Jean-Marc Fontaine and Yi Ouyang

Theory of p-adic Galois Representations

Springer

Contents

1

ℓ-adic representations of local fields: an overview

1.1 ℓ-adic Galois representations

1.1.1 Linear representations of topological groups.

Let G be a topological group and E be a field.

Definition 1.1. *A* linear representation of G with coefficients in E *is a finite dimensional E-vector space V equipped with a linear action of G; equivalently, a linear representation is a homomorphism*

$$\rho : \quad G \longrightarrow \mathrm{Aut}_E(V) \simeq \mathrm{GL}_h(E)$$

where $h = \dim_E(V)$.

If V is equipped with a topological structure, and if the action of G is continuous, the representation is called continuous*. In particular, if E is a topological vector field, V is given the induced topology, then such a continuous representation is called a* continuous E-linear representations of G*.*

If moreover, $G = \mathrm{Gal}(K^s/K)$ for K a field and K^s a separable closure of K, such a representation is called a Galois representation*.*

We consider a few examples:

Example 1.2. Let K be a field, L be a Galois extension of K, $G = \mathrm{Gal}(L/K)$ be the Galois group of this extension. Put the discrete topology on V and consider continuous representations. The continuity of a representation means that it factors through a suitable finite Galois extension F of K contained in L:

$$\begin{tikzcd}
G \arrow[r] \arrow[d] & \mathrm{GL}_E(V) \\
\mathrm{Gal}(F/K) \arrow[ur] &
\end{tikzcd}$$

Example 1.3. Assume that E is a completion of a number field. Then either $E = \mathbb{R}$ or $\mathbb{C}$, or E is a finite extension of $\mathbb{Q}_\ell$ for a suitable prime number ℓ.

If $E = \mathbb{R}$ or $\mathbb{C}$, and $\rho : G \longrightarrow \mathrm{Aut}_E(V)$ is a representation, then ρ is continuous if and only if $\mathrm{Ker}\,(\rho)$ is an open normal subgroup of G.

If E is a finite extension of $\mathbb{Q}_\ell$, and $\rho : G \to \mathrm{Aut}_E(V)$ is a representation, $[E : \mathbb{Q}_\ell] = d$, $h = \dim_E(V)$, then $\dim_{\mathbb{Q}_\ell}(V) = h\,d$, $\mathrm{Aut}_E(V) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$, and we can view the representation as a representation over $\mathbb{Q}_\ell$. To give a continuous E-linear representation of G is the same as to give a continuous $\mathbb{Q}_\ell$-linear representation of G together with an embedding $E \hookrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell[G]}(V)$.

1.1.2 ℓ-adic representations.

From now on, let K be a field, L be a Galois extension of K, $G = \mathrm{Gal}(L/K)$ be the Galois group of this extension.

Definition 1.4. *An* ℓ-adic representation *of G is a finite dimensional $\mathbb{Q}_\ell$-vector space equipped with a continuous and linear action of G.*

If $G = \mathrm{Gal}(K^s/K)$ for K^s a separable closure of K, such a representation is called an ℓ-adic Galois representation.

Example 1.5. The *trivial representation* is $V = \mathbb{Q}_\ell$ with $g(v) = v$ for all $g \in G$ and $v \in \mathbb{Q}_\ell$.

Definition 1.6. *Let V be an ℓ-adic representation of G of dimension d. A* lattice *in V is a sub $\mathbb{Z}_\ell$-module of finite type generating V as a $\mathbb{Q}_\ell$-vector space, equivalently, a free sub $\mathbb{Z}_\ell$-module of V of rank d.*

Definition 1.7. *A* $\mathbb{Z}_\ell$-representation *of G is a free $\mathbb{Z}_\ell$-module of finite type, equipped with a linear and continuous action of G.*

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 $\mathbb{Z}_\ell$, it is also a basis of V over $\mathbb{Q}_\ell$, thus

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

and $V = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T$.

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

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

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.

Assume $G = \mathrm{Gal}(K^s/K)$. Then $(K^s)^{H_n} = K_n$ is a finite Galois extension of K with the following diagram:

$$\begin{tikzcd}
G \arrow[r, "\rho_n"] \arrow[d, "surj."] & \mathrm{Aut}(T/l^n T) \\
\mathrm{Gal}(K_n/K) \arrow[ur, hook]
\end{tikzcd}$$

We also set $K_\infty = \bigcup K_n$, and $K_\infty = (K^s)^H$ with $H = \mathrm{Ker}\,(\rho)$. So we get a sequence of field extensions:

$$\begin{tikzcd}
K \arrow[r, dash] \arrow[rrr, dash, bend right] & K_n \arrow[r, dash] & K_{n+1} \arrow[r, dotted, dash] & K_\infty \arrow[r, dash] & K^s.
\end{tikzcd}$$

1.1.3 Representations arising from linear algebra.

Through linear algebra, we can build *new* representations starting from *old* representations:

