1)$. Let $M_0 = (a_{ir})$, $M_1 = (b_{ir})$ and $M_2 = (c_{ir})$, then $M_0, \; M_2 \in M_h(\mathfrak{m}_R)$, $\det M_0 \ne 0$ and $M_1 \in \mathrm{GL}_h(R)$. By change of variables we may assume that M_1 is the identity matrix, hence we are now in the situation of Lemma 7.48. Hence the equations $(P_0 = b_0, \dots, P_{h-1} = b_{h-1})$ has exactly q^h distinct solutions. In particular, $\bar{f}$ is surjective.

It remains to prove that the kernel of $\bar{f}$ is 1-dimensional over $\mathbb{F}_{p^h}$. Let Z_0 be the solutions of $Q_0 = \cdots = Q_{h-1} = 0$. Then argument above tells that Z_0 has q^h distinct points. Similar to the previous proposition, it suffices to show that $Z_0 \cap \varphi(S)$ has exactly q^{h-1} distinct points. Note that $Z_0 \cap \varphi(S)$ is the solutions of $Q_0 \circ \varphi = \cdots = Q_{h-1} \circ \varphi = 0$, $Q_r \circ \varphi = Q_{r+1}^p$ for $0 \le r \le h-1$, and

$$Q_h = Q_{h-1} \circ \varphi = \sum_{i=1}^{h} \sum_{n=-1}^{1} \hat{\lambda}_i \hat{p}^{-n} X_i^{q^{n+1}}. \tag{7.66}$$

Let $c_h = \hat{\lambda}_h \xi_s^q$, and

$$P_h = c_h^{-1} Q_h(\xi_{m(1)}Y_1, \cdots, \xi_{m(h)}Y_h) = c_h^{-1} \sum_{i=1}^{h} \sum_{n=-1}^{1} \hat{\lambda}_i \hat{p}^{-n} \xi_{m(i)}^{q^{n+1}} Y_i^{q^{n+1}}. \tag{7.67}$$

Then $Z_0 \cap \varphi(S)$ has the same cardinality of the solutions of $P_1 = \cdots = P_h = 0$. By calculation,

$$v(\hat{\lambda}_i \hat{p}^{-n} \xi_{m(i)}^{q^{n+1}}) = v(\lambda_i) + p^{nh+h}\rho_{m(i)} - n \geq v_s + q\rho_s = 1 + v_1 + \rho_1,$$

with equality only at the terms $\hat{\lambda}_i \hat{p}\ \xi_1$ for $m(i) = 1$ and $\hat{\lambda}_i \xi_s$ for $m(i) = s$. Then

$$\overline{P_h} = \sum_{m(i)=s} \mu_i Y_i^q + c \sum_{m(i)=1} \mu_i Y_i$$

where $c = (\hat{\lambda}_{n_1} \hat{p}\ \xi_1)/(\hat{\lambda}_h \xi_s^q)$. By similar argument of Lemma 7.48, one knows that the equations $P_1 = \cdots = P_h = 0$ has exactly q^{h-1} distinct solutions.

Corollary 7.49. *Suppose $\lambda_1, \ldots, \lambda_h \in C$ are linearly independent over $\mathbb{Q}_p$. Then there exist $a_1, \ldots, a_h \in P_{h,1}^+$ such that*

(1) $\sum_{i=1}^h \lambda_i \theta(\varphi^j(a_i)) = 0$ *for* $j = 0, 1, \ldots, h-1$;
(2) *let* $A = (a_{ij})_{1 \leq i,j \leq h}$ *with* $a_{ij} = \varphi^{i-1}(a_j)$, *then* $\det A \neq 0$.

Proof. Suppose $a = (a_1, \cdots a_h) \in \mathrm{Ker}\ \eta \subseteq (P_{h,1}^+)^h$ is a generator of the 1-dimensional H-module $\mathrm{Ker}\,\eta$, then $\{a, \varphi(a), \cdots, \varphi^{h-1}(a)\}$ is a $\mathbb{Q}_{p^h}$-basis of $\mathrm{Ker}\,\eta$ and the $\mathbb{Q}_{p^h}$-linear map $u_a : \mathbb{Q}_{p^h}^h \to \mathrm{Ker}\,\eta$,

$$u_a(t_0, \ldots, t_{h-1}) = t_0 a + t_1 \varphi(a) + \cdots + t_{h-1}\varphi^{h-1}(a)$$

is an isomorphism. Then $a_1, \cdots a_h$ satisfy (1) and (2).

Suppose A is given as in the above corollary. Write $d = \det A$. Then $\varphi(d) = (-1)^{h-1} d$. We can write $d = \kappa t$ with $\kappa \in \mathbb{Q}_{p^2}^\times$. Suppose $A' \in M_h(B_{\mathrm{cris}}^+)$ such that $A'A = AA' = tI$. In particular, $\det A' = \kappa^{-1} t^{h-1}$.

For any lifting $(\hat{\lambda}_1, \cdots, \hat{\lambda}_h)$ of $(\lambda_1, \cdots, \lambda_h)$ in B_{cris}^+, then

$$A(\hat{\lambda}_1, \hat{\lambda}_2, \cdots, \hat{\lambda}_h)^T = (t\beta_1, t\beta_2, \cdots, t\beta_h)^T$$

(where ^{T} means the transpose of a matrix), thus

$$(\hat{\lambda}_1, \hat{\lambda}_2, \cdots, \hat{\lambda}_h)^T = A'(\beta_1, \beta_2, \cdots, \beta_h)^T.$$

If varying $\hat{\lambda}_i$, we then get an identity of matrices

$$P := (\hat{\lambda}_i^j) = A'(\beta_i^j) := A'B' \tag{7.68}$$

with $\hat{\lambda}_i^j$ a lifting of λ_i for every $1 \leq j \leq h$. If we let $\hat{\lambda}_i^j = \hat{\lambda}_i + \delta_{ij} t$ with δ_{ij} the Kronecker symbol. Then $\det P = (\hat{\lambda}_1 + \cdots + \hat{\lambda}_h + t)t^{h-1}$, $\det B'$ is a unit in B_{cris}^+ and $B' \in \mathrm{GL}_h(B_{\mathrm{cris}}^+)$. We have a decomposition $A' = PB$ with $P \in M_h(B_{\mathrm{cris}}^+)$ and $B = (B')^{-1} \in \mathrm{GL}_h(B_{\mathrm{cris}}^+)$.

7.4.3 The proof

Proof (Proof of Theorem 7.41). Our proof is divided into two steps:

(1) Suppose $\lambda_1, \cdots, \lambda_h$ are linearly independent over $\mathbb{Q}_p$. Choose $a_1, \cdots, a_h$ as in Corollary 7.49, as define A and $A' = PB$ as above. We shall define an isomorphism

$$\alpha : Y \to P_{h,1}^+, \quad y = (u_1, \cdots, u_h) \mapsto x = \sum_{i=1}^{h} a_i \frac{u_i}{t}. \tag{7.69}$$

First $\varphi^h(x) = px$ since $\varphi^h(a_i) = pa_i$ and $\varphi(u_i/t) = u_i/t$. To see that $x \in P_{h,1}^+$, we just need to show $x \in B_{\mathrm{cris}}^+$. However, $tx = \sum a_i u_i \in B_{\mathrm{cris}}^+$, by Theorem 7.26(1), it suffice to show $\theta(\varphi^j(tx)) = 0$ for all $j \in \mathbb{N}$, or even for $0 \le j \le h-1$. In this case, $\varphi^j(tx) = p^j \sum\limits_{i=1}^{h} \varphi^j(a_i) u_i$ and $\theta(\varphi^j(tx)) = cp^j \sum\limits_{i=1}^{h} \theta(\varphi^j(a_i))\lambda_i = 0$.

We define a map $\alpha' : P_{h,1}^+ \to Y$ and check it is invertible to α. Note that $A(\frac{u_1}{t}, \frac{u_2}{t}, \cdots, \frac{u_h}{t})^T = (x, \varphi(x), \cdots, \varphi^{h-1}(x))^T$. Set

$$\alpha'(x) = (x, \varphi(x), \cdots, \varphi^{h-1}(x)) A'^T = (x, \varphi(x), \cdots, \varphi^{h-1}(x)) B^T P^T.$$

It is clear to see that $\alpha'(x) \in Y$. From the construction one can check α and α' are inverse to each other.

The composite map $P_{h,1}^+ \xrightarrow{\alpha^{-1}} Y \xrightarrow{\rho} C(1)$ then sends $x \in P_{h,1}^+$ to

$$\begin{aligned} &(b_1, \cdots, b_h) A' (x, \varphi(x), \cdots, \varphi^{h-1}(x))^T \\ =&(b_1, \cdots, b_h) PB (x, \varphi(x), \cdots, \varphi^{h-1}(x))^T = \sum_{j=1}^{h} c_j \varphi^{j-1}(x). \end{aligned}$$

Since $\theta((b_1, \cdots, b_h)P) = 0$, $\theta(c_j) = 0$. Thus the composite map is nothing but

$$x \mapsto t \cdot \sum_{j=1}^{h} \theta\Big(\frac{c_j}{t}\Big) \theta(\varphi^{h-1}(x)).$$

By Proposition 7.42, ρ is either identically zero, or is onto and $\operatorname{Ker} \rho$ is a $\mathbb{Q}_p$-vector space of dimension h.

(2) Suppose $\lambda_1, \ldots, \lambda_h$ are not linearly independent over $\mathbb{Q}_p$. We suppose $\lambda_1, \ldots, \lambda_{h'}$ are linearly independent and $\lambda_{h'+1}, \ldots, \lambda_h$ are generated by $\lambda_1, \ldots, \lambda_{h'}$. Suppose

$$\lambda_j = \sum_{i=1}^{h'} a_{ij} \lambda_i, \ a_{ij} \in \mathbb{Q}_p. \tag{7.70}$$

Write $v_j = u_j - \sum\limits_{i=1}^{h'} a_{ij} u_i$ for $j > h'$, then $\theta(v_j) = 0$ and $v_j \in \mathbb{Q}_p(1)$.

Let Y' be the corresponding Y for $\lambda_1, \cdots, \lambda_{h'}$. One checks easily that the map $Y \to Y' \oplus \mathbb{Q}_p(1)^{h-h'}$,

$$(u_1, \ldots, u_h) \longmapsto (u_1, \cdots, u_{h'}, v_{h'+1}, \cdots, v_h) \tag{7.71}$$

is a bijection. Now

$$\rho(x) = \sum_{i=1}^{h'} \Big(b_i + \sum_{j=h'+1}^{h} b_j a_{ij} \Big) u_i + \sum_{j=h'+1}^{h} b_j v_j. \tag{7.72}$$

For $1 \leq i \leq h'$, let $c_i = b_i + \sum_{j=s'+1}^{s} b_j a_{ij}$.

If c_i are not all zero, then by (7.70),

$$\begin{aligned} \sum_{i=1}^{h'} \lambda_i \theta(c_i) &= \sum_{i=1}^{h'} \lambda_i \theta(b_i) + \sum_{i=1}^{h'} \sum_{j=h'+1}^{h} \theta(b_j) a_{ij} \lambda_i \\ &= \sum_{i=1}^{h'} \lambda_i \theta(b_i) + \sum_{j=h'+1}^{h} \lambda_j \theta(b_j) = 0, \end{aligned}$$

we are in situation (1), thus the map

$$\rho' : \ Y' \to B_2, \ (u_1, \cdots, u_{h'}) \mapsto \sum_{i=1}^{h'} c_i u_i \tag{7.73}$$

is surjective, and then ρ is surjective. Since $\operatorname{Ker} \rho / \operatorname{Ker} \rho' \simeq \mathbb{Q}_p(1)^{h-h'}$, $\dim_{\mathbb{Q}_p} \operatorname{Ker} \rho = \dim_{\mathbb{Q}_p} \operatorname{Ker} \rho' + h - h' = h$.

If for all $1 \leq i \leq h'$, $c_i = 0$, then $\rho(x) = \sum\limits_{j=h'+1}^{h} b_j v_j$, thus $\operatorname{Im} \rho = \rho(\mathbb{Q}_p(1)^{h-h'})$ and $\dim_{\mathbb{Q}_p} \operatorname{Im} \rho \leq h$.

7.4.4 Application: B_e is an almost Euclidean domain.

Recall that an *Euclidean domain* is an integral ring B such that there exists a map $\deg : B \to \mathbb{N} \cup \{-\infty\}$, called an *Euclidean stathme*, satisfying:

(i) $\deg(ab) \geq \deg(a) + \deg(b)$ and $\deg(a) = -\infty$ if and only if $a = 0$;
(ii) if $a, b \in B$ and $a \neq 0$, there exist unique $q, r \in B$ such that $b = qa + r$ and $\deg(r) < \deg(a)$.

It is well known that an Euclidean domain is automatically a principal ideal domain.

Definition 7.50. *An* almost Euclidean domain *is an integral ring B such that there exists a map* $\deg : B \to \mathbb{N} \cup \{-\infty\}$ *satisfying the following three conditions:*

(i) $\deg(ab) \geq \deg(a) + \deg(b)$ *and* $\deg(a) = -\infty$ *if and only if* $a = 0$*;*
(ii) *if* $a, b \in B$ *and* $a \neq 0$*, there exist* $q, r \in B$ *such that* $b = qa + r$ *and* $\deg(r) \leq \deg(a)$*;*
(iii) *if* $a, b \in B$ *and* $\deg(a) = \deg(b) \neq -\infty$*, then either there exists* $x \in B$ *such that* $b = ax$*, or there exists* $x, y \in B$ *such that* $-\infty < \deg(ax + by) < \deg(a)$.

The above map deg *is called an* almost Euclidean stathme.

It is clear from the definition an Euclidean domain is almost Euclidean.

Proposition 7.51. *An almost Euclidean domain is a principal ideal domain.*

Proof. Suppose I is a non-zero ideal of an almost Euclidean ring B, we need to show I is principal. Let $d = d(I) = \min\{\deg(b) : b \in I, b \neq 0\}$, then by (ii), I is generated by elements $b \in I$ such that $\deg(b) = d$. Let $a \in I$ and $\deg(a) = d$. For any $b \in I$ and $\deg(b) = d$, by (iii), if $b \neq ax$, there exists $x, y \in B$ such that $\deg(ax+by) < \deg(a) = d$ and $ax+by \neq 0$, a contradiction to the minimality of d, hence $b = ax$. As a consequence, $I = (a)$ is principal.

Definition 7.52. *Suppose B is an integral ring and B_η its field of fractions. An* almost Euclidean degree *over B is an almost Euclidean stathme over B satisfying*

(o) *there exists a valuation v over B_η such that* $\deg(b) = -v(b)$ *for all* $b \in B$*;*
(iv) *one can choose x, y with degree* ≤ 1 *in* (iii) *of the above definition.*

We prove the following important result using the Fundamental Lemma:

Theorem 7.53. *The map* $\deg = \deg_\infty$ *given in* (7.29) *is an almost Euclidean degree over the ring B_e, hence B_e is almost Euclidean and principal.*

Proof. We only have to check the conditions (ii) and (iv).

For (ii), suppose $a, b \in B_e$ and $\deg(a) = r \neq -\infty$ and $\deg(b) = s$. We may assume $r < s$, otherwise, just let $q = 0$ and $r = a$. It suffices to find $q \in B_e$ such that $\deg(b - qa) < s$.

Write $a = t^{-r}a_0$ and $b = t^{-s}b_0$, then $\theta(a_0)$ and $\theta(b_0)$ are both not zero. Suppose $q_0 \in P^+_{1,s-r}$, $\theta(q_0) = \theta(b_0)/\theta(a_0)$, and $q = t^{r-s}q_0$, then $q \in B_e$ and $\deg(b - qa) < s$. (ii) is proven.

For (iv), let $\deg x = \deg y = d > -\infty$, $x_0 = xt^d$, $y_0 = yt^d \in B^+_{\mathrm{cris}}$. Use the Fundamental Lemma (Theorem 7.41), let $b_1 = \overline{x_0}$ and $b_2 = \overline{y_0}$ in B_2, then there exist $u_1, u_2 \in U$ such that $b_1u_1 + b_2u_2 = 0$ and $x_0u_1 + y_0u_2 \in \mathrm{Fil}^2 B_{\mathrm{dR}}$,

$$x_0\frac{u_1}{t} + y_0\frac{u_2}{t} \in \mathrm{Fil}^1 B_{\mathrm{dR}}.$$

Thus $\deg(xu_1/t + yu_2/t) < d$ and $u_1/t, u_2/t \in B_e$ are of degree ≤ 1.

Remark 7.54. By a generalization of the Fundamental Lemma, one can show $B_{e,h}$ and ${}^hB_e$ are almost Euclidean and hence principal.

8

B_{st} and semi-stable representations

8.1 B_{st} and semi-stable representations

8.1.1 B_{st} and its properties.

Definition 8.1. *The ring of semi-stable periods or log-crystalline periods* B_{st} *is the ring* $B_{\mathrm{cris}}[\mathbf{u}]$, *the sub-*$B_{\mathrm{cris}}$*-algebra of* B_{dR} *generated by* $\mathbf{u} = \log[\varpi]$.

Remark 8.2. Historically B_{st} is called the ring of semi-stable periods. However, in light of current development, the ring of log-crystalline periods seems to be a more appropriate name.

Since $\mathbf{u}$ is transcendental over C_{cris} (Proposition 7.14), we have

Theorem 8.3. *The homomorphism of* B_{cris}*-algebras*

$$B_{\mathrm{cris}}[x] \longrightarrow B_{\mathrm{st}}, \quad x \longmapsto \mathbf{u}$$

is an isomorphism.

Clearly B_{st} and $C_{\mathrm{st}} = \mathrm{Frac}\, B_{\mathrm{st}}$ are stable under the action of G_K (even of G_{K_0}).

Theorem 8.4. (1) *The map*

$$\iota : K \otimes_{K_0} B_{\mathrm{st}} \longrightarrow B_{\mathrm{dR}}, \quad \lambda \otimes b \mapsto \lambda b$$

is injective.
(2) $(C_{\mathrm{st}})^{G_K} = K_0$, *hence*

$$(B_{\mathrm{cris}}^{+})^{G_K} = (B_{\mathrm{cris}})^{G_K} = (B_{\mathrm{st}})^{G_K} = K_0.$$

Proof. By Proposition 7.8, $K \otimes_{K_0} B_{\mathrm{cris}} \subset B_{\mathrm{dR}}$ is a domain and thus $\mathrm{Frac}(K \otimes_{K_0} B_{\mathrm{cris}})$ is a finite extension over C_{cris}, and $\mathbf{u}$ is still transcendental over $\mathrm{Frac}(K \otimes_{K_0} B_{\mathrm{cris}})$. Therefore

$$K \otimes_{K_0} B_{\mathrm{st}} = K \otimes_{K_0} B_{\mathrm{cris}}[\mathbf{u}]] = (K \otimes_{K_0} B_{\mathrm{cris}})[\mathbf{u}] \subset B_{\mathrm{dR}}$$

and (1) is proved.

For (2), we know that

$$K_0 \subset (B^+_{\mathrm{cris}})^{G_K} \subset (B_{\mathrm{cris}})^{G_K} \subset (B_{\mathrm{st}})^{G_K} \subset (C_{\mathrm{st}})^{G_K}$$

and by (1),

$$(C_{\mathrm{st}})^{G_K} \otimes_{K_0} K \subset (B_{\mathrm{dR}})^{G_K} = K.$$

Thus $C_{\mathrm{st}}^{G_K}$ must be K_0.

B_{st} is also endowed with two operators: the Frobenius φ and the monodromy operator N. By the definition of the logarithm map, we extend $\varphi : B_{\mathrm{cris}} \to B_{\mathrm{cris}}$ to an endomorphism of B_{st} by requiring

$$\varphi(\mathbf{u}) = p\mathbf{u}. \tag{8.1}$$

Then φ commutes with the action of G_K. One sees that $\varphi : B_{\mathrm{st}} \to B_{\mathrm{st}}$ is injective.

Definition 8.5. *The* monodromy operator

$$\begin{aligned} N : B_{\mathrm{st}} &\longrightarrow B_{\mathrm{st}} \\ \sum_{n\in\mathbb{N}} b_n \mathbf{u}^n &\longmapsto -\sum_{n\geq 1} n b_n \mathbf{u}^{n-1} \end{aligned}$$

is the unique B_{cris}-derivation such that $N(\mathbf{u}) = -1$.

Proposition 8.6. *The monodromy operator N is a nilpotent operator satisfying*

(1) *the sequence*

$$0 \longrightarrow B_{\mathrm{cris}} \longrightarrow B_{\mathrm{st}} \xrightarrow{N} B_{\mathrm{st}} \longrightarrow 0 \tag{8.2}$$

is exact;

(2) *$gN = Ng$ for every $g \in G_{K_0}$;*

(3) *$N\varphi = p\varphi N$.*

Proof. (1) is clear from definition.

(2) Since $g(\mathbf{u}) = \mathbf{u} + \eta(g)t$, but $\eta(g)t \in B_{\mathrm{cris}}$ and $N(\eta(g)t) = 0$, we have

$$N(gb) = g(Nb), \text{ for all } b \in B_{\mathrm{st}}, g \in G_{K_0}.$$

(3) Since

$$\begin{aligned} N\varphi(\sum_{n\in\mathbb{N}} b_n \mathbf{u}^n) =& N(\sum_{n\in\mathbb{N}} \varphi(b_n) p^n \mathbf{u}^n) \\ =& -\sum_{n\in\mathbb{N}} n\varphi(b_n) p^n \mathbf{u}^{n-1} \\ =& p\varphi N(\sum_{n\in\mathbb{N}} b_n \mathbf{u}^n), \end{aligned}$$

we have $N\varphi = p\varphi N$.

8.1.2 Crystalline and semi-stable representations

Proposition 8.7. *The rings B_{cris} and B_{st} are $(\mathbb{Q}_p, G_K)$-regular, which means that*

(1) *B_{cris} and B_{st} are domains,*
(2) *$B_{\mathrm{cris}}^{G_K} = B_{\mathrm{st}}^{G_K} = C_{\mathrm{st}}^{G_K} = K_0$,*
(3) *If $b \in B_{\mathrm{cris}}$ (resp. B_{st}), $b \neq 0$, such that $\mathbb{Q}_p b$ is stable under G_K, then b is invertible in B_{cris} (resp. B_{st}).*

Proof. (1) is immediate, since $B_{\mathrm{cris}} \subset B_{\mathrm{st}} \subset B_{\mathrm{dR}}$. (2) is just Theorem 8.4 (2).

For (3), we know B_{cris} contains $P_0 = W(\bar{k})[\frac{1}{p}]$. Let $\overline{P}$ be the algebraic closure of P_0 in C, then B_{dR} is a $\overline{P}$-algebra.

If $b \in B_{\mathrm{dR}}$, $b \neq 0$, such that $\mathbb{Q}_p b$ is stable under G_K, multiplying b by t^{-i} for some $i \in \mathbb{Z}$, we may assume $b \in B_{\mathrm{dR}}^+$ but $b \notin \mathrm{Fil}^1 B_{\mathrm{dR}}$. Suppose $g(b) = \eta(g)b$. Let $\bar{b} = \theta(b)$ be the image of $b \in C$. Then $\mathbb{Q}_p \bar{b} \cong \mathbb{Q}_p(\eta)$ is a one-dimensional $\mathbb{Q}_p$-subspace of C stable under G_K, by Sen's result (Corollary 4.45), this implies that $\eta(I_K)$ is finite and $\bar{b} \in \overline{P} \subset B_{\mathrm{dR}}^+$. If $b' = b - \bar{b} \neq 0$, then $b' \in \mathrm{Fil}^i B_{\mathrm{dR}} - \mathrm{Fil}^{i+1} B_{\mathrm{dR}}$ for some $i \geq 1$. Note that $\mathbb{Q}_p b'$ is also stable by G_K whose action is defined by the same η. Then the G_K-action on $\mathbb{Q}_p \theta(t^{-i}b')$ is defined by $\chi^{-i}\eta$ where χ is the cyclotomic character and $\chi^{-i}\eta(I_K)$ is finite. However, $\chi^{-i}\eta(I_K)$ and $\eta(I_K)$ can not be both finite, hence $b' = 0$ and $b = \bar{b} \in \overline{P}$.

Now since t^i is always invertible in $B_{\mathrm{cris}} \subset B_{\mathrm{st}}$, it suffices to show $\overline{P} \cap B_{\mathrm{st}} = P_0 \subset B_{\mathrm{cris}}$. Indeed, suppose $\overline{P} \cap B_{\mathrm{st}} = Q \supsetneq P_0$. Then $\mathrm{Frac}(Q)$ contains a nontrivial finite extension L of P_0. Note that $L_0 = P_0$ and by (2), $B_{\mathrm{st}}^{G_L} = P_0$, but $\mathrm{Frac}(Q)^{G_L} = L$, which is a contradiction!

Remark 8.8. The proof implies that if $b \in B_{\mathrm{dR}}$ such that $\mathbb{Q}_p b$ is stable by the G_K-action, then $b = t^i b'$ for some $i \in \mathbb{Z}$ and $b' \in \overline{P}$.

For any p-adic representation V, we denote

$$\mathbf{D}_{\mathrm{st}}(V) := (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K}, \quad \mathbf{D}_{\mathrm{cris}}(V) := (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)^{G_K}. \tag{8.3}$$

Note that $\mathbf{D}_{\mathrm{st}}(V)$ and $\mathbf{D}_{\mathrm{cris}}(V)$ are K_0-vector spaces and the maps

$$\alpha_{\mathrm{st}}(V) : B_{\mathrm{st}} \otimes_{K_0} \mathbf{D}_{\mathrm{st}}(V) \to B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V$$
$$\alpha_{\mathrm{cris}}(V) : B_{\mathrm{cris}} \otimes_{K_0} \mathbf{D}_{\mathrm{cris}}(V) \to B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V$$

are always injective.

Definition 8.9. *For a p-adic representation V of G_K,*

(i) *V is called* semi-stable *or* log-crystalline *if it is B_{st}-admissible, i.e., if the map $\alpha_{\mathrm{st}}(V)$ is an isomorphism;*
(ii) *V is called* crystalline *if it is B_{cris}-admissible, i.e., if the map $\alpha_{\mathrm{cris}}(V)$ is an isomorphism.*

Clearly, for any p-adic Galois representation V, $\mathbf{D}_{\mathrm{cris}}(V)$ is a subspace of $\mathbf{D}_{\mathrm{st}}(V)$ and hence

$$\dim_{K_0} \mathbf{D}_{\mathrm{cris}}(V) \leq \dim_{K_0} \mathbf{D}_{\mathrm{st}}(V) \leq \dim_{\mathbb{Q}_p} V.$$

Therefore we have

Proposition 8.10. (1) *A p-adic representation V is semi-stable (resp. crystalline) if and only if* $\dim_{K_0} \mathbf{D}_{\mathrm{st}}(V) = \dim_{\mathbb{Q}_p} V$ *(resp.* $\dim_{K_0} \mathbf{D}_{\mathrm{cris}}(V) = \dim_{\mathbb{Q}_p} V$*).*
(2) *A crystalline representation is always semi-stable.*

Suppose V is a p-adic representation of G_K. ince $K \otimes_{K_0} B_{\mathrm{st}} \to B_{\mathrm{dR}}$ is injective (Theorem 8.4), we see that

$$\begin{aligned} K \otimes_{K_0} \mathbf{D}_{\mathrm{st}}(V) &= K \otimes_{K_0} (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K} \\ &= (K \otimes_{K_0} (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V))^{G_K} \\ &= ((K \otimes_{K_0} B_{\mathrm{st}}) \otimes_{\mathbb{Q}_p} V)^{G_K} \\ &\hookrightarrow (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K} = \mathbf{D}_{\mathrm{dR}}(V). \end{aligned}$$

Thus $K \otimes_{K_0} \mathbf{D}_{\mathrm{st}}(V) \subset \mathbf{D}_{\mathrm{dR}}(V)$ as K-vector spaces.

Assume furthermore that V is semi-stable, then

$$\dim_K K \otimes_{K_0} \mathbf{D}_{\mathrm{st}}(V) = \dim_{\mathbb{Q}_p} V \leq \dim \mathbf{D}_{\mathrm{dR}}(V) \leq \dim_{\mathbb{Q}_p} V$$

implies that

$$\dim \mathbf{D}_{\mathrm{dR}} V = \dim_{\mathbb{Q}_p} V,$$

i.e., V is de Rham. Thus we have

Proposition 8.11. *If V is a semi-stable p-adic representation of G_K, then it is de Rham, and*

$$\mathbf{D}_{\mathrm{dR}}(V) = K \otimes_{K_0} \mathbf{D}_{\mathrm{st}}(V).$$

Suppose V is a p-adic representation of G_K. On $\mathbf{D}_{\mathrm{st}}(V)$ there are a lot of structures because of the maps φ and N on B_{st}. We define two corresponding maps φ and N on $B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V$ by

$$\begin{aligned} \varphi(b \otimes v) &= \varphi b \otimes v \\ N(b \otimes v) &= Nb \otimes v \end{aligned}$$

for $b \in B_{\mathrm{st}},\ v \in V$. The maps φ and N commute with the action of G_K and satisfy $N\varphi = p\varphi N$, and φ is injective.

Lemma 8.12. $D = \mathbf{D}_{\mathrm{st}}(V)$ *is a finite dimensional K_0-vector space of dimension* $\leq \dim_{\mathbb{Q}_p} V$*, such that*

(1) *D is stable under φ and N, N is K_0-linear and nilpotent, φ is σ-semi-linear and bijective, and $N\varphi = p\varphi N$ on D;*

(2) $D_K = K \otimes_{K_0} \mathbf{D}_{\mathrm{st}}(V) \subset \mathbf{D}_{\mathrm{dR}}(V)$ *is a filtered* K*-vector space with the induced filtration*

$$\mathrm{Fil}^i D_K = D_K \bigcap \mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(V).$$

(3) $D_{\mathrm{cris}}(V) = D_{N=0}$*, hence* V *is crystalline if and only if* V *is semi-stable and* $N = 0$ *on* $\mathbf{D}_{\mathrm{st}}(V)$*.*

Proof. The bijectivity of $\varphi : D \to D$ follows from that D is finite dimensional and φ is injective. The rest is clear.

8.2 (φ, N)-modules and filtered (φ, N)-modules

8.2.1 (φ, N)-modules over K_0.

Definition 8.13. *The category of* (φ, N)*-module over* K_0 *(or over* k*), denoted by* $\mathbf{Mod}_{K_0}(\varphi, N)$*, is the following category:*

(i) *An object in* $\mathbf{Mod}_{K_0}(\varphi, N)$ *is a finite dimensional* K_0*-vector space* D *equipped with two maps*

$$\varphi, N : D \longrightarrow D$$

satisfying the following properties:

(a) φ *is bijective and semi-linear with respect to the absolute Frobenius* σ *on* K_0*,*

(b) N *is a* K_0*-linear map,*

(c) $N\varphi = p\varphi N$*.*

(ii) *A morphism* $\eta : D_1 \to D_2$ *between two* (φ, N)*-modules is a* K_0*-linear map commuting with* φ *and* N*.*

Definition 8.14. *The category of* φ*-module over* K_0*, denoted by* $\mathbf{Mod}_{K_0}(\varphi)$*, is the full sub-category* $\mathbf{Mod}_{K_0}(\varphi, N = 0)$ *of* $\mathbf{Mod}_{K_0}(\varphi, N)$*. An object of it is also called a* φ-isocrystal *of* k*.*

Remark 8.15. (a) Take $E = k$ and $\mathcal{E} = K_0$, the definition of φ-module is slightly stronger than the one in §3.3. Here we require

$$\dim_{K_0} D < \infty \text{ and } \varphi \text{ is bijective,}$$

the latter is equivalent to that

$$\Phi : D_\varphi = K_0 \, {}_\sigma\!\otimes_{K_0} D \to D, \quad \Phi(\lambda \otimes d) = \lambda\varphi(d)$$

is an isomorphism of K_0-vector spaces. However, these conditions are satisfied for étale φ-modules over K_0.

(b) In analogue of isocrystals, we may also call a (φ, N)-module over K_0 a *log-φ-isocrystal of* k.

(c) The forgetful functor from $\mathbf{Mod}_{K_0}(\varphi, N)$ to $\mathbf{Mod}_{K_0}(\varphi)$ is exact.

The category $\mathbf{Mod}_{K_0}(\varphi, N)$ of (φ, N)-modules is an abelian category. In fact, it is the category of left modules over the non-commutative ring generated by K_0 and two elements φ and N with relations

$$\varphi\lambda = \sigma(\lambda)\varphi, \quad N\lambda = \lambda N, \quad \text{for all } \lambda \in K_0$$

and

$$N\varphi = p\varphi N.$$

Moreover, there exist tensor products, unit and dual objects in $\mathbf{Mod}_{K_0}(\varphi, N)$.

(i) For D_1 and D_2 in $\mathbf{Mod}_{K_0}(\varphi, N)$, the *tensor product* $D_1 \otimes D_2 = D_1 \otimes_{K_0} D_2$ with

$$\varphi(d_1 \otimes d_2) = \varphi d_1 \otimes \varphi d_2, \quad N(d_1 \otimes d_2) = Nd_1 \otimes d_2 + d_1 \otimes Nd_2.$$

(ii) K_0 has a structure of (φ, N)-module by $\varphi = \sigma$ and $N = 0$. Moreover

$$K_0 \otimes D = D \otimes K_0 = D,$$

therefore K_0 is the *unit object* in $\mathbf{Mod}_{K_0}(\varphi, N)$.

(iii) If D is an object $\mathbf{Mod}_{K_0}(\varphi, N)$, the *dual object* $D^* = \mathscr{L}(D, K_0)$ of D is the set of linear maps $\eta : D \to K_0$ with φ and N given by

$$\varphi(\eta) = \sigma \circ \eta \circ \varphi^{-1}, \quad N(\eta) = -\eta \circ N.$$

Remark 8.16. If in the definition of (φ, N)-modules, we drop the condition that

$$\dim_{K_0} D < \infty \text{ and } \varphi \text{ is bijective,}$$

we get an abelian category which has tensor product and unit object, of which $\mathbf{Mod}_{K_0}(\varphi, N)$ is a full sub-category. However, there is no dual object.

Proposition 8.17. *The operator N is nilpotent.*

Proof. If N is not nilpotent, let h be an integer such that $N^h(D) = N^{h+1}(D) = \cdots = N^m(D)$ for all $m \geq h$. Then $D' = N^h(D) \neq 0$ is invariant by N, and by φ since $N^m\varphi = p^m\varphi N^m$ for every integer $m > 0$. Thus D' is a (φ, N)-module such that N and φ are both bijective.

Pick a basis of D' and suppose under this basis, the matrices of φ and N are A and B respectively. Then A and B must be both invertible by the bijectivity of φ and N. By the relation $N\varphi = p\varphi N$ we have $BA = pA\sigma(B)$. Consequently $v_p(\det(B)) = \dim D' + v_p(\det(\sigma(B))) = \dim D' + v_p(\det(B))$, hence $\det(B) = 0$, which is impossible.

8.2.2 $t_N(D)$ and Theorem of Dieudonné-Manin.

Assume D is a φ-module over K_0 (i.e, a φ-isocrystal over k). We associate an integer $t_N(D)$ to D in two steps. Note that this extends naturally to (φ, N)-modules by setting $t_N(D) = t_N(F(D))$ where F is the forgetful functor.

Step one: assume first that $\dim_{K_0} D = 1$. Then $D = K_0 d$ with $\varphi d = \lambda d$, for $d \neq 0 \in D$ and $\lambda \in K_0$. φ is bijective implies that $\lambda \neq 0$.

Assume $d' = ad$, $a \in K_0$, $a \neq 0$, such that $\varphi d' = \lambda' d'$. One can compute easily that

$$\varphi d' = \sigma(a)\lambda d = \frac{\sigma(a)}{a}\lambda d',$$

hence

$$\lambda' = \lambda \frac{\sigma(a)}{a}.$$

As $\sigma : K_0 \to K_0$ is an automorphism, $v_p(\lambda) = v_p(\lambda') \in \mathbb{Z}$ is independent of the choice of the basis of D. We define

Definition 8.18. *If D is a φ-module over K_0 of dimension 1, set*

$$t_N(D) := v_p(\lambda) \tag{8.4}$$

where $\lambda \in \mathrm{GL}_1(K_0) = K_0^\times$ is the matrix of φ under some (any) basis.

Remark 8.19. The letter N in the expression $t_N(D)$ stands for the word *Newton*, not for the monodromy map $N : D \to D$.

Step two: assume $\dim_{K_0} D = r$ is arbitrary. The r-th exterior product $\bigwedge_{K_0}^r D$ is a one-dimensional K_0-vector space with induced φ-module structure by tensor product.

Definition 8.20. *If D is a φ-module over K_0 of dimension r, set*

$$t_N(D) := t_N(\bigwedge\nolimits_{K_0}^r D). \tag{8.5}$$

Suppose $\{e_1, \cdots, e_r\}$ is a basis of D over K_0, then $\varphi(e_i) = \sum_{j=1}^r a_{ij} e_j$. the matrix of φ under this basis is $A = (a_{ij})_{1\leq i,j\leq r} \in \mathrm{GL}_r(K_0)$. Suppose $\{e'_1, \cdots, e'_r\}$ is another basis and A' the matrix of φ under this basis, suppose the transformation matrix of these two bases is P, then $A = \sigma(P)A'P^{-1}$. By linear algebra, then we have

Proposition 8.21.

$$t_N(D) = v_p(\det A). \tag{8.6}$$

Proposition 8.22. *One has*

(1) *If $0 \to D' \to D \to D'' \to 0$ is a short exact sequence of φ-modules, then $t_N(D) = t_N(D') + t_N(D'')$.*

(2) $t_N(D_1 \otimes D_2) = \dim_{K_0}(D_2) t_N(D_1) + \dim_{K_0}(D_1) t_N(D_2)$.
(3) $t_N(D^*) = -t_N(D)$.

Proof. (1) Choose a K_0-basis $\{e_1, \cdots, e_{r'}\}$ of D' and extend it to a basis $\{e_1, \cdots, e_r\}$ of D, then $\{\bar{e}_{r'+1}, \cdots, \bar{e}_r\}$ is a basis of D''. Under these bases, suppose the matrix of φ over D' is A, over D'' is B, then over D the matrix of φ is $\left(\begin{smallmatrix} A & * \\ 0 & B \end{smallmatrix}\right)$. Thus

$$t_N(D) = v_p(\det(A) \cdot \det(B)) = t_N(D') + t_N(D'').$$

(2) If the matrix of φ over D_1 to a certain basis $\{e_i\}$ is A, and over D_2 to a certain basis $\{f_j\}$ is B, then $\{e_i \otimes f_j\}$ is a basis of $D_1 \otimes D_2$ and under this basis, the matrix of φ is $A \otimes B = (a_{i_1,i_2} B)$, the Kronecker product of A and B. Thus $\det(A \otimes B) = \det(A)^{\dim D_2} \det(B)^{\dim D_1}$ and

$$t_N(D_1 \otimes D_2) = v_p(\det(A \otimes B)) = \dim_{K_0}(D_2) t_N(D_1) + \dim_{K_0}(D_1) t_N(D_2).$$

(3) If the matrix of φ over D to a certain basis $\{e_i\}$ is A, then under the dual basis $\{e_i^*\}$ of D^*, the matrix of φ is $\sigma(A^{-1})$, hence $t_N(D^*) = v_p(\det \sigma(A^{-1})) = -v_p(\det A) = -t_N(D)$.

Definition 8.23. *The* slope *of a nonzero φ-module D over K_0 is defined to be* $\mu(D) = \frac{t_N(D)}{\dim_{K_0} D}$.

A φ-module D is called pure of slope μ *if there exists a W-lattice M of D such that $p^{-d}\varphi^h(M) = M$ where $\mu = \frac{d}{h}$, $d, h \in \mathbb{Z}$ and $h \geq 1$.*

Remark 8.24. (a) A φ-module pure of slope 0 is nothing but an étale φ-module over K_0.
(b) Suppose $D = K_0 e_1 \oplus \cdots \oplus K_0 e_n$, $\varphi(e_i) = e_{i+1}$ for $1 \leq i \leq n-1$ and $\varphi(e_n) = pe_1$, then D is pure of slope $\frac{1}{n}$.

The following theorem of Dieudonné-Manin (see [Man63]) classifies all φ-modules.

Theorem 8.25 (Dieudonné-Manin). *For a φ-module D over K_0, then*

$$D = \bigoplus_{\mu \in \mathbb{Q}} D_\mu,$$

where D_μ is the part of D pure of slope μ and $D_\mu = 0$ for all but finitely many μ. Hence $\mu \dim_{K_0} D_\mu \in \mathbb{Z}$ and

$$t_N(D) = \sum_{\mu \in \mathbb{Q}} \mu \dim_{K_0} D_\mu. \tag{8.7}$$

Imitating the theory of étale φ-modules for k in Chapter 3 (especially Lemma 3.21, Theorem 3.22 and Proposition 3.33), one can get

Corollary 8.26. *Suppose k is algebraically closed.*

(1) *If D is pure of slope $\mu = \frac{d}{h}$ with $d, h \in \mathbb{Z}, h \geq 1$, then $D \cong K_0 \otimes_{\mathbb{Q}_{p^h}} D_{\varphi^h = p^d}$.*
(2) *A short exact sequence of φ-modules always splits.*

The rest of this subsection is devoted to the proof of Dieudonné-Manin's Theorem as given in Ding-Ouyang [DO12]. One can skip the details here.

Suppose D is a φ-module. For $h, d \in \mathbb{Z}$ and $h \geq 1$, we write $\varphi_{h,d} = p^{-d}\varphi^h$. Then $\varphi_{h,d}$ is bijective in D. Let M be a W-lattice of D, we set $M_{h,d} = \cap_{n \geq 0} \varphi_{h,d}^{-n}(M)$ and $D^\mu = M_{h,d}[\frac{1}{p}]$ where $\mu = d/h \in \mathbb{Q}$. Clearly by definition $M_{h,d}$ is a sub-W-module of M stable under $\varphi_{h,d}$.