- Suppose V_1 and V_2 are two ℓ-adic representations of G, then the *tensor product* $V_1 \otimes V_2 = V_1 \otimes_{\mathbb{Q}_\ell} V_2$ with $g(v_1 \otimes v_2) = gv_1 \otimes gv_2$ is an ℓ-adic representation.
- The r-th *symmetric power* of an ℓ-adic representation V: $\mathrm{Sym}^r_{\mathbb{Q}_\ell} V$, with the natural actions of G, is an ℓ-adic representation.
- The r-th *exterior power* of an ℓ-adic representation V: $\bigwedge^r_{\mathbb{Q}_\ell} V$, with the natural actions of G, is an ℓ-adic representation.
- For V an ℓ-adic representation, $V^* = \mathscr{L}_{\mathbb{Q}_\ell}(V, \mathbb{Q}_\ell)$ with a G-action $g\cdot\varphi \in V^*$ for $\varphi \in V^*, g \in G$ defined by $(g \cdot \varphi)(v) = \varphi(g^{-1} \cdot v)$, is again an ℓ-adic representation, which is called the *dual representation* of V.

1.1.4 Examples of ℓ-adic Galois representations.

We assume that K is a field, K^s is a fixed separable closure of K, $G = \mathrm{Gal}(K^s/K)$ in this subsection.

(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,

$$\boldsymbol{\mu}_{l^n}(F) = \{a \in F \mid a^{\ell^n} = 1\}. \tag{1.1}$$

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* $\mathbb{G}_m$

$$T_\ell(\mathbb{G}_m) = \varprojlim_{n \in \mathbb{N}} \boldsymbol{\mu}_{\ell^n}(K^s). \tag{1.2}$$

$T_\ell(\mathbb{G}_m)$ 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 $T_\ell(G_m) = \mathbb{Z}_\ell t$, equipped with the following $\mathbb{Z}_\ell$-action

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

The Galois group G acts on $T_\ell(\mathbb{G}_m)$ and also on $V_\ell(\mathbb{G}_m) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(\mathbb{G}_m)$. Usually we write

$$T_\ell(\mathbb{G}_m) = \mathbb{Z}_\ell(1), \qquad V_\ell(\mathbb{G}_m) = \mathbb{Q}_\ell(1) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(1). \tag{1.3}$$

If V is any 1-dimensional ℓ-adic representation of G, then

$$V = \mathbb{Q}_\ell e, \ \ g(e) = \eta(g) \cdot e, \ \text{for all } g \in G$$

where $\eta : G \to \mathbb{Q}_\ell^\times$ is a continuous homomorphism. In the case of $T_\ell(\mathbb{G}_m)$, η is called the *cyclotomic character* and usually denoted as χ, the image $\mathrm{Im}(\chi)$ is a closed subgroup of $\mathbb{Z}_\ell^\times$.

Remark 1.8. If $K = \mathbb{Q}_\ell$ or $\mathbb{Q}$, the cyclotomic character $\chi : G \to \mathbb{Z}_\ell^\times$ is surjective.

From $\mathbb{Z}_\ell(1)$ and $\mathbb{Q}_\ell(1)$, we define for $r \in \mathbb{N}^*$

$$\mathbb{Q}_\ell(r) = \mathrm{Sym}^r_{\mathbb{Q}_\ell}(\mathbb{Q}_\ell(1)), \quad \mathbb{Q}_\ell(-r) = \mathscr{L}(\mathbb{Q}_\ell(r), \mathbb{Q}_\ell) = \text{the dual of } \mathbb{Q}_\ell(r). \tag{1.4}$$

Then for $r \in \mathbb{Z}$,

$$\mathbb{Q}_\ell(r) = \mathbb{Q}_\ell \cdot t^r, \text{ with the action } g(t^r) = \chi^r(g) \cdot t^r \text{ for } g \in G.$$

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

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

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

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

with the roots α_1, α_2, $\alpha_3 \in K^s$ all distinct. Let E be the corresponding elliptic curve. Then

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

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

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

where for a field F over K, $E_{\ell^n}(F) = \{A \in E(F) \mid \ell^n A = O\}$. If $\ell \neq \operatorname{char} K$, then $E_{\ell^n}(K^s) \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^2$. If $\ell = \operatorname{char} K$, then either $E(K^s)_{\ell^n} \simeq \mathbb{Z}/\ell^n\mathbb{Z}$ in the ordinary case, or $E(K^s)_{\ell^n} \simeq \{0\}$ in the supersingular case.

With the transition maps

$$\begin{array}{lll} E_{\ell^{n+1}}(K^s) & \longrightarrow & E_{\ell^n}(K^s) \\ A & \longmapsto & \ell A \end{array}$$

the *Tate module of* E is defined as

$$T_\ell(E) = \varprojlim_n E_{\ell^n}(K^s). \tag{1.5}$$

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 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 $\dim A = g$. We have

- $A(K^s)$ is an abelian group;
- $A(K^s)_{\ell^n} \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$ if $\ell \neq \operatorname{char} K$. If $\ell = \operatorname{char} K$, then $A(K^s)_{\ell^n} \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^r$, with $0 \leq r \leq g$.

We get the ℓ-adic representations:

$$\begin{aligned} T_\ell(A) &= \varprojlim A(K^s)_{l^n} \simeq \begin{cases} \mathbb{Z}_\ell^{2g}, & \text{if } \operatorname{char} K \neq \ell; \\ \mathbb{Z}_\ell^r, & \text{if } \operatorname{char} K = \ell. \end{cases} \\ V_\ell(A) &= \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(A). \end{aligned} \tag{1.6}$$

(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

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

This is a finite abelian group killed by ℓ^n. From the maps

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

we can get the inverse limit $\varprojlim H^m(Y_{\text{ét}}, \mathbb{Z}/\ell^n\mathbb{Z})$, which is a $\mathbb{Z}_\ell$-module of finite type. 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.

For example, 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

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

Remark 1.9. This construction extends to more generality and conjecturally to motives. To any motive M over K, one expects to associate an ℓ-adic realization of M to it.

1.2 ℓ-adic representations of finite fields

In this section, let K be a finite field of characteristic p with q elements. Let K^s be a fixed algebraic closure of K and $G = G_K = \mathrm{Gal}(K^s/K) \simeq \widehat{\mathbb{Z}}$ be the Galois group over K. Let K_n be the unique extension of K of degree n inside K^s for $n \geq 1$. Let $\tau_K = \varphi_K^{-1} \in G$ be the geometric Frobenius of G.

1.2.1 ℓ-adic Galois representations of finite fields.

Recall the geometric Frobenius $\tau_K(x) = x^{q^{-1}}$ for any $x \in K^s$ is a topological generator of G. An ℓ-adic representation of G is given by

$$\begin{aligned} \rho : G \ &\longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(V) \\ \tau_K \ &\longmapsto \quad u. \end{aligned}$$

For $n \in \mathbb{Z}$, it is clear that $\rho(\tau_K^n) = u^n$. For $n \in \widehat{\mathbb{Z}}$,

$$\rho(\tau_K^n) = \lim_{\substack{m\in\mathbb{Z} \\ m\longmapsto n}} u^m.$$

That is, ρ is uniquely determined by u.

Given any $u \in \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$, there exists a continuous $\rho : G \longmapsto \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$ such that $\rho(\tau_K) = u$ if and only if the above limit makes sense.

Proposition 1.10. *This is the case if and only if the eigenvalues of u in a chosen algebraic closure of $\mathbb{Q}_\ell$ are ℓ-adic units, i.e. $P_u(t) = \det(u - t \cdot \mathrm{Id}_V)(\in \mathbb{Q}_\ell[t]\,)$ is an element of $\mathbb{Z}_\ell[t]$ and the constant term is a unit.*

Proof. The proof is easy and left to the readers. □

Definition 1.11. *The characteristic polynomial of τ_K, $P_V(t) = \det(\mathrm{Id}_V - t\tau_K)$ is called the* characteristic polynomial of the representation *V.*

We have $P_V(t) = (-t)^h P_V\,(1/t)$.

Remark 1.12. V is semi-simple if and only if $u = \rho(\tau_K)$ is semi-simple. Hence, isomorphism classes of semi-simple ℓ-adic representations V of G are determined by $P_V(t)$.

1.2.2 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:

$$Z_X(t) = \exp\left(\sum_{n=1}^{\infty} \frac{C_n}{n} t^n\right) \in \mathbb{Z}[[t]]. \tag{1.7}$$

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 $Z_X(t)$ has an Euler product

$$Z_X(t) = \prod_{\substack{x \in |X| \\ x \text{ closed}}} \frac{1}{1 - t^{\deg(x)}}. \tag{1.8}$$

Theorem 1.13 (Weil's conjecture, proved by Deligne). *Let X be a projective, smooth, and geometrically connected variety over a finite field K. Then*

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

$$Z_X(t) = \frac{P_1(t)P_3(t)\cdots P_{2d-1}(t)}{P_0(t)P_2(t)\cdots P_{2d}(t)}. \tag{1.9}$$

where $q = \#(K)$, $d = \dim X$. If we make an embedding $\overline{\mathbb{Z}} \hookrightarrow \mathbb{C}$, and decompose

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

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

(2). There exists a functional equation

$$Z_X\left(\frac{1}{q^d t}\right) = \pm q^{d\beta} t^{2\beta} Z_X(t) \tag{1.10}$$

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

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: 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

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

Remark 1.14. Consider ℓ, ℓ', two different prime numbers not equal to p. Denote $G_K = \mathrm{Gal}(K^s/K) \simeq \widehat{\mathbb{Z}}$. We have the representations

$$\begin{aligned} \rho :\ & G_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell} H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell), \\ \rho' :\ & G_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}'_\ell} H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_{\ell'}). \end{aligned}$$

If $\mathrm{Im}(\rho)$ is not finite, then

$$\begin{aligned} \mathrm{Im}(\rho) &\simeq \mathbb{Z}_\ell \times (\text{ finite cyclic group}), \\ \mathrm{Im}(\rho') &\simeq \mathbb{Z}_{\ell'} \times (\text{ finite cyclic group }). \end{aligned}$$

Definition 1.15. *Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and $w \in \mathbb{Z}$. A* Weil number of weight w *(relatively to K) is an element $\alpha \in \overline{\mathbb{Q}}$ satisfying*

(1) there exists an $i \in \mathbb{N}$ such that $q^i\alpha \in \overline{\mathbb{Z}}$;

(2) for any embedding $\sigma : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, $|\sigma(\alpha)| = q^{w/2}$.