Proposition 8.27. *Suppose D is a φ-module over K_0, $\mu = \frac{d}{h} \in \mathbb{Q}$. Then*

(1) *D^μ is independent of the choices of the lattice M and the pair (h, d).*
(2) *$x \in D^\mu$ if and only if the W-module $W[x, \varphi_{h,d}(x) \cdots, \varphi_{h,d}^n(x), \cdots]$ is a finite module, in particular D^μ is a φ-submodule of D.*
(3) *$\{D^\mu\}_{\mu \in \mathbb{Q}}$ forms a decreasing filtration of D which is separate and exhaustive, in other words,*
    (i) *if $\mu \leq \mu'$, then $D^\mu \supset D^{\mu'}$;*
    (ii) *$D^\mu = D$ for $\mu \ll 0$ and $D^\mu = 0$ for $\mu \gg 0$.*

Proof. (1) Suppose $M' = TM$ is another lattice of D where $T \in \mathrm{GL}(D)$. We choose $k \in \mathbb{N}$ such that $TM \supset p^k M$. For $x \in M_{h,d}[\frac{1}{p}]$, suppose $p^a x \in M_{h,d}$, then $\varphi_{h,d}^n(p^a x) \in M$ for all $n \in \mathbb{N}$ and $\varphi_{h,d}^n(p^{a+k}x) \in p^k M \subset M'$ for all $n \in \mathbb{N}$, thus $p^{a+k}x \in M'_{h,d}$ and $x \in M'_{h,d}[\frac{1}{p}]$. This proves the independence of M.

Now for $(h', d') = (kh, kd)$, we let $M' = \cap_{0 \leq j \leq k-1} \varphi_{h,d}^j(M)$. Then M' is a lattice in D and $M'_{kh,kd} = M_{h,d}$. Thus $M_{kh,kd}[\frac{1}{p}] = M'_{kh,kd}[\frac{1}{p}] = M_{h,d}[\frac{1}{p}]$. This proves the independence of the pair (h, d).

(2) Let $\mu = \frac{d}{h}$. Suppose M is a lattice in D. Then $x \in D^\mu$ means that there exists $k \in \mathbb{N}$, $p^k x \in M_{h,d}$, or equivalently $\varphi_{h,d}^n(p^k x) \in M$ for $n \in \mathbb{N}$, so $W_{\mathcal{O}_E}[x, \varphi_{h,d}(x) \cdots, \varphi_{h,d}^n(x), \cdots] \supset p^{-k}M$ is a finite W-module. Conversely, if the W-module $W[x, \varphi_{h,d}(x) \cdots, \varphi_{h,d}^n(x), \cdots]$ is a finite W-module, we extend it to a W-lattice M of D, then $x \in M_{h,d} \subset D^\mu$.

(3) If $d < d'$, then by definition $M_{h,d} \supset M_{h,d'}$, this proves (i). Suppose $p^{d_2}M \subset \varphi(M) \subset p^{d_1}M$, then for $d > d_2$, $M_{1,d} = 0$ and for $d < d_1$, $M_{1,d} = M$, this proves (ii).

Lemma 8.28. *Suppose $0 \to D_1 \to D \to D_2 \to 0$ is a short exact sequence of φ-modules, then*

(1) *the sequence $0 \to D_1^\mu \to D^\mu \to D_2^\mu$ is exact;*
(2) *if moreover $D_1 = D^{\mu_0}$ for some μ_0, then $0 \to D_1^\mu \to D^\mu \to D_2^\mu \to 0$ is exact.*

Proof. (1) follows easily from Proposition 8.27(2).

(2) The case $\mu > \mu_0$ follows from the case $\mu = \mu_0$. So we need only to prove the exactness in the case $\mu \leq \mu_0$. We first show the case $\mu = \mu_0$, which is equivalent to the claim $(D/D^{\mu_0})^{\mu_0}$=0. We assume $D = D^{\lambda}$, $\mu_0 = \frac{d_0}{h}$ and $\lambda = \frac{d}{h}$.

We claim there exists a W-lattice M in D such that M is stable under $\varphi_{h,d}$ and $M \cap D^{\mu_0}$ is stable under φ_{h,d_0}. To see this, we first find a W-lattice L in D which is stable under $\varphi_{h,d}$, then the image of L in D/D^{μ_0} is a W-lattice. Suppose it is generated by $\bar{e}_1, \bar{e}_2, \cdots \bar{e}_r$. For each i, take a preimage of $\bar{e}_i$ in L, denoted by e_i. Choose a W-lattice L_0 in D^{μ_0} which is stable under φ_{h,d_0}. Then there exists $N \in \mathbb{N}$, such that $L \cap D^{\mu_0} \subseteq p^{-N} L_0$. Take $e_{r+1}, e_{r+2}, \cdots e_n$ as a basis of $p^{-N} L_0$. (Note that $p^{-N} L_0$ is still stable under φ_{h,d_0}). Then the lattice M generated by $e_1, e_2, \cdots e_n$ is what we need. That's because $\varphi_{h,d}(e_i) \in L \subseteq M$ when $i \leq r$, and $\varphi_{h,d}(e_i) = p^{d_0 - d} \varphi_{h,d_0}(e_i) \in p^{-N} L_0 \subseteq M$ when $i \geq r+1$.

If $(D/D^{\mu_0})^{\mu_0} \neq 0$, then there exists $x \in D, x \notin D^{\mu_0}$, $\varphi_{h,d_0}^n(x) \in M + D^{\mu_0}$ for any n. For $n \geq 1$, let k_n be the smallest integer such that $\varphi_{h,d_0}^n(x) = x_n + p^{-k_n} y_n$ where $x_n \in M$, $y_n \in M \cap D^{\mu_0}$ (if $\varphi_{h,d_0}^n(x) \in M$, let $k_n = 0$). In fact, k_n is also the smallest integer such that $\varphi_{h,d_0}^n(x) \in p^{-k_n} M$.

We have $\varphi_{h,d_0}(x_n + p^{-k_n} y_n) = x_{n+1} + p^{-k_{n+1}} y_{n+1} = \varphi_{h,d_0}(x_n) + p^{-k_n} z_n$, where $z_n \in M \cap D^{\mu_0}$. Since $\varphi_{h,d_0}(M) \subseteq p^{-(d_0-d)} M$, it's easy to see $k_{n+1} \leq \max(k_n, d_0 - d)$. Take $N = \max(k_1, d_0 - d)$, then $k_n \leq N$ is bounded. This implies that $p^N x \in \cap_{n \geq 0} \varphi_{h,d_0}^{-n}(M)$. Hence $p^N x$ and $x \in D^{\mu_0}$, a contradiction. Thus we have shown $(D/D^{\mu_0})^{\mu_0}$=0.

Now for the case $\mu < \mu_0$, if $D^{\mu} = D$, then by (1), $D/D^{\mu_0} \supseteq (D/D^{\mu_0})^{\mu} \supseteq D^{\mu}/(D^{\mu_0})^{\mu} = D/D^{\mu_0}$, so all must be equal. In the general case, the exact sequence

$$0 \to D^{\mu}/D^{\mu_0} \to D/D^{\mu_0} \to D/D^{\mu} \to 0.$$

and the fact $(D/D^{\mu})^{\mu} = 0$ implies that $(D^{\mu}/D^{\mu_0})^{\mu} = (D/D^{\mu_0})^{\mu}$. Together with $(D^{\mu}/D^{\mu_0})^{\mu} = D^{\mu}/D^{\mu_0}$, we get $(D/D^{\mu_0})^{\mu} = D^{\mu}/D^{\mu_0}$.

For $\mu \in \mathbb{Q}$, we let $D^{>\mu}$ be the union of all $D^{\mu'}$ for $\mu' > \mu$ and $D^{<\mu}$ be the intersection of all $D^{\mu'}$ for $\mu' < \mu$.

Lemma 8.29. (1) *For any μ, there exists $\mu' < \mu$, $D^{\mu'} = D^{\mu}$. In particular, the filtration $\{D^{\mu}\}$ is left continuous, i.e., $D^{<\mu} = D^{\mu}$.*
(2) *For $\mu = \frac{d}{h}$ and $\dim_{K_0} D^{\mu}$=l, if $D^{\mu} = D^{>\mu}$, then $D^{\mu'} = D^{\mu}$ where $\mu' = \frac{ld+1}{lh}$.*

Proof. (1) By Lemma 8.28(2), we can replace D by D/D^{μ} and assume $D^{\mu} = 0$. Let $\mu = \frac{d}{h}$. Take a lattice M in D, then $\bigcap_{i=0}^{\infty} \varphi_{h,d}^{-i}(M) = 0$, and there exists k such that $\bigcap_{i=0}^{k} \varphi_{h,d}^{-i}(M) \subseteq p^2 M$. One can show easily that $\bigcap_{i=0}^{Nk} \varphi_{h,d}^{-i}(M) \subseteq p^{2N} M$ for $N \geq 1$ by induction.

Let L be the lattice $\bigcap_{i=0}^{k} \varphi_{h,d}^{-i}(M)$, Then $\varphi_{kh,kd}^{-j}(L) = \bigcap_{i=kj}^{k(j+1)} \varphi_{h,d}^{-i}(M)$ and

$$\bigcap_{i=0}^{j} \varphi_{kh,kd}^{-i}(L) = \bigcap_{i=0}^{k(j+1)} \varphi_{h,d}^{-i}(M) \subseteq p^{2(j+1)} M.$$

So we have

$$\bigcap_{i=0}^{j} \varphi_{kh,kd-1}^{-i}(L) = \bigcap_{i=0}^{j} p^{-i}\varphi_{kh,kd}^{-i}(L) \subseteq \bigcap_{i=0}^{j} p^{-j}\varphi_{kh,kd}^{-i}(L) \subseteq p^j M.$$

As a consequence $\bigcap_{i=0}^{\infty} \varphi_{kh,kd-1}^{-i}(L) = 0$, which implies that $D^{\mu'} = 0$ for $\mu' = \frac{kd-1}{kh}$.

(2) By Lemma 8.28(1), we can replace D by $D \cap D^{\mu}$ and assume $D = D^{\mu}$. The fact $D^{>\mu} = D$ implies that there exists $\alpha \in \mathbb{N}$, $D^{\frac{\alpha d+1}{\alpha h}} = D$. Therefore we have a lattice M which is stable under $\varphi_{\alpha h, \alpha d+1}$, and consequently stable under $\varphi_{\alpha h,\alpha d}$. It's easy to see $\varphi_{\alpha h,\alpha d}^n(M) = \varphi_{\alpha h,\alpha d+1}^n(p^n M) \to 0$ as $n \to \infty$. Therefore for any lattice L stable under $\varphi_{h,d}$, $\varphi_{h,d}^n(L) \to 0$ as $n \to \infty$; in particular, $\varphi_{h,d}^n(L) \subset pL$ when n is sufficiently large.

If L is stable under $\varphi_{h,d}$, then $\varphi_{h,d}^i(L) \supset \varphi_{h,d}^{i+1}(L)$, and there exists a chain of sub-k-vector spaces of L/pL

$$\frac{L}{pL} \supset \dots \frac{\varphi_{h,d}^{i-1}(L)}{\varphi_{h,d}^{i}(L) \cap pL} \supset \frac{\varphi_{h,d}^{i}(L)}{\varphi_{h,d}^{i}(L) \cap pL} \supset \frac{\varphi_{h,d}^{i+1}(L)}{\varphi_{h,d}^{i+1}(L) \cap pL} \supset \cdots.$$

It's easy to check that if $\dim_k \frac{\varphi_{h,d}^{i}(L)}{\varphi_{h,d}^{i}(L)\cap pL} = \dim_k \frac{\varphi_{h,d}^{i+1}(L)}{\varphi_{h,d}^{i+1}(L)\cap pL}$, then $\dim_k \frac{\varphi_{h,d}^{j}(L)}{\varphi_{h,d}^{j}(L)\cap pL} = \dim_k \frac{\varphi_{h,d}^{i}(L)}{\varphi_{h,d}^{i}(L)\cap pL}$ for any $j > i$. Since $\dim_k \frac{\varphi_{h,d}^{j}(L)}{\varphi_{h,d}^{j}(L)\cap pL} = 0$ when j is sufficiently large, the fact $\dim_k \frac{L}{pL} = l$ implies that $\varphi_{h,d}^{l}(L) \subseteq pL$. This means that L is stable under $\varphi_{lh,ld+1}$ and hence $D^{\frac{ld+1}{lh}} = D$.

Corollary 8.30. *Let $a = \sup\{\lambda \in \mathbb{Q} : D^{\lambda} = D\}$, then a is a rational number and $D^a = D$.*

Proof. Suppose $\dim_{K_0} D = l$. If a is not rational, by Dirichlet's Approximation Theorem, there exist infinitely many pairs of integers (p, q) such that $\frac{p}{q} < a < \frac{p}{q} + \frac{1}{q^2}$. Choose $q > l$ and let $(p, q) = (d, h)$. By the above Lemma, $D^{\frac{d}{h}+\frac{1}{lh}} = D^{\frac{d}{h}} = D$ and hence $\frac{d}{h} + \frac{1}{lh} < a$, a contradiction.

The second part of the corollary follows from Lemma 8.29(1).

Proposition 8.31. *Set $\mathrm{gr}_{\mu} D = D^{\mu}/D^{>\mu}$, then $\mathrm{gr}_{\mu} D$ is pure of slope μ.*

Proof. By Lemma 8.28, we can replace D by $D^{\mu}/D^{>\mu}$, and assume $D^{\mu} = D$ and $D^{>\mu} = 0$.

Let $\mu = \frac{d}{h}$, then there exists a W-lattice M of $D^{\mu} = D$ which is stable under $\varphi_{h,d}$. The filtration of sub-k-vector spaces

$$\dots \subseteq \frac{\varphi_{h,d}^{n}(M)}{\varphi_{h,d}^{n}(M) \cap pM} \subseteq \frac{\varphi_{h,d}^{n}(M)}{\varphi_{h,d}^{n}(M) \cap pM} \subseteq \dots \subseteq \frac{M}{pM}$$

of M/pM is stable since $\dim_k M/pM = \dim_{K_0} D$ is finite.

If $\frac{\varphi_{h,d}^N(M)}{\varphi_{h,d}^N(M)\cap pM} = 0$ when N is sufficiently large, then $\varphi_{Nh,Nd}^n(M) \subseteq p^n M$ for all $n \in \mathbb{N}$, which implies that $M \subseteq \cap_{n\geq 0}\varphi_{Nh,Nd+1}^{-n}(M)$. This is not possible since $D^{>\mu} = 0$. As a consequence, when N is sufficiently large, we have a bijection of the nonzero k-vector space $\frac{\varphi_{h,d}^N(M)}{\varphi_{h,d}^N(M)\cap pM}$ to itself

$$\varphi_{h,d}^n : \frac{\varphi_{h,d}^N(M)}{\varphi_{h,d}^N(M)\cap pM} \to \frac{\varphi_{h,d}^N(M)}{\varphi_{h,d}^N(M)\cap pM}$$

for $n \in \mathbb{N}$. Replace (h,d) by (Nh, Nd) and still denote it by (h,d), then we get a bijection

$$\varphi_{h,d}^n : \frac{\varphi_{h,d}(M)}{\varphi_{h,d}(M)\cap pM} \to \frac{\varphi_{h,d}(M)}{\varphi_{h,d}(M)\cap pM}$$

for any $n \in \mathbb{N}$.

If $\varphi_{h,d} : M \to M$ is not bijective, then there exists x_1 satisfying $\varphi_{h,d}(x_1) \in pM$ and $x_1 \notin pM$. Indeed, if $\varphi_{h,d} : M \to M$ is not surjective, we can find an element $x \in M$ and $x \notin \varphi_{h,d}(M)$. Since $\varphi_{h,d}(M)$ is still a W-lattice in D, we can find $k \in \mathbb{N}$ such that $p^k x \in \varphi_{h,d}(M)$, and $p^{k-1}x \notin \varphi_{h,d}(M)$. Then take $x_1 \in M$ to be the preimage of $p^k x$.

We now construct by induction a sequence (x_n) such that $x_n - x_{n-1} \in p^{n-1}M$ and $\varphi_{h,d}^i(x_n) \in p^i M$ for any $1 \leq i \leq n$. Suppose $x_1, x_2 \cdots x_n$ have been constructed and $\varphi_{h,d}^n(x_n) = p^n z_n$. Let $x_{n+1} = x_n + p^n y$. It's easy to see $\varphi_{h,d}^i(x_{n+1}) \in p^i M$ for $1 \leq i \leq n$ if $y \in M$. Since $\varphi_{h,d}^{n+1}(x_{n+1}) = p^n(\varphi_{h,d}(z_n) + \varphi_{h,d}^{n+1}(y))$, to have $\varphi_{h,d}^{n+1}(x_{n+1}) \in p^{n+1}M$, it's sufficient to find $y \in M$ such that $\varphi_{h,d}(z_n) + \varphi_{h,d}^{n+1}(y) \in pM$, but this is guaranteed by the bijection

$$\varphi_{h,d}^n : \frac{\varphi_{h,d}(M)}{\varphi_{h,d}(M)\cap pM} \to \frac{\varphi_{h,d}(M)}{\varphi_{h,d}(M)\cap pM}.$$

Take $x = \lim_{n\to\infty} x_n$, then $x \in M$, $x \neq 0$. It's easy to see $\varphi_{h,d}^n(x) \in p^n M$ for any $n \geq 0$, so $x \in \cap_{n\geq 0}\varphi_{h,d+1}^{-n}(M)$ which contradicts to $D^{>\mu} = 0$.

Since D is of finite dimension, $\mathrm{gr}_\mu D = 0$ for all but finitely many μ. Suppose $\mu_1 > \mu_2 > \cdots > \mu_r$ are all the μ's such that $\mathrm{gr}_\mu D \neq 0$. In fact we can take $\mu_1 = \sup\{\lambda \in \mathbb{Q} : D^\lambda \neq 0\}$ and $\mu_i = \sup\{\lambda \in \mathbb{Q} : D^\lambda \supsetneq D^{\mu_{i-1}}\}$ when $i > 1$. By Lemma 2.3 (1), $D^{\mu_i} \supsetneq D^{\mu_{i-1}}$, and if $\mu_i > \mu > \mu_{i+1}$, then $D^\mu = D^{\mu_i}$. We have

Proposition 8.32. *Suppose D is a φ-module. Then the filtration*

$$0 \subsetneq D^{\mu_1} = \mathrm{gr}_{\mu_1} D \subsetneq D^{\mu_2} \subsetneq \cdots \subsetneq D^{\mu_r} = D$$

is the Harder-Narasimhan filtration *of D, i.e., the unique filtration $\cdots \subsetneq D_i \subsetneq D_{i+1} \subsetneq \cdots$ of φ-modules such that the D_i/D_{i-1}'s are pure of strictly decreasing slopes.*

Proof. The existence follows from Proposition 8.31. For the uniqueness, by Lemma 8.28, for a Harder-Narasimhan filtration $0 = D_0 \subsetneq D_1 \subsetneq \cdots \subsetneq D_s = D$ of D, then $D^\mu = 0$ for $\mu > \mu(D_1)$ and $D^{\mu(D_1)} = D_1 \neq 0$. We also have $D^\mu = 0$ for $\mu > \mu_1$ and $D^{\mu_1} \neq 0$. Thus $\mu(D_1) = \mu_1$ and $D_1 = D^{\mu_1}$. Now the rest follows from induction on the length of the filtration.

Proposition 8.33. *Suppose $0 \to D_1 \to D \to D_2 \to 0$ is a short exact sequence of φ-modules, then for every $\mu \in \mathbb{Q}$, $0 \to D_1^\mu \to D^\mu \to D_2^\mu \to 0$ is also exact.*

Proof. We prove by induction on the dimension of D. The case $\dim D = 1$ is trivial. In general, suppose $\dim D \geq 2$ and D_1 is a non-zero proper sub-object of D. We assume D' is the second to last term of the Harder-Narasimhan filtration of D, and $D'' = D/D'$, then for the exact sequence $0 \to D' \to D \to D'' \to 0$ and $\mu \in \mathbb{Q}$, the complex $0 \to D'^\mu \to D^\mu \to D''^\mu \to 0$ is always exact. We have the following commutative diagram with exact rows and columns:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & D_1' \arrow[r] \arrow[d] & D' \arrow[r] \arrow[d] & D_2' \arrow[r] \arrow[d, "i_1"] & 0 \\
0 \arrow[r] & D_1 \arrow[r] \arrow[d] & D \arrow[r] \arrow[d] & D_2 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & D_1'' \arrow[r, "i_2"] \arrow[d] & D'' \arrow[r] \arrow[d] & D_2'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

where $D_1' = D_1 \cap D'$ and $D_2' = D'/D_1'$ and $D_1'' = D_1/D_1'$, the injections i_1 and i_2 are defined by diagram chasing, and $D_2'' = D''/D_1'' \cong D_2/D_2'$ is obtained by snake lemma. Now take the μ-invariant of the above diagram, by induction, we have exact sequences in all rows and columns except the middle row, then the middle row must also be exact by diagram chasing.

Proof (Proof of Theorem 8.25). We are now ready to prove the theorem of Dieudonné-Manin. Suppose D is a φ-module over k, such that

$$0 = D_0 \subsetneq D_1 \subsetneq \cdots \subsetneq D_{r-1} \subsetneq D_r = D$$

is the Harder-Narasimhan filtration of D, suppose $\mu_i = \mu(D_i/D_{i-1})$. Since φ is bijective on D, replace φ and σ by φ^{-1} and σ^{-1}, then D can be regarded as a φ^{-1}-module and we can develop the Harder-Narasimhan filtration for D as a φ^{-1}-modules, i.e., D possesses a unique filtration

$$0 = D'_0 \subsetneq D'_1 \subsetneq \cdots \subsetneq D'_{s-1} \subsetneq D'_s = D$$

such that D'_i/D'_{i-1} are pure of slope $\mu'_i = \mu'(\varphi^{-1}, D'_i/D'_{i-1})$ as φ^{-1}-modules and μ'_i's are strictly decreasing. By definition we see that a φ^{-1}-module pure of slope μ is nothing but a φ-module pure of slope $-\mu$, thus $0 = D'_0 \subsetneq D'_1 \subsetneq \cdots \subsetneq D'_{s-1} \subsetneq D'_s = D$ is the unique filtration of D such that the sequences $\mu(D'_i/D'_{i-1}) = -\mu'_i$ are strictly increasing.

It suffices to show that $D = \oplus(D_i/D_{i-1})$. We show it by induction on the length s of the (φ^{-1})- Harder-Narasimhan filtration of D. The case $s = 1$ is trivial. In general, we have $D^{\mu} = 0$ for $\mu > \mu_1$ and $D^{\mu_1} = D_1 \neq 0$. By Proposition 8.33 and induction hypothesis, we also have $D^{\mu} = 0$ for $\mu > -\mu'_s$ and $D^{-\mu'_s} \cong D/D'_{s-1} \neq 0$, thus $\mu_1 = -\mu'_s$ and $D_1 \cong D/D'_{s-1}$ is a direct summand of D. By induction, this finishes the proof of the theorem.

8.2.3 Filtered (φ, N)-modules over K.

We have defined $\mathbf{Fil}_K$, the category of filtered K-vector spaces in § 6.2.4, and $\mathbf{Mod}_{K_0}(\varphi, N)$, the category of (φ, N)-modules over K_0 in § 8.2.1.

Definition 8.34. *The category of* filtered (φ, N)-modules *over K, denoted by $\mathbf{MF}_K(\varphi, N)$, is the following category:*

(1) *An object of $\mathbf{MF}_K(\varphi, N)$ is a pair $D = (D, D_K)$, where*
  (i) *D is a (φ, N)-module over K_0, i.e.,*
  D is a finite dimensional K_0-vector space equipped with two maps φ and N, such that φ is bijective and semi-linear, N is linear and $N\varphi = p\varphi N$;
  (ii) *$D_K = K_0 \otimes_{K_0} D \in \mathbf{Fil}_K$, i.e.,*
  D_K is equipped with a decreasing filtration of K-vector spaces $\cdots \subset \mathrm{Fil}^i D_K \subset \mathrm{Fil}^{i+1} D_K \subset \cdots$ such that $\bigcap_{i\in\mathbb{Z}} \mathrm{Fil}^i D_K = 0$ (aka. separated) and $\bigcup_{i\in\mathbb{Z}} \mathrm{Fil}^i D_K = D_K$ (aka. exhaustive).

(2) *A morphism $\eta : D_1 \to D_2$ between two filtered (φ, N)-modules is a morphism of (φ, N)-modules such that the induced K-linear map $\eta_K : K \otimes_{K_0} D_1 \to K \otimes_{K_0} D_2$ is a morphism of $\mathbf{Fil}_K$, i.e.,*

$$\eta_K(\mathrm{Fil}^i D_{1K}) \subset \mathrm{Fil}^i D_{2K}, \ \textit{for all } i \in \mathbb{Z}.$$

Similar to the category $\mathbf{Fil}_K$, the category $\mathbf{MF}_K(\varphi, N)$ is also an additive category with kernels and cokernels. Let $\eta : D_1 \to D_2$ be a morphism of $\mathbf{MF}_K(\varphi, N)$, then $(\mathrm{Ker}\,\eta)_K$ and $(\mathrm{Coker}\,\eta)_K$ are the kernel and cokernel of η_K as filtered K-vector spaces.

Exercise 8.35. Suppose $\eta : D_1 \to D_2$ is a morphism of (φ, N)-modules over K. Then the induced morphism from $\mathrm{coIm}\,\eta$ to $\mathrm{Im}\,\eta$ is an isomorphism if and only if η_K is a strict morphism. In this case we call η a *strict morphism of (φ, N)-modules.*

Again similar to $\mathbf{Fil}_K$ and $\mathbf{Mod}_{K_0}(\varphi, N)$, there exist tensor products, unit and dual objects in $\mathbf{MF}_K(\varphi, N)$:

(i) For two filtered (φ, N)-modules D_1 and D_2, the tensor product

$$D_1 \otimes D_2 = D_1 \otimes_{K_0} D_2$$

as (φ, N)-module over K_0, with the filtration on

$$(D_1 \otimes D_2)_K = K \otimes_{K_0} (D_1 \otimes_{K_0} D_2) = (K \otimes_{K_0} D_1) \otimes (K \otimes_{K_0} D_2) = D_{1K} \otimes_K D_{2K}$$

defined by

$$\mathrm{Fil}^i (D_{1K} \otimes_K D_{2K}) = \sum_{i_1 + i_2 = i} \mathrm{Fil}^{i_1} D_{1K} \otimes_K \mathrm{Fil}^{i_2} D_{2K}.$$

(ii) K_0 can be viewed as a filtered (φ, N)-module with $\varphi = \sigma$ and $N = 0$, and

$$\mathrm{Fil}^i K = \begin{cases} K, & i \leqslant 0; \\ 0, & i > 0. \end{cases}$$

Then for any filtered (φ, N)-module D, $K_0 \otimes D \simeq D \otimes K_0 \simeq D$. Thus K_0 is the *unit element* in the category.

(iii) The *dual object* D^* of D is the dual of D as (φ, N)-module with the filtration given by

$$\begin{aligned} (D^*)_K &= K \otimes_{K_0} D^* = (D_K)^* \simeq \mathscr{L}(D_K, K), \\ \mathrm{Fil}^i (D^*)_K &= (\mathrm{Fil}^{-i+1} D_K)^*. \end{aligned}$$

8.2.4 $t_H(D)$.

Definition 8.36. *Suppose $\Delta \in \mathbf{Fil}_K$ is a finite dimensional filtered K-vector space.*

(1) *If $\dim_K \Delta = 1$, define*

$$t_H(\Delta) := \max\{i \in \mathbb{Z} : \mathrm{Fil}^i \Delta = \Delta\}. \tag{8.8}$$

Thus it is the integer i such that $\mathrm{Fil}^i \Delta = \Delta$ and $\mathrm{Fil}^{i+1} \Delta = 0$.

(2) *If $\dim_K \Delta = h$, define*

$$t_H(\Delta) := t_H(\bigwedge\nolimits_K^h \Delta), \tag{8.9}$$

where $\bigwedge_K^h \Delta$ is the h-th exterior algebra of Δ with the induced filtration.

Suppose

$$\mathrm{gr}\, \varDelta = \bigoplus_{t=1}^{s} \mathrm{gr}^{i_t}\, \varDelta,\ i_1 < \cdots < i_s.$$

Take any basis of $\mathrm{Fil}^{i_s}\, \varDelta$, expanding successively to a basis of $\mathrm{Fil}^{i_{s-1}}\, \varDelta$, $\cdots$, $\varDelta = \mathrm{Fil}^{i_1}\, \varDelta$. Then we get a basis $\{e_1, \cdots, e_h\}$ of $\varDelta$ over K which is compatible to the filtration, i.e., if we define $\delta_j \in \mathbb{Z}$ by the condition $e_j \in \mathrm{Fil}^{\delta_j}\, \varDelta - \mathrm{Fil}^{\delta_j+1}\, \varDelta$ for $1 \leq j \leq h$, then

$$\mathrm{Fil}^i(\varDelta) = \bigoplus_{\delta_j \geqslant i} K e_j.$$

This means

$$t_H(\varDelta) = \sum_{j=1}^{h} \delta_j = \sum_{t=1}^{s} i_t \dim \mathrm{gr}^{i_t}\, \varDelta.$$

Consequently

Proposition 8.37.

$$t_H(\varDelta) = \sum_{i \in \mathbb{Z}} i \cdot \dim_K \mathrm{gr}^i\, \varDelta. \tag{8.10}$$

Proposition 8.38. (1) *If* $0 \to \varDelta' \to \varDelta \to \varDelta'' \to 0$ *is a short exact sequence of filtered* K*-vector spaces, then*

$$t_H(\varDelta) = t_H(\varDelta') + t_H(\varDelta'').$$

(2) $t_H(\varDelta_1 \otimes \varDelta_2) = \dim_K(\varDelta_2) t_H(\varDelta_1) + \dim_K(\varDelta_1) t_H(\varDelta_2)$.
(3) $t_H(\varDelta^*) = -t_H(\varDelta)$.

Proof. (1) If $0 \to \varDelta' \to \varDelta \to \varDelta'' \to 0$ is exact, then $0 \to \mathrm{gr}^i\, \varDelta' \to \mathrm{gr}^i\, \varDelta \to \mathrm{gr}^i\, \varDelta'' \to 0$ is exact for all $i \in \mathbb{Z}$, thus (1) follows from Proposition 8.37.

(2) Let $\{e_1, \cdots, e_r\}$ and $\{f_1, \cdots, f_{r'}\}$ be bases of $\varDelta_1$ and $\varDelta_2$ respectively, compatible with the filtration. Then $\{e_i \otimes f_j \mid 1 \leq i \leq r,\ 1 \leq j \leq r'\}$ is a basis of $\varDelta_1 \otimes \varDelta_2$, compatible with the filtration. Then (2) follows from an easy computation.

(3) follows from definition.

8.2.5 Admissible filtered (φ, N)-modules.

Let D be a filtered (φ, N)-module D over K, we set

$$t_H(D) := t_H(D_K). \tag{8.11}$$

Then D is associated with two invariants: $t_N(D)$ which depends only on the Frobenius map φ on D and $t_H(D)$ which depends only on the filtration on D_K.

Definition 8.39. *A filtered (φ, N)-module D over K is called* admissible *if*

(i) $t_H(D) = t_N(D)$,
(ii) *For any sub-object D' of D, i.e. a sub K_0-vector space D' stable under (φ, N)-action and with induced filtration, $t_H(D') \leq t_N(D')$.*

Denote by $\mathbf{MF}_K^{ad}(\varphi, N)$ the full sub-category of $\mathbf{MF}_K(\varphi, N)$ consisting of admissible filtered (φ, N)-modules.

Remark 8.40. The additivity of t_N and t_H

$$t_N(D) = t_N(D') + t_N(D''), \quad t_H(D) = t_H(D') + t_H(D'')$$

implies that the admissibility is equivalent to that

(i) $t_H(D) = t_N(D)$,
(ii) $t_H(D'') \geq t_N(D'')$, for any quotient object D'' of D in $\mathbf{MF}_K(\varphi, N)$.

Proposition 8.41. *The category $\mathbf{MF}_K^{ad}(\varphi, N)$ is an abelian category. More precisely, if D_1 and D_2 are two objects of $\mathbf{MF}_K^{ad}(\varphi, N)$ and $\eta : D_1 \to D_2$ is a morphism, then*

(1) *The kernel* $\mathrm{Ker}\,\eta = \{x \in D_1 \mid \eta(x) = 0\}$*, with the obvious (φ, N)-module structure over K_0 and with the filtration given by* $\mathrm{Fil}^i\,\mathrm{Ker}\,\eta_K = \mathrm{Ker}\,\eta_K \bigcap \mathrm{Fil}^i\,D_{1K}$ *for $\eta_K : D_{1K} \to D_{2K}$ and* $\mathrm{Ker}\,\eta_K = K \otimes_{K_0} \mathrm{Ker}\,\eta$*, is an admissible filtered (φ, N)-module.*
(2) *The cokernel* $\mathrm{Coker}\,\eta = D_2/\eta(D_1)$*, with the induced (φ, N)-module structure over K_0 and with the filtration given by* $\mathrm{Fil}^i\,\mathrm{Coker}\,\eta_K = \mathrm{Im}(\mathrm{Fil}^i\,D_{2K})$ *for* $\mathrm{Coker}\,\eta_K = K \otimes_{K_0} \mathrm{Coker}\,\eta$*, is an admissible filtered (φ, N)-module.*
(3) $\mathrm{Im}(\eta) \xrightarrow{\sim} \mathrm{CoIm}(\eta)$.

Proof. We first prove (3) assuming $\mathrm{Im}(\eta)$ and $\mathrm{CoIm}(\eta)$ are admissible. Since $\mathrm{Im}(\eta)$ and $\mathrm{CoIm}(\eta)$ are isomorphic in the abelian category of (φ, N)-modules, and since η_K is strictly compatible with the filtrations, $\mathrm{Im}(\eta) \xrightarrow{\sim} \mathrm{CoIm}(\eta)$ in $\mathbf{MF}_K^{ad}(\varphi, N)$.

To show (1), it suffices to show that $t_H(\mathrm{Ker}\,\eta) = t_D(\mathrm{Ker}\,\eta)$. We have $t_H(\mathrm{Ker}\,\eta) \leq t_D(\mathrm{Ker}\,\eta)$ as $\mathrm{Ker}\,\eta$ is a sub-object of D_1, we also have $t_H(\mathrm{Im}\,\eta) \leq t_D(\mathrm{Im}\,\eta)$ as $\mathrm{Im}\,\eta \cong \mathrm{CoIm}\,\eta$ is a sub-object of D_2, by the exact sequence of filtered (φ, N)-modules

$$0 \longrightarrow \mathrm{Ker}\,\eta \longrightarrow D_1 \longrightarrow \mathrm{Im}\,\eta \longrightarrow 0,$$

we have

$$t_H(D_1) = t_H(\mathrm{Ker}\,\eta) + t_H(\mathrm{Im}\,\eta) \leq t_D(\mathrm{Ker}\,\eta) + t_D(\mathrm{Im}\,\eta) = t_D(D_1).$$

As $t_H(D_1) = t_D(D_1)$, we must have

$$t_H(\mathrm{Ker}\,\eta) = t_D(\mathrm{Ker}\,\eta), \quad t_H(\mathrm{Im}\,\eta) = t_D(\mathrm{Im}\,\eta)$$

and $\mathrm{Ker}\,\eta$ is admissible.

The proof of (2) is similar to (1) and we omit it here.

Remark 8.42. (a) If D is an object of the category $\mathbf{MF}_K^{ad}(\varphi, N)$, then a sub-object D' in $\mathbf{MF}_K^{ad}(\varphi, N)$ is a sub-object in $\mathbf{MF}_K(\varphi, N)$ satisfying $t_H(D') = t_N(D')$, which is isomorphic to $\mathrm{Ker}\,(\eta : D \to D_2)$ for another admissible filtered (φ, N)-module D_2.

(b) The category $\mathbf{MF}_K^{ad}(\varphi, N)$ is *Artinian*: an object of this category is simple if and only if it is not 0 and if D' is a sub K_0-vector space of D stable under (φ, N) and such that $D' \neq 0, D' \neq D$, then $t_H(D') < t_N(D')$.

We give an alternative description of the admissibility condition. Let D be a filtered (φ, N)-module over K. We associate two convex polygons: the *Newton polygon* $P_N(D)$ and the *Hodge polygon* $P_H(D)$ whose origins are both $(0,0)$ in the usual Cartesian plane.

Definition 8.43. *For a φ-module D over K_0, suppose $D = \bigoplus_{j=1}^{m} D_{\alpha_j}$, where $0 \neq D_{\alpha_j}$ is the part of D of slope $\alpha_j \in \mathbb{Q}$ and $\alpha_1 < \alpha_2 < \cdots \alpha_m$. The* Newton polygon *$P_N(D)$ of D is the convex polygon with break points $(0,0)$ and $(v_1 + \cdots + v_j, \alpha_1 v_1 + \cdots + \alpha_j v_j)$ for $1 \leq j \leq m$ where $v_j = \dim_{K_0} D_{\alpha_j}$. Thus the end point of $P_N(D)$ is just $(\dim D, t_N(D))$.*

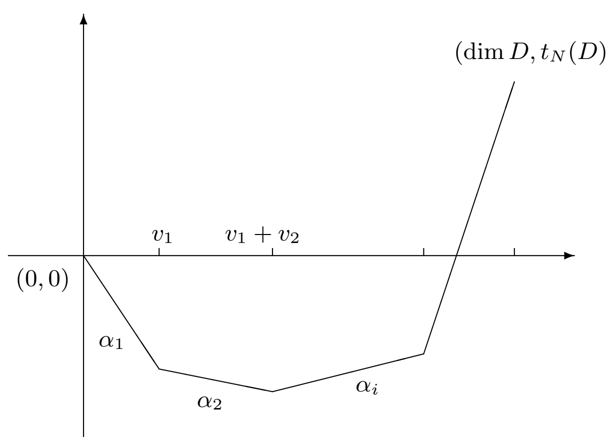


Fig. 8.1. The Newton Polygon $P_N(D)$

As $\alpha \dim_{K_0} D_\alpha \in \mathbb{Z}$, the break points of $P_N(D)$ have integer coordinates.

Definition 8.44. *For $\varDelta \in \mathrm{Fil}_K$, suppose $\mathrm{gr}\,\varDelta = \bigoplus_{j=1}^{m} \mathrm{gr}^{i_j}\,\varDelta$ with $i_1 < \cdots < i_m$ and $\mathrm{gr}^{i_j}\,\varDelta$ a nonzero K-vector space of dimension h_j. The* Hodge polygon *$P_H(\varDelta)$ of $\varDelta$ is the convex polygon with break points $(0,0)$ and $(h_1 + \cdots + h_j, i_1 h_1 + \cdots + i_j h_j)$ for $1 \leq j \leq m$. Thus the end point of $P_H(\varDelta)$ is just $(\dim \varDelta, t_H(\varDelta))$.*

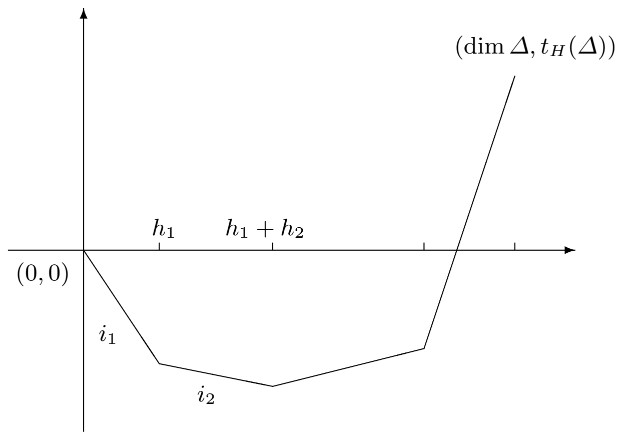


Fig. 8.2. The Hodge Polygon $P_H(\Delta)$

Clearly the brak points of $P_H(\Delta)$ have integer coordinates.

For a filtered (φ, N)-module D, we let $P_N(D)$ be the Newton polygon of D regarded as φ-module, and let $P_H(D) = P_H(D_K)$. The definition of admissibility can be rephrased in terms of the Newton and Hodge polygons:

Proposition 8.45. *Let D be a filtered (φ, N)-module over K such that $\dim_{K_0} D$ is finite and φ is bijective on D. Then D is admissible if and only if the following two conditions are satisfied:*

(1) *For any sub-object D' in $\mathbf{MF}_K(\varphi, N)$, $t_H(D') \leq t_N(D')$.*
(2) *$P_H(D)$ and $P_N(D)$ end up at the same point.*

8.3 Statement of Theorem A and Theorem B

8.3.1 de Rham implies potentially semi-stable.

Let B be a $\mathbb{Q}_p$-algebra on which G_K acts. Let K' be a finite extension of K contained in $\overline{K}$. Assume the condition

(H) $\qquad B$ is $(\mathbb{Q}_p, G_{K'})$-regular for any K'

holds.

Definition 8.46. *Let V be a p-adic representation of G_K. V is called* potentially B-admissible *if there exists a finite extension K' of K contained in $\overline{K}$ such that V is B-admissible as a representation of $G_{K'}$, i.e.*

$$B \otimes_{B^{G_{K'}}} (B \otimes_{\mathbb{Q}_p} V)^{G_{K'}} \longrightarrow B \otimes_{\mathbb{Q}_p} V$$

is an isomorphism, or equivalently,

$$\dim_{B^{G_{K'}}} (B \otimes_{\mathbb{Q}_p} V)^{G_{K'}} = \dim_{\mathbb{Q}_p} V.$$

It is easy to check that if $K \subset K' \subset K''$ is a tower of finite extensions of K contained in $\overline{K}$, then the map

$$B^{G_{K''}} \otimes_{B^{G_{K'}}} (B \otimes_{\mathbb{Q}_p} V)^{G_{K''}} \longrightarrow (B \otimes_{\mathbb{Q}_p} V)^{G_{K'}}$$

is always injective. Therefore, if V is admissible as a representation of $G_{K'}$, then it is also admissible as a representation of $G_{K''}$.