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

Remark 1.16. (1) This is an *intrinsic notion.*

(2) 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 $w + 2i$ (so it is effective if $i \gg 0$).

Definition 1.17. *An ℓ-adic representation V of G_K is said to be* pure of weight w *if all the roots of the characteristic polynomial of the geometric Frobenius τ_K acting on V are Weil numbers of weight w. Consider the characteristic polynomial*

$$P_V(t) = \det(1 - \tau_K t) = \prod_{j=1}^{m}(1 - \alpha_j t) \in \mathbb{Q}_\ell[t], \quad \alpha_j \in \overline{\mathbb{Q}_\ell} \supset \overline{\mathbb{Q}}.$$

One says that V is effective of weight w *if moreover $\alpha_j \in \overline{\mathbb{Z}}$ for $1 \leq j \leq m$.*

Remark 1.18. (1) 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.

(2) 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 1.19. *An ℓ-adic representation V of G_K is said to be* geometric *if the following conditions holds:*

(1) it is semi-simple;

(2) it can be written as a direct sum $V = \bigoplus_{w\in\mathbb{Z}} V_w$, with almost all $V_w = 0$, and V_w pure of weight w.

Let $\mathbf{Rep}_{\mathbb{Q}_\ell}(G_K)$ be the category of all ℓ-adic representations of G_K, and $\mathbf{Rep}_{\mathbb{Q}_\ell,\,\text{geo}}(G_K)$ be the full sub-category of geometric representations. This is a sub-Tannakian category of $\mathbf{Rep}_{\mathbb{Q}_\ell}(G_K)$, i.e. it is stable under subobjects, quotients, $\oplus$, $\otimes$, dual, and $\mathbb{Q}_\ell$ is the unit representation as a geometric representation.

Denote by $\mathbf{Rep}_{\mathbb{Q}_\ell,\,\text{GEO}}(G_K)$ the smallest sub-Tannakian category of $\mathbf{Rep}_{\mathbb{Q}_\ell}(G_K)$ containing all the objects isomorphic to $H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)$ for X projective smooth varieties over K and $m \in \mathbb{N}$. This is also the smallest full sub-category of $\mathbf{Rep}_{\mathbb{Q}_\ell}(G_K)$ containing all the objects isomorphic to $H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)(i)$ for all $X, m \in \mathbb{N}, i \in \mathbb{Z}$, stable under sub-objects and quotients.

Conjecture 1.20. $\mathbf{Rep}_{\mathbb{Q}_\ell,\,\text{geo}}(G_K) = \mathbf{Rep}_{\mathbb{Q}_\ell,\,\text{GEO}}(G_K)$.

Theorem 1.21. *We have* $\mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{geo}}(G_K) \subsetneq \mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{GEO}}(G_K)$.

The only thing left in Conjecture 1.20 is to prove that $H^m_{\text{ét}}(X_{K^s}, \mathbb{Q}_\ell)$ is geometric. We do know that it is pure of weight w, but it is not known in general if it is semi-simple.

1.3 ℓ-adic representations of local fields

1.3.1 ℓ-adic representations of local fields.

Let K be a local field. Let k be the residue field of K, which is perfect of characteristic $p > 0$. Let $\mathcal{O}_K$ be the ring of integers of K. Let K^s be a separable closure of K. Let $G_K = \mathrm{Gal}(K^s/K)$, I_K be the inertia subgroup of G_K, and P_K be the wild inertia subgroup of G_K.

We have the following exact sequences

$$1 \longrightarrow I_K \longrightarrow G_K \longrightarrow \quad G_k \quad \longrightarrow 1,$$

$$1 \longrightarrow P_K \longrightarrow G_K \longrightarrow G_K/P_K \longrightarrow 1.$$

Let ℓ be a fixed prime number, $\ell \neq p$. Then there is the following isomorphism

$$I_K/P_K \simeq \widehat{\mathbb{Z}}'(1) = \prod_{\ell \neq p} \mathbb{Z}_\ell(1) = \mathbb{Z}_\ell(1) \times \prod_{\ell' \neq \ell, p} \mathbb{Z}_{\ell'}(1).$$

We define $P_{K,\,\ell}$ to be the inverse image of $\prod_{\ell' \neq p, \ell} \mathbb{Z}_{\ell'}(1)$ in I_K, and define $G_{K,\ell}$ the quotient group to make the short exact sequences

$$1 \longrightarrow \ P_{K,\ell} \longrightarrow \ \ G_K \longrightarrow \ G_{K,\,\ell} \longrightarrow 1,$$

$$1 \longrightarrow \mathbb{Z}_\ell(1) \longrightarrow G_{K,\,\ell} \longrightarrow \ \ G_k \ \longrightarrow \ \ 1.$$

Let V be an ℓ-adic representation of G_K, and T be the corresponding $\mathbb{Z}_\ell$-lattice stable under G_K. Hence we have

$$\begin{tikzcd}
G_K \arrow[r, "\rho"] \arrow[dr] & \mathrm{Aut}_{\mathbb{Z}_\ell}(T) \arrow[d, hook] & \simeq \mathrm{GL}_h(\mathbb{Z}_\ell) \\
& \mathrm{Aut}_{\mathbb{Q}_\ell}(V) & \simeq \mathrm{GL}_h(\mathbb{Q}_\ell)
\end{tikzcd}$$

where $h = \dim_{\mathbb{Q}_\ell}(V)$. The image $\rho(G_K)$ is a closed subgroup of $\mathrm{Aut}_{\mathbb{Z}_\ell}(T)$.

Consider the following diagram

$$1 \longrightarrow N_1 \longrightarrow \mathrm{GL}_h(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_h(\mathbb{F}_\ell) \longrightarrow 1,$$

where N_1 is the kernel of the reduction map. Let N_n be the set of matrices congruent to $1 \bmod \ell^n$ for $n \geq 1$. As N_1/N_n is a finite group of order equal to a power of ℓ for each n, $N_1 \simeq \varprojlim N_1/N_n$ is a pro-ℓ group. Since $P_{K,\ell}$ is the inverse limit of finite groups of orders prime to ℓ, $\rho(P_{K,\ell}) \cap N_1 = \{1\}$. Consider the exact sequence

$$1 \longrightarrow P_K \longrightarrow P_{K,\ell} \longrightarrow \prod_{\ell' \neq p,\, \ell} \mathbb{Z}_{\ell'}(1) \longrightarrow 1,$$

as $\rho(P_{K,\,\ell})$ injects into $\mathrm{GL}_h(\mathbb{F}_\ell)$, $\rho(P_{K,\,\ell})$ is a finite group.

Definition 1.22. *Let V be an ℓ-adic representation of G_K with $\rho : G_K \longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$.*

(1) We say that V is unramified *or has* good reduction *if I_K acts trivially.*

(2) We say that V has potentially good reduction *if $\rho(I_K)$ is finite, in other words, if there exists a finite extension K' of K contained in K^s such that V, as an ℓ-adic representation of $G_{K'} = \mathrm{Gal}(K^s/K')$, has good reduction.*

(3) We say that V is semi-stable *if I_K acts unipotently, in other words, if the semi-simplification of V has good reduction.*

(4) We say that 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 1.23. 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 has potentially good reduction.

Theorem 1.24. *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. As $\boldsymbol{\mu}_{\ell^\infty}(k) \simeq \boldsymbol{\mu}_{\ell^\infty}(K)$, this is the case if k is finite.*

Proof. By 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 $\bar{\rho}(t)$ is a product of polynomials of degree 1. Let $V' = E \otimes_{\mathbb{Q}_\ell} V$. The group $G_{K,\,\ell}$ acts on $E \otimes_{\mathbb{Q}_\ell} V$ by

$$g(\lambda \otimes v) = \lambda \otimes g(v).$$

Let $\bar{\rho} : G_{K,\ell} \longrightarrow \mathrm{Aut}_E(V')$ be the representation over E, let a be an eigenvalue of $\bar{\rho}(t)$. Then there exists $v \in V'$, $v \neq 0$ such that $\bar{\rho}(t)(v) = a \cdot v$.

If $g \in G_{K,\ell}$, then $gtg^{-1} = t^{\chi_\ell(g)}$, where $\chi_\ell : G_{K,\ell} \longrightarrow \mathbb{Z}_\ell^*$ is a 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 $\mathbb{Z}_\ell^*$. Thus there are infinitely many such n's. This implies a is 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 1.25 (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. Then we can get a field K_0 which is of finite type over the prime field of K (joined by the 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 1.26. *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 $I_K = G_K$.

Step 1. At first, we assume that the Galois representation is semi-stable. Then the action of $P_{K,\ell}$ must be trivial from above discussions, 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. Let V be such a representation:

$$\begin{tikzcd}
G_K \arrow[rr, "\rho"] \arrow[dr] & & \mathrm{Aut}_{\mathbb{Q}_\ell}(V) \\
& G_{K,\ell} \arrow[ur, "\bar{\rho}"'] &
\end{tikzcd}$$

so $\bar{\rho}(t) \in \mathrm{Aut}_{\mathbb{Q}_\ell}(V)$.