Remark 8.47. The condition (H) is satisfied by $B = \overline{K}$, C, B_{HT}, B_{dR}, B_{st}. The reason is that $\overline{K}$ is also an algebraic closure of any finite extension K' of K contained in $\overline{K}$, and consequently the associated $\overline{K}$, C, B_{HT}, B_{dR}, B_{st} for K' are the same one for K.

For $B = \overline{K}$, C, B_{HT} and B_{dR}, then B is a $\overline{K}$-algebra. Moreover, $B^{G_{K'}} = K'$. In this case, assume V is a p-adic representation of G_K which is potentially B-admissible. Then there exists K', a finite Galois extension of K contained in $\overline{K}$, such that V is B-admissible as a $G_{K'}$-representation.

Let $J = \mathrm{Gal}(K'/K)$, $h = \dim_{\mathbb{Q}_p}(V)$, then

$$\Delta = (B \otimes_{\mathbb{Q}_p} V)^{G_{K'}}$$

is a K'-vector space, and $\dim_{K'} \Delta = h$. Moreover, J acts semi-linearly on Δ, and

$$(B \otimes_{\mathbb{Q}_p} V)^{G_K} = \Delta^J.$$

By Hilbert Theorem 90, Δ is a trivial representation, thus $K' \otimes_K \Delta^J \to \Delta$ is an isomorphism, i.e.

$$\dim_K \Delta^J = \dim_{K'} \Delta = \dim_{\mathbb{Q}_p} V,$$

and hence V is B-admissible. We have the following proposition:

Proposition 8.48. *Let $B = \overline{K}$, C, B_{HT} or B_{dR}. Then potentially B-admissible is equivalent to B-admissible.*

However, the analogy is not true for $B = B_{\mathrm{st}}$.

Definition 8.49. (i) *A p-adic representation of G_K is called* K'-semi-stable *if it is semi-stable as a $G_{K'}$-representation.*
(ii) *A p-adic representation of G_K is called* potentially semi-stable *if it is K'-semi-stable for a suitable K', or equivalently, it is potentially B_{st}-admissible.*

Let V be a potentially semi-stable p-adic representation of G_K, then V is de Rham as a representation of $G_{K'}$ for some finite extension K' of K. Therefore V is de Rham as a representation of G_K by Proposition 8.48.

The converse is also true.

Theorem A. *A de Rham representation of G_K is always potentially semi-stable.*

Remark 8.50. Theorem A was known as the *p-adic Monodromy Conjecture.* The first proof was given by Berger ([Ber02]) in 2002. He used the theory of (φ, Γ)-modules to reduce the proof to a conjecture by Crew in p-adic differential equations. Crew Conjecture has three different proofs given by André ([And02a]), Mebkhout([Meb02]), and Kedlaya([Ked04]) respectively.

Remark 8.51. Assume V is a de Rham representation of G_K of dimension h, and let $\Delta = \mathbf{D}_{\mathrm{dR}}(V)$. Then there exists a natural isomorphism

$$B_{\mathrm{dR}} \otimes_K \Delta \cong B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V.$$

Let $\{v_1, \cdots, v_h\}$ be a basis of V over $\mathbb{Q}_p$, and $\{\delta_1, \cdots, \delta_h\}$ a basis of Δ over K. We identify v_i with $1 \otimes v_i$, and δ_i with $1 \otimes \delta_i$, for $i = 1, \cdots, h$. Then $\{v_1, \cdots, v_h\}$ and $\{\delta_1, \cdots, \delta_h\}$ are both bases of $B_{\mathrm{dR}} \otimes_K \Delta \cong B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$ over B_{dR}. Thus

$$\delta_j = \sum_{i=1}^{h} b_{ij} v_i \text{ with } (b_{ij}) \in \mathrm{GL}_h(B_{\mathrm{dR}}).$$

Since the natural map $K' \otimes_{K_0'} B_{\mathrm{st}} \to B_{\mathrm{dR}}$ is injective, Theorem A is equivalent to the claim that there exists a finite extension K' of K contained in $\overline{K}$ such that $(b_{ij}) \in \mathrm{GL}_h(K' \otimes_{K_0'} B_{\mathrm{st}})$.

8.3.2 Weakly admissible implies admissible.

Let V be any p-adic representation of G_K and consider $\mathbf{D}_{\mathrm{st}}(V) = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K}$. We know that $\mathbf{D}_{\mathrm{st}}(V)$ is a filtered (φ, N)-module over K such that $\dim_{K_0} \mathbf{D}_{\mathrm{st}}(V) < \infty$ and φ is bijective on $\mathbf{D}_{\mathrm{st}}(V)$, and

$$\mathbf{D}_{\mathrm{st}} : \mathbf{Rep}_{\mathbb{Q}_p}(G_K) \longrightarrow \mathbf{MF}_K(\varphi, N)$$

is a covariant additive $\mathbb{Q}_p$-linear functor.

On the other hand, let D be a filtered (φ, N)-module over K. We can give $B_{\mathrm{st}} \otimes D$ the filtered (φ, N)-module structure, where the tensor product is in the category of filtered (φ, N)-modules:

$$\begin{aligned} &B_{\mathrm{st}} \otimes D = B_{\mathrm{st}} \otimes_{K_0} D, \\ &\varphi(b \otimes d) = \varphi b \otimes \varphi d, \\ &N(b \otimes d) = Nb \otimes d + b \otimes Nd, \end{aligned}$$

and $K \otimes_{K_0} (B_{\mathrm{st}} \otimes D)$ is equipped with the induced filtration from $B_{\mathrm{dR}} \otimes_K D_K$ by the inclusion

$$K \otimes_{K_0} (B_{\mathrm{st}} \otimes D) = (K \otimes_{K_0} B_{\mathrm{st}}) \otimes_K D_K \subset B_{\mathrm{dR}} \otimes_K D_K.$$

We identify $B_{\mathrm{st}} \otimes D$ with its image in $K \otimes_{K_0} (B_{\mathrm{st}} \otimes D)$ by $x \mapsto 1 \otimes x$ and set

$$\mathrm{Fil}^i(B_{\mathrm{st}} \otimes D) = \mathrm{Fil}^i(K \otimes_{K_0} (B_{\mathrm{st}} \otimes D)) \cap (B_{\mathrm{st}} \otimes D).$$

The group G_K acts on $B_{\mathrm{st}} \otimes D$ by

$$g(b \otimes d) = g(b) \otimes d,$$

which commutes with φ and N and is compatible with the filtration.

Definition 8.52. *For a filtered (φ, N)-module D over K, set*

$$\begin{aligned}\mathbf{V}_{\mathrm{st}}(D) :=&\{v \in B_{\mathrm{st}} \otimes D \mid \varphi v = v, Nv = 0, v \in \mathrm{Fil}^0(B_{\mathrm{st}} \otimes D)\} \\ =&\{v \in B_{\mathrm{st}} \otimes D \mid \varphi v = v, Nv = 0, 1 \otimes v \in \mathrm{Fil}^0(K \otimes_{K_0} (B_{\mathrm{st}} \otimes D))\}.\end{aligned}$$

Then $\mathbf{V}_{\mathrm{st}}(D)$ is a sub $\mathbb{Q}_p$-vector space of $B_{\mathrm{st}} \otimes D$, stable under G_K.

Theorem B. (1) *If V is a semi-stable p-adic representation of G_K, then $\mathbf{D}_{\mathrm{st}}(V)$ is an admissible filtered (φ, N)-module over K.*
(2) *If D is an admissible filtered (φ, N)-module over K, then $\mathbf{V}_{\mathrm{st}}(D)$ is a semi-stable p-adic representation of G_K.*
(3) *The functor $\mathbf{D}_{\mathrm{st}} : \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K) \longrightarrow \mathbf{MF}^{ad}_K(\varphi, N)$ is an equivalence of categories and $\mathbf{V}_{\mathrm{st}} : \mathbf{MF}^{ad}_K(\varphi, N) \longrightarrow \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K)$ is a quasi-inverse of $\mathbf{D}_{\mathrm{st}}$. Moreover, they are compatible with tensor product, dual, etc.*

Remark 8.53. $\mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K)$ is a sub-Tannakian category of $\mathbf{Rep}_{\mathbb{Q}_p}(G_K)$, and as an exercise, it's easy to check that

- $\mathbf{D}_{\mathrm{st}}(V_1 \otimes V_2) = \mathbf{D}_{\mathrm{st}}(V_1) \otimes \mathbf{D}_{\mathrm{st}}(V_2)$;
- $\mathbf{D}_{\mathrm{st}}(V^*) = \mathbf{D}_{\mathrm{st}}(V)^*$;
- $\mathbf{D}_{\mathrm{st}}(\mathbb{Q}_p) = K_0$.

Therefore by Theorem B, $\mathbf{MF}^{ad}_K(\varphi, N)$ is stable under tensor product and dual.

On the other hand, without assuming Theorem B.

(a) One can prove directly that if D_1, D_2 are admissible filtered (φ, N)-modules, then $D_1 \otimes D_2$ is again admissible. But the proof is far from trivial. The first proof is given by Faltings [Fal94] for the case $N = 0$ on D_1 and D_2. Later on, Totaro [Tot96] proved the general case.
(b) It is easy to check directly that if D is an admissible filtered (φ, N)-module, then D^* is also admissible.

The proof of Theorem B splits into two parts: Proposition B1 and Proposition B2.

Proposition B1. *If V is a semi-stable p-adic representation of G_K, then $\mathbf{D}_{\mathrm{st}}(V)$ is admissible and there is a natural (functorial in a natural way) isomorphism*

$$V \xrightarrow{\sim} \mathbf{V}_{\mathrm{st}}(\mathbf{D}_{\mathrm{st}}(V)).$$

Exercise 8.54. If Proposition B1 holds, then

$$\mathbf{D}_{\mathrm{st}} : \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K) \longrightarrow \mathbf{MF}^{ad}_K(\varphi, N)$$

is an exact and fully faithful functor. It induces an equivalence

$$\mathbf{D}_{\mathrm{st}} : \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K) \longrightarrow \mathbf{MF}^{?}_K(\varphi, N)$$

where $\mathbf{MF}^{?}_K(\varphi, N)$ is the essential image of $\mathbf{D}_{\mathrm{st}}$, i.e, for D a filtered (φ, N)-module inside it, there exists a semi-stable p-adic representation V such that $D \cong \mathbf{D}_{\mathrm{st}}(V)$, and

$$\mathbf{V}_{\mathrm{st}} : \mathbf{MF}^{?}_K(\varphi, N) \longrightarrow \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K)$$

is a quasi-inverse functor.

Proposition B2. *For any object D of $\mathbf{MF}^{ad}_K(\varphi, N)$, there exists an object V of $\mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K)$ such that $\mathbf{D}_{\mathrm{st}}(V) \cong D$.*

Remark 8.55. The first proof of Proposition B2 is given by Colmez and Fontaine ([CF00]) in 2000. It was known as the *weakly admissible implies admissible conjecture*. In the old terminology, weakly admissible means admissible in this book, and admissible means ? as in Exercise 8.54.

Finally we give some complements about Theorem A and Theorem B.

Assume V is a de Rham p-adic representation of G_K of dimension h. By Theorem A, it is K'-semi-stable for some finite Galois extension K' of K.

Let $J = \mathrm{Gal}(K'/K)$. Let $K_0' = \mathrm{Frac}(W(k'))$, where k' is the residue field of K'. Let $I(K'/K)$ be the inertia subgroup of J, then J acts on K_0' through the isomorphism $\mathrm{Gal}(K_0'/K_0) = J/I(K'/K)$

By Theorem B, then

$$D' = \mathbf{D}_{\mathrm{st},K'}(V) = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_{K'}}$$

is an admissible filtered (φ, N)-module over K' of dimension h, and

$$\mathbf{D}_{\mathrm{dR},K'}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_{K'}} \cong K' \otimes_{K_0'} D'.$$

The group J acts on $D' = \mathbf{D}_{\mathrm{st},K'}(V)$ semi-linearly with respect to the action of J on K_0': if $\tau \in J$, $\lambda \in K_0'$ and $\delta \in D'$, then $\tau(\lambda\delta) = \tau(\lambda)\tau(\delta)$. Then $J = G_K/G_{K'}$ acts naturally on $(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_{K'}}$ on one hand, and on $K' \otimes_{K_0'} D'$ by $\tau(\lambda \otimes d') = \tau(\lambda) \otimes \tau(d')$ for $\lambda \in K'$ and $d' \in D'$. These two actions are equivalent, inducing the isomorphism

$$\mathbf{D}_{\mathrm{dR}}(V) = (\mathbf{D}_{\mathrm{dR},K'}(V))^J \cong (K' \otimes_{K_0'} D')^J.$$

We identify $\mathbf{D}_{\mathrm{dR}}(V)$ and $(K' \otimes_{K_0'} D')^J$ by this isomorphism.

Definition 8.56. *A* filtered $(\varphi, N, \mathrm{Gal}(K'/K))$-module over K *is a finite dimensional K_0'-vector space D' equipped with actions of $(\varphi, N, \mathrm{Gal}(K'/K))$ and a structure of filtered K-vector spaces on $(K' \otimes_{K_0'} D')^{\mathrm{Gal}(K'/K)}$.*

We get an equivalence of categories between K'-semi-stable p-adic representations of G_K and the category of admissible filtered $(\varphi, N, \mathrm{Gal}(K'/K))$-modules over K.

By passage to the limit over K' and using Theorem A, we get

Theorem 8.57. *There is an equivalence of categories between de Rham representations of G_K and admissible filtered (φ, N, G_K)-modules over K.*

This is an analogy result for potentially semi-stable p-adic representations to Theorem 2.30 in Chapter 2 for potentially semi-stable ℓ-adic representations.

9

Proof of Theorem A and Theorem B

This chapter is devoted to the proof of Theorem A and Theorem B.

9.1 Certain General Facts

9.1.1 Unramified representations and modules with trivial filtration.

Definition 9.1. *A filtered K-vector space Δ is said to have* trivial filtration *if*

$$\mathrm{Fil}^0 \Delta = \Delta \text{ and } \mathrm{Fil}^1 \Delta = 0.$$

We claim that

Lemma 9.2. *A filtered (φ, N)-module D over K with trivial filtration is admissible if and only if D is pure of slope 0. In this case $N = 0$.*

Proof. If the filtration on D_K is trivial, then the Hodge polygon $P_H(D)$ is a straight line from $(0,0)$ to $(h,0)$. In particular, $t_H(D') = 0$ for any sub-object D' of D.

Assume that D is admissible. Then $t_N(D') \geq 0$ for any sub-object D, in particular all slopes of D are ≥ 0. But $t_N(D) = 0$, hence D must be pure of slope 0. Since $N\varphi = p\varphi N$, we have $N(D_\alpha) \subset D_{\alpha-1}$, in this case then $N = 0$.

Conversely, assume that D is pure of slope 0. Then for any sub-object D' of D, D' is also pure of slope 0, hence $t_H(D') = t_N(D') = 0$ and D is admissible.

If V is an unramified representation of G_K of dimension h, by Theorem 3.35, we know

$$D = \mathbf{D}(V) = (P_0 \otimes_{\mathbb{Q}_p} V)^{G_k} = (P_0 \otimes_{\mathbb{Q}_p} V)^{G_K}$$

is an étale φ-modules over K_0 of dimension h, hence a φ-module pure of slope 0, and
$$P_0 \otimes_{\mathbb{Q}_p} V = P_0 \otimes_{K_0} D.$$
The inclusion $P_0 \subset B^+_{\mathrm{cris}} \subset B_{\mathrm{st}}$ implies that V is crystalline and semi-stable, and $\mathbf{D}_{\mathrm{cris}}(V) = \mathbf{D}_{\mathrm{st}}(V) = D$. Hence $N = 0$ on D. Since $P_0 \subset B^+_{\mathrm{cris}} \subset B^+_{\mathrm{dR}} \setminus \mathrm{Fil}^1 B^+_{\mathrm{dR}}$, D is also of trivial filtration. Hence $D = \mathbf{D}(V)$ is an admissible filtered (φ, N)-module of dimension h with trivial filtration.

On the other hand, suppose D is an admissible filtered (φ, N)-module of dimension h with trivial filtration. Then D is pure of slope 0 and $N = 0$, hence D is an étale φ-module over K_0. Again by Theorem 3.35,
$$V = \mathbf{V}(D) = (P_0 \otimes_{K_0} D)_{\varphi=1}$$
is a p-adic representation of G_k of dimension h, hence a unramified p-adic representation of G_K of dimension h, and
$$D = \mathbf{D}(V) = (P_0 \otimes_{\mathbb{Q}_p} V)^{G_k} = (P_0 \otimes_{\mathbb{Q}_p} V)^{G_K}.$$
By the identification $P_0 \otimes_{\mathbb{Q}_p} V = P_0 \otimes_{K_0} D$, we have
$$\begin{aligned}\mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D_K) =& B^+_{\mathrm{dR}} \otimes_{K_0} D = B^+_{\mathrm{dR}} \otimes_{P_0} (P_0 \otimes_{K_0} D)\\ =& B^+_{\mathrm{dR}} \otimes_{P_0} (P_0 \otimes_{\mathbb{Q}_p} V) = B^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V,\end{aligned}$$
and
$$(B_{\mathrm{st}} \otimes_{K_0} D)_{\varphi=1,N=0} = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)_{\varphi=1,N=0} = B_e \otimes_{\mathbb{Q}_p} V,$$
hence
$$\mathbf{V}_{\mathrm{st}}(\mathbf{D}) = (B_e \otimes_{\mathbb{Q}_p} V) \cap (B^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V) = V.$$
In conclusion, we have the following result:

Proposition 9.3. *Every unramified p-adic representation of G_K is crystalline and $\mathbf{D}_{\mathrm{st}}$ induces an equivalence of categories between $\mathbf{Rep}^{\mathrm{ur}}_{\mathbb{Q}_p}(G_K)$, the category of unramified p-adic representations of G_K (equivalently $\mathbf{Rep}_{\mathbb{Q}_p}(G_k)$) and the category of admissible filtered (φ, N)-modules with trivial filtration (equivalently, of étale φ-modules over K_0).*

9.1.2 Change of filtrations and residue fields.

Recall for V a p-adic representation and $i \in \mathbb{Z}$, the Tate twist $V(i)$ is the representation $V(i) = V \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(i)$. For filtered (φ, N)-modules, we can also define the Tate twists.

Definition 9.4. *Suppose D is a filtered (φ, N)-module. For $i \in \mathbb{Z}$, the i-*th Tate twist *$D\langle i\rangle$ of D is the following filtered (φ, N)-module:*

(i) *$D\langle i\rangle = D$ as K_0-vector spaces,*

(ii) $\mathrm{Fil}^r(D\langle i\rangle)_K = \mathrm{Fil}^{r+i} D_K$ *for* $r \in \mathbb{Z}$*;*
(iii) *the* φ*- and* N*-actions are given by*

$$N|_{D\langle i\rangle} = N|_D, \quad \varphi|_{D\langle i\rangle} = p^{-i}\varphi|_D. \tag{9.1}$$

Lemma 9.5. (1) *A* p*-adic representation* V *of* G_K *is de Rham (resp. semi-stable, crystalline) if and only if any Tate twist* $V(i)$ *is de Rham (resp. semi-stable, crystalline).*
(2) *A filtered* (φ, N)*-module* D *is admissible if and only if any Tate twist* $D\langle i\rangle$ *is admissible.*
(3) *For* $i \in \mathbb{Z}$, $\mathbf{D}_{\mathrm{st}}(V(i)) \xrightarrow{\sim} \mathbf{D}_{\mathrm{st}}(V)\langle i\rangle$.

Proof. (1) and (2) are clear. We only prove (3).

For $D = \mathbf{D}_{\mathrm{st}}(V) = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K}$ and $D' = \mathbf{D}_{\mathrm{st}}(V(i)) = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V(i))^{G_K}$, let t be a generator of $\mathbb{Z}_p(1)$, then t^i is a generator of $\mathbb{Q}_p(i)$ and $V(i) = \{v \otimes t^i \mid v \in V\}$. Then the isomorphism $D\langle i\rangle \to D'$ is given by

$$d = \sum b_n \otimes v_n \longmapsto d' = \sum b_n t^{-i} \otimes (v_n \otimes t^i) = (t^{-i} \otimes t^i)d$$

where $b_n \in B_{\mathrm{st}}$, $v_n \in V$.

In many occasions, the study of representations would be easier if the residue field k is algebraically closed. Recall I_K is the inertia subgroup of G_K and the sequence

$$1 \to I_K \to G_K \to G_k \to 1$$

is exact.

Proposition 9.6. (1) V *is de Rham as a representation of* G_K *if and only if* V *is de Rham as a representation of* I_K*.*
(2) V *is semi-stable as a* p*-adic representation of* G_K *if and only if it is semi-stable as a* p*-adic representation of* I_K*.*

Proof. (1) Let $\overline{P}$ be an algebraic closure of $P = P_0K = \widehat{K}^{\mathrm{ur}}$ inside of C. Then $\overline{P} \subset B_{\mathrm{dR}}^+$ and $I_K = \mathrm{Gal}(\overline{P}/P)$. Note that $B_{\mathrm{dR}}(\overline{P}/P) = B_{\mathrm{dR}}(\overline{K}/K) = B_{\mathrm{dR}}$, then $B_{\mathrm{dR}}^{I_K} = P$.

If V is a p-adic representation of G_K,

$$D_{\mathrm{dR},P}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{I_K}$$

is a P-vector space with

$$\dim_P D_{\mathrm{dR},P}(V) \leqslant \dim_{\mathbb{Q}_p} V,$$

and V is a de Rham representation of I_K if and only if the equality holds. Note that $D_{\mathrm{dR},P}(V)$ is a P-semilinear representation of G_k and moreover, it is trivial, since

$$P \otimes_K (D_{\mathrm{dR},P}(V))^{G_k} \to D_{\mathrm{dR},P}(V)$$

is an isomorphism by Proposition 3.32. However

$$(D_{\mathrm{dR},P}(V))^{G_k} = D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K},$$

we have (1).

(2) For $D_{\mathrm{st},P}(V) = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{I_K}$, since $B_{\mathrm{st}}^{I_K} = P_0$, $D_{\mathrm{st},P}(V)$ is a P_0-semilinear representation of G_k, again by Proposition 3.32,

$$P_0 \otimes_{K_0} (D_{\mathrm{st},P}(V))^{G_k} \to D_{\mathrm{st},P}(V)$$

is an isomorphism, and $\mathbf{D}_{\mathrm{st}}(V) = (D_{\mathrm{st},P}(V))^{G_k}$.

Proposition 9.7. *Let V be a p-adic representation of G_K, associated with*

$$\rho : G_K \to \mathrm{Aut}_{\mathbb{Q}_p}(V).$$

Assume $\rho(I_K)$ is finite, then

(1) *V is potentially crystalline (potentially semi-stable) and hence de Rham.*
(2) *The following three conditions are equivalent:*
  (a) *V is semi-stable.*
  (b) *V is crystalline.*
  (c) *$\rho(I_K)$ is trivial, i.e., V is unramified.*

Proof. Because of Proposition 9.6, we may assume $k = \bar{k}$, equivalently $K = P$, or $I_K = G_K$.

(2) $\Rightarrow$ (1) is obvious. $(c) \Rightarrow (b)$ is by Proposition 9.3. The only thing left to prove is: (a) V is semi-stable $\Rightarrow$ (c) $\rho(I_K)$ is trivial.

Let $H = \mathrm{Ker}\,\rho$ be an open normal subgroup of I_K, then $\overline{K}^H = L$ is a finite Galois extension of K. Write $J = G_K/H$. Then

$$\begin{aligned}\mathbf{D}_{\mathrm{st}}(V) =&(B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K} = ((B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^H)^J\\ =&(B_{\mathrm{st}}^H \otimes_{\mathbb{Q}_p} V)^J = (K_0 \otimes_{\mathbb{Q}_p} V)^J = K_0 \otimes_{\mathbb{Q}_p} V^J\end{aligned}$$

since $B_{\mathrm{st}}^H = L_0 = K_0$. Therefore

$$V \text{ is semi-stable } \Leftrightarrow \dim_{K_0} \mathbf{D}_{\mathrm{st}}(V) = \dim_{\mathbb{Q}_p} V^J = \dim_{\mathbb{Q}_p} V \Leftrightarrow V^J = V,$$

which means that $\rho(I_K)$ is trivial.

9.1.3 Admissible filtered (φ, N)-modules of dimension 1.

Let D be a filtered (φ, N)-module of dimension 1 over K_0. Write $D = K_0 d$. Then $\varphi(d) = \lambda d$ for some $\lambda \in K_0^\times$ and N must be zero since N is nilpotent. Thus $t_N(D) = v_p(\lambda)$.

Since $D_K = D \otimes_{K_0} K = Kd$ is 1-dimensional over K, there exists $i \in \mathbb{Z}$ such that

$$\operatorname{Fil}^r D_K = \begin{cases} D_K, & \text{for } r \leq i, \\ 0, & \text{for } r > i. \end{cases}$$

Then $t_H(D) = i$. Therefore D is admissible if and only if $v_p(\lambda) = i$.

Conversely, suppose $\lambda \in K_0^\times$, we can associate to it an admissible filtered (φ, N)-module D_λ of dimension 1 given by

$$D_\lambda = K_0,\ \varphi = \lambda\sigma,\ N = 0,\ \operatorname{Fil}^r D_K = \begin{cases} D_K, & \text{if } r \leq v_p(\lambda), \\ 0, & \text{if } r > v_p(\lambda). \end{cases} \tag{9.2}$$

Theorem 9.8. *Any admissible (φ, N)-module over K of dimension 1 is of the form D_λ for some $\lambda \in K_0^\times$. Moreover,*

(1) *$D_\lambda \cong D_{\lambda'}$ if and only if there exists $u \in W^\times$ such that $\lambda' = \lambda \cdot \frac{\sigma(u)}{u}$.*
(2) *In the special case that $K = K_0 = \mathbb{Q}_p$ and $\sigma = \mathrm{Id}$, $D_\lambda \cong D_{\lambda'}$ if and only if $\lambda = \lambda'$.*

Proof. (1) and (2) are easy exercises.

9.1.4 Representations of dimension 1.

Let V be a p-adic representation of G_K of dimension 1. Write $V = \mathbb{Q}_p v$, then $g(v) = \eta(g)v$ where

$$\eta : G_K \to \mathbb{Q}_p^\times$$

is a character (i.e. a continuous group homomorphism). Moreover, we can make η factors through $\mathbb{Z}_p^\times$.

Definition 9.9. *η is called B-*admissible *if V is B-admissible.*

By definition, we have

(i) η is C*-admissible* if and only if η is $\overline{P}$-admissible, or if and only if $\eta(I_K)$ is finite (see Proposition 4.44).
(ii) Recall

$$\mathbf{D}_{\mathrm{HT}}(V) = \bigoplus_{i \in \mathbb{Z}} (C(-i) \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

Then V (and η) is Hodge-Tate if and only if there exists a unique $i \in \mathbb{Z}$ such that $(C(-i) \otimes_{\mathbb{Q}_p} V)^{G_K} \neq 0$. Because

$$(C(-i) \otimes_{\mathbb{Q}_p} V)^{G_K} = (C \otimes_{\mathbb{Q}_p} V(-i))^{G_K},$$

the Hodge-Tate condition is also equivalent to that $V(-i)$ is C-admissible. By Sen's Theorem (Corollary 4.45), this is equivalent to that $\eta\chi^{-i}(I_K)$ is finite where χ is the cyclotomic character. In this case we write $\eta = \eta_0\chi^i$.

Proposition 9.10. *Suppose $\eta : G_K \to \mathbb{Z}_p^\times$ is a continuous homomorphism. Then*

(1) *η is Hodge-Tate if and only if η is of the form $\eta = \eta_0\chi^i$ where $i \in \mathbb{Z}$ and $\eta_0(I_K)$ is finite.*
(2) *η is de Rham if and only if η is Hodge-Tate.*
(3) *The followings are equivalent:*
  (a) *η is semi-stable.*
  (b) *η is crystalline.*
  (c) *There exist $\eta_0 : G_K \to \mathbb{Z}_p^\times$ which is unramified and $i \in \mathbb{Z}$ such that $\eta = \eta_0\chi^i$.*

Proof. We have proved (1). As for (2), V is de Rham implies that V is Hodge-Tate, η is de Rham implies that η is Hodge-Tate, therefore the condition is necessary. On the other hand, if η is Hodge-Tate, $V(-i)$ is $\overline{P}$-admissible and hence de Rham, so $V = V(-i)(i)$ is also de Rham.

(3) follows from Proposition 9.7.

Theorem 9.11. *The functor $\mathbf{D}_{\mathrm{st}}$ gives a bijection of crystalline (equivalently semi-stable) representations of G_K of dimension 1 with admissible filtered (φ, N)-modules over K_0 of dimension 1.*

Proof. If V is crystalline of dimension 1, then $V = V_0(i)$ with $i \in \mathbb{Z}$ and V_0 unramified by Proposition 9.10, hence $\mathbf{D}_{\mathrm{st}}(V) = \mathbf{D}_{\mathrm{st}}(V_0)\langle i\rangle$ is an admissible filtered (φ, N)-module over K_0 of dimension 1.

On the other hand, if D is an admissible filtered (φ, N)-module over K_0 of dimension 1. Suppose $\mathrm{Fil}^i D_K = D_K$ and $\mathrm{Fil}^{i+1} D_K = 0$. Then $D\langle i\rangle$ is with trivial filtration and $V_0 = \mathbf{V}_{\mathrm{st}}(D\langle i\rangle)$ is unramified. Hence $V_0(-i) = \mathbf{V}_{\mathrm{st}}(D)$ is crystalline.

The following special case is extremely useful:

Lemma 9.12. *If $b \in B_{\mathrm{cris}}$ satisfies $\varphi b = \lambda b$ with $\lambda \in K_0$ and $v_p(\lambda) = r$, and if b is also in $\mathrm{Fil}^{r+1} B_{\mathrm{dR}}$, then $b = 0$.*

Proof. Let $D = K_0 e$ be the one-dimensional filtered (φ, N)-module with $\varphi e = \frac{1}{\lambda}e$, $Ne = 0$, and

$$\mathrm{Fil}^i D_K = \begin{cases} K, & \text{if } i \le -r, \\ 0, & \text{if } i > -r. \end{cases}$$

Then $t_N(D) = t_H(D) = -r$ and D is admissible. Then $D\langle -r\rangle$ is admissible with trivial filtration. Thus $\mathbf{V}_{\mathrm{st}}(D) = \mathbf{V}_{\mathrm{st}}(D\langle -r\rangle)(r)$ is a crystalline representation of dimension 1. Then $\mathbf{V}_{\mathrm{st}}(D) = \mathbb{Q}_p b_0 \otimes e$ for any $\varphi b_0 = \lambda b_0$, $b_0 \neq 0$. Thus $b_0 \in \mathrm{Fil}^r B_{\mathrm{dR}}$ but $\notin \mathrm{Fil}^{r+1} B_{\mathrm{dR}}$.

9.1.5 Admissible filtered (φ, N)-modules of dimension 2.

Let D be a filtered (φ, N)-module of $\dim_{K_0} D = 2$. Then there exists a unique $i \in \mathbb{Z}$ such that

$$\mathrm{Fil}^i D_K = D_K, \quad \mathrm{Fil}^{i+1} D_K \neq D_K.$$

Replacing D by $D\langle i\rangle$, we may assume that $i = 0$. There are two cases.

Case 1: $\mathrm{Fil}^1 D_K = 0$. This means that the filtration is trivial. This case has already been discussed this case in § 9.1.1.

Case 2: $\mathrm{Fil}^1 D_K \neq 0$. Then $\mathrm{Fil}^1 D_K = \mathcal{L}$ is a 1-dimensional sub K-vector space of D_K. Hence there exists a unique $r \geq 1$ such that

$$\mathrm{Fil}^j D_K = \begin{cases} D_K, & \text{if } j \leq 0, \\ \mathcal{L} & \text{if } 1 \leq j \leq r, \\ 0, & \text{if } j > r \end{cases}.$$

So the Hodge polygon $P_H(D)$ is as Fig. 9.1.

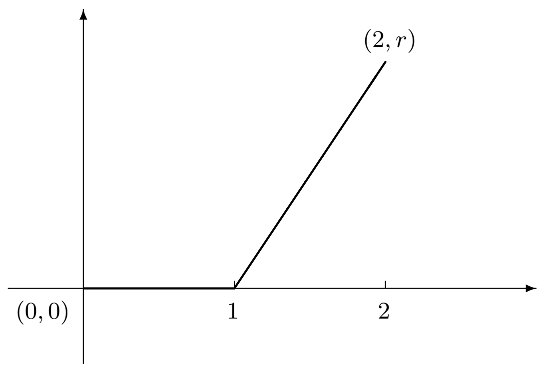


Fig. 9.1.

Consider the special case $K = \mathbb{Q}_p$. Then $K_0 = \mathbb{Q}_p$, $D = D_K$, $\sigma = \mathrm{Id}$ and φ is bilinear. Let $P_\varphi(X)$ be the characteristic polynomial of φ acting on D. Then

$$P_\varphi(X) = X^2 + aX + b = (X - \lambda_1)(X - \lambda_2)$$

for some a, $b \in \mathbb{Q}_p$, λ_1, $\lambda_2 \in \overline{\mathbb{Q}}_p^{\times}$. If $v_p(\lambda_1) \neq v_p(\lambda_2)$, then $P_\varphi(X)$ is reducible over $\mathbb{Q}_p$ and $\lambda_1, \lambda_2 \in \mathbb{Q}_p$.

We may assume $v_p(\lambda_1) \leq v_p(\lambda_2)$. Then $P_N(D)$ is as Fig. 9.2

The admissibility condition implies that

$$v_p(\lambda_1) \geq 0 \text{ and } v_p(\lambda_1) + v_p(\lambda_2) = r. \tag{9.3}$$

We have the following two cases to consider:

Case 2A: $N \neq 0$. Recall that $N(D_\alpha) \subset D_{\alpha-1}$. Then

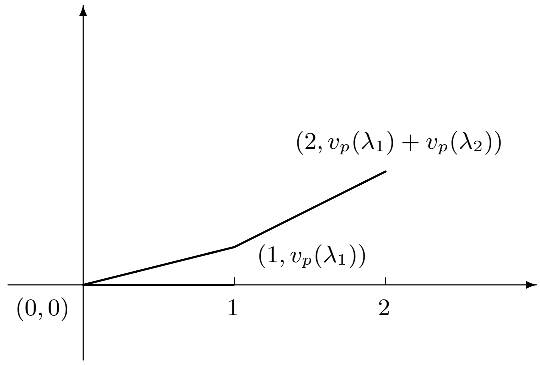


Fig. 9.2.

$$v_p(\lambda_2) = v_p(\lambda_1) + 1 \neq v_p(\lambda_1).$$

In particular λ_1, $\lambda_2 \in \mathbb{Q}_p^\times$. Let $v_p(\lambda_1) = m$. Then $m \geq 0$ and $r = 2m + 1$.

Assume e_2 is an eigenvector for λ_2, i.e.

$$\varphi(e_2) = \lambda_2 e_2.$$

Let $e_1 = N(e_2)$, which is not zero as $N \neq 0$. Applying $N\varphi = p\varphi N$ to e_2, one can see that e_1 is an eigenvector of the eigenvalue λ_2/p of φ, thus $\lambda_2 = p\lambda_1$. Therefore

$$D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2,\ \lambda_1 \in \mathbb{Z}_p - \{0\}$$

with

$$\begin{aligned} \varphi(e_1) &= \lambda_1 e_1, & N(e_1) &= 0, \\ \varphi(e_2) &= p\lambda_1 e_2, & N(e_2) &= e_1. \end{aligned}$$

Now the remaining question is: what is $\mathcal{L}$? To answer this question, we have to check the admissibility conditions, i.e.

- $t_H(D) = t_N(D)$;
- $t_H(D') \leq t_N(D')$ for any sub-object D' of D.

The only non-trivial sub-object is $D' = \mathbb{Q}_p e_1$. We have

$$t_N(D') = m < r, \qquad t_H(D') = \begin{cases} r, & \text{if } \mathcal{L} = D'; \\ 0, & \text{otherwise.} \end{cases}$$

The admissibility condition implies that $t_H(D') = 0$, i.e. $\mathcal{L}$ can be any line $\neq D'$. Therefore there exists a unique $\alpha \in \mathbb{Q}_p$ such that $\mathcal{L} = \mathbb{Q}_p(e_2 + \alpha e_1)$.

Conversely, given $\lambda_1 \in \mathbb{Z}_p - \{0\}$, $\alpha \in \mathbb{Q}_p$, we can associate a 2-dimensional filtered (φ, N)-module $D_{\{\lambda_1, \alpha\}}$ of $\mathbb{Q}_p$ to the pair (λ_1, α), where

$$D_{\{\lambda_1,\alpha\}} = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2 \tag{9.4}$$

with

$$\varphi(e_1) = \lambda_1 e_1, \qquad N(e_1) = 0,$$
$$\varphi(e_2) = p\lambda_1 e_2, \qquad N(e_2) = e_1.$$

$$\mathrm{Fil}^j\, D_{\{\lambda_1,\alpha\}} = \begin{cases} D_{\{\lambda_1,\alpha\}}, & \text{if } j \leq 0, \\ \mathbb{Q}_p(e_2 + \alpha e_1), & \text{if } 1 \leq j \leq 2v_p(\lambda_1) + 1, \\ 0, & \text{otherwise.} \end{cases}$$

Exercise 9.13. $D_{\{\lambda_1,\alpha\}} \cong D_{\{\lambda_1',\alpha'\}}$ if and only if $\lambda_1 = \lambda_1'$ and $\alpha = \alpha'$.

To conclude, we have

Theorem 9.14. *The map*

$$(i, \lambda_1, \alpha) \longmapsto D_{\{\lambda_1,\alpha\}}\langle i\rangle$$

from $\mathbb{Z} \times (\mathbb{Z}_p - \{0\}) \times \mathbb{Q}_p$ to the set of isomorphism classes of 2-dimensional admissible filtered (φ, N)-modules over $\mathbb{Q}_p$ with $N \neq 0$ is a bijection.

Remark 9.15. We claim that $D_{\{\lambda_1,\alpha\}}$ is irreducible if and only if $v_p(\lambda_1) > 0$.

Indeed, $D_{\{\lambda_1,\alpha\}}$ is not irreducible if and only if there exists a nontrivial subobject of it in the category of admissible filtered (φ, N)-modules. We have only one candidate: $D' = \mathbb{Q}_p e_1$. And D' is admissible if and only if $t_H(D') = t_N(D')$. Note that the former number is 0 and the latter one is $v_p(\lambda_1)$.

Case 2B: $N = 0$. By the admissibility condition, we need to check that for all lines D' of D stable under φ, $t_H(D') \leq t_N(D')$. By the filtration of D, the following holds:

$$t_H(D') = \begin{cases} 0, & \text{if } D' \neq \mathcal{L}, \\ r, & \text{if } D' = \mathcal{L}. \end{cases}$$

Again there are two cases.

(a) If the polynomial $P_\varphi(X) = X^2 + aX + b$ is irreducible on $\mathbb{Q}_p[X]$. Then there is no non-trivial sub-object of D. Let $\mathcal{L} = \mathbb{Q}_p e_1$, $\varphi(e_1) = e_2$, then $\varphi(e_2) = -be_1 - ae_2$ and $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$ is always admissible and irreducible, isomorphic to $D_{a,b}$ in the following exercise.

Exercise 9.16. Let a, $b \in \mathbb{Z}_p$ with $r = v_p(b) > 0$ such that $X^2 + aX + b$ is irreducible over $\mathbb{Q}_p$. Set

$$D_{a,b} = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2 \tag{9.5}$$

with

$$\begin{cases} \varphi(e_1) = e_2, \\ \varphi(e_2) = -be_1 - ae_2, \end{cases} \qquad N = 0,$$

$$\operatorname{Fil}^j D_{a,b} = \begin{cases} D_{a,b}, & \text{if } j \leq 0, \\ \mathbb{Q}_p e_1, & \text{if } 1 \leq j \leq r, \\ 0, & \text{otherwise.} \end{cases}$$

Then $D_{a,b}$ is admissible and irreducible.

(b) If the polynomial $P_\varphi(X) = X^2 + aX + b = (x - \lambda_1)(x - \lambda_2)$ is reducible on $\mathbb{Q}_p[X]$, suppose $v_p(\lambda_1) \leq v_p(\lambda_2)$, $r = v_p(\lambda_1) + v_p(\lambda_2)$. Let e_1 and e_2 be the eigenvectors of λ_1 and λ_2 respectively. Then $D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$ and $\mathbb{Q}_p e_1$ and $\mathbb{Q}_p e_2$ are the only two non-trivial sub-objects of D. Suppose D is not a direct sum of two admissible (φ, N)-modules. Check the admissibility condition, then $\mathcal{L}$ is neither $\mathbb{Q}_p e_1$ or $\mathbb{Q}_p e_2$. By scaling e_1 and e_2 appropriately, we can assume $\mathcal{L} = \mathbb{Q}_p(e_1 + e_2)$. Then D is isomorphic to D'_{λ_1,λ_2} in the following easy exercise.

Exercise 9.17. Let $\lambda_1,\ \lambda_2 \in \mathbb{Z}_p - \{0\}$, $\lambda_1 \neq \lambda_2$, and $v_p(\lambda_1) \leq v_p(\lambda_2)$. Let $r = v_p(\lambda_1) + v_p(\lambda_2)$. Set

$$D'_{\lambda_1,\lambda_2} = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$$

with

$$\begin{cases} \varphi(e_1) = \lambda_1 e_1, \\ \varphi(e_2) = \lambda_2 e_2, \end{cases} \qquad N = 0,$$

$$\operatorname{Fil}^j D'_{\lambda_1,\lambda_2} = \begin{cases} D'_{\lambda_1,\lambda_2}, & \text{if } j \leq 0, \\ \mathbb{Q}_p(e_1 + e_2), & \text{if } 1 \leq j \leq r, \\ 0, & \text{otherwise.} \end{cases}$$

Then D'_{λ_1,λ_2} is admissible. Moreover, it is irreducible if and only if $v_p(\lambda_1) > 0$.