For each integer $n \geq 1$, there exists a unique (up to isomorphism) representation V_n of dim n which is semi-stable and in-decomposable. Write it as $V_n = \mathbb{Q}_\ell^n$, and

$$\bar{\rho}(t) = \begin{pmatrix} 1 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}.$$

As $V_n \simeq \mathrm{Sym}_{\mathbb{Q}_\ell}^{n-1}(V_2)$, 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 ℓ-adic representations of dimension 1 coming from algebraic geometry. We apply the case for some $q \in \mathfrak{m}_K$, $q \neq 0$. Then from Tate's theorem, let E be an elliptic curve over K such that $E(K^s) \simeq (K^s)^*/q^{\mathbb{Z}}$, with

$$E(K^s)_{\ell^n} = \Big\{ a \in (K^s)^* \mid \exists\, m \in \mathbb{Z} \text{ such that } a^{\ell^n} = q^m \Big\} \Big/ q^{\ell^n}$$

and

$$V_\ell(E) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(E), \quad T_\ell(E) = \varprojlim E(K^s)_{\ell^n}.$$

An element $\alpha \in T_\ell(E)$ is given by

$$\alpha = (\alpha_n)_{n\in\mathbb{N}}, \quad \alpha_n \in E(K^s)_{l^n}, \quad \alpha_{n+1}^{\ell} = \alpha_n.$$

From the exact sequence

$$0 \longrightarrow \boldsymbol{\mu}_{\ell^n}(K) \longrightarrow E(K^s)_{\ell^n} \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z} \longrightarrow 0$$

we have

$$0 \longrightarrow \mathbb{Q}_\ell(1) \longrightarrow V_\ell(E) \longrightarrow \mathbb{Q}_\ell \longrightarrow 0.$$

The action of G_K on the left $\mathbb{Q}_\ell(1)$ of the above exact sequence is trivial, since it comes from the action of unramified extensions. And the extension $V_\ell(E)$ is non-trivial.

Step 2. Assume the representation is potentially semi-stable. Let V be a potentially semi-stable ℓ-adic representation of G_K. 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

$$V_\ell(A) = \mathrm{Ind}_{G_{K'}}^{G_K} V_\ell(E).$$

an ℓ-adic representation of G_K of dimension $2 \cdot [K' : K]$. All the ℓ-adic representations of G_K, which are semi-stable ℓ-adic representations of $G_{K'}$, come from $V_\ell(A)$. □

1.3.2 An alternative description of potentially semi-stable ℓ-adic representations.

Let the notations be as in the previous subsection. To any $q \in \mathfrak{m}_K$, $q \neq 0$, let E be the corresponding Tate elliptic curve. Thus

$$V_\ell(E) = V_\ell\left((K^s)^*/q^{\mathbb{Z}}\right) = \mathbb{Q}_\ell \otimes \varprojlim \left((K^s)^*/q^{\mathbb{Z}}\right)_{\ell^n}.$$

Let t be a generator of $\mathbb{Q}_\ell(1)$. Then we have the short exact sequence

$$0 \longrightarrow \mathbb{Q}_\ell \longrightarrow V_\ell\left((K^s)^*/q^{\mathbb{Z}}\right)(-1) \longrightarrow \mathbb{Q}_\ell(-1) \longrightarrow 0.$$

Write $\mathbb{Q}_\ell(-1) = \mathbb{Q}_\ell \cdot t^{-1}$, and let $u \in V_\ell\left((K^s)^*/q^{\mathbb{Z}}\right)(-1)$ be a lifting of t^{-1}. Put

$$B_\ell = \mathbb{Q}_\ell[u],$$

then $b \otimes t^{-1} \in B_\ell(-1) = B_\ell \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell(-1)$. We define the following map

$$\begin{aligned} N : B_\ell &\longrightarrow B_\ell(-1) \\ b &\longmapsto -b' \otimes t^{-1} = -\tfrac{db}{du} \otimes t^{-1}. \end{aligned}$$

Let V be an ℓ-adic representation of G_K, and $\mathcal{H}$ be the set of open normal subgroups of I_K. Define

$$\mathbf{D}_\ell(V) = \varinjlim_{H \in \mathcal{H}} \left(B_\ell \otimes_{\mathbb{Q}_\ell} V\right)^H. \tag{1.11}$$

Proposition 1.27. $\dim_{\mathbb{Q}_\ell} \mathbf{D}_\ell(V) \leq \dim_{\mathbb{Q}_\ell} V$.

The map N extends to $N : \mathbf{D}_\ell(V) \longrightarrow \mathbf{D}_\ell(V)(-1)$. And we define a category $\mathscr{C}$ = the category of pairs (D, N), in which

- D is an ℓ-adic representation of G_K with potentially good reduction; $N : D \longrightarrow D(-1)$ 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.

- $\mathrm{Hom}_{\mathscr{C}}\left((D,N),(D',N')\right)$ 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

$$\begin{tikzcd} D \arrow[r, "\eta"] \arrow[d, "N"'] & D' \arrow[d, "N'"] \\ D(-1) \arrow[r, "\eta(-1)"'] & D'(-1) \end{tikzcd}$$

commutes.

We may view $\mathbf{D}_\ell$ as a functor from the category of ℓ-adic representations of G_K to the category $\mathscr{C}$. There is a functor in the other direction

$$\mathbf{V}_\ell : \mathscr{C} \longrightarrow \mathbf{Rep}_{\mathbb{Q}_\ell}(G_K).$$

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

$$N(b \otimes \delta) = Nb \otimes \delta + b \otimes N\delta.$$

Now set

$$\mathbf{V}_\ell(D,N) = \mathrm{Ker}\left(N : B_\ell \otimes_{\mathbb{Q}_\ell} D \longrightarrow (B_\ell \otimes_{\mathbb{Q}_\ell} D)(-1)\right).$$

Proposition 1.28. *(1)* $\mathbf{V}_\ell(D,N)$ *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.*

(2). 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.*

The above result implies that $\mathbf{D}_\ell$ induces an equivalence of categories between 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 $\mathbf{D}_\ell$.

Exercise 1.29. Let (D,N) be an object of $\mathscr{C}$. The map

$$\begin{array}{rl} \mathbf{V}_\ell(D) \subset B_\ell \otimes_{\mathbb{Q}_\ell} D & \longrightarrow D \\ \sum_i P_i(u) \otimes \delta_i & \longmapsto \sum_i P_i(0) \otimes \delta_i \end{array}$$

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.

1.3.3 The case of a finite residue field.

Assume k is a finite field with q elements. We have the short exact sequence

$$1 \longrightarrow I_K \longrightarrow G_K \longrightarrow G_k \longrightarrow 1,$$

and let $\tau_k \in G_k$ denote the geometric Frobenius. By definition, the *Weil group* of k is

$$W_K = \{g \in G_K \mid \exists m \in \mathbb{Z} \text{ such that } g|_{\bar{k}} = \varphi_k^m\}\,.$$

Hence there is a map

$$\rho : W_K \longrightarrow \mathbb{Z}$$

with $\rho(g) = m$ if $g|_{\bar{k}} = \varphi_k^m$, and it induces the exact sequence

$$1 \longrightarrow I_K \longrightarrow W_K \longrightarrow \mathbb{Z} \longrightarrow 1.$$

If E is any field of characteristic 0, we may consider E-linear continuous representations of W_K with the discrete topology on E. Such a representation is a finite dimensional E-vector space V plus a homomorphism of groups

$$\rho : W_K \longrightarrow \mathrm{Aut}_E(V)$$

such that $\mathrm{Ker}\,(\rho) \cap I_K$ is open in I_K.

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.

We will now consider the following

- WD_K = the *Weil-Deligne* group of K.
- Let E be any field of characteristic 0, there is the category of E-linear representations of WD_K, denoted by $\mathbf{Rep}_E(WD_K)$.

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 W_K acts, such that I_K acts trivially and the action of τ_k is multiplication by q^{-1}.

An object of $\mathbf{Rep}_E(WD_K)$ is 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 (This implies N is nilpotent).

Let $\mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{pst}}(G_K)$ be the category of potentially semi-stable ℓ-adic representation of G_K. We consider the functor

$$\begin{aligned}\mathbf{Rep}_{\mathbb{Q}_\ell,\,\mathrm{pst}}(G_K) &\longrightarrow \mathbf{Rep}_E(WD_K)\\ V &\longmapsto (\mathbf{D}_\ell(V), N),\end{aligned}$$

which is fully faithful.

Now consider E and F, which are two fields of characteristic 0 (for instance, $E = \mathbb{Q}_\ell$, and $F = \mathbb{Q}_{\ell'}$). Let

- D = an E-linear representation of WD_K.

– D' = an F-linear 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 1.30. *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 1.31. 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 1.32. 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.

1.3.4 Geometric ℓ-adic representations of G_K.

We will describe geometric E-linear representation of WD_K for any field E of characteristic 0. A *geometric ℓ-adic representation* of G_K for $\ell \neq p$ will be an ℓ-adic representation such that the associated $\mathbb{Q}_\ell$-linear representation of WD_K is geometric.

Let V be an E-linear continuous representation of W_K. Choose $\varphi \in W_K$ a lifting of τ_k:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I_K & \longrightarrow & W_K & \longrightarrow & \mathbb{Z} & \longrightarrow & 1 \\ & & & & \varphi & \longmapsto & 1. & & \end{array}$$

Choose $w \in \mathbb{Z}$.

Definition 1.33. *The representation V is* pure of weight w *if all the roots of the characteristic polynomial of φ 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, $\lambda \in \bar{\mathbb{Q}}$ and for any embedding $\sigma : \bar{\mathbb{Q}} \longrightarrow \bar{E}$, we have*

$$\mid \sigma(\lambda) \mid = q^{w/2}.$$

The definition is independent of the choices.

Let V be any E-linear continuous representation of W_K, and let $r \in \mathbb{N}$. Set

$$D = V \oplus V(-1) \oplus V(-2) \oplus \cdots \oplus V(-r)$$

and $N : D \longrightarrow D(-1)$ given by

$$N(v_0, v_{-1}, v_{-2}, \cdots, v_{-r}) = (v_{-1}, v_{-2}, \cdots, v_{-r}, 0).$$

This is a representation of WD_K.

Definition 1.34. *An E-linear representation of WD_K is* elementary and pure of weight $w+r$ *if it is isomorphic to such a D with V satisfying*

(1) V is pure of weight w;

(2) V is semi-simple.