To conclude, we have

Theorem 9.18. *Suppose D is an admissible filtered (φ, N)-module over $\mathbb{Q}_p$ of dimension 2 with $N = 0$ such that $\operatorname{Fil}^0 D = D$, and $\operatorname{Fil}^1 D \notin \{D, 0\}$. If D is not a direct sum of two admissible (φ, N)-modules of dimension 1, then either $D \cong D_{a,b}$ for a uniquely determined (a, b), or $D \cong D'_{\lambda_1,\lambda_2}$ for a uniquely determined (λ_1, λ_2).*

9.2 Reduction of Theorem B and outline of the proof

9.2.1 Proof of Proposition B1

We shall prove

Proposition B1. *If V is a semi-stable p-adic representation of G_K, then $\mathbf{D}_{\mathrm{st}}(V)$ is admissible and there is a natural (functorial in a natural way) isomorphism*

$$V \longrightarrow \mathbf{V}_{\mathrm{st}}(\mathbf{D}_{\mathrm{st}}(V)).$$

Proof. Let V be a semi-stable p-adic representation of G_K of dimension h. Let $D = \mathbf{D}_{\mathrm{st}}(V)$. Our proof is divided into two steps.

I. Construction of the natural isomorphism $V \xrightarrow{\sim} \mathbf{V}_{\mathrm{st}}(D)$:

The natural map

$$\alpha_{\mathrm{st}} : B_{\mathrm{st}} \otimes_{K_0} D \to B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V$$

as defined in § 8.1.2 is an isomorphism. We identify them and call them X.

Let $\{v_1, \cdots, v_h\}$ be a basis of V over $\mathbb{Q}_p$ and $\{\delta_1, \cdots, \delta_h\}$ be a basis of D over K_0 respectively. Identify v_i with $1 \otimes v_i$ and δ_i with $1 \otimes \delta_i$, then $\{v_1, \cdots, v_h\}$ and $\{\delta_1, \cdots, \delta_h\}$ are two bases of X over B_{st}.

An element of X can be written as a sum of the form $b \otimes \delta$ where $b \in B_{\mathrm{st}}$, $\delta \in D$ and also a sum of the form $c \otimes v$, where $c \in B_{\mathrm{st}}$, $v \in V$. The actions of G_K, φ, and N on X are listed below:

$$\begin{array}{lll} G_K\text{-action}: & g(b \otimes \delta) = g(b) \otimes \delta, & g(c \otimes v = g(c) \otimes g(v). \\ \varphi\text{-action}: & \varphi(b \otimes \delta) = \varphi(b) \otimes \varphi(\delta), & \varphi(c \otimes v) = \varphi(c) \otimes v. \\ N\text{-action}: & N(b \otimes \delta) = N(b) \otimes \delta + b \otimes N(\delta), & N(c \otimes v) = N(c) \otimes v. \end{array}$$

We also know that X is endowed with a filtration. By the map $x \mapsto 1 \otimes x$, one has the inclusion

$$X \subset X_{\mathrm{dR}} = B_{\mathrm{dR}} \otimes_{B_{\mathrm{st}}} X = B_{\mathrm{dR}} \otimes_K D_K = B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V.$$

Then the filtration of X is induced by

$$\mathrm{Fil}^i X_{\mathrm{dR}} = \mathrm{Fil}^i B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V = \sum_{r+s=i} \mathrm{Fil}^r B_{\mathrm{dR}} \otimes_K \mathrm{Fil}^s D_K.$$

Recall the definition of $\mathbf{V}_{\mathrm{st}}$ in Definition 8.52:

$$\begin{aligned} \mathbf{V}_{\mathrm{st}}(D) =& \{x \in X \mid \varphi(x) = x, N(x) = 0, x \in \mathrm{Fil}^0 X\} \\ =& \{x \in X \mid \varphi(x) = x, N(x) = 0, x \in \mathrm{Fil}^0 X_{\mathrm{dR}}\}. \end{aligned}$$

Note that $V \subset X$ satisfies the conditions in the right hand side. We only need to check that $\mathbf{V}_{\mathrm{st}}(D) = V$.

Write $x = \sum\limits_{n=1}^{h} b_n \otimes v_n \in \mathbf{V}_{\mathrm{st}}(D)$, where $b_n \in B_{\mathrm{st}}$.

(a) First $N(x) = 0$, i.e. $\sum\limits_{n=1}^{h} N(b_n) \otimes v_n = 0$, then $N(b_n) = 0$ for all $1 \le n \le h$, which implies that $b_n \in B_{\mathrm{cris}}$ for all n.
(b) Secondly, the condition $\varphi(x) = x$ means

$$\sum_{n=1}^{h} \varphi(b_n) \otimes v_n = \sum_{n=1}^{h} b_n \otimes v_n.$$

Then $\varphi(b_n) = b_n$, which implies that $b_n \in B_e$ for all $1 \le n \le h$.

(c) The condition $x \in \mathrm{Fil}^0 X_{\mathrm{dR}}$ implies that $b_n \in \mathrm{Fil}^0 B_{\mathrm{dR}} = B_{\mathrm{dR}}^+$ for all $1 \le n \le h$.

Applying the fundamental exact sequence (7.27)

$$0 \to \mathbb{Q}_p \to B_e \to B_{\mathrm{dR}}/B_{\mathrm{dR}}^+ \to 0,$$

we have that $b_n \in \mathbb{Q}_p$. Therefore $x \in V$, which implies that $V = \mathbf{V}_{\mathrm{st}}(D)$.

II. Admissibility of D.

Let D' be a sub K_0-vector space of D stable under φ and N. It suffices to prove

$$t_H(D') \leqslant t_N(D'). \tag{9.6}$$

(1) Assume first that $\dim_{K_0} D' = 1$. Let $\{v_1, \cdots, v_h\}$ be a basis of V over $\mathbb{Q}_p$. Write $D' = K_0\delta$, then

$$\varphi\delta = \lambda\delta, \qquad \lambda \in K_0^\times.$$

Thus

$$t_N(D') = v_p(\lambda) = r \quad \text{and} \quad N\delta = 0.$$

Write $\delta = \sum_{i=1}^{h} b_i \otimes v_i$. Then

$$\varphi\delta = \sum_{i=1}^{h} \varphi b_i \otimes v_i \text{ and } N\delta = \sum_{i=1}^{h} N b_i \otimes v_i,$$

so $\varphi b_i = \lambda b_i$ and $N b_i = 0$ for all $1 \le i \le h$, which implies that $b_i \in B_{\mathrm{cris}}$.

Assume $t_H(D') = s$. Then $\delta \in \mathrm{Fil}^s(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)$ but $\notin \mathrm{Fil}^{s+1}(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)$. The filtration

$$\mathrm{Fil}^s(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V) = \mathrm{Fil}^s B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$$

implies that $b_i \in \mathrm{Fil}^s B_{\mathrm{dR}}$ for all i. Pick any nonzero b_i, then Lemma 9.12 implies that $s \le r$.

Furthermore, we see that if $D = D'$ is of dimension 1, then $t_H(D) = t_N(D)$.

(2) General case. Let $\dim_{K_0} D' = m$. We want to prove $t_H(D') \leqslant t_N(D')$, and the inequality becomes an equality if $m = h$.

Let $V_1 = \bigwedge^m V$, which is a quotient of $V \otimes \cdots \otimes V$ (m copies). The tensor product is a semi-stable representation, so V_1 is also semi-stable. Then

$$\mathbf{D}_{\mathrm{st}}(V_1) = \bigwedge^m \mathbf{D}_{\mathrm{st}}(V) = \bigwedge_{K_0}^m D.$$

Now $\bigwedge^m D' \subset \bigwedge^m D$ is a subobject of dimension 1, and

$$t_H(\bigwedge^m D') = t_H(D'), \quad t_N(\bigwedge^m D') = t_N(D'),$$

the general case is reduced to the one dimensional case.

9.2.2 Reduction of Proposition B2.

Lemma 9.19. *Let F be a field. Let J be a subgroup of the group of automorphisms of F and $E = F^J$. Let Δ be a finite dimensional E-vector space, and*

$$\Delta_F = F \otimes_E \Delta.$$

J acts on Δ_F through

$$j(\lambda \otimes \delta) = j(\lambda) \otimes \delta, \text{ if } j \in J, \ \lambda \in F, \ \delta \in \Delta.$$

By the map $\delta \mapsto 1 \otimes \delta$, we identify Δ with $1 \otimes_E \Delta = (\Delta_F)^J$. Let L be a sub F-vector space of Δ_F. Then there exists Δ', a sub E-vector space of Δ such that $L = F \otimes_E \Delta'$ if and only if $g(L) = L$ for all $g \in J$, i.e., L is stable under the action of J.

Proof. The only if part is trivial. If L is stable under the action of J, then we have an exact sequence of F-vector spaces with J-action

$$0 \longrightarrow L \longrightarrow \Delta_F \longrightarrow \Delta_F/L \longrightarrow 0,$$

Taking the J-invariants, we have an exact sequence of E-vector spaces

$$0 \longrightarrow L^J \longrightarrow \Delta \longrightarrow (\Delta_F/L)^J.$$

Then

$$\dim_E \Delta = \dim_F \Delta_F = \dim_F L + \dim_F(\Delta_F/J) \leq \dim_E L^J + \dim_E(\Delta_F/L)^J,$$

but

$$\dim_E L^J \leq \dim_F L, \quad \dim_E(\Delta_F/L)^J \leq (\Delta_F/J),$$

we must have $\dim_E L^J = \dim_F L$ and $\Delta' = L^J$ satisfies $L = F \otimes_E \Delta'$.

Proposition 9.20. *Let D be an admissible filtered (φ, N)-module over K of dimension $h \geqslant 1$. Let $V = \mathbf{V}_{\mathrm{st}}(D)$. Then $\dim_{\mathbb{Q}_p} V \leqslant h$, V is semi-stable and $\mathbf{D}_{\mathrm{st}}(V) \subset D$ is a subobject.*

Remark 9.21. The above proposition implies that, if D is admissible, the following conditions are equivalent:

(a) $D \cong \mathbf{D}_{\mathrm{st}}(V)$ where V is some semi-stable p-adic representation.
(b) $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) \geqslant h$.
(c) $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) = h$.

Proof. We may assume $V \neq 0$. Apply the above Lemma to the case

$$\Delta = D, \ F = C_{\mathrm{st}} = \mathrm{Frac}\, B_{\mathrm{st}}, J = G_K, E = C_{\mathrm{st}}^{G_K} = K_0,$$

Then

$$\Delta_F = C_{\mathrm{st}} \otimes_{K_0} D \supset B_{\mathrm{st}} \otimes_{K_0} D \supset V.$$

Let L be the sub-C_{st}-vector space of $C_{\mathrm{st}} \otimes_{K_0} D$ generated by V. The actions of φ and N on B_{st} extend to C_{st}, thus L is stable under φ, N and G_K-actions. By the lemma, there exists a sub K_0-vector space D' of D such that

$$L = C_{\mathrm{st}} \otimes_{K_0} D'.$$

The fact that L is stable by φ and N implies that D' is also stable by φ and N.

Choose a basis $\{v_1, \cdots, v_r\}$ of L over C_{st} consisting of elements of V. Choose a basis $\{d_1, \cdots, d_r\}$ of D' over K_0, which is also a basis of L over C_{st}. Since $V \subset B_{\mathrm{st}} \otimes_{K_0} D$,

$$v_i = \sum_{j=1}^{r} b_{ij} d_j, \quad b_{ij} \in B_{\mathrm{st}}.$$

By the inclusion $B_{\mathrm{st}} \otimes_{K_0} D' \subset B_{\mathrm{st}} \otimes_{K_0} D$, we have

$$\bigwedge\nolimits_{B_{\mathrm{st}}}^{r} (B_{\mathrm{st}} \otimes_{K_0} D') \subset \bigwedge\nolimits_{B_{\mathrm{st}}}^{r} (B_{\mathrm{st}} \otimes_{K_0} D),$$

equivalently,

$$B_{\mathrm{st}} \otimes_{K_0} \bigwedge\nolimits_{K_0}^{r} D' \subset B_{\mathrm{st}} \otimes_{K_0} \bigwedge\nolimits_{K_0}^{r} D.$$

Let $b = \det(b_{ij}) \in B_{\mathrm{st}}$. Let

$$v_0 = v_1 \wedge v_2 \wedge \cdots \wedge v_r, \quad d_0 = d_1 \wedge d_2 \wedge \cdots \wedge d_r,$$

then d_0 is a basis of $\bigwedge_{K_0}^{r} D'$, and $v_0 = b d_0$ hence $b \neq 0$. Since $N = 0$ in $\bigwedge_{K_0}^{r} D'$, $b \in B_{\mathrm{cris}}$. Suppose $\varphi(d_0) = \lambda d_0$, then $t_N(\bigwedge_{K_0}^{r} D') = v_p(\lambda) := r$. Now since $\varphi(b) = \lambda^{-1} b$, by Lemma 9.12, $b \in \mathrm{Fil}^{-s} B_{\mathrm{dR}}$ for $-s \leq -r$. Then $d_0 = b^{-1} v_0 \in \mathrm{Fil}^{s} B_{\mathrm{dR}}$ for some $s \geq r$. Thus

$$t_H(\bigwedge\nolimits^{r} D') \geqslant t_N(\bigwedge\nolimits^{r} D').$$

The admissibility condition $t_H(D') \leq t_N(D')$ then implies $t_H(\bigwedge^{r} D') = t_N(\bigwedge^{r} D')$, thus $\bigwedge^{r} D'$ is an admissible filtered (φ, N)-module of dimension 1, and $\mathbf{V}_{\mathrm{st}}(\bigwedge^{r} D')$ is a crystalline representation of dimension 1. Since $v_i \in \mathbf{V}_{\mathrm{st}}(D')$ and hence $v_0 \in \mathbf{V}_{\mathrm{st}}(\bigwedge^{r} D')$, we have

$$\mathbf{V}_{\mathrm{st}}(\bigwedge\nolimits^{r} D') = \mathbb{Q}_p v_0.$$

For any $v \in \mathbf{V}_{\mathrm{st}}(D') = V$, write $v = \sum\limits_{i=1}^{r} c_i v_i$ with $c_i \in C_{\mathrm{st}}$, $1 \leqslant i \leqslant r$, then

$$v_1 \wedge \cdots \wedge v_{i-1} \wedge v \wedge v_{i+1} \wedge \cdots \wedge v_r = c_i v_0 \in \bigwedge\nolimits_{\mathbb{Q}_p}^{r} V \subset \mathbf{V}_{\mathrm{st}}(\bigwedge\nolimits^{r} D') = \mathbb{Q}_p v_0,$$

therefore $c_i \in \mathbb{Q}_p$. Thus V as a $\mathbb{Q}_p$-vector space is generated by $\{v_1, \cdots, v_r\}$ and
$$r = \dim_{K_0} D' \leqslant \dim_{K_0} D.$$
Because
$$\mathbf{V}_{\mathrm{st}}(D') = V \text{ and } \mathbf{D}_{\mathrm{st}}(V) = D',$$
V is also semi-stable.

9.2.3 Outline of the Proof.

By Proposition 9.20, to prove Theorem A and Theorem B, it suffices to prove

Proposition A (Theorem A). *Let V be a p-adic representation of G_K which is de Rham. Then V is potentially semi-stable.*

Proposition B. *Let D be an admissible filtered (φ, N)-module over K. Then $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) = \dim_{K_0} D$.*

Let D_K be the associated filtered K-vector space, where
$$D_K = \begin{cases} D_{\mathrm{dR}}(V), & \text{Case A,} \\ K \otimes_{K_0} D, & \text{Case B.} \end{cases}$$
Let $d = \dim_K D_K$ and let the Hodge polygon
$$P_H(D_K) = \begin{cases} P_H(V), & \text{Case A,} \\ P_H(D), & \text{Case B.} \end{cases}$$
We shall prove Proposition A and Proposition B by induction on the *complexity* of P_H. The proof is divided in several steps.

Step 1: P_H is trivial. i.e. the filtration is trivial.

Proof (Proposition A in this case). From the following exact sequence:
$$0 \to \mathrm{Fil}^1 B_{\mathrm{dR}} \to \mathrm{Fil}^0 B_{\mathrm{dR}} = B_{\mathrm{dR}}^+ \to C \to 0,$$
$\otimes V$ and then take the invariant under G_K, we have
$$0 \to \mathrm{Fil}^1 D_K \to \mathrm{Fil}^0 D_K \to (C \otimes_{\mathbb{Q}_p} V)^{G_K}.$$
Because the filtration is trivial, $\mathrm{Fil}^1 D_K = 0$ and $\mathrm{Fil}^0 D_K = D_K$, then we have a monomorphism $D_K = \mathrm{Fil}^0 D_K \to (C \otimes_{\mathbb{Q}_p} V)^{G_K}$, and
$$\dim_K (C \otimes_{\mathbb{Q}_p} V)^{G_K} \geqslant \dim_K D_K = \dim_{\mathbb{Q}_p} V,$$
thus the inequality is an equality and V is C-admissible. This implies that the action of I_K is finite, hence V is potentially semi-stable (even potentially crystalline, cf. Proposition 9.7).

Proof (Proposition B in this case). We know that in this case, $D \simeq \mathbf{D}_{\mathrm{st}}(V)$ where

$$V = (P_0 \otimes_{K_0} D)_{\varphi=1}$$

is an unramified representation.

Step 2: Show the following Propositions 2A (however, we only prove it in the finite residue case) and 2B and thus reduce to the case that V and D are irreducible.

Proposition 2A. *If $0 \to V' \to V \to V'' \to 0$ is a short exact sequence of p-adic representations of G_K, and if V', V'' are semi-stable and V is de Rham, then V is also semi-stable.*

Proposition 2B. *If $0 \to D' \to D \to D'' \to 0$ is a short exact sequence of admissible filtered (φ, N)-modules over K, and if*

$$\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D') = \dim_{K_0} D', \quad \dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D'') = \dim_{K_0} D'',$$

then $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) = \dim_{K_0} D$.

Step 3: Reduce the proof to the case that $t_H = 0$.

Step 4: Prove Proposition A and Proposition B in the case $t_H = 0$.

9.3 Proof of Proposition 2A and Proposition 2B

9.3.1 $H^1_g = H^1_{\mathrm{st}}$ when k is finite.

Proposition 2A in the finite residue field case is due to Hyodo [Hyo88]. The original proof of Hyodo, using decomposition of iso-crystals and unramified representations, was never published. Proposition 2A in the arbitrary residue field case is due to Berger [Ber01, Chapitre VI], using the theory of (φ, Γ)-modules. In [Ber02] he also gave a proof of Proposition 2A as a corollary of Theorem A. However Berger's proof was much more involved. Here we give a proof of Hyodo's result just using Galois cohomology and Tate duality.

In this subsection, the cohomology is the continuous cohomology. We set $\widetilde{B}_{\mathrm{dR}} = B_{\mathrm{dR}}/B^+_{\mathrm{dR}}$ and, for all $b \in B_{\mathrm{dR}}$, we denote $\tilde{b}$ its image in $\widetilde{B}_{\mathrm{dR}}$.

Let V be a p-adic representation of G_K. Let $D = \mathbf{D}_{\mathrm{st}}(V)$.

Definition 9.22. Kato's filtration *for $H^1(K,V)$ is the sub-$\mathbb{Q}_p$-vector spaces*

$$0 \subset H^1_e(K,V) \subset H^1_f(K,V) \subset H^1_{\mathrm{st}}(K,V) \subset H^1_g(K,V) \subset H^1(K,V)$$

where

$$H^1_e(K,V) := \mathrm{Ker}\left(H^1(K,V) \longrightarrow H^1(K, B_e \otimes_{\mathbb{Q}_p} V)\right), \tag{9.7}$$
$$H^1_f(K,V) := \mathrm{Ker}\left(H^1(K,V) \longrightarrow H^1(K, B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)\right), \tag{9.8}$$
$$H^1_{\mathrm{st}}(K,V) := \mathrm{Ker}\left(H^1(K,V) \longrightarrow H^1(K, B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)\right), \tag{9.9}$$
$$H^1_g(K,V) := \mathrm{Ker}\left(H^1(K,V) \longrightarrow H^1(K, B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)\right). \tag{9.10}$$

Definition 9.23. *The* tangent space of V *is the* K*-vector space*

$$t_V := H^0(K, \widetilde{B}_{\mathrm{dR}} \otimes V).$$

We now compute these cohomology groups.

(1) $H^1_e(K, V)$. Tensoring the fundamental exact sequence with V, we get a short exact sequence

$$0 \longrightarrow V \longrightarrow B_e \otimes V \longrightarrow \widetilde{B}_{\mathrm{dR}} \otimes V \longrightarrow 0,$$

which induces a long exact sequence

$$0 \to H^0(K, V) \to D_{N=0,\varphi=1} \to t_V \longrightarrow H^1_e(K, V) \longrightarrow 0 \tag{9.11}$$

where

$$D_{N=0,\varphi=1} = H^0(K, B_e \otimes V) = \{x \in D \mid Nx = 0\ ,\ \varphi(x) = x\}.$$

(2) $H^1_f(K, V)$. Consider the map $B_{\mathrm{cris}} \to B_{\mathrm{cris}} \oplus \widetilde{B}_{\mathrm{dR}}$ sending b to $(\varphi b - b, \tilde{b})$. By the fundamental exact sequence and $0 \to B_{\mathrm{cris}} \to B_{\mathrm{st}} \xrightarrow{N} B_{\mathrm{st}} \to 0$, we get the exactness of

$$0 \longrightarrow \mathbb{Q}_p \longrightarrow B_{\mathrm{cris}} \longrightarrow B_{\mathrm{cris}} \oplus \widetilde{B}_{\mathrm{dR}} \longrightarrow 0. \tag{9.12}$$

Tensoring with V, we get a short exact sequence

$$0 \longrightarrow V \longrightarrow B_{\mathrm{cris}} \otimes V \longrightarrow (B_{\mathrm{cris}} \otimes V) \oplus (\widetilde{B}_{\mathrm{dR}} \otimes V) \longrightarrow 0$$

which induces a long exact sequence

$$0 \to H^0(K, V) \to D_{N=0} \to D_{N=0} \oplus t_V \longrightarrow H^1_f(K, V) \longrightarrow 0. \tag{9.13}$$

(3) $H^1_{\mathrm{st}}(K, V)$. Let

$$B'_{\mathrm{st}} = \big\{(x, y) \in (B_{\mathrm{st}})^2 \mid p\varphi x - x = Ny\big\}.$$

If $z \in B_{\mathrm{st}}$, then $(Nz, \varphi z - z) \in B'_{\mathrm{st}}$. We denote $\iota : B_{\mathrm{st}} \to B'_{\mathrm{st}} \oplus \widetilde{B}_{\mathrm{dR}}$ the map $z \mapsto ((Nz, \varphi z - z), \tilde{z})$.

Lemma 9.24. *The sequence*

$$0 \longrightarrow \mathbb{Q}_p \longrightarrow B_{\mathrm{st}} \xrightarrow{\iota} B'_{\mathrm{st}} \oplus \widetilde{B}_{\mathrm{dR}} \longrightarrow 0 \tag{9.14}$$

is exact.

Proof. It is clear that $\mathrm{Ker}\,(\iota) = B_{\mathrm{st}}^{N=0,\varphi=1} \bigcap B_{\mathrm{dR}}^{+} = \mathbb{Q}_p$. We only need to show ι is surjective. Let $((x,y),w) \in B'_{\mathrm{st}} \oplus \widetilde{B}_{\mathrm{dR}}$. By surjectivity of $N : B_{\mathrm{st}} \to B_{\mathrm{st}}$, there is a $z_1 \in B_{\mathrm{st}}$ such that $Nz_1 = x$. We have $N(y - (\varphi z_1 - z_1)) = p\varphi x - x - N(\varphi z_1 - z_1) = 0$, i.e. $y - (\varphi z_1 - z_1) \in B_{\mathrm{cris}}$. By surjectivity of $\varphi - 1 : B_{\mathrm{cris}} \to B_{\mathrm{cris}}$, there is a $z_2 \in B_{\mathrm{cris}}$ such that $\varphi z_2 - z_2 = y - (\varphi z_1 - z_1)$. By surjectivity of $B_e \to \widetilde{B}_{\mathrm{dR}}$, there is a $z_3 \in B_e$ such that $\tilde{z}_3 = w - (\tilde{z}_1 + \tilde{z}_2)$. Let $z = z_1 + z_2 + z_3 \in B_{\mathrm{st}}$, then we have $\iota(z) = ((x,y),w)$.

Tensoring (9.14) with V, we get a short exact sequence

$$0 \longrightarrow V \longrightarrow B_{\mathrm{st}} \otimes V \longrightarrow (B'_{\mathrm{st}} \otimes V) \oplus (\widetilde{B}_{\mathrm{dR}} \otimes V) \longrightarrow 0,$$

which induces a long exact sequence

$$0 \to H^0(K,V) \to D \to D' \oplus t_V \longrightarrow H^1_{\mathrm{st}}(K,V) \longrightarrow 0 \tag{9.15}$$

where $D' = H^0(K, B'_{\mathrm{st}})$.

Moreover D' can be easily computed from D:

Proposition 9.25. *Denote $x \mapsto \overline{x}$ the projection of D onto D/ND and consider the maps*

$$\begin{aligned}
&\iota_0 : D_{N=0} \longrightarrow D \oplus D_{N=0}\ , \quad w \mapsto (w, -\varphi w + w),\\
&\iota_1 : D \oplus D_{N=0} \to D \oplus D\ , \quad (u,v) \mapsto (Nu, \varphi u - u + v),\\
&\iota_2 : D' \to D/ND\ , \quad (x,y) \mapsto \overline{x}.
\end{aligned}$$

The image of ι_1 is contained in D', the image of ι_2 is contained in $(D/ND)_{\varphi=p^{-1}}$ and the sequence

$$0 \longrightarrow D_{N=0} \xrightarrow{\iota_0} D \oplus D_{N=0} \xrightarrow{\iota_1} D' \xrightarrow{\iota_2} (D/ND)_{\varphi=p^{-1}} \longrightarrow 0$$

is exact.

Proof. The inclusions

$$\mathrm{Im}(\iota_1) \subset D' \text{ and } \mathrm{Im}(\iota_2) \subset (D/ND)_{\varphi=p^{-1}}$$

are obvious. We have

$$D' = \left\{(x,y) \in D^2 \mid p\varphi x - x = Ny\right\}.$$

If $x \in D$ lifts $s \in (D/ND)_{\varphi=p^{-1}}$, then there exists $y \in D$ such that $Ny = p\varphi x - x$ and (x,y) is in D' and such that $\iota_2(x,y) = s$, hence ι_2 is onto.

If $(u,v) \in D \oplus D_{N=0}$, we have $\iota_2(\iota_1(u,v)) = \iota_2(Nu, \varphi u - u + v) = 0$. Conversely, if $(x,y) \in D'$ lies in the kernel of ι_2, it means there exists $u \in D$ such that $Nu = x$. Hence $(x,y) - \iota_1(u,0)$ is an element of D' of the form $(0,v)$ and $Nv = 0$. Hence $(x,y) = \iota_1(u,v)$ and the image of ι_1 is the kernel of ι_2.

If $w \in D_{N=0}$, then $\iota_1(\iota_0(w)) = \iota_1(w, -\varphi w + w) = (Nw, \varphi w - w - \varphi w + w) = 0$. Conversely, if (u,v) lies in the kernel of ι_1, we have $Nu = 0$ and $v = -\varphi u + u$, hence $(u,v) = \iota_0(u)$.

The map ι_0 is obviously injective and it concludes the proof.

The following result is now obvious:

Proposition 9.26. *The quotient $\mathbb{Q}_p$-vector spaces $H^1_f(K,V)/H^1_e(K,V)$ and $H^1_{\mathrm{st}}(K,V)/H^1_e(K,V)$ are finite dimensional:*

$$\dim_{\mathbb{Q}_p} H^1_f(K,V)/H^1_e(K,V) = \dim_{\mathbb{Q}_p} D_{N=0,\varphi=1} \tag{9.16}$$
$$\dim_{\mathbb{Q}_p} H^1_{\mathrm{st}}(K,V)/H^1_f(K,V) = \dim_{\mathbb{Q}_p}(D/ND)_{\varphi=p^{-1}}. \tag{9.17}$$

Moreover, we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^0(K,V) \arrow[r] \arrow[d, equal] & D_{N=0,\varphi=1} \arrow[r] \arrow[d, hook] & t_V \arrow[r] \arrow[d, hook] & H^1_e(K,V) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & H^0(K,V) \arrow[r] \arrow[d, equal] & D_{N=0} \arrow[r] \arrow[d, hook] & D_{N=0} \oplus t_V \arrow[r] \arrow[d, hook] & H^1_f(K,V) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & H^0(K,V) \arrow[r] & D \arrow[r] & D' \oplus t_V \arrow[r] & H^1_{\mathrm{st}}(K,V) \arrow[r] & 0.
\end{tikzcd}$$

From now on in this subsection we assume that k is finite, i.e. K is a finite extension of $\mathbb{Q}_p$. Recall the following result of Bloch and Kato ([BK90], prop.3.8):

Theorem 9.27. *Suppose K is a finite extension of $\mathbb{Q}_p$ and V is semi-stable. Under the perfect pairing of class field theory*

$$H^1(K,V) \times H^1(K,V^*(1)) \longrightarrow H^2(K,\mathbb{Q}_p(1)) \xrightarrow{\sim} \mathbb{Q}_p,$$

given by the cup-product, we have

(1) $H^1_g(K,V^*(1)) = H^1_e(K,V)^{\perp}$,
(2) $H^1_e(K,V^*(1)) = H^1_g(K,V)^{\perp}$,
(3) $H^1_f(K,V^*(1)) = H^1_f(K,V)^{\perp}$.

We have Hyodo's celebrated result (cf. [Hyo88]):

Theorem 9.28. *For a potentially semi-stable representation V,*

$$H^1_g(K,V) = H^1_{\mathrm{st}}(K,V). \tag{9.18}$$

Proof. (I) We first reduce the proof to the semi-stable case.

By definition, we have the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & H^1_{\mathrm{st}}(K,V) \arrow[r] \arrow[d] & H^1(K,V) \arrow[r, "\alpha_K"] \arrow[d, "\cong"] & \Im(\alpha_K) \arrow[r] \arrow[d, "\beta_K|_{\Im(\alpha_K)}"] & 0 \\
0 \arrow[r] & H^1_g(K,V) \arrow[r] & H^1(K,V) \arrow[r] & H^1(K,B_{\mathrm{dR}} \otimes V) &
\end{tikzcd}$$

By the Snake Lemma, we know that $H^1_{\mathrm{st}}(K,V) = H^1_g(K,V)$ is equivalent to the injectivity of $\beta_K|_{\mathrm{Im}(\alpha_K)}$.

Consider the commutative diagram

$$\begin{tikzcd} H^1(K,V) \arrow[r, "\alpha_K"] \arrow[d, "\mathrm{res}"] & H^1(K,B_{\mathrm{st}}\otimes V) \arrow[r, "\beta_K"] \arrow[d, "\mathrm{res}"] & H^1(K,B_{\mathrm{dR}}\otimes V) \arrow[d, "\mathrm{res}"] \\ H^1(L,V) \arrow[r, "\alpha_L"] & H^1(L,B_{\mathrm{st}}\otimes V) \arrow[r, "\beta_L"] & H^1(L,B_{\mathrm{dR}}\otimes V) \end{tikzcd}$$

where L is a finite extension of K. The vertical arrows are injective by the relation $\mathrm{Cor}\circ\mathrm{res} = [L:K]$. Then the injectivity of $\beta_L|_{\mathrm{Im}(\alpha_L)}$ implies the injectivity of $\beta_K|_{\mathrm{Im}(\alpha_K)}$.

(II) Assume V is semi-stable. By Bloch-Kato's Theorem, then

$$\dim_{\mathbb{Q}_p} H^1_g(K,V)/H^1_f(K,V) = \dim_{\mathbb{Q}_p} H^1_f(K,V^*(1))/H^1_e(K,V^*(1)).$$

By Proposition 9.26, the latter one is equal to

$$\dim_{\mathbb{Q}_p} D_{\mathrm{st}}(V^*(1))_{N=0,\varphi=1} = \dim_{\mathbb{Q}_p} D_{\mathrm{st}}(V^*)_{N=0,\varphi=p^{-1}}.$$

By duality, this is equal to

$$\dim_{\mathbb{Q}_p}((D/ND)^*)^{\varphi=p^{-1}} = \dim_{\mathbb{Q}_p}(D/ND)^{\varphi=p^{-1}},$$

which is equal to $\dim_{\mathbb{Q}_p} H^1_{\mathrm{st}}(K,V)/H^1_f(K,V)$ by using Proposition 9.26 again. This concludes the proof.

Let X and Y be p-adic representations of G_K. Recall an extension of X by Y is a p-adic representation E such that

$$0 \to Y \to E \to X \to 0$$

is exact. The isomorphism classes of all extensions of X by Y form the group $\mathrm{Ext}(X,Y)$, which is identified with $\mathrm{Ext}^1_K(X,Y) = \mathrm{Ext}^1_{\mathbb{Q}_p[G_K]}(X,Y)$. For $* =$ ur, f, st or g, we let $\mathrm{Ext}^1_{K,*}(X,Y)$ be the isomorphism classes $[E]$ such that E is an unramified, crystalline, semi-stable or de Rham representation (which we call a $*$-representation).

Lemma 9.29. *Under the isomorphism* $\mathrm{Ext}^1_K(X,Y) \cong \mathrm{Ext}^1_K(\mathbb{Q}_p,\mathrm{Hom}(X,Y)) = H^1(K,\mathrm{Hom}(X,Y))$*, then* $\mathrm{Ext}^1_{K,*}(X,Y) \cong H^1_*(K,\mathrm{Hom}(X,Y))$.

Proof. We first give the isomorphism $\mathrm{Ext}^1_K(X,Y) \cong \mathrm{Ext}^1_K(\mathbb{Q}_p,\mathrm{Hom}(X,Y))$. Suppose $0 \to Y \to E \to X \to 0$ is an extension of X by Y. Then

$$0 \to \mathrm{Hom}(X,Y) \to \mathrm{Hom}(X,E) \to \mathrm{Hom}(X,X)$$

is exact. Take the pullback of the lime $\mathbb{Q}_p 1_X \subseteq \mathrm{Hom}(X,X)$, then we get an extension of $\mathbb{Q}_p$ by $\mathrm{Hom}(X,Y)$. Conversely, from an extension $0 \to \mathrm{Hom}(X,Y) \to E' \to \mathbb{Q}_p \to 0$, we have

$$0 \to X \otimes \mathrm{Hom}(X,Y) \to X \otimes E' \to X \to 0.$$

Then the pushout of $X \otimes \mathrm{Hom}(X,Y) \to Y$ gives an extension of X by Y.

As we know, the sub-quotients, tensor product and Hom of $*$-representations are still $*$-representations, the correspondence gives the bijection $\mathrm{Ext}^1_{K,*}(X,Y) \cong H^1_*(K, \mathrm{Hom}(X,Y))$.

Hyodo's Theorem and Lemma 9.29 imply Proposition 2A under the condition that k is finite:

Proposition 2A. *If $0 \to V' \to V \to V'' \to 0$ is a short exact sequence of p-adic representations of G_K where K is a finite extension of $\mathbb{Q}_p$, and if V', V'' are semi-stable and V is de Rham, then V is also semi-stable.*

Corollary 9.30 (Proposition 6.36(3)). *Suppose V is a non-trivial extension of $\mathbb{Q}_p(1)$ by $\mathbb{Q}_p$, then V is not de Rham.*

Proof. If not, then V is semi-stable and

$$0 \to \mathbf{D}_{\mathrm{st}}(\mathbb{Q}_p) \to \mathbf{D}_{\mathrm{st}}(V) \to \mathbf{D}_{\mathrm{st}}(\mathbb{Q}_p(1)) \to 0$$

is exact. However, there is no non-trivial admissible filtered (φ, N)-module of dimension 2 which is an extension of $\mathbf{D}_{\mathrm{st}}(\mathbb{Q}_p(1)) = K_0\langle 1\rangle$ by $\mathbf{D}_{\mathrm{st}}(\mathbb{Q}_p) = K_0$.

9.3.2 The fundamental complex of *D*.

To prove Proposition 2B, we need to introduce the so-called *fundamental complex of D*. Set

$$\mathbf{V}^0_{\mathrm{st}}(D) := \{b \in B_{\mathrm{st}} \otimes_{K_0} D \mid Nb = 0,\ \varphi b = b\}, \tag{9.19}$$

$$\mathbf{V}^1_{\mathrm{st}}(D) := B_{\mathrm{dR}} \otimes_K D_K / \operatorname{Fil}^0(B_{\mathrm{dR}} \otimes_K D_K) \tag{9.20}$$

where

$$\operatorname{Fil}^0(B_{\mathrm{dR}} \otimes_K D_K) = \sum_{i \in \mathbb{Z}} \operatorname{Fil}^i B_{\mathrm{dR}} \otimes_K \operatorname{Fil}^{-i} D_K.$$

There is a natural map $\mathbf{V}^0_{\mathrm{st}}(D) \to \mathbf{V}^1_{\mathrm{st}}(D)$ induced by

$$B_{\mathrm{st}} \otimes_{K_0} D \subset B_{\mathrm{dR}} \otimes_K D_K \twoheadrightarrow \mathbf{V}^1_{\mathrm{st}}(D_K).$$

Then we have an exact sequence

$$0 \to \mathbf{V}_{\mathrm{st}}(D) \to \mathbf{V}^0_{\mathrm{st}}(D) \to \mathbf{V}^1_{\mathrm{st}}(D),$$

which is called the *fundamental complex of D*.

Proposition 9.31. *If $0 \to D' \to D \to D'' \to 0$ is a short exact sequence of filtered (φ, N)-modules over K, then for $i = 0, 1$, the sequence*

$$0 \to \mathbf{V}_{\mathrm{st}}^{i}(D') \to \mathbf{V}_{\mathrm{st}}^{i}(D) \to \mathbf{V}_{\mathrm{st}}^{i}(D'') \to 0 \tag{9.21}$$

is exact.

Proof. For $i = 1$. By assumption, the exact sequence $0 \to D'_K \to D_K \to D''_K \to 0$ implies that the sequences

$$0 \to B_{\mathrm{dR}} \otimes_K D'_K \to B_{\mathrm{dR}} \otimes_K D_K \to B_{\mathrm{dR}} \otimes_K D''_K \to 0$$

and

$$0 \to \mathrm{Fil}^i B_{\mathrm{dR}} \otimes_K \mathrm{Fil}^{-i} D'_K \to \mathrm{Fil}^i B_{\mathrm{dR}} \otimes_K \mathrm{Fil}^{-i} D_K \to \mathrm{Fil}^i B_{\mathrm{dR}} \otimes_K \mathrm{Fil}^{-i} D''_K \to 0$$

are exact. Thus we have a commutative diagram (where we write $B_{\mathrm{dR}} \otimes D$ for $B_{\mathrm{dR}} \otimes_K D_K$)

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes D') \arrow[r] \arrow[d] & \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes D) \arrow[r] \arrow[d] & \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes D'') \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & B_{\mathrm{dR}} \otimes D' \arrow[r] \arrow[d] & B_{\mathrm{dR}} \otimes D \arrow[r] \arrow[d] & B_{\mathrm{dR}} \otimes D'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{V}_{\mathrm{st}}^{1}(D') \arrow[r] \arrow[d] & \mathbf{V}_{\mathrm{st}}^{1}(D) \arrow[r] \arrow[d] & \mathbf{V}_{\mathrm{st}}^{1}(D'') \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

where the three columns and the top and middle rows of the above diagram are exact, hence the bottom row is also exact and we get the result for $i = 1$.

For $i = 0$, note that

$$\mathbf{V}_{\mathrm{st}}^{0}(D) = \{x \in B_{\mathrm{st}} \otimes_{K_0} D \mid Nx = 0,\ \varphi x = x\}.$$

Let

$$\mathbf{V}_{\mathrm{cris}}^{0}(D) = \{y \in B_{\mathrm{cris}} \otimes_{K_0} D \mid \varphi y = y\}.$$

Recall that $\mathbf{u} = \log[\varpi]$,

$$B_{\mathrm{st}} = B_{\mathrm{cris}}[\mathbf{u}],\ N = -\frac{d}{d\mathbf{u}} \text{ and } \varphi\mathbf{u} = p\mathbf{u}.$$

With obvious convention, any $x \in B_{\mathrm{st}} \otimes_{K_0} D$ can be written as

$$x = \sum_{n=0}^{+\infty} x_n \mathbf{u}^n, \ x_n \in B_{\mathrm{cris}} \otimes_{K_0} D$$

and almost all $x_n = 0$. The map

$$x \mapsto x_0$$

defines a $\mathbb{Q}_p$-linear bijection between $\mathbf{V}^0_{\mathrm{st}}(D)$ and $\mathbf{V}^0_{\mathrm{cris}}(D)$ which is functorial (however, which is not Galois equivalent). Thus it suffices to show that

$$0 \to \mathbf{V}^0_{\mathrm{cris}}(D') \to \mathbf{V}^0_{\mathrm{cris}}(D) \to \mathbf{V}^0_{\mathrm{cris}}(D'') \to 0$$

is exact. The only thing which matters is the structure of φ-isocrystals. There are two cases.

(a) k is algebraically closed. In this case, the exact sequence

$$0 \to D' \to D \to D'' \to 0$$

splits as a sequence of φ-isocrystals as a consequence of Dieudonnè-Manin Theorem (Corollary 8.26). Then $D \simeq D' \oplus D''$ and $\mathbf{V}^0_{\mathrm{cris}}(D) = \mathbf{V}^0_{\mathrm{cris}}(D') \oplus \mathbf{V}^0_{\mathrm{cris}}(D'')$.

(b) k is arbitrary. Then

$$\mathbf{V}^0_{\mathrm{cris}}(D) = \{y \in B_{\mathrm{cris}} \otimes_{K_0} D \mid \varphi y = y\} = \{y \in B_{\mathrm{cris}} \otimes_{P_0} (P_0 \otimes_{K_0} D) \mid \varphi y = y\}$$

with $P_0 = \operatorname{Frac} W(\bar{k})$ and $B_{\mathrm{cris}} \supset P_0 \supset K_0$. $P_0 \otimes_{K_0} D$ is a φ-isocrystal over P_0 whose residue field is $\bar{k}$, thus the following exact sequence

$$0 \to P_0 \otimes_{K_0} D' \to P_0 \otimes_{K_0} D \to P_0 \otimes_{K_0} D'' \to 0$$

splits and hence the result follows.

Proposition 9.32. *If V is semi-stable and $D = \mathbf{D}_{\mathrm{st}}(V)$, then the sequence*

$$0 \to \mathbf{V}_{\mathrm{st}}(D) \to \mathbf{V}^0_{\mathrm{st}}(D) \to \mathbf{V}^1_{\mathrm{st}}(D) \to 0 \tag{9.22}$$

is exact.

Proof. Use the fact

$$B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V = B_{\mathrm{st}} \otimes_{K_0} D \ \subset \ B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V = B_{\mathrm{dR}} \otimes_K D_K,$$

then

$$\mathbf{V}^0_{\mathrm{st}}(D) = \{x \in B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V \mid Nx = 0, \ \varphi x = x\}.$$

As $N(b \otimes v) = Nb \otimes v$ and $\varphi(b \otimes v) = \varphi b \otimes v$, then

$$\mathbf{V}_{\mathrm{st}}^0(D) = B_e \otimes_{\mathbb{Q}_p} V.$$

By definition and the above fact,

$$\mathbf{V}_{\mathrm{st}}^1(D) = (B_{\mathrm{dR}}/B_{\mathrm{dR}}^+) \otimes_{\mathbb{Q}_p} V.$$

From the fundamental exact sequence (7.27)

$$0 \to \mathbb{Q}_p \to B_e \to B_{\mathrm{dR}}/B_{\mathrm{dR}}^+ \to 0$$

tensoring V over $\mathbb{Q}_p$, we have

$$0 \to V \to B_e \otimes_{\mathbb{Q}_p} V \to (B_{\mathrm{dR}}/B_{\mathrm{dR}}^+) \otimes_{\mathbb{Q}_p} V \to 0$$

is also exact. Since $V = \mathbf{V}_{\mathrm{st}}(D)$,

$$0 \to \mathbf{V}_{\mathrm{st}}(D) \to \mathbf{V}_{\mathrm{st}}^0(D) \to \mathbf{V}_{\mathrm{st}}^1(D) \to 0$$

is exact.

We now prove Proposition 2B:

Proposition 2B. *If* $0 \to D' \to D \to D'' \to 0$ *is a short exact sequence of admissible filtered* (φ, N)*-modules over* K*, and if*

$$\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D') = \dim_{K_0} D', \quad \dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D'') = \dim_{K_0} D'',$$

then $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) = \dim_{K_0} D$.

Proof. The short exact sequence $0 \to D' \to D \to D'' \to 0$ induces the following commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathbf{V}_{\mathrm{st}}(D') \arrow[r] \arrow[d] & \mathbf{V}_{\mathrm{st}}^0(D') \arrow[r] \arrow[d] & \mathbf{V}_{\mathrm{st}}^1(D') \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{V}_{\mathrm{st}}(D) \arrow[r] \arrow[d] & \mathbf{V}_{\mathrm{st}}^0(D) \arrow[r] \arrow[d] & \mathbf{V}_{\mathrm{st}}^1(D) \arrow[d] & \\
0 \arrow[r] & \mathbf{V}_{\mathrm{st}}(D'') \arrow[r] & \mathbf{V}_{\mathrm{st}}^0(D'') \arrow[r] \arrow[d] & \mathbf{V}_{\mathrm{st}}^1(D'') \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 &
\end{tikzcd}$$

which is exact in rows and columns by Propositions 9.31 and 9.32. A diagram chasing shows that $\mathbf{V}_{\mathrm{st}}(D) \to \mathbf{V}_{\mathrm{st}}(D'')$ is onto, thus $\dim_{K_0} D = \dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D)$.

9.4 Reuction to $t_H = 0$

9.4.1 $\mathbb{Q}_{p^r}$-representations and filtered (φ^r, N)-modules.

Let $r \in \mathbb{N}$, $r \geq 1$. The Galois group $\mathrm{Gal}(\mathbb{Q}_{p^r}/\mathbb{Q})$ is a cyclic group of order r generated by the restriction of φ to $\mathbb{Q}_{p^r}$, which is just σ, and

$$\mathbb{Q}_{p^r} \subset P_0 \subset B^+_{\mathrm{cris}} \subset B_{\mathrm{st}}$$

is stable under G_K- and φ-actions.

Definition 9.33. *A* $\mathbb{Q}_{p^r}$-representation *of* G_K *is a finite dimensional* $\mathbb{Q}_{p^r}$*-vector space on which* G_K *acts continuously and semi-linearly:*

$$g(v_1 + v_2) = g(v_1) + g(v_2), \quad g(\lambda v) = g(\lambda) g(v).$$

A $\mathbb{Q}_{p^r}$*-representation of* G_K *is* de Rham (semi-stable, crystalline, etc.) *if it is de Rham (semi-stable, crystalline, etc.) as a p-adic representation.*

We note that if V is a $\mathbb{Q}_{p^r}$-representation of dimension h, then V is of dimension rh as a $\mathbb{Q}_p$-representation.

Suppose V is a $\mathbb{Q}_{p^r}$-representation. Then we have a decomposition

$$B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V = B_{\mathrm{st}} \otimes_{\mathbb{Q}_{p^r}} (\mathbb{Q}_{p^r} \otimes_{\mathbb{Q}_p} V) = \bigoplus_{m=0}^{r-1} B_{\mathrm{st}} \ {}_{\sigma^m}\!\otimes_{\mathbb{Q}_{p^r}} V,$$

where ${}_{\sigma^m}\!\otimes_{\mathbb{Q}_{p^r}}$ is the twisted tensor product by σ^m. Each component of this decomposition is stable by the G_K-action, and

$$\varphi^j : B_{\mathrm{st}} \ {}_{\sigma^m}\!\otimes_{\mathbb{Q}_{p^r}} V \to B_{\mathrm{st}} \ {}_{\sigma^{\overline{m+j}}}\!\otimes_{\mathbb{Q}_{p^r}} V$$

is a bijection, where $0 \leq \overline{m+j} < r$ is the remainder of $m+j$ by r. By the same reason, we also have

$$B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V = \bigoplus_{m=0}^{r-1} B_{\mathrm{dR}} \ {}_{\sigma^m}\!\otimes_{\mathbb{Q}_{p^r}} V,$$

with each component stable by the G_K-action, and

$$1 \otimes \varphi^j : B_{\mathrm{dR}} \ {}_{\sigma^m}\!\otimes_{\mathbb{Q}_{p^r}} V = B_{\mathrm{dR}} \otimes_{B_{\mathrm{st}}} \left(B_{\mathrm{st}} \ {}_{\sigma^m}\!\otimes_{\mathbb{Q}_{p^r}} V \right) \to B_{\mathrm{dR}} \ {}_{\sigma^{\overline{m+j}}}\!\otimes_{\mathbb{Q}_{p^r}} V$$

is a bijection.

Definition 9.34. *For a* $\mathbb{Q}_{p^r}$*-representation* V*,* $0 \leq m < r$*, set*

$$\mathbf{D}^{(m)}_{\mathrm{st},r}(V) := (B_{\mathrm{st}} \ {}_{\sigma^m}\!\otimes_{\mathbb{Q}_{p^r}} V)^{G_K}, \tag{9.23}$$

$$\mathbf{D}^{(m)}_{\mathrm{dR},r}(V) := (B_{\mathrm{dR}} \ {}_{\sigma^m}\!\otimes_{\mathbb{Q}_{p^r}} V)^{G_K}. \tag{9.24}$$

Set $\mathbf{D}_{\mathrm{st},r}(V) := \mathbf{D}^{(0)}_{\mathrm{st},r}(V)$ *and* $\mathbf{D}_{\mathrm{dR},r}(V) := \mathbf{D}^{(0)}_{\mathrm{dR},r}(V)$*.*

Then $\mathbf{D}_{\mathrm{st},r}^{(m)}(V)$ $(0 \le m < r)$ are K_0-vector spaces, stable by the actions of φ^r and N, and

$$\mathbf{D}_{\mathrm{st}}(V) = \bigoplus_{m=0}^{r-1} \mathbf{D}_{\mathrm{st},r}^{(m)}(V); \tag{9.25}$$

and $\mathbf{D}_{\mathrm{dR},r}^{(m)}(V))$ $(0 \le m < r)$ are filtered K-vector spaces,

$$\mathbf{D}_{\mathrm{dR}}(V) = \bigoplus_{m=0}^{r-1} \mathbf{D}_{\mathrm{dR},r}^{(m)}(V). \tag{9.26}$$

Moreover, one has the injection

$$K \otimes_{K_0} \mathbf{D}_{\mathrm{st},r}^{(m)}(V) \hookrightarrow \mathbf{D}_{\mathrm{dR},r}^{(m)}(V).$$

We thus have

Proposition 9.35. *For $0 \le m < r$, the maps $\varphi^j : \mathbf{D}_{\mathrm{st},r}^{(m)}(V) \to \mathbf{D}_{\mathrm{st},r}^{(\overline{m+j})}(V)$ and $1 \otimes \varphi^j : \mathbf{D}_{\mathrm{dR},r}^{(m)}(V) \to \mathbf{D}_{\mathrm{dR},r}^{(\overline{m+j})}(V)$ is bijective and*

$$\begin{aligned}
\dim_{K_0} \mathbf{D}_{\mathrm{st},r}^{(m)}(V) &= \dim_{K_0} \mathbf{D}_{\mathrm{st},r}(V) \le \dim_{\mathbb{Q}_{p^r}} V \\
\dim_{K_0} \mathbf{D}_{\mathrm{dR},r}^{(m)}(V) &= \dim_{K_0} \mathbf{D}_{\mathrm{dR},r}(V) \le \dim_{\mathbb{Q}_{p^r}} V.
\end{aligned}$$

Consequently,

(1) *V is semi-stable if and only if $\dim_{K_0} \mathbf{D}_{\mathrm{st},r}(V) = \dim_{\mathbb{Q}_{p^r}} V$, and in this case for every m,*

$$\mathbf{D}_{\mathrm{dR},r}^{(m)}(V) = K \otimes_{K_0} \mathbf{D}_{\mathrm{st},r}^{(m)}(V) = K\ {}_{\varphi^m}\!\otimes_{K_0} \mathbf{D}_{\mathrm{st},r}(V). \tag{9.27}$$

(2) *V is de Rham if and only if $\dim_{K_0} \mathbf{D}_{\mathrm{dR},r}(V) = \dim_{\mathbb{Q}_{p^r}} V$.*

Definition 9.36. *A* filtered (φ^r, N)-module *over K is a K_0-vector space Δ equipped with two operators*

$$\varphi^r,\ N :\ \Delta \to \Delta$$

such that N is K_0-linear, φ^r is σ^r-semi-linear and bijective, and

$$N\varphi^r = p^r \varphi^r N,$$

and there is a structure of filtered K vector space on

$$\Delta_{K,m} := K \otimes_{K_0} \Delta_m = K\ {}_{\varphi^m}\!\otimes_{K_0} \Delta$$

for each $m = 0, 1, 2, \cdots, r-1$, where $\Delta_m := K_0\ {}_{\varphi^m}\!\otimes_{K_0} \Delta$.

Definition 9.37. *Suppose Δ is a filtered (φ^r, N)-module over K, the associated filtered (φ, N)-module over K is the module*

$$D := \mathbb{Q}_p[\varphi] \otimes_{\mathbb{Q}_p[\varphi^r]} \Delta = \sum_{m=0}^{r-1} \Delta_m.$$

Δ is called admissible *if the associated D is admissible.*

By Proposition 9.35, if V is a semi-stable $\mathbb{Q}_{p^r}$-representation of G_K, set $\Delta = \mathbf{D}_{\mathrm{st},r}(V)$, then Δ has a natural structure of a filtered (φ^r, N)-module over K, $\Delta_m = \mathbf{D}^{(m)}_{\mathrm{st},r}(V)$ and $\Delta_{K,m} = \mathbf{D}^{(m)}_{\mathrm{dR},r}(V)$, and the associated admissible filtered $\varphi, N)$-module $D = \mathbf{D}_{\mathrm{st}}(V)$,

Example 9.38. For the trivial $\mathbb{Q}_{p^r}$-representation $\mathbb{Q}_{p^r}$, the associated (φ^r, N)-module $\mathbf{D}_{\mathrm{st},r}(\mathbb{Q}_{p^r}) = K_0$ where $\varphi^r = \sigma^r$, $N = 0$, and all filtrations are trivial.

Proposition 9.39. *Let $\mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_{p^r}}(G_K)$ denote the category of semi-stable $\mathbb{Q}_{p^r}$-representations of G_K and $\mathbf{MF}^{ad}_K(\varphi^r, N)$ denote the category of admissible filtered (φ^r, N)-modules over K. Then the functor*

$$\mathbf{D}_{\mathrm{st},r} : \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_{p^r}}(G_K) \to \mathbf{MF}^{ad}_K(\varphi^r, N)$$

is an exact and fully faithful functor.

Proof. This follows from the above association and the fact that

$$\mathbf{D}_{\mathrm{st}} : \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K) \to \mathbf{MF}^{ad}_K(\varphi, N)$$

is an exact and fully faithful functor.

For a filtered (φ^r, N)-module Δ, one can then define the Galois, φ^r-, N-actions on $B_{\mathrm{st}} \otimes \Delta$, and the filtration on

$$K \otimes_{K_0} (B_{\mathrm{st}} \otimes \Delta) \hookrightarrow B_{\mathrm{dR}} \otimes_K \Delta_K.$$

We identify $v \in B_{\mathrm{st}} \otimes \Delta$ with $1 \otimes v \in K \otimes_{K_0} (B_{\mathrm{st}} \otimes \Delta)$.

Definition 9.40. *Set*

$$\mathbf{V}_{\mathrm{st},r}(\Delta) := (B_{\mathrm{st}} \otimes \Delta)_{\varphi^r=1,\, N=0} \cap \mathrm{Fil}^0(K \otimes_{K_0} (B_{\mathrm{st}} \otimes \Delta)). \tag{9.28}$$

Since the G_K-action commutes with φ^r- and N-actions, $\mathbf{V}_{\mathrm{st},r}(\Delta)$ is a $\mathbb{Q}_{p^r}$-vector space with a continuous action of G_K.

Proposition 9.41. *If V is a semi-stable $\mathbb{Q}_{p^r}$-representation, then*

$$\mathbf{V}_{\mathrm{st},r}(\mathbf{D}_{\mathrm{st},r}(V)) = V.$$

Proof. Analogous to the proof of $\mathbf{V}_{\mathrm{st}}(\mathbf{D}_{\mathrm{st}}(V)) = V$ in § 9.2.1, just applying the fundamental exact sequence (7.39) of the ring $B_{e,r}$.

Let V_1 and V_2 be two $\mathbb{Q}_{p^r}$-representations. Then $V_1 \otimes_{\mathbb{Q}_{p^r}} V_2$ is also a $\mathbb{Q}_{p^r}$-representation. If V_1 and V_2 are both semi-stable, then $V_1 \otimes_{\mathbb{Q}_p} V_2$ is a semi-stable $\mathbb{Q}_p$-representation, thus $V_1 \otimes_{\mathbb{Q}_{p^r}} V_2$, as a quotient of $V_1 \otimes_{\mathbb{Q}_p} V_2$, is also semi-stable. Therefore in this case, for every $m = 0, \cdots, r-1$,

$$\mathbf{D}_{\mathrm{st},r}^{(m)}(V_1) \otimes_{K_0} \mathbf{D}_{\mathrm{st},r}^{(m)}(V_2) \longrightarrow \mathbf{D}_{\mathrm{st},r}^{(m)}(V_1 \otimes_{\mathbb{Q}_{p^r}} V_2)$$

is an isomorphism. Similarly, if V_1 and V_2 are both de Rham, then $V_1 \otimes_{\mathbb{Q}_{p^r}} V_2$ is also de Rham and

$$\mathbf{D}_{\mathrm{dR},r}^{(m)}(V_1) \otimes_{K} \mathbf{D}_{\mathrm{dR},r}^{(m)}(V_2) \longrightarrow \mathbf{D}_{\mathrm{dR},r}^{(m)}(V_1 \otimes_{\mathbb{Q}_{p^r}} V_2)$$

is an isomorphism.

Let Δ and Δ' be two filtered (φ^r, N)-modules. Then $\Delta \otimes_{K_0} \Delta'$ is naturally equipped with the actions of φ^r and N satisfying $N\varphi^r = p^r \varphi^r N$. Moreover,

$$(\Delta \otimes_{K_0} \Delta')_{K,m} \xrightarrow{\sim} \Delta_{K,m} \otimes_K \Delta'_{K,m}$$

as filtered K-vector spaces. Thus $\Delta \otimes_{K_0} \Delta'$ is a filtered (φ^r, N)-module.

Proposition 9.42. (1) *If V is a de Rham $\mathbb{Q}_{p^r}$-representation, set $\Delta_{K,m} = \mathbf{D}_{\mathrm{dR},r}^{(m)}(V)$ and $t_{H,m}(V) = t_H(\Delta_{K,m})$, then $t_H(V) = \sum_{m=0}^{r-1} t_{H.m}(V)$.*

(2) *If V_1 and V_2 are de Rham $\mathbb{Q}_{p^r}$-representations of $\mathbb{Q}_{p^r}$-dimension h_1 and h_2 respectively, let $V = V_1 \otimes_{\mathbb{Q}_{p^r}} V_2$. Then*

$$t_H(V) = h_2 t_H(V_1) + h_1 t_H(V_2). \tag{9.29}$$

In particular, if $s = rb$ is a multiple of r and V is a de Rham $\mathbb{Q}_{p^r}$-representation, then

$$t_H(\mathbb{Q}_{p^s} \otimes_{\mathbb{Q}_{p^r}} V) = bt_H(V). \tag{9.30}$$

Proof. (1) Clear.

(2) Suppose V_1 and V_2 are two de Rham $\mathbb{Q}_{p^r}$-representations, of dimension h_1 and h_2 respectively. Let $V = V_1 \otimes_{\mathbb{Q}_{p^r}} V_2$. Then V is de Rham and $\Delta_{K,m} \cong (\Delta_1)_{K,m} \otimes_K (\Delta_2)_{K,m}$ and hence by Proposition 8.38,

$$t_{H,m}(V) = h_2 t_{H,m}(V_1) + h_1 t_{H,m}(V_2). \tag{9.31}$$

The special case is clear.

Example 9.43. We compute the t_H-value of the Lubin-Tate representation $V_r = (B_{\mathrm{cris}}^+)^{\varphi^r = p} \cap \mathrm{Fil}^1 B_{\mathrm{dR}}$. We know in §7.3.2 that V_r is a $\mathbb{Q}_{p^r}$-representation of dimension 1 generated by the Lubin-Tate element t_r satisfying (i) t_r is invertible in B_{cris}, (ii) $t_r \in \mathrm{Fil}^1 B_{\mathrm{dR}} - \mathrm{Fil}^2 B_{\mathrm{dR}}$ and (iii) $\varphi^m(t_r) \in \mathrm{Fil}^0 B_{\mathrm{dR}} - \mathrm{Fil}^1 B_{\mathrm{dR}}$ for $1 \leq m < r$. Thus V_r is a crystalline representation. Let $e = t_r^{-1} \otimes t_r \in \mathbf{D}_{\mathrm{st},r}(V_r)$ and $e_m = \varphi^m(t_r^{-1}) \otimes t_r = \varphi^m(e) \in \mathbf{D}_{\mathrm{st},r}^{(m)}(V_r)$. Then $D = \mathbf{D}_{\mathrm{cris}}(V_r)$ is a K_0-vector space with basis $\{e_m \mid 0 \leq m < r\}$, and

$$\mathbf{D}_{\mathrm{st},r}^{(m)}(V_r) = K_0 e_m,\ \varphi^r e_m = p^{-1} e_m,\ Ne = 0.$$

Then $\Delta = \mathbf{D}_{\mathrm{st},r}(V_r) = K_0 e$, and

$$\Delta_{K,m} = K\ {}_{\varphi^m}\otimes_{K_0} K_0 e = K e_m, \quad e_m = 1 \otimes e = \varphi^m(e)$$

for $m = 0, 1, \cdots, r-1$. If $m > 0$, then

$$\mathrm{Fil}^i\, \Delta_{K,m} = \begin{cases} K e_m, & \text{if } i \leq 0; \\ 0, & \text{if } i > 0. \end{cases}$$

If $m = 0$, then

$$\mathrm{Fil}^i\, \Delta_{K,0} = \begin{cases} K e_0, & \text{if } i < 0; \\ 0, & \text{if } i \geq 0. \end{cases}$$

Thus $t_{H,0}(V_r) = -1$ and $t_{H,m}(V_r) = 0$ for $m \neq 0$, and $t_H(V_r) = -1$.

Furthermore, for $a \in \mathbb{Z}$, set

$$V_r^a = \begin{cases} \mathrm{Sym}^a_{\mathbb{Q}_{p^r}} V_r, & \text{if } a \geq 0; \\ \mathscr{L}_{\mathbb{Q}_{p^r}}(V_r^{-a}, \mathbb{Q}_{p^r}), & \text{if } a < 0. \end{cases}$$

Then V_r^a is a $\mathbb{Q}_{p^r}$-representation of dimension 1 generated by t_r^a, and $\mathbf{D}_{\mathrm{st},r}^{(m)}(V_r^a)$ is generated by $\varphi^m(t_r^{-a} \otimes t_r^a) = \varphi^m(t_r^{-a}) \otimes t_r^a$. By the same computation as for V_r, we have $t_{H,0}(V_r^a) = -a$ and $t_{H,m}(V_r^a) = 0$ for $0 < m < r$, hence $t_H(V_r^a) = -a$.

9.4.2 Reduction to $t_H = 0$.

Case A.

In this case $D_K = \mathbf{D}_{\mathrm{dR}}(V)$ and $t_H(V) = t_H(D_K)$.

For any $i \in \mathbb{Z}$, we know that V is de Rham if and only if $V(i)$ is de Rham. Let $d = \dim_K D_K$, then $t_H(V(i)) = t_H(D_K) - i \cdot d$. Choose $i = \frac{t_H(V)}{d}$, then $t_H(V(i)) = 0$. If the result is known for $V(i)$, then it is also known for $V = V(i)(-i)$. However, this trick works only if $\frac{t_H(V)}{d} \in \mathbb{Z}$.

Definition 9.44. *If V is a p-adic representation of G_K, let $r \geq 1$ be the biggest integer such that we can endow V with the structure of a $\mathbb{Q}_{p^r}$-representation, then the* reduced dimension *of V is defined to be the integer* $\frac{\dim_{\mathbb{Q}_p} V}{r} = \dim_{\mathbb{Q}_{p^r}} V$.

We have

Proposition 9.45. *For $h \in \mathbb{N},\ h \geq 1$, the following are equivalent:*

(1) *Any p-adic de Rham representation V of G_K of reduced dimension $\leqslant h$ and with $t_H(V) = 0$ is potentially semi-stable.*

(2) *Any p-adic de Rham representation of G_K of reduced dimension $\leqslant h$ is potentially semi-stable.*

Proof. We just need to show (1) $\Rightarrow$ (2). Let V be a p-adic de Rham representation of G_K of reduced dimension h, we need to show that V is potentially semi-stable.

There exists an integer $r \geq 1$, such that we may consider V as a $\mathbb{Q}_{p^r}$-representation of dimension h. For $s \geq 1$ and for any $a \in \mathbb{Z}$, let V_s be the Lubin-Tate $\mathbb{Q}_{p^s}$-representation as given in § 7.3.2, then V_s^a is also a $\mathbb{Q}_{p^s}$-representation of dimension 1. Choose $s = rb$ with $b \geq 1$ and $a \in \mathbb{Z}$, and let

$$V' = V \otimes_{\mathbb{Q}_{p^r}} V_s^a,$$

it is a $\mathbb{Q}_{p^s}$-representation of dimension h. Since V_s is crystalline, it is also de Rham, thus V_s^a is de Rham and V' is also de Rham.

By (9.29) and the fact $t_H(V_s^a) = -a$, then

$$t_H(V') = \dim_{\mathbb{Q}_{p^r}} V \cdot t_H(V_s^a) + \dim_{\mathbb{Q}_{p^r}} V_s^a \cdot t_H(V) = bt_H(V) - ah.$$

Choose a and b in such a way that $t_H(V') = 0$. Applying (1), then V' is potentially semi-stable. Thus

$$V' \otimes_{\mathbb{Q}_{p^s}} V_s^{-a} = V \otimes_{\mathbb{Q}_{p^r}} \mathbb{Q}_{p^s} \supset V$$

is also potentially semi-stable.

Case B.

Definition 9.46. *If D is a filtered (φ, N)-module over K, let $r \geq 1$ be the biggest integer such that we can associate D with a filtered (φ^r, N)-module Δ over K, i.e. $D = \Delta \otimes_{\mathbb{Q}_p[\varphi^r]} \mathbb{Q}_p[\varphi]$, then the* reduced dimension *of D is defined to be the integer $\frac{\dim_{K_0} D}{r} = \dim_{K_0} \Delta$.*

We have

Proposition 9.47. *For $h \in \mathbb{N}$, $h \geq 1$, the following are equivalent:*

(1) *Any admissible filtered (φ, N)-module D over K of reduced dimension $\leq h$ and with $t_H(D) = 0$ satisfies $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) = \dim_{K_0}(D)$.*
(2) *Any admissible filtered (φ, N)-module D over K of reduced dimension $\leq h$ satisfies $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) = \dim_{K_0}(D)$.*

Proof. We just need to show (1) $\Rightarrow$ (2). Let D be an admissible filtered (φ, N)-module D over K of reduced dimension h and of dimension $d = rh$. Let Δ be the associated (φ^r, N)-module. We need to show $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) = \dim_{K_0}(D) = rh$.

By Proposition 2B, we may assume that D is irreducible. Then $N = 0$, otherwise $\mathrm{Ker}\,(N : D \to D)$ is a nontrivial admissible sub-object of D.

Moreover, for any nonzero $x \in D$, D is generated as a K_0-vector space by $\{x, \varphi(x), \cdots, \varphi^{rh-1}(x)\}$ and Δ is generated as a K_0-vector space by $\{x, \varphi^r(x), \cdots, \varphi^{r(h-1)}(x)\}$. Indeed, let $D(x)$ be generated by $\varphi^i(x)$, then $D(x)$ is invariant by φ and D is a direct sum of φ-modules of the form $D(x)$, thus $D(x)$ is admissible and it must be D by the irreducibility of D.

Let $a = t_H(D)$, $b = h$. Let $D_{rh} = \mathbf{D}_{\mathrm{st}}(V_{rh}^a)$, and let $\Delta_{(rh)} = \mathbf{D}_{\mathrm{st},rh}(V_{rh}^a)$ which is one-dimensional. We also have $N = 0$ in this case. We consider the tensor product $D' = D \otimes_{\varphi^r\text{-module}} D_{(rh)}$ as φ^r-module. Then D' is associated with the φ^{rh}-module $\Delta' = \Delta \otimes_{\mathbb{Q}_p[\varphi^r]} \Delta_{(rh)}$ and is of reduced dimension $\leq h$. Moreover, let $\{e_1, \cdots, e_h\}$ be a K_0-basis of Δ, f be a generator of $\Delta_{(rh)}$, then Δ'_m $(m = 0, 1, \cdots, rh-1)$ is generated by $\{\varphi^m(e_1 \otimes f), \cdots, \varphi^m(e_h \otimes f)\}$. We claim that D' is admissible and $t_H(D') = 0$.

The second claim is easy, since by the above construction and the definition of t_H, we have $t_H(D') = h(t_H(D) - a) = 0$.

For the first claim, for $x \neq 0$, $x \in D$, let D_x be the K_0-subspace of D generated by $\varphi^{rhi}(x)$ for $i \in \mathbb{N}$, let D'_x be the K_0-subspace of D' generated by $\varphi^m(z \otimes f)$ for all $z \in D_x$. Then D'_x is the minimal sub-object of D' containing $x \otimes f$ and every sub-object D'_1 of D' is a direct sum of D'_x. However, we have $t_H(D'_x) = \dim_{K_0} D_x \cdot t_H(D_{(rh)}) + ht_H(D_x)$ and $t_N(D'_x) = \dim_{K_0} D_x \cdot t_N(D_{(rh)}) + ht_N(D_x)$, thus the admissibility of D implies the admissibility of D'.

Now by (1), D' satisfies $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D') = \dim_{K_0} D'$, which means $V' = \mathbf{V}_{\mathrm{st}}(D')$ is a semi-stable $\mathbb{Q}_{p^{rh}}$-representation. Thus $W = V' \otimes_{\mathbb{Q}_{p^{rh}}} V_{rh}^{-a}$ is also semi-stable, whose associated (φ^{rh}, N)-module is given by $\Delta' \otimes_{\mathbb{Q}_p[\varphi^{rh}]} \Delta^*_{(rh)}$. One sees that D is a direct factor of $\mathbf{D}_{\mathrm{st}}(W)$, hence is also semi-stable and (2) holds.

9.5 End of the proof

Let $r, h \in \mathbb{N}^*$. By Propositions 9.45 and 9.47, we are reduced to show

Proposition 3A. *Let V be a de Rham $\mathbb{Q}_{p^r}$-representation of dimension h with $t_H(V) = 0$, then V is potentially semi-stable.*

Proposition 3B. *Let Δ be an admissible filtered (φ^r, N)-module over K_0 of K_0-dimension h, D be the associated filtered (φ, N)-module with $t_H(D) = 0$. Then*

$$\dim_{\mathbb{Q}_{p^r}} \mathbf{V}_{\mathrm{st}}(D) = h.$$

9.5.1 Application of the Fundamental Lemma.

Recall $U = \{u \in B_{\mathrm{cris}} \mid \varphi(u) = pu\} \cap B^+_{\mathrm{dR}} = P^+_{1,1}$ and $B_2 = B^+_{\mathrm{dR}} / \mathrm{Fil}^2 B_{\mathrm{dR}}$. If V is a finite dimensional $\mathbb{Q}_p$-vector space, we let $V_C = C \otimes_{\mathbb{Q}_p} V$. By tensoring the diagram at the start of § 7.4.1 by $V(-1)$, we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & V & \longrightarrow & U(-1)\otimes_{\mathbb{Q}_p} V & \longrightarrow & V_C(-1) & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle \mathrm{incl}} & & \Big\downarrow{\scriptstyle \mathrm{incl}} & & \Big\downarrow{\scriptstyle \mathrm{Id}} & & \\
0 & \longrightarrow & V_C & \longrightarrow & B_2(-1)\otimes_{\mathbb{Q}_p} V & \xrightarrow{\theta} & V_C(-1) & \longrightarrow & 0
\end{array}$$

where all rows are exact and all the vertical arrows are injective.

Proposition 9.48. *Suppose* $\dim_{\mathbb{Q}_p} V = h \geq 2$. *Suppose there is a surjective* B_2*-linear map* $\eta : B_2(-1)\otimes_{\mathbb{Q}_p} V \to B_2(-1)$ *which passes to the quotient map* $\overline{\eta} : V_C(-1) \to C(-1)$. *Suppose* $\overline{X}$ *is a sub-*C*-vector space of dimension* 1 *of* $V_C(-1)$ *and* X *its inverse image of* $U(-1)\otimes_{\mathbb{Q}_p} V$, *i.e. we have a diagram*

$$\begin{array}{ccccccc}
X & \hookrightarrow & U(-1)_{\mathbb{Q}_p}V & \hookrightarrow & B_2(-1)_{\mathbb{Q}_p}V & \xrightarrow{\eta} & B_2(-1) \\
\Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle \theta} \\
\overline{X} & \hookrightarrow & V_C(-1) & = & V_C(-1) & \xrightarrow{\overline{\eta}} & C(-1).
\end{array}$$

If $\overline{X} \subset \operatorname{Ker}\overline{\eta}$, *then the restriction* $\eta_X : X \to B_2(-1)$ *of* η *factors through* $X \to C$. *Moreover, if* $\eta(V) \neq \eta(X)$, *then* η_X *is surjective and its kernel is a* $\mathbb{Q}_p$*-vector space of dimension* h.

Proof. Suppose $\{e_1, e_2, \cdots, e_h\}$ is a basis of V over $\mathbb{Q}_p$. Then $\{e'_n = t^{-1}\otimes e_n\}$ forms a basis of the free B_2-module $B_2(-1)\otimes_{\mathbb{Q}_p} V$. Write $\eta(e'_n) = b_n \otimes t^{-1}$ with $b_n \in B_2$.

The images $\overline{e}'_n$ of e'_n in $V_C(-1)$ forms a basis of it as a C-vector space. Suppose $\lambda = \sum_{n=1}^{h} \lambda_n \overline{e}'_n$ is a nonzero element of $\overline{X}$. The fact that $\overline{X} \subset \operatorname{Ker}\overline{\eta}$ implies that $\sum \lambda_n \theta(b_n) = 0$, hence $\theta \circ \eta(X) = 0$ and η_X factors through $X \to C$.

Let Y and ρ be given by (7.40) and (7.41) corresponding to (λ_n) and (b_n). The map $\nu : U^h \to U(-1)\otimes_{\mathbb{Q}_p} V$ which sends $(u_1, u_2, \cdots, u_h)$ to $\sum (u_n \otimes t^{-1})\otimes e_n$ is bijective and its restriction ν_Y on Y is a bijection from Y to X. One thus have a commutative diagram

$$\begin{array}{ccc}
Y & \xrightarrow{\rho} & C(1) \\
{\scriptstyle \nu_Y}\Big\downarrow & & \Big\downarrow{\scriptstyle \times t^{-1}} \\
X & \xrightarrow{\eta_X} & C
\end{array}$$

whose vertical lines are bijection. The proposition is nothing but a reformulation of the Fundamental Lemma (Theorem 7.41).

Proposition 9.49. *Let* V_1 *be a* $\mathbb{Q}_p$*-vector space of finite dimension* $h \geq 2$ *and* $\Lambda_1 = B^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_1$. *Suppose* Λ_2 *is a sub-*B^+_{dR}*-module of* $\Lambda_1(-1)$ *such that* $(\Lambda_1 + \Lambda_2)/\Lambda_1$ *and* $(\Lambda_1 + \Lambda_2)/\Lambda_s$ *are simple* B^+_{dR}*-modules. Let* X *be the inverse image of* $\Lambda_1 + \Lambda_2$ *in* $U(-1)\otimes_{\mathbb{Q}_p} V_1$ *and*

$$\rho : U(-1) \otimes_{\mathbb{Q}_p} V_1 \longrightarrow \Lambda_1(-1)/\Lambda_2$$

be the natural projection. Then

(1) *either* $\dim_{\mathbb{Q}_p} \rho(X) \leq h$ *and* $\mathrm{Ker}\,(\rho)$ *is not finite dimensional over* $\mathbb{Q}_p$*;*
(2) *or* ρ *is surjective and* $\mathrm{Ker}\,(\rho)$ *is a* $\mathbb{Q}_p$*-vector space of dimension* h*.*

Proof. Since B_{dR}^+ is a discrete valuation ring whose residue field is C, the hypotheses indicate that $(\Lambda_1 + \Lambda_2)/\Lambda_1$ and $(\Lambda_1 + \Lambda_2)/\Lambda_2$ are C-vector spaces of dimension 1. Then we can find elements $\{e_1, e_2, \cdots, e_h\}$ in Λ_1 such that

$$\Lambda_1 = B_{\mathrm{dR}}^+ \cdot e_1 \oplus B_{\mathrm{dR}}^+ \cdot e_2 \oplus \Lambda_0, \quad \Lambda_2 = B_{\mathrm{dR}}^+ \cdot t^{-1}e_1 \oplus B_{\mathrm{dR}}^+ \cdot te_2 \oplus \Lambda_0$$

where $\Lambda_0 = \bigoplus_{i=3}^{h} B_{\mathrm{dR}}^+ e_i$. One thus has two commutative diagrams, which are exact on the rows:

$$\begin{tikzcd}
0 \arrow[r] & V_1 \arrow[r] \arrow[d, equal] & X \arrow[r] \arrow[d, hook] & \frac{\Lambda_1+\Lambda_2}{\Lambda_1} \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & V_1 \arrow[r] & U(-1) \otimes_{\mathbb{Q}_p} V_1 \arrow[r] \arrow[d, two heads] & \frac{\Lambda_1(-1)}{\Lambda_1} \arrow[r] \arrow[d, two heads] & 0 \\
& & \frac{\Lambda_1(-1)}{\Lambda_1+\Lambda_2} \arrow[r, equal] & \frac{\Lambda_1(-1)}{\Lambda_1+\Lambda_2} &
\end{tikzcd}$$

$$\begin{tikzcd}
0 \arrow[r] & X \arrow[r] \arrow[d] & U(-1) \otimes_{\mathbb{Q}_p} V_1 \arrow[r] \arrow[d, "\rho"] & \frac{\Lambda_1(-1)}{\Lambda_1+\Lambda_2} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \frac{(\Lambda_1+\Lambda_2)}{\Lambda_2} \arrow[r] & \frac{\Lambda_1(-1)}{\Lambda_2} \arrow[r] & \frac{\Lambda_1(-1)}{\Lambda_1+\Lambda_2} \arrow[r] & 0.
\end{tikzcd}$$

Let ϵ_i denote the image of $t^{-1}e_i$ in $B_2(-1) \otimes_{\mathbb{Q}_p} V_1 = \Lambda_1(-1)/\Lambda_1(1)$, then $\{\epsilon_1 \mid 1 \leq i \leq h\}$ is a basis of $\Lambda_1(-1)/\Lambda_1(1)$ as a free B_2-module of rank h.

We denote by $\eta : B_2(-1) \otimes V_1 \to B_2(-1)$ the map which sends $\sum_i a_i \epsilon_i$ to $a_2 t^{-1}$. The image of the restriction η_X of η on X is contained in C and the diagram above induces the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & X \arrow[r] \arrow[d, "\eta_X"] & U(-1) \otimes_{\mathbb{Q}_p} V_1 \arrow[r] \arrow[d, "\rho"] & \frac{\Lambda_1(-1)}{\Lambda_1+\Lambda_2} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & C \arrow[r] & \frac{\Lambda_1(-1)}{\Lambda_2} \arrow[r] & \frac{\Lambda_1(-1)}{\Lambda_1+\Lambda_2} \arrow[r] & 0.
\end{tikzcd}$$

where $C \to \Lambda_1(-1)/\Lambda_2$ is the map $c \mapsto ct^{-1}\epsilon_2$.

One can see that the image $\overline{X}$ of X in $\Lambda_1(-1)/\Lambda_1 = (C \otimes V_1)(-1)$ is a C-vector space of dimension 1 contained in the kernel of $\overline{\eta}$, and X is the inverse image of $\overline{X}$ in $U(-1) \otimes V_1$. Applying the precedent proposition, if $\eta(V_1) = \eta(X)$ we are in case (1); otherwise, η_X is surjective, so is ρ and $\mathrm{Ker}\,(\rho) = \mathrm{Ker}\,(\eta_X)$ is of dimension h over $\mathbb{Q}_p$.

9.5.2 Recurrence of the Hodge polygon and end of proof.

We are now ready to prove Proposition 3A (resp. 3B), and thus finish the proof of Theorem A (resp. B).

We say V (resp. Δ or D) is of dimension (r,h) if V (resp. Δ) is a $\mathbb{Q}_{p^r}$-representation (resp. a (φ^r, N)-module) of dimension h. From now on, we assume that V (resp. Δ) satisfies $t_H(V) = 0$ (resp. $t_H(D) = 0$.

We prove Proposition 3A (resp. 3B) by induction on h. Suppose Proposition 3A (resp. 3B) is known for all V' (resp. Δ') of dimension (r', h') with $h' < h$ and r' arbitrary, we want to prove it is also true for V (resp. Δ) of dimension (r,h).

Consider the set of all convex polygons with origin $(0,0)$ and end point $(hr, 0)$. The Hodge polygon P_H of V (resp. D) is an element of this set. By Step 1, we know Proposition 3A (resp. 3B) is true if P_H is trivial. By induction to the complexity of P_H, we may assume Proposition 3A (resp. 3B) is known for all V' (resp. Δ') of dimension (r,h) but its Hodge polygon is strictly above $P_H(V)$ (resp. above $P_H(D)$). By Proposition 2A (resp. 2B), we may assume V (resp. D) is irreducible.

Recall $D_K = \mathbf{D}_{\mathrm{dR}}(V)$ (resp. $D_K = D \otimes_{K_0} K$). For V, we let $\Delta_{K,m} = \mathbf{D}^{(m)}_{\mathrm{dR},r}(V)$. Then in both cases,

$$D_K = \bigoplus_{m=0}^{r-1} \Delta_{K,m}, \quad \mathrm{Fil}^i D_K = \bigoplus_{m=0}^{r-1} \mathrm{Fil}^i D_K \cap \Delta_{K,m}.$$

We can choose a K-basis $\{\delta_j \mid 1 \leq j \leq rh\}$ of D_K which is compatible with the filtration $\{\mathrm{Fil}^i D_K\}$ and the decomposition $D_K = \bigoplus\limits_{m=0}^{r-1} \Delta_{K,m}$. To be precise,

(a) If let
$$i_j := \max\{i \in \mathbb{Z} \mid \delta_j \in \mathrm{Fil}^i D_K\},$$
then the set $\{\delta_j \mid i_j \geq i\}$ is a K-basis of $\mathrm{Fil}^i D_K$ for every $i \in \mathbb{Z}$.

(b) For every $0 \leq m < r$, $\Delta_{K,m}$ has a K-basis $\{\delta_j \mid \delta_j \in \Delta_{K,m}\}$.

By this way, then

$$h_i = \dim_K \mathrm{Fil}^i D_K / \mathrm{Fil}^{i+1} D_K = \#\{1 \leq j \leq rh \mid i_j = i\}, \tag{9.32}$$

$$t_H = \sum_{j=1}^{rh} i_j = 0. \tag{9.33}$$

Since P_H is not trivial, by changing the order of δ_j, we may assume that $i_2 \geq i_1 + 2$.

We fix such a basis of D_K.

Proof of Proposition 3B.

We consider the (φ^r, N)-module Δ' defined as follows:

(i) the underlying (φ^r, N)-module structure is the same as of Δ;
(ii) since $D'_K = D_K$, for the basis $\{\delta_j \mid 1 \leq j \leq rh\}$ of D_K, the filtration is given as follows:

$$i'_1 = i_1 + 1,\ i'_2 = i_2 - 1,\ i'_j = i_j \text{ for } j \geq 2.$$

Then Δ' is a filtered (φ^r, N)-module of dimension h. Let D' be the associated (φ, N)-module. Then $t_H(D') = t_H(D) - 1 + 1 = t_H(D) = 0$ and $t_N(D') = t_N(D)$. Moreover, let E' be any sub-object of D' as (φ, N)-module, different from 0 and D', then it is identified with a sub-object E of D as (φ, N)-module, different from 0 and D. Then one has $t_N(E') = t_N(E)$, and $t_H(E') = t_H(E) + \epsilon$ with $\epsilon \in \{-1, 0, 1\}$. Since D is admissible and irreducible, $t_H(E) < t_N(E)$ and we have $t_H(E') \leq t_N(E')$, which implies that D' is an admissible (φ, N)-module.

Let $V_1 = \mathbf{V}_{\mathrm{st}}(D')$ and $V_2 = \mathbf{V}_{\mathrm{st}}(D)$. We need to show $\dim_{\mathbb{Q}_p} V_2 \geq rh$.

Since the Hodge polygon of D' is strictly above that of D, by induction hypothesis, we have $\dim_{\mathbb{Q}_{p^r}} V_1 = h$, which means that V_1 is semi-stable and $\mathbf{D}_{\mathrm{st}}(V_1) = D'$. Then $B_{\mathrm{st}} \otimes_{K_0} D = B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V_1$ and

$$\mathbf{V}^0_{\mathrm{st}}(D) = \mathbf{V}^0_{\mathrm{st}}(D') = \{x \in B_{\mathrm{st}} \otimes_{K_0} D \mid \varphi(x) = x,\ Nx = 0\} = B_e \otimes_{\mathbb{Q}_p} V_1.$$

Suppose $W = B_{\mathrm{dR}} \otimes_K D_K = B_{\mathrm{dR}} \otimes_K D'_K$, $\Lambda_1 = \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D'_K) = \sum_{i \in \mathbb{Z}} \mathrm{Fil}^{-i} B_{\mathrm{dR}} \otimes_K \mathrm{Fil}^i D'_K$ and $\Lambda_2 = \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D_K)$. Then we have exact sequences

$$0 \to V_i \to \mathbf{V}^0_{\mathrm{st}}(D) \to W/\Lambda_i$$

for $i = 1, 2$. Since V_1 is semi-stable,

$$\Lambda_1 = \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D'_K) \cong \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_1) = B^+_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_1.$$

In this case, by Proposition 9.32, one has an exact sequence

$$0 \to V_1 \to \mathbf{V}^0_{\mathrm{st}}(D) \to W/\Lambda_1 = \mathbf{V}^1_{\mathrm{st}}(D) \to 0.$$

Note that Λ_2 is a sub-B^+_{dR}-module of $\Lambda_1(-1)$ and that $(\Lambda_1 + \Lambda_2)/\Lambda_1$ and $(\Lambda_1 + \Lambda_2)/\Lambda_2$ are simple B^+_{dR}-modules. We can apply Proposition 9.49. By the inclusion $U(-1) \subset B_e$, we have a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ker}\,\rho \arrow[r] \arrow[d, hook] & U(-1) \otimes_{\mathbb{Q}_p} V_1 \arrow[r, "\rho"] \arrow[d, hook] & \Lambda_1(-1)/\Lambda_2 \arrow[r] \arrow[d, hook] & 0 \\ 0 \arrow[r] & V_2 \arrow[r] & B_e \otimes_{\mathbb{Q}_p} V_1 \arrow[r] & W/\Lambda_2. \end{tikzcd}$$

where $\mathrm{Ker}\,\rho \subset V_2$ implies ρ must be surjective. Thus $\mathrm{Ker}\,\rho$ must be of finite dimension rh, as a result $\dim_{\mathbb{Q}_p} V_2 \geq rh$ and Proposition 3B is proved, so is Theorem B.

Proof of Proposition 3A.

Lemma 9.50. *There exists no G_K-equivariant $\mathbb{Q}_p$-linear section of B_2 to C.*

Proof. Suppose V_0 is a nontrivial extension of $\mathbb{Q}_p(1)$ by $\mathbb{Q}_p$. We know it exists and is not de Rham by Corollary 9.30. Thus $\dim_K \mathbf{D}_{\mathrm{dR}}(V_0) = 1$ and hence $\mathbf{D}_{\mathrm{dR}}(V_0^*) = \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V_0, B_{\mathrm{dR}})$ is also of dimension 1.

Assume the Lemma is false and there is a G_K-equivariant $\mathbb{Q}_p$-linear section $s: C \to B_2$. Let $B_i = B_{\mathrm{dR}}^+/\operatorname{Fil}^i B_{\mathrm{dR}}$ for $i \geq 2$. By the exact sequence

$$0 \to C(i) \to B_{i+1} \to B_i \to 0,$$

and the fact $H^1(K, C(i)) = 0$ (see Proposition 4.46), then $\mathrm{Hom}_{\mathbb{Q}_p[G_K]}(C, B_{i+1}) \to \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(C, B_i)$ is surjective. By induction, the section s extends to a G_K-equivariant $\mathbb{Q}_p$-linear section $C \to B_{\mathrm{dR}}^+ = \varprojlim_{i \geq 2} B_i$.

We now construct two linearly independent maps of $\mathbb{Q}_p[G_K]$-modules from V_0 to B_{dR} and thus induce a contradiction. The first one is the composition $V_0 \to \mathbb{Q}_p(1) \to B_{\mathrm{dR}}$. For the second one, since $\mathrm{Ext}^1_{\mathbb{Q}_p[G_K]}(\mathbb{Q}_p(1), C) = H^1_{\mathrm{cont}}(K, C(-1)) = 0$ (again see Proposition 4.46), we have an exact sequence $\mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V_0, C) \to \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(\mathbb{Q}_p, C) \to 0$, thus the inclusion $\mathbb{Q}_p \to C$ is extendable to $V_0 \to C$. Composing it with the section $C \to B_{\mathrm{dR}}^+$, we get another G_K-equivariant $\mathbb{Q}_p$-linear map from V_0 to $B_{\mathrm{dR}}^+ \hookrightarrow B_{\mathrm{dR}}$. It is clear that thees two maps constructed are independent.

Definition 9.51. *A B_{dR}^+-*representation of G_K *is a B_{dR}^+-module of finite type endowed with a linear and continuous action of G_K. It is called* Hodge-Tate *if it is a direct sum of B_{dR}^+-representations of the form*

$$B_m(i) := \operatorname{Fil}^i B_{\mathrm{dR}}/\operatorname{Fil}^{i+m} B_{\mathrm{dR}} = (B_{\mathrm{dR}}^+/t^m B_{\mathrm{dR}}^+)(i)$$

for $m \in \mathbb{N} - \{0\}$ and $i \in \mathbb{Z}$.

Remark 9.52. The category $\mathbf{Rep}_{B_{\mathrm{dR}}^+}(G_K)$ of all B_{dR}^+-representations, with morphisms being G_K-equivariant B_{dR}^+-maps, is an abelian category.

(a) Moreover it is artinian: $B_m(i)$ is an indecomposable object in this category.

(b) The sub-objects and quotients of a Hodge-Tate B_{dR}^+-representation is still Hodge-Tate.

Lemma 9.53. *Suppose*

$$0 \to W' \to W \to W'' \to 0$$

is an exact sequence of Hodge-Tate B_{dR}^+-representations. For this sequence to be split, it is necessary and sufficient that there exists a G_K-equivariant $\mathbb{Q}_p$-linear section of the projection of W to W''.

Proof. The condition is obviously necessary. We now prove that it is also sufficient. We can find a decomposition of $W = \bigoplus_{n=1}^t W_n$ as a direct sum of indecomposable $B_m(i)$'s, such that $W_n' = W' \cap W_n$ and $W' = \bigoplus_{n=1}^t W_n'$, then W'' is a direct sum of W_n/W_n'. By this decomposition, we can assume $t = 1$. It suffices to prove that for $r, s, i \in \mathbb{Z}$ with $r, s \geq 1$, there exists no G_K-equivariant section of the projection $B_{r+s}(i)$ to $B_r(i)$. If not, the section $B_r(i) \to B_{r+s}(i)$ induces a G_K-equivariant map

$$C(i+r-1) = \frac{t^{i+r-1}B_{\mathrm{dR}}^+}{t^{i+r}B_{\mathrm{dR}}^+} \to \frac{t^{i+r-1}B_{\mathrm{dR}}^+}{t^{i+r+s}B_{\mathrm{dR}}^+} \to \frac{t^{i+r-1}B_{\mathrm{dR}}^+}{t^{i+r+1}B_{\mathrm{dR}}^+} = B_2(i+r-1)$$

which is a section of the projection $B_2(i+r-1)$ to $C(i+r-1)$. By tensoring $\mathbb{Z}_p(1-r-i)$, we get a G_K-equivariant $\mathbb{Q}_p$-linear section of B_2 to C, which contradicts the previous lemma.

We now apply Proposition 9.49 with $V_1 = V$. Since V is de Rham, we let $\Lambda_1 = B_{\mathrm{dR}}^+ \otimes_{\mathbb{Q}_p} V = \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D_K)$. This is a free B_{dR}^+-module with a basis $\{e_j = t^{-i_j} \otimes \delta_j \mid 1 \leq j \leq rh\}$. Suppose

$$e_1' = t^{-1}e_1,\ e_2' = te_2,\ \text{and } e_j' = e_j \text{ for all } 3 \leq j \leq rh.$$

The sub-B_{dR}^+-module Λ_2 of $\Lambda_1(-1)$ with a basis $\{e_j' \mid 1 \leq j \leq rh\}$ satisfies the hypotheses of Proposition 9.49. With notations of that proposition, the quotient $(\Lambda_1 + \Lambda_2)/\Lambda_1$ is a C-vector space of dimension 1 generated by the image of $e_1' = t^{-i_1-1} \otimes \delta_1$ and is isomorphic to $C(-i_1-1)$. One has an exact sequence

$$0 \to V \to X \to C(-i_1-1) \to 0. \tag{9.34}$$

This sequence does not admit a G_K-equivariant $\mathbb{Q}_p$-linear section. In fact, one has an injection $X \to U(-1) \otimes V \to B_2(-1) \otimes V = \Lambda_1(-1)/\Lambda_1(1)$. The last one is a free B_2-module of basis b_j the image of $t^{-i_j-1} \otimes \delta_j$. The factor with basis b_1 is isomorphic to $B_2(-i_1-1)$ and the projection parallel to this factor induces a G_K-equivariant commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & V \arrow[r] \arrow[d] & X \arrow[r] \arrow[d] & C(-i_1-1) \arrow[r] \arrow[d, "\mathrm{Id}"'] & 0 \\
0 \arrow[r] & C(-i_1) \arrow[r] & B_2(-i_1-1) \arrow[r] & C(-i_1-1) \arrow[r] & 0
\end{tikzcd}$$

whose rows are exact. If the sequence at the top splits, so is the one at the bottom, which contradicts Lemma 9.50.

Note that $V = V_1$ is not contained in the kernel of ρ: otherwise V is contained in Λ_2, and it is also contained in the sub-B_{dR}^+-module of $\Lambda_1(-1)$ generated by V_1 which is Λ_1, which is not the case.

Since the map ρ is G_K-equivariant and since V is irreducible, the restriction of ρ on V is injective. We have $\rho(V) \neq \rho(X)$ (otherwise, $X = V \oplus \operatorname{Ker} \rho$, contradiction to that (9.34) is not split). Therefore $\dim_{\mathbb{Q}_p} \rho(X) \geq rh$. By Proposition 9.49, ρ is surjective and its kernel V_2 is of dimension rh over $\mathbb{Q}_p$. We see that V_2 is actually a $\mathbb{Q}_{p^r}$-representation of dimension h.

Lemma 9.54. *The B_{dR}^+-linear map $B_{\mathrm{dR}}^+ \otimes_{\mathbb{Q}_p} V_2 \to \Lambda_2$ induced by the inclusion $V_2 \to \Lambda_2$ is an isomorphism.*

Proof. Since both $B_{\mathrm{dR}}^+ \otimes V_2$ and Λ are free B_{dR}^+-modules of the same rank, it suffices to show that the map is surjective. By Nakayama Lemma, it suffice to show that, if let Λ_{V_2} be the sub-B_{dR}^+-module of Λ_2 generated by V_2 and $t\Lambda_2$, then $\Lambda_{V_2} = \Lambda_2$.

By composing the inclusion of $U(-1) \otimes V$ to $\Lambda_1(-1)$ with the projection of $\Lambda_1(-1)$ to $\Lambda_1(-1)/\Lambda_{V_2}$, we obtain the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & V_2 & \longrightarrow & U(-1) \otimes V & \longrightarrow & \Lambda_1(-1)/\Lambda_2 & \longrightarrow & 0 \\
 & & {\scriptstyle 0}\big\downarrow & & \big\downarrow & & \big\downarrow{\scriptstyle \mathrm{Id}} & & \\
0 & \longrightarrow & \Lambda_2/\Lambda_{V_2} & \longrightarrow & \Lambda_1(-1)/\Lambda_{V_2} & \longrightarrow & \Lambda_1(-1)/\Lambda_2 & \longrightarrow & 0
\end{array}$$

with exact rows, which implies that there exists a $\mathbb{Q}_p$-linear G_K-equivariant section of the last row. Since $\Lambda_1(-1)/\Lambda_{V_2}$, as a quotient of $\Lambda_1(-1)/\Lambda_2(1)$, is a Hodge-Tate B_{dR}^+-representation, by Lemma 9.53, the last row exact sequence splits as B_{dR}^+-modules.

If, for $1 \leq j \leq rh$, let u_j (resp. $\overline{u}_j$) denote the image of $t^{-i_j-1} \otimes \delta_j$ in $\Lambda_1(-1)/\Lambda_{V_2}$ (resp. $\Lambda_1(-1)/\Lambda_2$), then $\overline{u}_1 = 0$, $t\overline{u}_j = 0$ for $j \geq 3$, and $\Lambda_1(-1)/\Lambda_2$ is the direct sum of the free B_2-module with basis $\overline{u}_2$ and the C-vector space with basis $\{\overline{u}_j \mid j \geq 3\}$. Since Λ_2/Λ_{V_2} is killed by t, one then deduces that $t^2 u_2 = t^2(u_2 - \overline{u}_2) = 0$ and $tu_j = 0$ for $j \leq 3$, then $t^{-i_2+1} \otimes \delta_2$ and $t^{-i_j} \otimes \delta_j$ for $j \geq 3$ are contained in Λ_{V_2}. Hence Λ_{V_2} contains the sub-B_{dR}^+-module generated by those elements and $t^{-i_1} \otimes \delta_1$, which is nothing but $\Lambda_1 \cap \Lambda_2$. Since $\Lambda_2/(\Lambda_1 \cap \Lambda_2)$ is a simple B_{dR}^+-module, it suffices to show that $\Lambda_{V_2} \neq \Lambda_1 \cap \Lambda_2$, or V_2 is not contained in Λ_1. This follows from $(U(-1) \otimes V) \cap \Lambda_1 = V$ and $V \cap V_2 = 0$ since the restriction of ρ at V is injective.

By inverting t, from the above lemma, we have an isomorphism of $B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V_2$ to $B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$ which is G_K-equivariant. We thus have an isomorphism $D'_K = \mathbf{D}_{\mathrm{dR}}(V_2)$ to $D_K = \mathbf{D}_{\mathrm{dR}}(V)$ and hence V_2 is a de Rham representation. Write $i'_1 = i_1 + 1$, $i'_2 = i_2 - 1$, and $i'_j = i_j$ for $3 \leq j \leq rh$. By $B_{\mathrm{dR}}^+ \otimes_{\mathbb{Q}_p} V = \Lambda_1$ and $B_{\mathrm{dR}}^+ \otimes_{\mathbb{Q}_p} V_2 = \Lambda_2$, for every $i \in \mathbb{Z}$, we have

$$\mathrm{Fil}^i D_K = \bigoplus_{i_j \geq i} K\delta_j, \text{ and } \mathrm{Fil}^i D'_K = \bigoplus_{i'_j \geq i} K\delta_j.$$

It follows that the Hodge polygon of V_2 is strictly above that of V. The inductive hypothesis then implies that V_2 is potentially semi-stable. Replacing K by a finite extension, we may assume that V_2 is semi-stable.

We regard V and V_2 as $\mathbb{Q}_p$-subspaces of B_{dR}-vector space $W = B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$. Suppose $A \in \mathrm{GL}_{rh}(B_{\mathrm{dR}})$ is the transition matrix from a chosen basis of V_2 over $\mathbb{Q}_p$ to a chosen basis of V over $\mathbb{Q}_p$. Since $t_H(V) = t_H(V_2) = 0$, $\det(A)$ is a unit in B_{dR}^+. Since $V_2 \subset U(-1) \otimes V$, the matrix A is of coefficients in $U(-1) \subset B_e$. As $B_e \cap B_{\mathrm{dR}}^+ = \mathbb{Q}_p$, $\det A$ is a nonzero element in $\mathbb{Q}_p$ and hence $A \in \mathrm{GL}_{rh}(B_e)$. Thus the inclusion of $V_2 \subset U(-1) \otimes V$ induces an isomorphism of $B_e \otimes V_2$ to $B_e \otimes V$, hence a fortiori of $B_{\mathrm{st}} \otimes V_2$ to $B_{\mathrm{st}} \otimes V$. By taking the G_K-invariant, we get an isomorphism of $\mathbf{D}_{\mathrm{st}}(V_2)$ to $\mathbf{D}_{\mathrm{st}}(V)$. Since V_2 is semi-stable, then $\dim_{K_0} \mathbf{D}_{\mathrm{st}}(V) = rh = \dim_{\mathbb{Q}_p}(V)$ and V is also semi-stable. This completes the proof of Proposition 3A and consequently of Theorem A.

10

Overconvergent rings and overconvergent representations

10.1 The generalized Tate-Sen's method.

The method of Sen to classify C-representations in § 4.3 is generalized to the following axiomatic set-up by Colmez.

10.1.1 Tate-Sen's conditions (TS1), (TS2) and (TS3).

Suppose G_0 is a profinite group and $\chi: \ G_0 \to \mathbb{Z}_p^\times$ is a continuous group homomorphism with open image. Set $n(g) = v_p(\log \chi(g))$ and $H_0 = \mathrm{Ker}\,\chi$.

Suppose $\tilde{\Lambda}$ is a $\mathbb{Z}_p$-algebra and

$$v: \ \tilde{\Lambda} \longrightarrow \mathbb{R} \cup \{+\infty\}$$

satisfies the following conditions:

(i) $v(x) = +\infty$ if and only if $x = 0$;
(ii) $v(xy) \geq v(x) + v(y)$;
(iii) $v(x+y) \geq \min(v(x), v(y))$;
(iv) $v(p) > 0, \ v(px) = v(p) + v(x)$.

Assume $\tilde{\Lambda}$ is complete for v, and G_0 acts continuously on $\tilde{\Lambda}$ such that $v(g(x)) = v(x)$ for all $g \in G_0$ and $x \in \tilde{\Lambda}$.

Definition 10.1. *The* Tate-Sen's conditions *for the quadruple* $(G_0, \chi, \tilde{\Lambda}, v)$ *are the following three conditions:*

(TS 1). *For any* $C_1 > 0$*, for all* $H_1 \subset H_2 \subset H_0$ *open subgroups, there exists an* $\alpha \in \tilde{\Lambda}^{H_1}$ *with*

$$v(\alpha) > -C_1 \text{ and } \sum_{\tau \in H_2/H_1} \tau(\alpha) = 1. \tag{10.1}$$

(In Faltings' terminology, $\tilde{\Lambda}/\tilde{\Lambda}^{H_0}$ *is called* almost étale.*)*

(TS 2). Tate's normalized trace maps*: there exists a constant $C_2 > 0$ such that for all open subgroups $H \subset H_0$, there exist $n(H) \in \mathbb{N}$ and $(\Lambda_{H,n})_{n \geq n(H)}$, an increasing sequence of sub $\mathbb{Z}_p$-algebras of $\tilde{\Lambda}^H$ and maps*

$$R_{H,n} : \tilde{\Lambda}^H \longrightarrow \Lambda_{H,n}$$

satisfying the following conditions:

(a) *if $H_1 \subset H_2$, then $\Lambda_{H_2,n} = (\Lambda_{H_1,n})^{H_2}$, and $R_{H_1,n} = R_{H_2,n}$ on $\tilde{\Lambda}^{H_2}$;*
(b) *for all $g \in G_0$, then*

$$g(\Lambda_{H,n}) = \Lambda_{gHg^{-1},n} \text{ and } g \circ R_{H,n} = R_{gHg^{-1},n} \circ g;$$

(c) *$R_{H,n}$ is $\Lambda_{H,n}$-linear and is equal to identity on $\Lambda_{H,n}$;*
(d) *$v(R_{H,n}(x)) \geq v(x) - C_2$ if $n \geq n(H)$ and $x \in \tilde{\Lambda}^H$;*
(e) $\lim\limits_{n \to +\infty} R_{H,n}(x) = x$.

(TS 3)*. There exists a constant C_3, such that for all open subgroups $G \subset G_0$, $H = G \cap H_0$, there exists $n(G) \geq n(H)$ such that if $n \geq n(G)$, $\gamma \in G/H$ and $n(\gamma) = v_p(\log \chi(\gamma)) \leq n$, then $\gamma - 1$ is invertible on $X_{H,n} = (R_{H,n} - 1)\tilde{\Lambda}^H$ and*

$$v((\gamma - 1)^{-1}x) \geq v(x) - C_3 \tag{10.2}$$

for $x \in X_{H,n}$.

Remark 10.2. $R_{H,n} \circ R_{H,n} = R_{H,n}$, so $\tilde{\Lambda}^H = \Lambda_{H,n} \oplus X_{H,n}$.

Example 10.3. In § 4.3, we are in the case $\tilde{\Lambda} = C$, $G_0 = G_K$, $v = v_p$, χ being the character $G_0 \to \Gamma \xrightarrow{\exp \circ p} \mathbb{Z}_p^\times$.

In this case we have $H_0 = \mathrm{Gal}(\overline{K}/K_\infty)$. For any open subgroup H of H_0, let $L_\infty = \overline{K}^H$, then $L_\infty = LK_\infty$ for L disjoint from K_∞ over K_n for $n \gg 0$. Let $\Lambda_{H,n} = L_n = LK_n$ and $R_{H,n}$ be Tate's normalized trace map. Then all the axioms (TS1), (TS2) and (TS3) are satisfied from results in § 1.4.2.

10.1.2 Almost étale descent

Lemma 10.4. *If $\tilde{\Lambda}$ satisfies* (TS 1)*, $a > 0$, and $\sigma \mapsto U_\sigma$ is a continuous 1-cocycle from H, an open subgroup of H_0, to $\mathrm{GL}_d(\tilde{\Lambda})$, and*

$$v(U_\sigma - 1) \geq a \text{ for any } \sigma \in H,$$

then there exists $M \in \mathrm{GL}_d(\tilde{\Lambda})$ such that

$$v(M - 1) \geq \frac{a}{2}, \quad v(M^{-1}U_\sigma \sigma(M) - 1) \geq a + 1.$$

Proof. The proof is parallel to Lemma 4.16, imitating the proof of Hilbert's Theorem 90.

Fix $H_1 \subset H$ open and normal such that $v(U_\sigma - 1) \geq a + 1 + a/2$ for $\sigma \in H_1$, which is possible by continuity. Because $\tilde{\Lambda}$ satisfies (TS1), we can find $\alpha \in \tilde{\Lambda}^{H_1}$ such that

$$v(\alpha) \geq -a/2, \qquad \sum_{\tau \in H/H_1} \tau(\alpha) = 1.$$

Let $S \subset H$ be a set of representatives of H/H_1, denote $M_S = \sum_{\sigma \in S} \sigma(\alpha) U_\sigma$, we have $M_S - 1 = \sum_{\sigma \in S} \sigma(\alpha)(U_\sigma - 1)$, this implies $v(M_S - 1) \geq a/2$ and moreover

$$M_S^{-1} = \sum_{n=0}^{+\infty} (1 - M_S)^n,$$

so we have $v(M_S^{-1}) \geq 0$ and $M_S \in \mathrm{GL}_d(\tilde{\Lambda})$.

If $\tau \in H_1$, then $U_{\sigma\tau} - U_\sigma = U_\sigma(\sigma(U_\tau) - 1)$. Let $S' \subset H$ be another set of representatives of H/H_1, then for any $\sigma' \in S'$, there exist a unique $\sigma \in S$ and $\tau_\sigma \in H_1$ such that $\sigma' = \sigma\tau_\sigma$, so we get

$$M_S - M_{S'} = \sum_{\sigma \in S} \sigma(\alpha)(U_\sigma - U_{\sigma\tau_\sigma}) = \sum_{\sigma \in S} \sigma(\alpha) U_\sigma (1 - \sigma(U_{\tau_\sigma})),$$

thus

$$v(M_S - M_{S'}) \geq a + 1 + a/2 - a/2 = a + 1.$$

For any $\tau \in H$,

$$U_\tau \tau(M_S) = \sum_{\sigma \in S} \tau\sigma(\alpha) U_\tau \tau(U_\sigma) = M_{\tau S}.$$

Then

$$M_S^{-1} U_\tau \tau(M_S) = 1 + M_S^{-1}(M_{\tau S} - M_S),$$

with $v(M_S^{-1}(M_{\tau S} - M_S)) \geq a + 1$. Take $M = M_S$ for any S, we get the result.

Corollary 10.5. *Under the same hypotheses as the above lemma, there exists $M \in \mathrm{GL}_d(\tilde{\Lambda})$ such that*

$$v(M - 1) \geq a/2, \;\; M^{-1} U_\sigma \sigma(M) = 1, \textit{for all } \sigma \in \;\; H.$$

Proof. Repeat the lemma ($a \mapsto a + 1 \mapsto a + 2 \mapsto \cdots$), and take the limit.

10.1.3 Decompletion.

Lemma 10.6. *Given constants $\delta > 0$, $b \geq 2C_2 + 2C_3 + \delta$, $b' > b$. Suppose H is an open subgroup of H_0. Suppose $n \geq n(H)$, $\gamma \in G/H$ with $n(\gamma) \leq n$, $U = 1 + U_1 + U_2$ such that*

$$U_1 \in \mathrm{M}_d(\Lambda_{H,n}),\ v(U_1) \geq b - C_2 - C_3$$
$$U_2 \in \mathrm{M}_d(\widetilde{\Lambda}^H),\ v(U_2) \geq b' \geq b.$$

Then, there exists $M \in \mathrm{GL}_d(\widetilde{\Lambda}^H), v(M-1) \geq b - C_2 - C_3$ such that

$$M^{-1}U\gamma(M) = 1 + V_1 + V_2,$$

with

$$V_1 \in \mathrm{M}_d(\Lambda_{H,n}),\ v(V_1) \geq b - C_2 - C_3,$$
$$V_2 \in \mathrm{M}_d(\widetilde{\Lambda}^H),\ v(V_2) \geq b + \delta.$$

Proof. Using (TS2) and (TS3), one gets $U_2 = R_{H,n}(U_2) + (1-\gamma)V$, with

$$v(R_{H,n}(U_2)) \geq v(U_2) - C_2, \quad v(V) \geq v(U_2) - C_2 - C_3.$$

Thus,

$$\begin{aligned}(1+V)^{-1}U\gamma(1+V) &= (1 - V + V^2 - \cdots)(1 + U_1 + U_2)(1 + \gamma(V)) \\ &= 1 + U_1 + (\gamma - 1)V + U_2 + (\text{terms of degree} \geq 2)\end{aligned}$$

Let $V_1 = U_1 + R_{H,n}(U_2) \in \mathrm{M}_d(\Lambda_{H,n})$ and W be the terms of degree ≥ 2. Thus $v(W) \geq b + b' - 2C_2 - 2C_3 \geq b' + \delta$. So we can take $M = 1 + V,\ V_2 = W$.

Corollary 10.7. *Keep the same hypotheses as in Lemma 10.6. Then there exists $M \in \mathrm{GL}_d(\widetilde{\Lambda}^H), v(M-1) \geq b - C_2 - C_3$ such that $M^{-1}U\gamma(M) \in \mathrm{GL}_d(\Lambda_{H,n})$.*

Proof. Repeat the lemma ($b \mapsto b + \delta \mapsto b + 2\delta \mapsto \cdots$), and take the limit.

Lemma 10.8. *Suppose $H \subset H_0$ is an open subgroup, $i \geq n(H)$, $\gamma \in G/H$, $n(\gamma) \leq i$ and $B \in M_{d\times s}(\widetilde{\Lambda}^H)$. If there exist $V_1 \in \mathrm{GL}_d(\Lambda_{H,i})$, $V_2 \in \mathrm{GL}_s(\Lambda_{H,i})$ such that*

$$v(V_1 - 1) > C_3, \quad v(V_2 - 1) > C_3, \quad \gamma(B) = V_1 B V_2,$$

then $B \in M_{d\times s}(\Lambda_{H,i})$.

Proof. Take $C = B - R_{H,i}(B)$. We have to prove $C = 0$. Note that C has entries in $X_{H,i} = (1 - R_{H,i})\widetilde{\Lambda}^H$, and $R_{H,i}$ is $\Lambda_{H,i}$-linear and commutes with γ. Thus,

$$\gamma(C) - C = V_1 C V_2 - C = (V_1 - 1)CV_2 + V_1 C(V_2 - 1) - (V_1 - 1)C(V_2 - 1)$$

Hence, $v(\gamma(C) - C) > v(C) + C_3$. By (TS3), this implies $v(C) = +\infty$, i.e. $C = 0$.

10.1.4 Applications to p-adic representations.

Proposition 10.9. *Assume that $\tilde{\Lambda}$ satisfies* (TS 1), (TS 2) *and* (TS 3). *Suppose $\sigma \mapsto U_\sigma$ is a continuous cocycle from G_0 to $\mathrm{GL}_d(\tilde{\Lambda})$. If $G \subset G_0$ is an open normal subgroup of G_0 such that $v(U_\sigma - 1) > 4C_2 + 4C_3$ for any $\sigma \in G$. Set $H = G \cap H_0$, then there exists $M \in \mathrm{GL}_d(\tilde{\Lambda})$ with $v(M-1) > C_2 + C_3$ such that*

$$\sigma \longmapsto V_\sigma = M^{-1} U_\sigma \sigma(M)$$

satisfies $V_\sigma \in \mathrm{GL}_d(\Lambda_{H,n(G)})$ and $V_\sigma = 1$ if $\sigma \in H$.

Proof. Let $\sigma \mapsto U_\sigma$ be a continuous 1-cocycle on G_0 with values in $\mathrm{GL}_d(\widetilde{\Lambda})$. Choose an open normal subgroup G of G_0 such that

$$\inf_{\sigma \in G} v(U_\sigma - 1) > 4(C_2 + C_3).$$

By Corollary 10.5, there exists $M_1 \in \mathrm{GL}_d(\widetilde{\Lambda})$, $v(M_1 - 1) > 2(C_2 + C_3)$ such that $\sigma \mapsto U'_\sigma = M_1^{-1} U_\sigma \sigma(M_1)$ is trivial in $H = G \cap H_0$. In particular, U'_σ has values in $\mathrm{GL}_d(\widetilde{\Lambda}^H)$.

Now we pick $\gamma \in G/H$ with $n(\gamma) = n(G)$. In particular, we want $n(G)$ big enough so that γ is in the center of G_0/H. Indeed, the center is open, since in the exact sequence:

$$1 \to H_0/H \to G_0/H \to G_0/H_0 \to 1,$$

$G_0/H_0 \cong \mathbb{Z}_p \times$ (finite) is abelian, and H_0/H is finite. It is an easy exercise to show that if A is a finite normal subgroup of a profinite group B such that the quotient $B/A \cong \mathbb{Z}_p$, then the center of B is open in B. So we are able to choose such an $n(G)$.

Then we have $v(U'_\gamma - 1) > 2(C_2 + C_3)$, and by Corollary 10.7, there exists $M_2 \in \mathrm{GL}_d(\widetilde{\Lambda}^H)$ satisfying

$$v(M_2 - 1) > C_2 + C_3 \text{ and } M_2^{-1} U'_\gamma \gamma(M_2) \in \mathrm{GL}_d(\Lambda_{H,n(G)}).$$

Take $M = M_1 \cdot M_2$, then the cocycle

$$\sigma \mapsto V_\sigma = M^{-1} U_\sigma \sigma(M)$$

is a cocycle trivial on H with values in $\mathrm{GL}_d(\widetilde{\Lambda}^H)$, and we have

$$v(V_\gamma - 1) > C_2 + C_3 \text{ and } V_\gamma \in \mathrm{GL}_d(\Lambda_{H,n(G)}).$$

This implies V_σ comes by inflation from a cocycle on G_0/H.

The last thing we need to prove is $V_\tau \in \mathrm{GL}_d(\Lambda_{H,n(G)})$ for any $\tau \in G_0/H$. Note that $\gamma\tau = \tau\gamma$ as γ is in the center, so

$$V_\tau \tau(V_\gamma) = V_{\tau\gamma} = V_{\gamma\tau} = V_\gamma \gamma(V_\tau)$$

which implies $\gamma(V_\tau) = V_\gamma^{-1} V_\tau \tau(V_\gamma)$. We now apply Lemma 10.8 with $V_1 = V_\gamma^{-1}, V_2 = \tau(V_\gamma)$ to complete the proof.

Proposition 10.10. *Let T be a $\mathbb{Z}_p$-representation of G_0 of rank d. Suppose $k \in \mathbb{N}$, $v(p^k) > 4C_2 + 4C_3$, and suppose $G \subset G_0$ is an open normal subgroup acting trivially on T/p^kT, and $H = G \cap H_0$. Let $n \in \mathbb{N}, n \geq n(G)$. Then there exists a unique $D_{H,n}(T) \subset \widetilde{\Lambda} \otimes T$, a free $\Lambda_{H,n}$-module of rank d, such that:*

(1) *$D_{H,n}(T)$ is fixed by H, and stable by G_0;*
(2) *$\widetilde{\Lambda} \otimes_{\Lambda_{H,n}} D_{H,n}(T) \xrightarrow{\sim} \widetilde{\Lambda} \otimes T$;*
(3) *there exists a basis $\{e_1, \ldots, e_d\}$ of $D_{H,n}$ over $\Lambda_{H,n}$ such that if $\gamma \in G/H$, then $v(V_\gamma - 1) > C_3$, V_γ being the matrix of γ.*

Proof. This is a translation of Proposition 10.9, by the correspondence

$$\widetilde{\Lambda}\text{-representations of } G_0 \text{ up to isomorphism } \longleftrightarrow \text{elements of } H^1(G_0, \mathrm{GL}_d(\widetilde{\Lambda})).$$

Let $\{v_1, \cdots, v_d\}$ be a $\mathbb{Z}_p$-basis of T, this is also regarded as a $\tilde{\Lambda}$-basis of $\tilde{\Lambda} \otimes T$, which is a $\tilde{\Lambda}$-representation of G_0. Let $\sigma \mapsto U_\sigma$ be the corresponding cocycle from G_0 to $\mathrm{GL}_d(\mathbb{Z}_p) \hookrightarrow \mathrm{GL}_d(\tilde{\Lambda})$. Then G is a normal subgroup of G_0 such that for every $\sigma \in G$, $v(U_\sigma - 1) > 4C_2 + 4C_3$. Therefore the conditions in Proposition 10.9 are satisfied. Then there exists $M \in \mathrm{GL}_d(\tilde{\Lambda})$, $v(M-1) > C_2 + C_3$, such that $\sigma \mapsto V_\sigma = M^{-1}U_\sigma\sigma(M)$ satisfies that $V_\sigma \in \mathrm{GL}_d(\Lambda_{H,n(G)})$ and $V_\sigma = 1$ for $\sigma \in H$.

Now let $(e_1, \cdots e_d) = (v_1, \cdots, v_d)M$. Then $\{e_1, \cdots, e_d\}$ is a basis of $\tilde{\Lambda} \times T$ with corresponding cocycle V_σ. For $n \geq n(G)$, let $D_{H,n}(T)$ be the free $\Lambda_{H,n}$-module generated by the e_i's. Clearly (1) and (2) are satisfied. Moreover, if $\gamma \in G/H$,

$$\begin{aligned} v(V_\gamma - 1) =& v(M^{-1}(U_\gamma - 1)M + M^{-1}U_\gamma(\gamma - 1)(M-1)) \\ \geq& v(M-1) > C_2 + C_3 > C_3. \end{aligned}$$

For the uniqueness, suppose D_1 and D_2 both satisfy the condition, let $\{e_1, \cdots, e_d\}$ and $\{e'_1, \cdots, e'_d\}$ be the basis of D_1 and D_2 respectively as given in (3). Let V_γ and W_γ be the corresponding cocycles, let P be the base change matrix of the two bases. Then

$$W_\gamma = P^{-1}V_\gamma\gamma(P) \quad \Rightarrow \quad \gamma(P) = V_\gamma^{-1}PW_\gamma.$$

By Lemma 10.8, then $P \in \mathrm{GL}_d(\Lambda_{H,n(G)})$ and $D_1 = D_2$.

Remark 10.11. H_0 acts through H_0/H (which is finite) on $D_{H,n}(T)$. If $\Lambda_{H,n}$ is étale over $\Lambda_{H_0,n}$ (the case in applications), and then $D_{H_0,n}(T) = D_{H,n}(T)^{(H_0/H)}$, is locally free over $\Lambda_{H_0,n}$ (in most cases it is free), and

$$\Lambda_{H,n} \bigotimes_{\Lambda_{H_0,n}} D_{H_0,n}(T) \xrightarrow{\sim} D_{H,n}(T). \tag{10.3}$$

10.2 Overconvergent rings

From now in this chapter, for convenience of our exposition, the following notations are adapted for the rings defined in §5.3:

$$A := \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \subset A^b := W(R), \qquad B := \widehat{\mathcal{E}^{\mathrm{ur}}} \subset B^b := W(R)[\frac{1}{p}],$$
$$\widetilde{A} = W(\mathrm{Fr}\, R), \qquad \widetilde{B} = \mathrm{Frac}(\widetilde{A}) = W(\mathrm{Fr}\, R)[\frac{1}{p}].$$

Here ^{b} stands for bounded.

10.2.1 The valuations v_r on $B^b = W(R)[\frac{1}{p}]$.

Definition 10.12. *For $x = \sum\limits_{n \gg -\infty} p^n [x_n] \in B^b$ with $x_n \in R$, set*

$$v_r(x) := \begin{cases} v_p(x) = p\text{-adic valuation of } x, & \text{if } r = \infty; \\ \inf\limits_{n\in\mathbb{Z}} \{v(x_n) + nr\} = \min\limits_{n\in\mathbb{Z}} \{v(x_n) + nr\}, & \text{if } 0 \le r < \infty. \end{cases} \tag{10.4}$$

Proposition 10.13. *For $0 \le r \le \infty$, v_r is a valuation on B^b. Moreover,*

(1) $v_0(x) = \lim\limits_{r\to 0^+} v_r(x)$.
(2) $v_\infty(x) = \lim\limits_{r\to +\infty} \frac{v_r(x)}{r}$.
(3) $v_r(g(x)) = v_r(x)$ *for* $g \in G_{K_0}$.
(4) $v_{pr}(\varphi(x)) = p v_r(x)$.

Proof. We just check v_r is a valuation, the rest is clear.

The case $r = \infty$ is trivial.

For $r > 0$, by Lemma 1.28, we immediately have

(a) $v_r(x) = +\infty$ if and only if $x = 0$,
(b) $v_r(x + y) \ge \min\{v_r(x), v_r(y)\}$,
(c) $v_r(x \cdot y) \ge v_r(x) + v_r(y)$.

Moreover, suppose $x = \sum p^n [x_n]$, $y = \sum p^n [y_n]$. Write

$$x \cdot y = \sum p^n [z_n].$$

Then by Lemma 1.28(2), z_n is a generalized polynomial of x_i and y_j, homogeneous of degree $(1, 1)$. Suppose

$$n_0 = \min\{n \mid v_r(x) = v(x_n) + nr\}, \quad m_0 = \min\{m \mid v_r(y) = v(y_m) + mr\},$$

then

$$z_{m_0+n_0} = \lambda_{m_0} \mu_{n_0} + \text{ terms whose valuation is bigger},$$

hence $v_r(x\cdot y)=v_r(x)+v_r(y)$.

For $r=0$, then $v_0(x)=\lim\limits_{r\to 0^+}v_r(x)$ if $x\in A^b$. Note that if $x\in A^b$, $r>r'>0$, then $v_r(x)\geq v'_r(x)$. Thus $v_0|_{A^b}$ is a valuation. Note that $v_0(p)=0$, then v_0 is a valuation on B^b.

Proposition 10.14. *The function $r\mapsto v_r(x)$ $(r>0)$ is a concave function. In particular, if $0<R_1\leq r\leq R_2$, then $v_r(x)\geq\min\{v_{R_1}(x),v_{R_2}(x)\}$.*

Proof. For every n,

$$v(x_n)\geq v_{R_1}(x)-nR_1,\ v(x_n)\geq v_{R_2}(x)-nR_2.$$

Let $r=tR_1+(1-t)R_2$, $0\leq t\leq 1$, then

$$v(x_n)\geq tv_{R_1}(x)+(1-t)v_{R_2}(x)-nr.$$

Hence $v_r(x)\geq tv_{R_1}(x)+(1-t)v_{R_2}(x)$, and the function $r\mapsto v_r(x)$ is concave

Definition 10.15. *For $x=\sum_n p^n[x_n]\in\widetilde{A}$, define*

$$w_k(x):=\min\{v(x_n)\mid 0\leq n\leq k\}. \tag{10.5}$$

Remark 10.16. One checks easily that for $\alpha\in\operatorname{Fr}R$, $w_k(x)\geq -v(\alpha)$ if and only if $[\alpha]x\in W(R)+p^{k+1}\widetilde{A}$.

Proposition 10.17. (1) *For $x\in A^b$ and $r>0$,*

$$v_r(x)=\inf_n(v(x_n)+nr)=\inf_n(w_n(x)+nr).$$

(2) *The sets $\{x\in A^b\mid w_n(x)\geq A\}$ $(n\geq 0, A>0)$, as well as the sets $\{x\in A^b\mid v_r(x)\geq B\}$ $(r>0,B>0)$, form a basis of neighborhood of 0 for the natural topology on A^b. Hence v_r is continuous.*

Proof. Exercise.

Remark 10.18. v_0 is NOT continuous in B^b. For example, if $x\in\mathfrak{m}_R\backslash\{0\}$, $v_0([1+x]-1)=0$, but $v_0(0)=+\infty$.

10.2.2 The rings of overconvergent elements.

From now on assume $0<r<+\infty$. It would be great if we can extend the valuations v_r to $\widetilde{A}$ and $\widetilde{B}$. However, for an element $x=\sum\limits_{n=0}^{+\infty}p^n[x_n]\in\widetilde{A}$,

$$v_r(x):=\inf_{k\in\mathbb{N}}(v(x_k)+kr)=\inf_{k\in\mathbb{N}}(w_k(x)+kr)\in\mathbb{R}\cup\{\pm\infty\}. \tag{10.6}$$

To extend the valuation, one must exclude those x such that $v_r(x)=-\infty$.

Definition 10.19. *The set of* overconvergent elements *with respect to r is*

$$\begin{aligned} \widetilde{A}_r := & \{x \in \widetilde{A} \mid \lim_{k\to+\infty}(v(x_k) + kr) = +\infty\} \\ = & \{x \in \widetilde{A} \mid \lim_{k\to+\infty}(w_k(x) + kr) = +\infty\}. \end{aligned} \tag{10.7}$$

For $x \in \widetilde{A}_r$, set $v_r(x)$ as in (10.6).

Proposition 10.20. *$\widetilde{A}_r$ is a ring and v_r defines a semi-valuation on $\widetilde{A}_r$ satisfying the following properties:*

(1) $v_r(x) = +\infty \Leftrightarrow x = 0$;
(2) $v_r(xy) \geq v_r(x) + v_r(y)$;
(3) $v_r(x+y) \geq \min(v_r(x), v_r(y))$;
(4) $v_r(px) = v_r(x) + r$;
(5) $v_r([\alpha]x) = v(\alpha) + v_r(x)$ *if* $\alpha \in \mathrm{Fr}\, R$;
(6) $v_r(g(x)) = v_r(x)$ *if* $g \in G_{K_0}$;
(7) $v_{pr}(\varphi(x)) = pv_r(x)$.

Moreover, $\widetilde{A}_r$ is complete under v_r.

Proof. This is an easy exercise.

Lemma 10.21. *For $x = \sum_{k=0}^{+\infty} p^k[x_k] \in \widetilde{A}$, the following conditions are equivalent:*

(1) $\sum_{k=0}^{+\infty} p^k[x_k]$ *converges in* B_{dR}^+.
(2) $\sum_{k=0}^{+\infty} p^k x_k^{(0)}$ *converges in* C.
(3) $\lim_{k\to+\infty}(k + v(x_k)) = +\infty$.
(4) $x \in \widetilde{A}_1$.

Proof. (3) $\Leftrightarrow$ (4) is by definition of $\widetilde{A}_1$. (2) $\Leftrightarrow$ (3) is by definition of v. (1) $\Rightarrow$ (2) is by continuity of $\theta : B_{\mathrm{dR}}^+ \to C$. So it remains to show (2) $\Rightarrow$ (1).

We know that

$$a_k = k + [v(x_k)] \to +\infty \text{ if } k \to +\infty.$$

Write $x_k = \varpi^{a_k - k} y_k$, then $y_k \in R$. We have

$$p^k[x_k] = \left(\frac{p}{[\varpi]}\right)^k [\varpi]^{a_k}[y_k] = p^{a_k}\left(\frac{\xi}{p} - 1\right)^{a_k - k}[y_k].$$

By expanding $(1-x)^a$ into power series, we see that

$$p^{a_k}\left(\frac{\xi}{p}-1\right)^{a_k-k} \in p^{a_k-m}W(R)+(\operatorname{Ker}\theta)^{m+1}$$

for all m. Thus, $a_k \to +\infty$ implies that $p^k[x_k] \to 0 \in B_{\mathrm{dR}}^+/(\operatorname{Ker}\theta)^{m+1}$ for every m, and therefore also in B_{dR}^+.

Remark 10.22. We just proved that $\widetilde{A}_1 = B_{\mathrm{dR}}^+ \cap \widetilde{A}$, and we can use the isomorphism

$$\varphi^{-n} : \widetilde{A}_{p^n} \xrightarrow{\sim} \widetilde{A}_1$$

to embed $\widetilde{A}_r$ in B_{dR}^+ for $r \leq p^n$.

Definition 10.23. *The ring of overconvergent elements*

$$\widetilde{A}^\dagger := \bigcup_{r>0} \widetilde{A}_r = \{x \in \widetilde{A} \mid \varphi^{-n}(x) \text{ converges in } B_{\mathrm{dR}}^+ \text{ for } n \gg 0\}.$$

Lemma 10.24. *An element $x = \sum_{k=0}^{+\infty} p^k[x_k]$ is a unit in $\widetilde{A}_r$ if and only if $x_0 \neq 0$ and $v(\frac{x_k}{x_0}) > -kr$ for all $k \geq 1$. In this case, $v_r(x) = v(x) = v(x_0)$.*

Proof. The if part is an easy exercise.

Now if $x = \sum_{k=0}^{+\infty} p^k[x_k]$ is a unit in $\widetilde{A}_r$, suppose $y = \sum_{k=0}^{+\infty} p^k[y_k]$ is its inverse. Certainly $x_0y_0 = 1$ and $x_0 \neq 0$. We may assume $x_0 = y_0 = 1$. Suppose m, n are maximal such that

$$v(x_m) + mr = v_r(x) \leq v(x_0) = 0, \quad v(y_n) + nr = v_r(y) \leq v(y_0) = 0.$$

We need to show $m = n = 0$. If not, then $v_r(x) < 0$ and $v_r(y) < 0$. Compare the coefficients of p^{m+n} in the identity $xy = 1$, we get

$$x_{m+n}y_0 + \cdots + x_my_n + \cdots x_0y_{m+n} = 0 \bmod p.$$

Note that x_my_n is of valuation $v_r(x)+v_r(y)-(m+n)r < 0$, and other terms in the left hand side is of valuation greater than $v_r(x)+v_r(y)-(m+n)r$, impossible. Thus $m = n = 0$ and for $k > 0$, $v(x_k)+kr > v(x_0)$ or equivalently, $v(\frac{x_k}{x_0}) > -kr$.

Definition 10.25. *For $0 < r < \infty$, set*

$$\widetilde{B}_r := \widetilde{A}_r[\frac{1}{p}] = \bigcup_{n\in\mathbb{N}} p^{-n}\widetilde{A}_r,$$

endowed with the topology of inductive limit, and

$$\widetilde{B}^\dagger := \bigcup_{r>0} \widetilde{B}_r,$$

again with the topology of inductive limit.

$\widetilde{B}^{\dagger}$ is found to be a field, called the *field of overconvergent elements*:

Theorem 10.26. *$\widetilde{B}^{\dagger}$ is a subfield of $\widetilde{B}$, stable by continuous φ- and G_{K_0}-actions.*

Proof. We only prove that non-zero elements are invertible in $\widetilde{B}^{\dagger}$. The continuity of φ- and G_{K_0}-actions is left as an exercise.

Suppose $x = \sum\limits_{k=k_0}^{+\infty} p^k[x_k] \in \widetilde{B}_r$ with $x_{k_0} \neq 0$, then $x = p^{k_0}[x_{k_0}]y$ with $y = \sum\limits_{k=0}^{+\infty} p^k[y_k] \in \widetilde{B}_r$ and $y_0 = 1$. It suffices to show that y is invertible in $\widetilde{B}^{\dagger}$. Suppose $v_r(y) \geq -C$ for some constant $C \geq 0$. Choose $s > 0$ such that $s - r > C$. Then $v(y_k) + ks > v(y_k) + kr + kC > 0$ if $k \geq 1$. By Lemma 10.24, y is invertible in $\widetilde{A}_s$.

Definition 10.27. *Set*

$$B^{\dagger} := \widetilde{B}^{\dagger} \cap B,\ \ A^{\dagger} := \widetilde{A}^{\dagger} \cap B \ \mathit{and} A_r := \widetilde{A}_r \cap B.$$

Assume L is a finite extension of K_0 and $H_L = \mathrm{Gal}(\overline{K}/L^{\mathrm{cyc}})$.

(i) *If $\Lambda \in \{A, B, \widetilde{A}^{\dagger}, \widetilde{B}^{\dagger}, A^{\dagger}, B^{\dagger}, A_r, B_r\}$, set $\Lambda_L := \Lambda^{H_L}$.*
(ii) *If $\Lambda \in \{A, B, A^{\dagger}, B^{\dagger}, A_r, B_r\}$ and $n \in \mathbb{N}$, set $\Lambda_{L,n} := \varphi^{-n}(\Lambda_L) \subset \widetilde{B}$.*

By definition, $B^{\dagger}$ is a subfield of B stable by φ- and G_{K_0}-actions.

From now on in this chapter, we suppose L is a finite Galois extension of K_0. Recall $k_L^{\mathrm{c}} = k_{L^{\mathrm{cyc}}}$ is a finite Galois extension of k. By Proposition 5.18. $E_L = k_L^{\mathrm{c}}((\overline{\pi}_L))$ where $\overline{\pi}_L$ is any uniformizer of E_L. Let $F' = F'_L = L^{\mathrm{cyc}} \cap K_0^{\mathrm{ur}} = \mathrm{Frac}\, W(k_L^{\mathrm{c}})$. We want to describe $A_{L,r} = \widetilde{A}_r \cap \mathcal{O}_{\mathcal{E}_L}$ more concretely. We know that

$$A_{K_0} = \mathcal{O}_{\mathcal{E}_0} = \widehat{W((\boldsymbol{\pi}))} = \left\{ \sum_{n=-\infty}^{+\infty} \lambda_n \boldsymbol{\pi}^n \mid \lambda_n \in W,\ \lambda_n \to 0 \text{ when } n \to -\infty \right\},$$

and $B_{K_0} = \widehat{W((\boldsymbol{\pi}))}[\frac{1}{p}]$, where $\boldsymbol{\pi} = [\varepsilon] - 1$.

Consider the extension E_L/E_0. There are two cases:

(i) If E_L/E_0 is unramified, then $E_L = k_L^{\mathrm{c}}((\pi))$. Then

$$A_L = \mathcal{O}_{\mathcal{E}_L} = \left\{ \sum_{n=-\infty}^{+\infty} \lambda_n \boldsymbol{\pi}^n \mid \lambda_n \in \mathcal{O}_{F'} = W(k_L^{\mathrm{c}}),\ \lambda_n \to 0 \text{ when } n \to -\infty \right\}.$$

Let $\tilde{\pi}_L = \boldsymbol{\pi}$ in this case.

(ii) In general, let $\overline{\pi}_L$ be a uniformizer of $E_L = k_L^{\mathrm{c}}((\overline{\pi}_L))$, and let $\overline{P}_L(X) \in E_{F'}[X] = k_L^{\mathrm{c}}((\pi))[X]$ be a minimal polynomial of $\overline{\pi}_L$. Let $P_L(X) \in W(k_L^{\mathrm{c}})[[\boldsymbol{\pi}]][X]$ be a monic lifting of $\overline{P}_L$. By Hensel's Lemma, there exists a unique $\tilde{\pi}_L \in A_L$ such that $P_L(\tilde{\pi}_L) = 0$ and $\overline{\pi}_L = \tilde{\pi}_L \bmod p$.

Lemma 10.28. *If we define*

$$r_L := \begin{cases} 1, & \textit{if in case } (\mathrm{i}), \\ 2v(\mathfrak{D}), & \textit{otherwise} . \end{cases} \tag{10.8}$$

where $\mathfrak{D}$ is the different of $E_L/E_{F'}$, then $\tilde{\pi}_L$ and $P_L'(\tilde{\pi}_L)$ are units in $A_{L,r}$ for all $r > r_L$.

Proof. We first show the case (i). We have $\boldsymbol{\pi} = [\varepsilon - 1] + p[x_1] + p^2[x_2] + \cdots$, where x_i is a polynomial in $\varepsilon^{p^{-i}} - 1$ with coefficients in $\mathbb{Z}$ and no constant term. Then $v(x_i) \geq v(\varepsilon^{p^{-i}} - 1) = \frac{1}{(p-1)p^{i-1}}$. This implies that $\boldsymbol{\pi} = [\varepsilon - 1](1 + p[a_1] + p^2[a_2] + \cdots)$, with $v(a_1) = v(x_1) - v(\varepsilon - 1) \geq -1$ and $v(a_i) \geq -v(\varepsilon - 1) \geq -i$ for $i \geq 2$. By Lemma 10.24, $\boldsymbol{\pi}$ is a unit in $A_{L,r}$ for $r > r_L$.

In general, by the construction of $\tilde{\pi}_L$ from Hensel's Lemma, we have $\tilde{\pi}_L = [\overline{\pi}_L] + p[\alpha_1] + p^2[\alpha_2] + \cdots$ and $v(\overline{\pi}_L) = \frac{1}{e}v(\pi) = \frac{p}{e(p-1)}$ where $e = [E_L : E_{F'}]$ is the ramification index. Then $v(\frac{\alpha_i}{\overline{\pi}_L}) \geq -v(\overline{\pi}_L) = -\frac{p}{e(p-1)}$. Thus $\tilde{\pi}_L$ is a unit $A_{L,r}$ for $r > \frac{p}{e(p-1)}$. It is easy to check $\frac{p}{e(p-1)} \geq 2v(\mathfrak{D}_{E_L/E_{F'}})$.

Similarly, $P_L'(\tilde{\pi}_L) = [\overline{P}_L'(\overline{\pi}_L)] + p[\beta_1] + p^2[\beta_2] + \cdots$, and

$$v\left(\frac{\beta_i}{\overline{P}_L'(\overline{\pi}_L)}\right) \geq -v(\overline{P}_L'(\overline{\pi}_L)) = -v(\mathfrak{D}_{E_L/E_{F'}}),$$

while the last equality follows from Proposition 1.80. Thus $P_L'(\tilde{\pi}_L)$ is a unit $A_{L,r}$ for $r > 2v(\mathfrak{D}_{E_L/E_{F'}})$.

Let $s : E_L \to A_L$ be the section of $x \mapsto \bar{x} \bmod p$ given by the formula

$$s\left(\sum_{k\in\mathbb{Z}} a_k \overline{\pi}_L^k\right) = \sum_{k\in\mathbb{Z}} [a_k]\tilde{\pi}_L^k. \tag{10.9}$$

For $x \in A_L$, define $\{x_n\}_{n\in\mathbb{N}}$ recursively by $x_0 = x$ and $x_{n+1} = \frac{1}{p}(x_n - s(\bar{x}_n))$. Then $x = \sum_{n=0}^{+\infty} p^n s(\bar{x}_n)$. By this way,

$$A_L = \{\sum_{n\in\mathbb{Z}} a_n \tilde{\pi}_L^n \mid a_n \in \mathcal{O}_{F'}, \lim_{n\to-\infty} v(a_n) = +\infty\} \tag{10.10}$$

Lemma 10.29. *Suppose $x \in A_L$.*

(1) *If $k \in \mathbb{N}$, then $w_k(\frac{x - s(\bar{x})}{p}) \geq \min(w_{k+1}(x), w_0(x) - (k+1)r_L)$.*
(2) *For the x_n's defined above, $v(\bar{x}_n) \geq \min_{0\leq i\leq n}(w_i(x) - (n-i)r_L)$.*

Proof. We first note that, since $\tilde{\pi}_L$ is a unit in $A_{L,r}$, if $\bar{y} \in E_L$ and $r > r_L$, then $s(\bar{y}) \in A_r$ and $v_r(s(\bar{y})) = v(\bar{y})$. Thus

$$w_k\left(\frac{x - s(\bar{x})}{p}\right) = w_{k+1}(x - s(\bar{x})) \geq \min\left(w_{k+1}(x), v(\bar{x}) - (k+1)r_L\right).$$

Now (1) follows from the fact $w_0(x) = v(\bar{x})$.

By (1), $w_k(x_{n+1}) \geq \min(w_{k+1}(x_n), w_0(x) - (k+1)r_L)$. By induction, one has

$$w_k(x_n) \geq \min\left(w_{k+n}(x), \min_{0\leq i\leq n-1} w_i(x) - (k+n-i)r_L\right).$$

Take $k = 0$, then (2) follows.

Proposition 10.30. (1) *If $r > r_L$, then*

$$A_{L,r} = \{f(\tilde{\pi}_L) = \sum_{k\in\mathbb{Z}} a_k \tilde{\pi}_L^k \mid a_k \in \mathcal{O}_{F'}, \lim_{k\to-\infty} (rv(a_k) + kv(\overline{\pi}_L)) = +\infty\}. \tag{10.11}$$

In this case, one has

$$v_r(f(\tilde{\pi}_L)) = \inf_{k\in\mathbb{Z}} (rv(a_k) + kv(\overline{\pi}_L)). \tag{10.12}$$

(2) *The map $f \mapsto f(\tilde{\pi}_L)$ is an isomorphism from bounded analytic functions with coefficients in F' on the annulus $0 < v_p(T) \leq \frac{1}{r}v(\overline{\pi}_L)$ to the ring $B_{L,r}$.*

Proof. (2) is a direct consequence of (1). Suppose $x = \sum_{k\in\mathbb{Z}} a_k \tilde{\pi}_L^k$. One can write $a_k\tilde{\pi}_L^k$ in the form $p^{v(a_k)}[\pi_L^k]u$ where u is a unit in the ring of integers of A_r. Hence $v_r(a_k\tilde{\pi}_L^k) = kv(\overline{\pi}_L) + rv(a_k)$. If $\lim\limits_{k\to-\infty}(rv(a_k) + kv(\overline{\pi}_L)) = +\infty$, then $x = \sum_{k\in\mathbb{Z}} a_k\tilde{\pi}_L^k$ converges in A_r and $v_r(x) \geq \inf\limits_{k\in\mathbb{Z}}(rv(a_k) + kv(\overline{\pi}_L))$.

On the other hand, if $x \in A_r$, suppose $(x_n)_{n\in\mathbb{N}}$ is the sequence constructed as above, and suppose $v_n = \frac{1}{v(\overline{\pi}_L)} \min\limits_{0\leq i\leq n}(w_i(x) + (i-n)r_L)$. By Lemma 10.29, one can write $\bar{x}_n$ as $\sum\limits_{k\geq v_n} \alpha_{n,k}\overline{\pi}_L^k$. Then $x = \sum_{k\in\mathbb{Z}} a_k\tilde{\pi}_L^k$, where $a_k = \sum\limits_{n\in I_k} p^n[\alpha_{k,n}] \in \mathcal{O}_{F'}$ and $I_k = \{n \in \mathbb{N} \mid v_n \leq k\}$. The p-adic valuation of a_k is bigger than or equal to the smallest element in I_k. But by definition, $v_n \leq k$ if and only if there exists $i \leq n$ such that $w_i(x) + (i-n)r_L \leq kv(\overline{\pi}_L)$, in other words, if and only if there exists $i \leq n$ such that

$$w_i(x) + ir + (n-i)(r - r_L) \leq krv(\overline{\pi}_L) + nr.$$

One then deduces that

$$rv(a_k) + kv(\overline{\pi}_L) \geq \min_{0\leq i\leq n}((w_i(x) + ir) + (n-i)(r - r_L)),$$

This implies $\lim\limits_{k\to-\infty}(rv(a_k)+kv(\overline{\pi}_L)) = +\infty$ and $v_r(x) \leq \inf\limits_{k\in\mathbb{Z}}(rv(a_k)+kv(\overline{\pi}_L))$.

Corollary 10.31. (1) *$A_{L,r}$ is a principal ideal domain;*

(2) *If L/M is a finite Galois extension over K_0, then $A_{L,r}$ is an étale extension of $A_{M,r}$ if $r > r_L$, and the Galois group is nothing but H_M/H_L.*

Define $\widetilde{\pi}_n = \varphi^{-n}(\boldsymbol{\pi})$, $\widetilde{\pi}_{L,n} = \varphi^{-n}(\tilde{\pi}_L)$. Let $L_n = L(\varepsilon^{(n)})$ for $n > 0$.

Proposition 10.32. *Suppose $r_L \geq p^n$. Then*

(1) *$\theta(\widetilde{\pi}_{L,n})$ is a uniformizer of L_n;*
(2) *$\widetilde{\pi}_{L,n} \in L_n[[t]] \subset B_{\mathrm{dR}}^+$.*

Proof. First by definition

$$\widetilde{\pi}_n = [\varepsilon^{1/p^n}] - 1 = \varepsilon^{(n)} e^{t/p^n} - 1 \in K_{0,n}[[t]] \subset B_{\mathrm{dR}}^+,$$

which implies the proposition in the unramified case.

For the ramified case, we proceed as follows.

By the definition of E_L, $\pi_{L,n} = \theta(\widetilde{\pi}_{L,n})$ is a uniformizer of $L_n \bmod \mathfrak{a} = \{x \mid v_p(x) \geq \frac{1}{p}\}$. Let ω_n be the image of $\pi_{L,n}$ in $L_n \bmod \mathfrak{a}$. So we just have to prove $\pi_{L,n} \in L_n$.

Suppose the minimal polynomial of $\tilde{\pi}_L$ is

$$P_L(x) = \sum_{i=0}^{d} a_i(\boldsymbol{\pi}) x^i,\ \ a_i(\boldsymbol{\pi}) \in \mathcal{O}_{F'}[[\boldsymbol{\pi}]].$$

Write $\pi_n = \theta(\tilde{\pi}_n)$. Define

$$P_{L,n}(x) = \sum_{i=0}^{d} a_i^{\varphi^{-n}}(\pi_n) x^i,$$

then $P_{L,n}(\pi_{L,n}) = \theta(\varphi(P_L(\tilde{\pi}_L))) = 0$. Then we have $v(P_{L,n}(\omega_n)) \geq \frac{1}{p}$ and

$$v(P'_{L,n}(\omega_n)) = \frac{1}{p^n} v(P'_L(\overline{\pi}_L)) = \frac{1}{p^n} v(\mathfrak{d}_{E_L/E_0}) < \frac{1}{2p} \text{ if } r_L > p^n.$$

Then one concludes by Hensel's Lemma that $\pi_{L,n} \in L_n$.

For (2), one uses Hensel's Lemma in $L_n[[t]]$ to conclude $\widetilde{\pi}_{L,n} \in L_n[[t]]$.

Corollary 10.33. *If $r > r_L$ and $r \geq p^n$, $\varphi^{-n}(A_{L,r}) \subseteq L_n[[t]] \subseteq B_{\mathrm{dR}}^+$.*

For $L = K_0$, we have the following results:

Lemma 10.34. *If $r > p^n$ and $i \in \mathbb{Z}_p^\times$, then $[\varepsilon]^{ip^n} - 1$ is a unit in $A_{K_0,r}$ and $v_r([\varepsilon]^{ip^n} - 1) = p^n v(\pi)$.*

Proof. We know that $\boldsymbol{\pi} = [\varepsilon] - 1$ is a unit in $A_{K_0,r}$ for $r > 1$, then $[\varepsilon]^{p^n} - 1 = \varphi^n(\boldsymbol{\pi})$ is a unit in $A_{K_0,r}$ for $r > p^n$. In general,

$$\frac{[\varepsilon]^{ip^n} - 1}{[\varepsilon]^{p^n} - 1} = i + \sum_{k=1}^{\infty} \binom{i}{k+1} ([\varepsilon]^{p^n} - 1)^k$$

is a unit in A_{K_0}, hence we have the lemma.

Lemma 10.35. *Let* $\gamma \in \Gamma_{K_0}$, *suppose* $\chi(\gamma) = 1 + up^n \in \mathbb{Z}_p^\times$ *with* $u \in \mathbb{Z}_p^\times$. *Then for* $r > p^n$,

(1) $v_r(\gamma(\boldsymbol{\pi}) - \boldsymbol{\pi}) = p^n v(\pi)$;
(2) $v_r(\gamma(x) - x) \geq v_r(x) + (p^n - 1)v(\pi)$ *for* $x \in A_{K_0,r}$.

Proof. We have $\gamma(\boldsymbol{\pi}) - \boldsymbol{\pi} = [\varepsilon]([\varepsilon]^{up^n} - 1)$. By Lemma 10.34, $[\varepsilon]^{up^n} - 1$ is a unit in $A_{K_0,r}$ for $r > p^n$, then $v_r(\gamma(\boldsymbol{\pi}) - \boldsymbol{\pi}) = v_r([\varepsilon]^{up^n} - 1) = p^n v(\pi)$. This finishes the proof of (1).

For (2), write $x = \sum_k a_k \boldsymbol{\pi}^k$ where $rv(a_k) + kv(\pi) \to +\infty$ as $k \to +\infty$. We know, by the proof of Proposition 10.30, that $v_r(x) = \min_k\{n_k v(\pi) + kr\}$ where $n_k = \min\{n \mid v(a_n) = k\}$. Now

$$\begin{aligned}
\gamma(\boldsymbol{\pi}^k) - \boldsymbol{\pi}^k =& \boldsymbol{\pi}^k \left(\frac{\gamma(\boldsymbol{\pi})^k}{\boldsymbol{\pi}^k} - 1 \right) \\
=& \boldsymbol{\pi}^k \sum_{j=1}^{\infty} \binom{k}{j} \left(\frac{\gamma(\boldsymbol{\pi})}{\boldsymbol{\pi}} - 1 \right)^j \\
=& \boldsymbol{\pi}^{k-1}(\gamma(\boldsymbol{\pi}) - \boldsymbol{\pi}) \sum_{j=0}^{\infty} \binom{k}{j+1} \left(\frac{\gamma(\boldsymbol{\pi})}{\boldsymbol{\pi}} - 1 \right)^j,
\end{aligned}$$

therefore

$$\gamma(x) - x = (\gamma(\boldsymbol{\pi}) - \boldsymbol{\pi}) \sum_k a_k \boldsymbol{\pi}^{k-1} \sum_{j=0}^{+\infty} \binom{k}{j+1} \left(\frac{\gamma(\boldsymbol{\pi})}{\boldsymbol{\pi}} - 1 \right)^j$$

and

$$v_r(\gamma(x) - x) \geq p^n v(\pi) + \min_k\{(n_k - 1)v(\pi) + kr\} = v_r(x) + (p^n - 1)v(\pi).$$

This finishes the proof of (2).

10.3 Overconvergent representations

The aim of this section is to prove the result of Cherbonnier-Colmez [CC98] that all p-adic representations are overconvergent by the generalized Tate-Sen's method.

If V is a free $\mathbb{Z}_p$-representation of rank d of G_K, we studied the associated $(\varphi, (\boldsymbol{\Gamma})$-module $\mathbf{D}(V)$ of V in § 5.3, which is a free A_K-module of rank d. Let

$$\mathbf{D}_r(V) := (A_r \otimes_{\mathbb{Z}_p} V)^{H_K} \subset \mathbf{D}(V) = (A \otimes_{\mathbb{Z}_p} V)^{H_K}. \tag{10.13}$$

This is an $A_{K,r}$-module stable by $\boldsymbol{\Gamma}_K$-action. Moreover, the Frobenius map φ sends $\mathbf{D}_r(V)$ to $\mathbf{D}_{pr}(V)$.

Definition 10.36. *A free $\mathbb{Z}_p$-representation V of G_K is called an* overconvergent representation *over K if there exists an $r_V \geq r_K > 0$ such that*

$$A_K \bigotimes_{A_{K,r_V}} \mathbf{D}_{r_V}(V) \xrightarrow{\sim} \mathbf{D}(V).$$

A p-adic representation of G_K is called overconvergent if it has an overconvergent G_K-stable $\mathbb{Z}_p$-lattice.

Remark 10.37. One may replace K by any finite extension L of K_0 to get overconvergent representations of L.

Suppose V is a free $\mathbb{Z}_p$-representation. If V is overconvergent, by definition, then for all $r > r_V$,

$$\mathbf{D}_r(V) = A_{K,r} \bigotimes_{A_{K,r_V}} \mathbf{D}_{r_V}(V).$$

We choose a basis $\{e_1, \cdots, e_d\}$ of $\mathbf{D}_{r/p}(V)$ over $A_{K,r/p}$ for $r/p \geq r_V$, then $x \in \mathbf{D}_r(V)$ can be written as $\sum_i x_i \varphi(e_i)$, we define the valuation v_r by

$$v_r(x) := \min_{1 \leq i \leq d} v_r(x_i). \tag{10.14}$$

One can see that for a different choice of basis, the valuation differs by a bounded constant.

Lemma 10.38. *Suppose V is an over-convergent $\mathbb{Z}_p$-representation over L. If $\{e_1, \cdots, e_d\}$ is a basis of $\mathbf{D}_r(V)$ over $A_{L,r}$ and $e_i \in \varphi(D(V))$ for every i, then $x = \sum x_i e_i \in \mathbf{D}_r(V)^{\psi=0}$ if and only if $x_i \in A_{L,r}^{\psi=0}$ for every i.*

Proof. One sees that $\psi(x) = 0$ if and only if $\varphi(\psi(x)) = 0$. As $e_i \in \varphi(D(V))$, $\varphi(\psi(e_i)) = e_i$ and $\varphi(\psi(x)) = \sum_i \varphi(\psi(x_i))e_i$. Therefore $\psi(x) = 0$ if and only if $\varphi(\psi(x_i)) = 0$ for every i, or equivalently, $\psi(x_i) = 0$ for every i.

Proposition 10.39. *If V is overconvergent over L, then there exists a constant C_V such that if $\gamma \in \mathbf{\Gamma}_L$, $n(\gamma) = v_p(\log(\chi(\gamma)))$ and $r > \max\{pr_V, p^{n(\gamma)}\}$, then $\gamma - 1$ is invertible in $\mathbf{D}_r(V)^{\psi=0}$ and*

$$v_r((\gamma - 1)^{-1}x) \geq v_r(x) - C_V - p^{n(\gamma)}v(\pi). \tag{10.15}$$

Remark 10.40. (a) Since through different choices of bases, v_r differs by a bounded constant, the result of the above proposition is independent of the choice of bases.
(b) We shall apply the result to $A_{L,r}^{\psi=0}$.

Proof. First, note that if replace V by $\mathrm{Ind}_{G_L}^{G_{K_0}} V$, we may assume that $L = K_0$.

Suppose $r > pr_V$, pick a basis $\{e_1, \cdots, e_d\}$ of $\mathbf{D}_{p^{-1}r}(V)$ over $A_{K_0,p^{-1}r}$, then $\{\varphi(e_1), \cdots, \varphi(e_d)\}$ is a basis of $\mathbf{D}_r(V)$ over $A_{K_0,r}$. By Lemma 10.38, every $x \in \mathbf{D}_r(V)^{\psi=0}$ can be written uniquely as $x = \sum_{i=1}^{p-1} [\varepsilon]^i \varphi(x_i)$ with $x_i = \sum_{j=1}^{d} x_{ij} e_j \in \mathbf{D}_{p^{-1}r}(V)$. Suppose $\chi(\gamma) = 1 + up^n$ for $u \in \mathbb{Z}_p^\times$ and $n = n(\gamma)$. Then

$$\begin{aligned}(\gamma - 1)x &= \sum_{i=1}^{p-1} [\varepsilon]^{i(1+up^n)} \varphi(\gamma(x_i)) - \sum_{i=1}^{p-1} [\varepsilon]^i \varphi(x_i) \\ &= \sum_{i=1}^{p-1} [\varepsilon]^i \varphi\left([\varepsilon]^{iup^{n-1}} \gamma(x_i) - x_i\right) := \sum_{i=1}^{p-1} [\varepsilon]^i \varphi f_i(x_i).\end{aligned}$$

We claim that the map $f : x \mapsto [\varepsilon]^{up^n} \gamma(x) - x$ is invertible in A_r for $r > \max\{r_V, p^n\}$ for $u \in \mathbb{Z}_p^\times$ and n is sufficiently large. Indeed, as the action of γ is continuous, we may assume $v_r((\gamma - 1)e_j) \geq 2v(\pi)$ for every $j = 1, \cdots, d$ for n sufficiently large. Then

$$\frac{f(x)}{[\varepsilon]^{up^n} - 1} = \frac{[\varepsilon]^{up^n}}{[\varepsilon]^{up^n} - 1} (\gamma(x) - x) + x := -y + x,$$

and

$$\gamma(x) - x = \sum_{j=1}^{d} (\gamma(x_j) - x_j) \gamma(e_j) + \sum_{j=1}^{d} x_j (\gamma(e_j) - e_j),$$

therefore by Lemma 10.35,

$$v_r(y) \geq v_r(x) + 2v(\pi)$$

for every $x \in \mathbf{D}_r(V)$. Thus

$$g(x) = ([\varepsilon]^{up^n} - 1)^{-1} \sum_{k=0}^{+\infty} y^k$$

is the inverse of f and moreover,

$$v_r\left(g(x) - \frac{x}{[\varepsilon]^{up^n} - 1}\right) \geq v_r(x) + v(\pi).$$

By the above claim, we see that if $n \gg 0$, $r > \max\{pr_V, p^n\}$, then $\gamma - 1$ has a continuous inverse $\sum_{i=1}^{p-1} [\varepsilon]^i \varphi^{-1} \circ f_i^{-1}$ in $\mathbf{D}_r(V)^{\psi=0}$ and

$$v_r((\gamma - 1)^{-1}(x)) \geq v_r(x) - p^n v(\pi) - C_V$$

for some constant C_V. In general, if $\gamma^p - 1$ is invertible in $\mathbf{D}_r(V)^{\psi=0}$ for $r > \max\{pr_V, p^{n+1}\}$, we just set

$$(\gamma - 1)^{-1}(x) = \varphi^{-1} \circ (\gamma^p - 1)^{-1} (1 + \cdots + \gamma^{p-1})(\varphi(x)),$$

which is an inverse of $\gamma - 1$ in $\mathbf{D}_r(V)^{\psi=0}$ for $r > \max\{pr_V, p^n\}$. The proposition follows inductively.

Theorem 10.41. *The quadruple*

$$\widetilde{\Lambda} = \widetilde{A}_1,\ v = v_1,\ G_0 = G_{K_0}, \Lambda_{H_{L,n}} = \varphi^{-n}(A_{L,1})$$

satisfies Tate-Sen's conditions.

Proof. We need to check the conditions (TS 1) – (TS 3).

(TS 1). Let $L \supset M \supset K_0$ be finite extensions. Suppose

$$\alpha = [\overline{\pi}_L](\sum_{\tau \in H_M/H_L} \tau([\overline{\pi}_L]))^{-1},$$

then for all n,

$$\sum_{\tau \in H_M/H_L} \tau(\varphi^{-n}(\alpha)) = 1,$$

and

$$\lim_{n \to +\infty} v_1(\varphi^{-n}(\alpha)) = 0.$$

(TS 2). First $\Lambda_{H_L,n} = \varphi^{-n}(A_{L,1})$. Suppose $r_L \geq p^n$. We can define $R_{L,n}$ by the following commutative diagram:

$$R_{L,n}: \quad \begin{tikzcd} & \widetilde{A}_{L,1} \arrow[r] & \varphi^{-n}(A_{L,1}) \\ \varphi^{-n-k}(A_{L,1}) \arrow[ur, hook] \arrow[urr, "\varphi^{-n}\circ\psi^k\circ\varphi^{n+k}"'] & & \end{tikzcd}$$

One verifies that $\varphi^{-n} \circ \psi^k \circ \varphi^{n+k}$ does not depend on the choice of k, using the fact $\psi\varphi = \mathrm{Id}$. By definition, for $x \in \bigcup_{k \geq 0} \varphi^{-n-k}(A_{L,1})$, we immediately have:

(a) $R_{L,n} \circ R_{L,n+m} = R_{L,n}$;
(b) If $x \in \varphi^{-n}(A_{L,1})$, $R_{L,n}(x) = x$;
(c) $R_{L,n}$ is $\varphi^{-n-k}(A_{L,1})$-linear;
(d) $\lim\limits_{n \to +\infty} R_{L,n}(x) = x$

Furthermore, for $x = \varphi^{-n-k}(y) \in \varphi^{-n-k}(A_{L,1})$,

$$R_{L,n}(x) = \varphi^{-n}(\psi^k(y)) = \varphi^{-n-k}(\varphi^k \circ \psi^k(y)).$$

Write y uniquely as $\sum_{i=0}^{p^k-1} [\varepsilon]^i \varphi^k(y_i)$, then by Corollary 5.30, $\psi^k(y) = y_0$. Thus

$$v_1(R_{L,n}(x)) = v_1(\varphi^{-n}(y_0)) \geq v_1(\varphi^{-n-k}(y)) = v_1(x).$$

By the above inequality, $R_{L,n}$ is continuous and can be extended to $\widetilde{\Lambda}$ as $\bigcup_{k \geq 0} \varphi^{-n-k}(A_{L,1})$ is dense in $\widetilde{A}^{(0,1]}$ and the condition (TS2) is satisfied.

(TS 3). Let $R^*_{L,n}(x) = R_{L,n+1}(x) - R_{L,n}(x)$, then

$$R^*_{L,n}(x) = \varphi^{-n-1}(1-\varphi\psi)(\psi^{k-1}(y)) \in \varphi^{-n-1}(A^{\psi=0}_{L,1}),$$

thus

$$\begin{aligned} R^*_{L,n}(x) \in \varphi^{-n-1}(A^{\psi=0}_{L,1}) \cap \tilde{A}_1 =& \varphi^{-n-1}(A^{\psi=0}_{L,1} \cap \tilde{A}_{p^{n+1}}) \\ =& \varphi^{-(n+1)}\left(A^{\psi=0}_{L,p^{n+1}}\right). \end{aligned}$$

For an element x such that $R_{L,n}(x) = 0$, we have

$$x = \sum_{i=0}^{+\infty} R^*_{L,n+i}(x), \text{ where } R^*_{L,n+i}(x) \in \varphi^{-(n+i+1)}\left(A^{\psi=0}_{L,p^{-(n+i+1)}}\right).$$

Apply Proposition 10.39 on $A^{\psi=0}_{L,p^{-(n+i+1)}}$, then if n is sufficiently large, one can define the inverse of $\gamma - 1$ in $(R_{L,n} - 1)\widetilde{\Lambda}$ as

$$(\gamma-1)^{-1}(x) = \sum_{i=0}^{+\infty} \varphi^{-(n+i+1)}(\gamma-1)^{-1}(\varphi^{n+i+1}R^*_{L,n+i}(x))$$

and for $x \in (R_{L,n} - 1)\widetilde{\Lambda}$,

$$v((\gamma-1)^{-1}x) \geq v(x) - C,$$

thus (TS3) is satisfied.

Theorem 10.42 (Cherbonnier-Colmez [CC98]). *All free $\mathbb{Z}_p$- and p-adic representations of G_K are overconvergent.*

Proof. One just needs to show the case for free $\mathbb{Z}_p$-representations. The p-adc representation case follows by $\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$.

For $(\widetilde{\Lambda}, v, G_0, \Lambda_{H_L,n})$ as in the above Theorem, Sen's method (§10.1, in particular Proposition 10.9) implies that for any continuous cocycle $\sigma \mapsto U_\sigma$ in $H^1_{\mathrm{cont}}(G_0, \mathrm{GL}_d(\widetilde{\Lambda}))$, there exists an $n > 0$, $M \in \mathrm{GL}_d(\widetilde{\Lambda})$ such that $V_\sigma \in \mathrm{GL}_d(\varphi^{-n}(A_{K,1}))$ for $\chi(\sigma) \gg 0$ and V_σ is trivial in H'_K.

If V is a $\mathbb{Z}_p$-representation of G_K, pick a basis of V over $\mathbb{Z}_p$, let U_σ be the matrix of $\sigma \in G_K$ under this basis, then $\sigma \mapsto U_\sigma$ is a continuous cocycle with values in $\mathrm{GL}_d(\mathbb{Z}_p)$. Now the fact $V(D(V)) = V$ means that the image of $H^1_{\mathrm{cont}}(H'_K, \mathrm{GL}_d(\mathbb{Z}_p)) \to H^1_{\mathrm{cont}}(H'_K, \mathrm{GL}_d(A))$ is trivial, thus there exists $N \in \mathrm{GL}_d(A)$ such that the cocycle $\sigma \mapsto W_\sigma = N^{-1}U_\sigma\sigma(N)$ is trivial over H'_K. Let $C = N^{-1}M$, then $C^{-1}V_\sigma\sigma(C) = W_\sigma$ for $\sigma \in G_K$. As V_σ and W_σ is trivial in H'_K, we have $C^{-1}V_\gamma\gamma(C) = W_\gamma$. Apply Lemma 10.8, when n is sufficiently large, $C \in \mathrm{GL}_d(\varphi^{-n}(A_{K,1}))$ and thus $M = NC \in \mathrm{GL}_d(\varphi^{-n}(A_{K,1}))$.

Translate the above results to results about representations, there exists an n and an $\varphi^{-n}(A_{K,1})$-module $D_{K,n} \subset \widetilde{A}_1 \bigotimes V$ such that

$$\widetilde{A}_1 \otimes_{\varphi^{-n}(A_{K,1})} D_{K,n} \xrightarrow{\sim} \widetilde{A}_1 \otimes V.$$

Moreover, one concludes that $D_{K,n} \subset \varphi^{-n}(\mathbf{D}(V))$ and $\varphi^n(D_{K,n}) \subset \mathbf{D}(V) \cap \varphi^n(\widetilde{A}_1 \bigotimes V) = \mathbf{D}_{p^n}(V)$. We can just take $r_V = p^n$.

References

[AGV73] M. Artin, A. Grothendieck, and J.-L. Verdier, *Théorie des topos et cohomologie étale des schémas*, Lecture Notes in Math., no. 269,270,305, Springer-Verlag, 1972, 1973, Séminaire de géométrie algébrique du Bois-Marie 1963-1964.

[AHHV17] N. Abe, G. Henniart, F. Herzig, and M-F. Vignéras, *A classification of irreducible admissible modp representations of p-adic reductive groups*, J. Amer. Math. Soc. **30** (2017), no. 2, 495–559.

[And02a] Y. André, *Filtrations de type Hasse-Arf et monodromie p-adique*, Invent. Math. **148** (2002), no. 2, 285–317.

[And02b] ———, *Représentations galoisiennes et opérateur de Bessel p-adiques*, Ann. Inst. Fourier(Grenoble) **52** (2002), no. 3, 779–808.

[Ax70] J. Ax, *Zeroes of polynomials over local fields- the Galois action*, J. Algebra **15** (1970), 417–428.

[Bar59] I. Barsotti, *Moduli canonici e gruppi analitici commutativi*, Ann. Scuola Norm. Sup. Pisa **13** (1959), 303–372.

[BB08] D. Benois and L. Berger, *Théorie d'Iwasawa des représentations cristallines ii*, Comment. Math. Helv. **83** (2008), 603–677.

[BB10] L. Berger and C. Breuil, *Sur quelques représentations potentiellement cristallines de* $\mathrm{GL}_2(\mathbb{Q}_p)$, Astérisque **330** (2010), 155–211.

[BD02] D. Benois and T. Nyuyen Quang Do, *Les nombres de Tamagawa locaux et la conjecture de Bloch et Kato pour les motifs* $\mathcal{Q}(m)$ *sur un corps abélien*, Ann. Sc. École Norm. Sup. (4) (2002).

[BD20] C. Breuil and Y. Ding, *Higher* $\mathcal{L}$*-invariants for* $\mathrm{GL}_3(\mathbb{Q}_p)$ *and local-global compatibility*, Camb. J. Math. **8** (2020), no. 4, 775–951.

[BDIP00] J. Bertin, J.-P. Demailly, L. Illusie, and C. Peters, *Introduction to Hodge Theory*, SMF/AMS Texts and Monographs, no. 8, American Mathematical Society, 2000, Translation from the 1996 French original by James Lewis and Peters.

[BE10] C. Breuil and M. Emerton, *Représentations p-adiques ordinaires de* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et compatibilité local-global*, Astérisque, no. 331, Soc. Math. de France, 2010.

[Ben00] D. Benois, *Iwasawa theory of crystalline reprersentations*, Duke Math. J. **104** (2000), no. 2, 211–267.

[Ber74] P. Berthelot, *Cohomologie cristalline des schémas de caractéristique* $p > 0$, Lecture Notes in Math., no. 407, Springer, 1974.

[Ber01] L. Berger, *Représentations* p*-adiques et équations différentielles*, Ph.D. thesis, Université Paris 6, 2001.

[Ber02] ______, *Représentations* p*-adiques et équations différentielles*, Invent. Math. **148** (2002), 219–284.

[Ber03] ______, *Bloch and Kato's exponetial map: three explicit formula*, Doc. Math. (2003), 99–129, Extra volume to Kazuya Kato's fiftieth birthday.

[Ber04a] ______, *An introduction to the theory of* p*-adic representations*, Geometric Aspects of Dwork Theory, Walter de Gruyter, Berlin, 2004, pp. 255–292.

[Ber04b] ______, *Limites de repésentations cristallines*, Compositio Math. **140** (2004), no. 6, 1473–1498.

[Ber04c] ______, *Représentations de de rham et normes universelles*, Bull. Soc. Math. France **133** (2004), no. 4, 601–618.

[Ber08] ______, *Équations différentielle* p*-adique et* (φ, N)*-modules filtrés*, Astérisque **319** (2008), 13–38.

[Ber16] ______, *Multivariable* (ϕ, Γ)*-modules and locally analytic vectors*, Duke Math. J. **165** (2016), no. 18, 3567–3595.

[BH15] C. Breuil and F. Herzig, *Ordinary representations of* $g(\mathbf{Q}_p)$ *and fundamental algebraic representations*, Duke Math. J. **164** (2015), no. 7, 1271–1352.

[BK86] S. Bloch and K. Kato, p*-adic étale cohomology*, Publ. Math. IHES. **63** (1986), 107–152.

[BK90] ______, L*-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift (P. Cartier et al., ed.), vol. I, Progress in Math., no. 86, Birkhaüser, Boston, 1990, pp. 333–400.

[BL94] L. Barthel and R. Leviné, *Irrreducible modular representations of* GL_2 *of a local field*, Duke Math. J. **75** (1994), no. 2, 261–292.

[BL95] ______, *Modular representations of* GL_2 *of a local field: the ordinary, unramified case*, J. Number Theory **55** (1995), no. 1, 1–27.

[BLZ04] L. Berger, H. Li, and H. Zhu, *Construction of some families of* 2*-dimensional crystalline representations*, Math. Ann. **329** (2004), no. 2, 365–377.

[BM02] C. Breuil and A. Mézard, *Multiplicitiés modulaires et représentations de* $\mathrm{GL}_2(\mathbb{Z}_p)$ *et de* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ *en* $\ell = p$, Duke Math. J. **115** (2002), no. 2, 205–310, Avec un appendice par Guy Henniart.

[BMS18] B. Bhatt, M. Morrow, and P. Scholze, *Integral* p*-adic Hodge theory*, Publ. Math. Inst. Hautes Études Sci. **128** (2018), 219–397.

[BO78] P. Berthelot and A. Ogus, *Notes on crystalline cohomology*, Princeton Univ. Press, 1978.

[BO83] ______, F*-isocrystals and de Rham cohomology i*, Invent. Math. **72** (1983), 159–199.

[Bog80] F. Bogomolov, *Sur l'algébricité des représentations* ℓ*-adiques*, CRAS Paris **290** (1980), 701–703.

[Bou89] N. Bourbaki, *Commutative Algebra*, Springer-Verlag, 1989.

[BP12] C. Breuil and V. Paskunas, *Towards a modulo* p *langlands correspondence for* GL_2, Mem. Amer. Math. Soc. **216** (2012), 1–114.

[BPX20] L. Berger, P.Schneider, and B. Xie, *Rigid character groups, Lubin-Tate theory, and* (ϕ, γ)*-modules*, vol. 263, Amer. Math. Soc., 2020.

[Bre98] C. Breuil, *Cohomologie étale de p-torsion et cohomologie cristalline en réduction semi-stable*, Duke Math. J. **95** (1998), 523–620.

[Bre99a] ———, *Représentations semi-stables et modules fortement divisibles*, Invent. Math. **136** (1999), no. 1, 89–122.

[Bre99b] ———, *Une remarque sur les représentations locale p-adiques et les congruences entre formes modulaires de hilbert*, Bull. Soc. Math. France **127** (1999), no. 3, 459–472.

[Bre00a] ———, *Groupes p-divisibles, groupes finis et modules filtrés*, Ann. of Math. (2) **152** (2000), 489–549.

[Bre00b] ———, *Integral p-adic Hodge theory*, Algebraic Geometry 2000, Azumino (Hotaka), 2000.

[Bre03a] ———, *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathbb{Q}_p)$, Compositio Math. **138** (2003), no. 2, 165–188.

[Bre03b] ———, *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathrm{Q}_p)$ *II*, J. Inst. Math. Jessieu **2** (2003), 23–58.

[Bre04] ———, *Invariant $\mathcal{L}$ et série spéciale p-adique*, Ann. Sc. Ecole Norm. Sup. (4) **37** (2004), no. 4, 459–610.

[Bre10] ———, *Série spéciale p-adiques et cohomologie éale complétée*, Astérisque **331** (2010), 65–115.

[CC98] F. Cherbonnier and P. Colmez, *Représentations p-adiques surconvergentes*, Invent. Math. **133** (1998), no. 3, 581–611.

[CC99] ———, *Théorie d'Iwasawa des représentations p-adiques d'un corps local*, J. Amer. Math. Soc. **12** (1999), 241–268.

[CDN20] P. Coleze, G. Dospinescu, and W. Niziol, *Cohomologie p-adique de la tour de Drinfeld: le cas de la dimension* 1, J. Amer. Math. Soc. **33** (2020), no. 2, 311–362.

[CDN21] P. Colmez, G. Dospinescu, and W. Niziol, *Integral p-adic étale cohomology of Drinfeld symmetric spaces*, Duke Math. J. **170** (2021), no. 3, 575–613.

[CF00] P. Colmez and J.-M. Fontaine, *Construction des représentations p-adiques semi-stables*, Invent. Math. **140** (2000), 1–43.

[CFS20] M. Chen, L. Fargues, and X. Shen, *On the structure of some p-adic period domains*, Camb. J. Math. **9** (2020), no. 1, 213–267.

[Che14] M. Chen, *Composantes connexes géométriques de la tour des espaces de modules de groupes p-divisibles*, Ann. Sci. Éc. Norm. Supér. (4) **47** (2014), no. 4, 723–764.

[Chr01] G. Christol, *About a Tsuzuki theorem*, p-adic functional analysis (Ioannina, 2000), Lecture Notes in Pure and Applied Math., vol. 222, Dekker, New York, 2001, pp. 63–74.

[CKV17] M. Chen, M. Kisin, and E. Viehmann, *Connected components of affine Deligne-Lusztig varieties in mixed characteristic*, Compos. Math. **151** (2017), no. 9, 1697–1762.

[CM97] G. Christol and Z. Mebkhout, *Sur le théorème de l'indice des équations différentielles p-adiques II*, Ann. of Math. (2) **146** (1997), no. 2, 345–410.

[CM00] ———, *Sur le théorème de l'indice des équations différentielles p-adiques III*, Ann. of Math. (2) **151** (2000), no. 2, 385–457.

[CM01] ———, *Sur le théorème de l'indice des équations différentielles p-adiques IV*, Invent. Math. **143** (2001), no. 3, 629–672.

[CM02] ———, *Équations différentielles p-adiques et coefficients p-adiques sur les courbes*, Cohomologies p-adiques et applications arithmétiques, II, Astérisque, vol. 279, Soc. Math. France, 2002, pp. 125–183.

[Coh46] I. S. Cohen, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math. Soc. **59** (1946), 54–106.

[Col93] P. Colmez, *Périodes des variétés abéliennes à multiplication complexe*, Ann. of Math. (2) **138** (1993), 625–683.

[Col94] ———, *Sur un résultat de Shankar Sen*, C. R. Acad. Sci. Paris Sér. I Math. **318** (1994), 983–985.

[Col99a] ———, *Représentations cristallines et représentations de hauteur finie*, J. Reine Angew. Math. **514** (1999), 119–143.

[Col99b] ———, *Théorie d'Iwasawa des représentations de de Rham d'un corps local*, Ann. of Math. (2) **148** (1999), 485–571.

[Col00] ———, *Fonctions L p-adiques*, Séminaire Bourbaki. Vol 1998/1999, Astérisque, vol. 266, Soc. Math. France, 2000, pp. 21–58.

[Col02] ———, *Espaces de Banach de dimension fine*, J. Inst. Math. Jussieu **1** (2002), no. 3, 331–439.

[Col03] ———, *Les conjectures de monodromie p-adiques*, Séminaire Bourbaki. Vol 2001/2002, Astérisque, vol. 290, Soc. Math. France, 2003, pp. 53–101.

[Col04a] ———, *La conjecture de Birch et Swinnerton-Dyer p-adiques*, Séminaire Bourbaki. Vol 2002/2003, Astérisque, vol. 294, Soc. Math. France, 2004, pp. 251–319.

[Col04b] P. Colmez, *Une correspondance de Langlands locale p-adiques pour les représentations semi-stables de dimension* 2, Prépublication (2004).

[Col05a] ———, *Fontaine's rings and p-adic L-functions*, 2005, Lecture Notes of a course given in Fall 2004 at Tsinghua University, Beijing, China.

[Col05b] ———, *Série principale unitaire pour* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et représentations triangulines de dimension* 2, Prépublication (2005).

[Col10a] ———, *Fonctions d'une variable p-adique*, Astérisque **330** (2010), 13–59.

[Col10b] ———, *Représentations de* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et Φ-Γ-modules*, Astérisque, no. 330, Soc. Math. de France, 2010.

[Cre98] R. Crew, *Finiteness theorems for the cohomology of an overconvergent isocrystal on a curve*, Ann. Sci. E.N.S. (4) **31** (1998), 717–763.

[Dee01] J. Dee, *Φ-Γ modules for families of Galois representations*, J. Algebra **235** (2001), no. 2, 636–664.

[Del70] P. Deligne, *Equations différentielles à points singuliers réguliers*, Lecture Notes in Math., no. 163, Springer, 1970.

[Del73] ———, *Les constantes des équations fonctionelles des fonctions L*, Modular Functions of One Variable, no. 349, Springer, 1973.

[Del74a] ———, *La conjecture de Weil, I*, Publ. Math. IHES **43** (1974), 273–308.

[Del74b] ———, *Théorie de Hodge, III*, Publ. Math. IHES **44** (1974), 5–77.

[Del80] ———, *La conjecture de Weil, II*, Publ. Math. IHES **52** (1980), 137–252.

[Del90] ———, *Catégories tannakiennes*, The Grothendieck Festschrift (P. Cartier et al., ed.), vol. II, Progress in Math., no. 87, Birkhaüser, Boston, 1990, pp. 111–195.

[Dem72] M. Demazure, *Lectures on p-divisible groups*, Lecture Notes in Math., no. 302, Springer, 1972.

[Die57] J. Dieudonné, *Groupes de Lie et hyperalgèbres de lie sur un corps de caractéristique* $p > 0$, Math. Ann. **134** (1957), 114–133.

[Din17a] Y. Ding, *$\mathcal{L}$-invariants, partially de Rham families, and local-global compatibility*, Ann. Inst. Fourier (Grenoble) **67** (2017), no. 4, 1457–1519.

[Din17b] ———, *Formes modulaires p-adiques sur les courbes de Shimura unitaires et compatibilité local-global*, Mém. Soc. Math. Fr. (N.S.) (2017), no. 155, 1–245.

[DM82] P. Deligne and J. S. Milne, *Tannakian categories*, Hodge Cycles, Motives and Shimura Varieties (P. Deligne et al, ed.), Lecture Notes in Math., no. 900, Springer, 1982, pp. 101–228.

[DO12] Y. Ding and Y. Ouyang, *A simple proof of Dieudonné-Manin classification Theorem*, Acta. Math. Sin. (Engl. Ser.) **28** (2012), no. 8, 1553–1558.

[Dwo60] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.

[Edi92] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594.

[EH14] M. Emerton and D. Helm, *The local Langlands correspondence for gl_n in families*, Ann. Sci. École Norm. Sup. (4) **47** (2014), no. 4, 655–722.

[Eme05] M. Emerton, *p-adic l-functions and unitary completions of representations of p-adic reductive groups*, Duke Math. J. **130** (2005), no. 2, 353–392.

[Eme06a] ———, *A local-global compatibility conjecture in the p-adic Langlands programme for $gl_{2\mathbf{Q}}$*, Pure Appl. Math. Q. **2** (2006), no. 2, 279–393.

[Eme06b] ———, *On the interpolation of systems of eigenvalues attached to automorphic Hecke eigenforms*, nvent. Math. **164** (2006), no. 1, 1–84.

[Fal87] G. Faltings, *Hodge-Tate structures and modular forms*, Math. Ann. **278** (1987), 133–149.

[Fal88] ———, *p-adic Hodge-Tate theory*, J. Amer. Math. Soc. **1** (1988), 255–299.

[Fal89] ———, *Crystalline cohomology and p-adic étale cohomology*, Algebraic analysis, geometry and number theory, The John Hopkins Univ. Press, 1989, pp. 25–80.

[Fal90] ———, *F-isocrystals on open varieties, results and conjectures*, The Grothendieck Festschrift (P. Cartier et al., ed.), vol. II, Progress in Math., no. 87, Birkhaüser, Boston, 1990, pp. 249–309.

[Fal94] ———, *Mumford-Stabilität in der algebraischen Geometrie*, Proceedings of the International Congress of Mathematicians (Zürich, 1994), Birkhaüser, Basel, 1994, pp. 648–655.

[Fal02] ———, *Almost étale extensions*, Cohomologies p-adiques et applications arithmétiques, II, Astérisque, vol. 279, Soc. Math. France, 2002, pp. 185–270.

[Far09] L. Fargues, *Filtration de monodromie et cycles évanescents formels*, Invent. Math. **177** (2009), 281–305.

[Far20] ———, *g-torseurs en théorie de Hodge p-adique*, Compos. Math. **156** (2020), 2076–2110.

[FF14] L. Fargues and J-M. Fontaine, *Vector bundles on curves and p-adic Hodge theory*, London Math. Soc. Lecture Note Ser., no. 415, Cambridge Univ. Press, 2014.

[FF18] ———, *Courbes et fibrés vectoriels en théorie de Hodge p-adique*, Astérisque, vol. 406, Soc. Math. France, 2018.

[FI93] J.-M. Fontaine and L. Illusie, *p-adic periods: a survey*, Proceedings of the Indo-French Conference on Geometry (Bombay, 1989) (Delhi), Hindustan Book Agency, 1993, pp. 57–93.

[FK88] E. Freitag and R. Kiehl, *Étale cohomology and the Weil conjecture*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), no. 13, Springer, 1988.

[FL82] J.-M. Fontaine and G. Laffaille, *Construction des représentations p-adiques*, Ann. Sci. E.N.S. (4) **15** (1982), 547–608.

[FM87] J.-M. Fontaine and W. Messing, *p-adic periods and p-adic étale cohomology*, Contemporary Mathematics **67** (1987), 179–207.

[FM95] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, Elliptic curves, modular forms, and Fermat's Last Theorem (HongKong, 1993) (J. Coates and S.T. Yau, eds.), International Press, Cambridge, MA, 1995, pp. 41–78.

[Fon71] J.-M. Fontaine, *Groupes de ramification et représentations d'Artin*, Ann. Sci. École Norm. Sup. (4) **4** (1971), 337–392.

[Fon79a] ______, *Groupe p-divisibles sur les corps locaux*, Astérisque, no. 47-48, Soc. Math. de France, 1979.

[Fon79b] ______, *Modules galoisiens, modules filtrés et anneaux de Barsotti-Tate*, Journées de Géométrie Algébrique de Rennes, vol. III, Astérisque, no. 65, Soc. Math. de France, 1979, pp. 3–80.

[Fon82a] ______, *Formes différentielles et modules de tate des variétés abéliennes sur les corps locaux*, Invent. Math. **65** (1982), 379–409.

[Fon82b] ______, *Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate*, Ann. Math. **115** (1982), 529–577.

[Fon83a] ______, *Cohomologie de de Rham, cohomologie cristalline et représentations p-adiques*, Algebraic Geometry Tokyo-Kyoto, Lecture Notes in Math., no. 1016, Springer, 1983, pp. 86–108.

[Fon83b] ______, *Représentations p-adique*, Proc. Int. Congress Math., PWN—Polish Scientific Publishers, Warsawa, 1983, pp. 475–486.

[Fon90] ______, *Représentations p-adiques des corps locaux, 1ère partie*, The Grothendieck Festschrift (P. Cartier et al., ed.), vol. II, Progress in Math., no. 87, Birkhaüser, Boston, 1990, pp. 249–309.

[Fon94a] ______, *Le corps des périodes p-adiques*, Périodes p-adiques, Astérisque, vol. 223, Soc. Math. France, 1994, With an appendix by P. Colmez, pp. 59–111.

[Fon94b] ______, *Représentations ℓ-adiques potentiellement semi-stables*, Périodes p-adiques, Astérisque, vol. 223, Soc. Math. France, 1994, Papers from the seminar held in Bures-sur-Yvette, 1988, pp. 321–347.

[Fon94c] ______, *Représentations p-adiques semi-stables*, Périodes p-adiques, Astérisque, vol. 223, Soc. Math. France, 1994, With an appendix by P. Colmez, pp. 113–184.

[Fon97] ______, *Deforming semistable Galois representations*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), no. 21, 11138–11141, Elliptic curves and modular forms (Washington, DC, 1996).

[Fon02] ______, *Analyse p-adique et représentations galoisiennes*, Proc. of I.C.M. Beijing 2002, Vol II, Higher Ed. Press, Beijing, 2002, pp. 139–148.

[Fon03] ______, *Presque $\mathbb{C}_p$-représentations*, Doc. Math. (2003), 285–385, Extra volume to Kazuya Kato's fiftieth birthday.

[Fon04a] ______, *Arithmétique des représentations galoisiennes p-adiques*, Cohomologies p-adiques et Applications Arithmétiques (III), Astérisque, Soc. Math. France, 2004.

[Fon04b] ———, *Représentations de de Rham et représentations semi-stables*, Prépublications, Université de Paris-Sud, Mathématiques (2004).

[FPR94] J.-M. Fontaine and B. Perrin-Riou, *Autour des conjectures de Bloch et Kato; cohomologie galoisienne et valeurs de donctions L*, Motives (Seattle, WA, 1991), Proc. Sympos. Pur Math., vol. 55, Part I, Amer. Math. Soc., Providence, RI, 1994, pp. 599–706.

[Frö68] A. Fröhlich, *Formal Groups*, Lecture Notes in Math., no. 74, Springer-Verlag, 1968.

[FvdP81] J. Fresnel and M. van der Put, *Géométrie analytique rigide et applications*, Prog. in Math., no. 18, Birkhäuser, 1981.

[FW79] J.-M. Fontaine and J.-P. Wintenberger, *Le "corps des normes" de certaines extensions algébriques de corps locaux*, C.R.A.S **288** (1979), 367–370.

[Gao17] H. Gao, *Galois lattices and strongly divisible lattices in the unipotent case*, J. Reine Angew. Math. **728** (2017), 263–299.

[GD60] A. Grothendieck and J. Dieudonné, *Le language des schémas*, vol. 4, 1960.

[GD61a] ———, *Étude cohomologique des faisceaux cohérents*, vol. 11, 17, 1961.

[GD61b] ———, *Étude globale élémentaire de quelques classes de morphismes*, vol. 8, 1961.

[GD67] ———, *Étude locale des schémas et des morphismes des schémas*, vol. 20,24,28,32, 1964,1965,1966,1967.

[GHLS17] T. Gee, F. Herzig, T. Liu, and D. Savitt, *Potentially crystalline lifts of certain prescribed types*, Doc. Math. **22** (2017), 397–422.

[GL14] H. Gao and T. Liu, *A note on potential diagonalizability of crystalline representations*, Math. Ann. **360** (2014), 481–487.

[GL20] ———, *Loose crystalline lifts and overconvergence of étale (φ, τ)-modules*, Amer. J. Math. **142** (2020), no. 6, 1733–1770.

[GLS07] T. Gee, T. Liu, and D. Savitt, *Torsion p-adic galois representations and a conjecture of Fontaine*, Ann. Sc. École Norm. Sup. (4) **40** (2007), 633–674.

[GLS14] ———, *The Buzzard-Diamond-Jarvis conjecture for unitary groups*, J. Amer. Math. Soc. **27** (2014), 389–435.

[GLS15] ———, *The weight part of Serre's conjecture for* $\mathrm{GL}(2)$, Forum Math. Pi **3** (2015), 1–52.

[GM87] H. Gillet and W. Messing, *Cycle classes and Riemann-Roch for crystalline cohomology*, Duke Math. J. **55** (1987), 501–538.

[God58] R. Godement, *Topologie algébrique et théorie des faisceaux*, Herman, Paris, 1958.

[Gro68] A. Grothendieck, *Crystals and the de Rham cohomology of schemes (notes by J. Coates and O. Jussila)*, Dix exposé sur la cohomologie étale des schémas, Masson et North Holland, 1968.

[Gro71] ———, *Groupes de Barsotti-Tate et cristaux*, Actes Congrès Int. Math. Nice 1970, t.1, Gauthiers-Villars, Paris, 1971.

[Gro74] ———, *Groupes de Barsotti-Tate et cristaux de Dieudonné*, Presses de l'Université de Montréal, 1974.

[Gro77] ———, *Cohomologie ℓ-adique et fonctions L*, Lecture Notes in Math., no. 589, Springer-Verlag, 1977.

[Gro85] M. Gros, *Classes de Chern et classes de cycles en cohomologie de Hodge-Witt logarithmique*, Mémoire Soc. Math. France, vol. 21, Gauthier-Villars, 1985.

[GZ67] P. Gabriel and M. Zisman, *Calculus of fractions and homotopy theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, no. 35, Springer-Verlag, 1967.

[Har77] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, 1977.

[Haz78] M. Hazewinkel, *Formal groups and applications*, Academic Press, 1978.

[Her98] L. Herr, *Sur la cohomologie galoisienne des corps p-adiques*, Bull. Soc. Math. France **126** (1998), 563–600.

[Her00] ———, *ϕ-γ-modules and Galois cohomology*, Invitation to higher local fields (Münster, 1999), Math. Institute, Univ. Warwick, 2000.

[Her01] ———, *Une approche nouvelle de la dualité locale de tate*, Math. Ann. **320** (2001), 307–337.

[Her09] F. Herzig, *The weight in a Serre-type conjecture for tame n-dimensional Galois representations*, Duke Math. J. **149** (2009), no. 1, 37–116.

[HK94] O. Hyodo and K. Kato, *Semi-stable reduction and crystalline cohomology with logarithmic poles*, Périodes p-adiques, Astérisque, vol. 223, Soc. Math. France, 1994, Papers from the seminar held in Bures-sur-Yvette, 1988, pp. 221–268.

[Hon70] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), 213–246.

[HP19] Y. Hu and V. Paskunas, *On crystabelline deformation rings of* $\mathrm{Gal}(\bar{\mathbf{q}}_p/(\mathbf{Q}_p)$*. With an appendix by Jack Shotton*, Math. Ann. **373** (2019), 421–487.

[HT15] Y. Hu and F. Tan, *The Breuil-Mézard conjecture for non-scalar split residual representations*, Ann. Sc. École Norm. Sup. (4) **48** (2015), 1383–1421.

[Hu21] Y. Hu, *Multiplicities of cohomological automorphic forms on* GL_2 *and mod p representations of* $\mathrm{GL}_2(\mathbf{Q}_p)$, J. Eur. Math. Soc. **23** (2021), 3625–3678.

[Hyo88] O. Hyodo, *A note on p-adic etale cohomology in the semi-stable reduction case*, Invent. Math. **91** (1988), 543–557.

[Hyo91] ———, *On the de Rham Witt complex attached to a semi-stable family*, Compositio Math. **78** (1991), 241–260.

[Hyo95] ———, $H^1_g = H^1_{st}$, 136–142, Volume en l'honneur de Hyodo.

[Ill75] L. Illusie, *Reports on crystalline cohomology*, Proc. Symp. Pure Math. **XXIX** (1975), 459–479.

[Ill76] ———, *Cohomologie cristalline, d'aprés P. Berthelot*, Lecture Notes in Math., vol. 514, Springer, 1976.

[Ill79a] ———, *Complexe de de Rham-Witt*, Journées de Géométrie Algébrique de Rennes (I), Astérisque, vol. 63, Soc. Math. France, 1979, pp. 83–112.

[Ill79b] ———, *Complexe de de Rham-Witt et cohomologie cristalline*, Ann. Sci. E.N.S. (4) **12** (1979), 501–661.

[Ill83] ———, *Finiteness, duality, and Künneth theorems in the cohomology of the de Rham-Witt complex*, Algebraic Geometry Tokyo-Kyoto, Lecture Notes in Mathematics, vol. 1016, Springer, 1983, pp. 20–72.

[Ill90] ———, *Cohomologie de de Rham et cohomologie étale p-adique*, Séminaire Bourbaki, exposé 726, Astérisque, vol. 189-190, Soc. Math. France, 1990, pp. 325–374.

[Ill94] ———, *Autour de théoréme de monodromie locale*, Périodes p-adiques, Astérisque, vol. 223, Soc. Math. France, 1994, Papers from the seminar held in Bures-sur-Yvette, 1988, pp. 9–57.

[Ill04] ———, *Algebraic Geometry*, 2004, Lecture Notes in Spring 2004, Tsinghua University, Beijing, China.

[Ill05] ———, *Grothendieck's existence theorem in formal geometry*, Fundamental algebraic geometry, Math. Surveys Monogr., vol. 123, Amer. Math. Soc., Providence, RI, 2005, pp. 179–233.

[IR83] L. Illusie and M. Raynaud, *Les suites spectrales associées au complexs de de Rham-Witt*, Publ. Math. IHES **57** (1983), 73–212.

[Jan88] U. Jannsen, *Continuous étale cohomology*, Math. Ann. **280** (1988), no. 2, 207–245.

[Jan89] ———, *On the ℓ-adic cohomology of varieties over number fields and its Galois cohomology*, Math. Sci. Res. Inst. Publ. **16** (1989), 315–360.

[Kat86] K. Kato, *On p-adic vanishing cycles, (Applications of ideas of Fontaine-Messing)*, Advanced Studies in Pure Math. **10** (1986), 207–251.

[Kat88] ———, *Logarithmic structures of Fontaine-Illusie*, Algebraic Analysis, Geometry and Number Theory, The John Hopkins Univ. Press, 1988, pp. 191–224.

[Kat93a] ———, *Iwasawa theory and p-adic Hodge theory*, Kodai Math. J. **16** (1993), no. 1, 1–31.

[Kat93b] ———, *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via* b_{dr}, Arithmetic Algebraic Geometry (Trento, 1991), vol. 1553, Springer, Berlin, 1993, pp. 50–163.

[Kat94] ———, *Semi-stable reduction and p-adic étale cohomology*, Périodes p-adiques, Astérisque, vol. 223, Soc. Math. France, 1994, Papers from the seminar held in Bures-sur-Yvette, 1988, pp. 269–293.

[Kat04] ———, *p-adic hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290.

[Ked04] K. Kedlaya, *A p-adic local monodromy theorem*, Ann. of Math. (2) **160** (2004), no. 1, 93–184.

[KL10] K. Kedlaya and R. Liu, *On families of* ϕ, Γ*-modules*, Algebra Number Theory **4** (2010), 943–967.

[KM74] N. Katz and W. Messing, *Some consequences of the Riemann hypothesis for varieties over finite fields*, Invent. Math. **23** (1974), 73–77.

[KM92] K. Kato and W. Messing, *Syntomic cohomology and p-adic étale cohomology*, Tohoku. Math. J (2) **44** (1992), no. 1, 1–9.

[KS90] M. Kashiwara and P. Schapira, *Sheaves on Manifolds*, 292 ed., Grundlehren der mathematischen Wissenschaften, Springer-Verlag, 1990.

[Laf80] G. Laffaille, *Groupes p-divisibles et modules filtrés: le cas ramifié*, Bull. Soc. Math. France **108** (1980), 187–206.

[Lan94] S. Lang, *Algebraic Number Theory*, 2 ed., Graduate Texts in Mathematics, vol. 110, Springer-Verlag, 1994.

[Liu02] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, 2 ed., Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, 2002.

[Liu08] R. Liu, *Cohomology and duality for* ϕ, Γ*-modules over the Robba ring*, Int. Math. Res. Not. **3** (2008), 1–32.

[Lub95] J. Lubin, *Sen's theorem on iteration of power series*, Proc. Amer. Math. Soc. **123** (1995), 63–66.

[LXZ12] R. Liu, B. Xie, and Y. Zhang, *Locally analytic vectors of unitary principal series of* $\mathrm{GL}_2(\mathbf{Q}_p)$, Ann. Sc. École Norm. Sup. (4) **45** (2012), 167–190.

[Man63] Y. Manin, *Theory of commutative formal groups over fields of finite characteristic*, Russian Math. Surveys **18** (1963), 1–83.

[Man65] ———, *Modular Fuchsiani*, Annali Scuola Norm. Sup. Pisa Ser. III **18** (1965), 113–126.

[Mat86] H. Matsumura, *Commutative ring theory*, Combridge Studies in Advanced Mathematics, vol. 8, Combridge University Press, 1986.

[Maz72] B. Mazur, *Frobenius and the Hodge filtration*, Bull. Amer. Math. Soc. **78** (1972), 653–667.

[Maz73] ———, *Frobenius and the Hodge filtration, estimates*, Ann. of Math. **98** (1973), 58–95.

[Meb02] Z. Mebkhout, *Analogue p-adique du théorème de Turrittin et le théorème de la monodromie p-adique*, Invent. Math. **148** (2002), 319–351.

[Mes72] W. Messing, *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, Lecture Notes in Math., no. 264, Springer, 1972.

[Mil80] J. M. Milne, *Étale cohomology*, Princeton University Press, 1980.

[MM74] B. Mazur and W. Messing, *Universal extensions and one dimensional crystalline cohomology*, Lecture Notes in Math., no. 370, Springer, 1974.

[MTT86] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.

[Nee02] A. Neeman, *A counter example to a 1961 "theorem" in homological algebra*, Invent. Math. **148** (2002), 397–420, With an appendix by P. Deligne.

[Nek93] J. Nekovar, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Prog. Math, vol. 108, Birkhäuser Boston, MA, 1993, pp. 127–202.

[Niz98] W. Niziol, *Crystalline Conjecture via K-theory*, Ann. Sci. E.N.S. **31** (1998), 659–681.

[Nyg81] N. Nygaard, *Slopes of powers of Frobenius on crystalline cohomology*, Ann. Sci. E.N.S. **14** (1981), 369–401.

[Pas13] V. Paskunas, *The image of Colmez's Montreal functor*, Publ. Math. IHES **118** (2013), 1–191.

[Plû09] J. Plût, *Espaces de Banach analytiques p-adiques et espaces de Banach-Colmez*, Ph.D. thesis, Université Paris-Sud XI, France, 2009.

[PR] B. Perrin-Riou, *Thé"orie d'iwasawa des représentations p-adiques semi-stables, year = 2001, series= Mém. Soc. Math. France.(N.S.), volume = 84* .

[PR92] ———, *Théorie d'Iwasawa et hauteurs p-adiques*, Invent. Math. **109** (1992), no. 1, 137–185.

[PR94a] ———, *Représentations p-adiques ordinaires*, Périodes p-adiques, Astérisque, vol. 223, Soc. Math. France, 1994, With an appendix by Luc Illusie, pp. 185–220.

[PR94b] ———, *Théorie d'Iwasawa des représentations p-adiques sur un corps local*, Invent. Math. **115** (1994), no. 1, 81–161.

[PR95] ———, *Fonctions L p-adiques des représentations p-adiques*, Astérisque, vol. 229, 1995.

[PR99] ———, *Théorie d'Iwasawa et loi explicite de réciprocité*, Doc. Math. **4** (1999), 219–273.

[PR00] ———, *Représentations p-adiques et normes universelles. I. Le cas cristalline*, J. Amer. Math. Soc. **13** (2000), no. 3, 533–551.

[Ray94] M. Raynaud, *Réalisation de de Rham des* 1*-motifs*, Périodes p-adiques, Astérisque, vol. 223, Soc. Math. France, 1994, Papers from the seminar held in Bures-sur-Yvette, 1988, pp. 295–319.

[RZ82] M. Rapoport and T. Zink, *Über die lokale Zetafunktion von Shimuravarietäten, Monodromièfiltration und verschwindende Zyklen in ungleicher Characteristik*, Invent. Math. **68** (1982), 21–201.

[RZ96] ———, *Period spaces for p-divisible groups*, Ann. Math. Studies, vol. 141, Princeton University Press, 1996.

[Sai88] M. Saito, *Modules de Hodge polarisables*, Publ. of the R.I.M.S, Kyoto Univ. **24** (1988), 849–995.

[Sai90] ———, *Mixed Hodge modules*, Publ. of the R.I.M.S, Kyoto Univ. **26** (1990), 221–333.

[Sch72] C. Schoeller, *Groupes affines, commutatifs, unipotents sur un corps non parfait*, Bull. Sco. Math. France **100** (1972), 241–300.

[Sch90] T. Scholl, *Motives for modular forms*, Invent. Math. **100** (1990), 419–430.

[Sch12] P. Scholze, *Perfectoid spaces*, Publ. Math. Inst. Hautes Études Sci. **116** (2012), 245–313.

[Sch13a] ———, *The local Langlands correspondence for* GL_n *over p-adic fields*, Invent. Math. **192** (2013), 663–715.

[Sch13b] ———, *p-adic Hodge theory for rigid-analytic varieties*, Forum Math. Pi **1** (2013), 1–77.

[Sch15] ———, *On torsion in the cohomology of locally symmetric varieties*, Ann. of Math. (2) **182** (2015), 945–1066.

[Sen72] S. Sen, *Ramification in p-adic Lie extensions*, Invent. Math. **17** (1972), 44–50.

[Sen73] ———, *Lie algebras of Galois groups arising from Hodge-Tate modules*, Ann. of Math. (2) **97** (1973), 160–170.

[Sen80] ———, *Continuous cohomologgy and p-adic Galois representations*, Invent. Math. **62** (1980), 89–116.

[Ser61] J.-P. Serre, *Sur les corps locaux á corps résiduel algébriquement clos*, Bull. Soc. Math. France **89** (1961), 105–154.

[Ser67a] ———, *Local class field theory*, Algebraic Number Theory (J.W.S. Cassels and A. Fröhlich, eds.), Academic Press, London, 1967, pp. 128–161.

[Ser67b] ———, *Résumé des cours 1965-66*, Annuaire du Collège France, Paris, 1967, pp. 49–58.

[Ser80] ———, *Local Fields*, Graduate Text in Mathematics, no. 67, Springer-Verlag, 1980, Translation from *Corps Locaux*, Hermann, Paris, 1962.

[Ser89] ———, *Abelian ℓ-adic representations and elliptic curves*, Advanced Book Classics series, Addison-Wesley, 1989.

[Ser02] ———, *Galois Cohomology*, 2 ed., Springer Monographs in Mathematics, Springer-Verlag, 2002.

[She14] X. Shen, *On the Hodge-Newton filtration for p-divisible groups with additional structures*, Int. Math. Res. Not. **13** (2014), 3582–3631.

[She18] ———, *On the l-adic cohomology of some p-adically uniformized Shimura varieties*, J. Inst. Math. Jussieu **17** (2018), 1197–1226.

[SR72] N. Saavedra Rivano, *Catégorie Tannakiennes*, Lecture Notes in Math., vol. 265, 1972.

[Ste76a] J. Steenbrink, *Limits of Hodge structures*, Invent. Math. **31** (1976), 229–257.

[Ste76b] ______, *Mixed Hodge structures on the vanishing cohomology*, Symp. in Math., Oslo, 1976.

[Tat67] J. Tate, *p-Divisible groups*, Proc. Conf. on Local Fields (T.A. Springer, ed.), Springer, 1967, pp. 158–183.

[Tat76] ______, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274.

[Tot96] B. Totaro, *Tensor products in p-adic Hodge Theory*, Duke Math. J. **83** (1996), 79–104.

[Tsu98a] N. Tsuzuki, *Finite local monodromy of overconvergent unit-root F-crystals on a curve*, Amer. J. Math. **120** (1998), 1165–1190.

[Tsu98b] ______, *Slope filtration of quasi-unipotent overconvergent F-isocrystals*, Ann. Inst. Fourier (Grenoble) **48** (1998), 379–412.

[Tsu99] T. Tsuji, *p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case*, Invent. Math. **137** (1999), 233–411.

[Tsu02] ______, *Semi-stable conjecture of Fontaine-Janssen: a survey*, Cohomologies p-adiques et applications arithmétiques, II, Astérisque., vol. 279, 2002, pp. 323–370.

[Ver96] J.-L. Verdier, *Des catégories dérivées des catégories abéliennes*, Astérisque, no. 239, 1996.

[Vig06] M.-F. Vignéras, *Série principale modulo p de groups réductifs p-adiques*, Prépublication (2006).

[Wac97] N. Wach, *Représentations cristallines de torsion*, Compositio Math. **108** (1997), 185–240.

[Win83] J.-P. Wintenberger, *Le corps des normes de certaines extensions infinied des corps locaux; applications*, Ann. Sci. E.N.S. **16** (1983), 59–89.

[Win84] ______, *Un scindage de la filtration de Hodge pour certaines variétés algébriques sur les corps locaux*, Ann. of Math. **119** (1984), 511–548.

[Win95] ______, *Relèvement selon une isogénie de systèmes l-adiques de représentations galoisiennes associées aux motifs*, Invent. Math. **120** (1995), 215–240.

[Win97] ______, *Propriétés du groupe tannakien des structures de Hodge p-adiques et torseur entre cohomologies cristalline et étale*, Ann. Inst. Fourier **47** (1997), 1289–1334.

[Wym69] B. F. Wyman, *Wildly ramified gamma extensions.*, Amer. J. Math. **91** (1969), 135–152.

[Xie12] B. Xie, *On families of filtered (ϕ, N)-modules*, Math. Res. Lett. **19** (2012), 667–689.

List of Notation

Index