Definition 1.35. *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.*

As a full sub-category of $\mathbf{Rep}_E(WD_K)$, these representations make an abelian category $\mathbf{Rep}^m_{E,\,\mathrm{geo}}(WD_K)$. 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 1.36. For $\ell \neq p$, $H^r(X_{K^s}, \mathbb{Q}_\ell)(i)$ should be an object of $\mathbf{Rep}^{r-2i}_{\mathbb{Q}_\ell,\,\mathrm{geo}}(WD_K)$ and these objects should generate the category.

In the category $\mathbf{Rep}_E(WD_K)$, let

$$\mathbf{Rep}^w_E(WD_K) = \text{the category of weighted } E\text{-linear representation of } WD_K.$$

An object of this category is an E-linear representation D of WD_K plus an increasing filtration

$$\cdots \subseteq W_mD \subseteq W_{m+1}D \subseteq \cdots$$

where W_mD is stable under WD_K, and

$$\begin{array}{lll} W_mD = D & \text{if} & m \gg 0, \\ W_mD = 0 & \text{if} & m \ll 0. \end{array}$$

Morphisms are morphisms of the representations of WD_K which respect the filtration. This is an additive category, but not an abelian category. Define

$$\mathbf{Rep}^w_{E,\,\mathrm{geo}}(WD_K),$$

the category of geometric weighted E-linear representations of WD_K, to be the full sub-category of $\mathbf{Rep}_E(WD_K)$ of those D's such that for all $m \in \mathbb{Z}$,

$$gr_mD = W_mD/W_{m-1}D$$

is a pure geometric representation of weight m.

Theorem 1.37. $\mathbf{Rep}^w_{E,\,\mathrm{geo}}(WD_K)$ *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 $\mathbf{Rep}^w_{\mathbb{Q}_\ell,\,\mathrm{geo}}(G_K)$.

2

p-adic Representations of fields of characteristic p

2.1 B-representations and regular G-rings

2.1.1 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 $g \in G$, $b_1, b_2 \in B$

$$g(b_1 + b_2) = g(b_1) + g(b_2), \qquad g(b_1 b_2) = g(b_1)g(b_2).$$

Example 2.1. $B = L$ is a Galois extension of a field K, $G = \mathrm{Gal}(L/K)$, both equipped with the discrete topology.

Definition 2.2. *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 $x, x_1, x_2 \in X$,*

$$g(x_1 + x_2) = g(x_1) + g(x_2), \qquad g(\lambda x) = g(\lambda)g(x).$$

If G acts trivially on B, we just have a linear representation. If $B = \mathbb{F}_p$ with the discrete topology, we say *mod p representation* instead of $\mathbb{F}_p$-representation. If $B = \mathbb{Q}_p$, with the p-adic topology, we say *p-adic representation* instead of $\mathbb{Q}_p$-representation.

Definition 2.3. *A* free B-representation *of G is a B-representation such that the underlying B-module is free.*

Example 2.4. Let F be a closed subfield of B^G and V be a 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 2.5. *We say that a free B-representation X of G is* trivial *if one of the following two conditions holds:*

(1) There exists a basis of X consisting of elements of X^G;

(2) $X \simeq B^d$ with the natural 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 $\{e_1, \cdots, e_d\}$ as a basis. For every $g \in G$, let

$$g(e_j) = \sum_{i=1}^{d} a_{ij}(g) e_i,$$

then we get a map $\alpha : G \to \mathrm{GL}_d(B)$,

$$\alpha(g) = (a_{ij}(g))_{1 \leq i,j \leq d}. \tag{2.1}$$

It is easy to check that 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 base change 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

$$\alpha'(g) = P^{-1} \alpha(g) g(P). \tag{2.2}$$

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 $g \in G$,

$$g(e_j) = \sum_{i=1}^{d} a_{ij}(g) e_i, \tag{2.3}$$

and $[X]$ is the class of α. Hence, we have the following proposition:

Proposition 2.6. *Let $d \in \mathbb{N}$. 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 $H^1_{\mathrm{cont}}(G, \mathrm{GL}_d(B))$.*

We see also what Hilbert's Theorem 90 means:

Proposition 2.7. *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.*

2.1.2 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 $C = \mathrm{Frac}\, B$ by

$$g\left(\frac{b_1}{b_2}\right) = \frac{g(b_1)}{g(b_2)}, \quad \text{for all } g \in G,\ b_1, b_2 \in B. \tag{2.4}$$

Definition 2.8. *We say that B is* (F,G)-regular *if the following conditions hold:*

(1) B is a domain.

(2) $B^G = C^G$.

(3) For every $b \in B, b \neq 0$ such that for any $g \in G$, if there exists $\lambda \in F$ with $g(b) = \lambda b$, then b is invertible in B.

Remark 2.9. This is always the case when 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:

- 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 $g(v_1 \otimes v_2) = g(v_1) \otimes g(v_2)$;
- Dual representation: if V is a F-representation of G, we set $V^* = \mathscr{L}(V, F) = \{\text{linear maps } V \to F\}$, with the G-action given by $(gf)(v) = f(g^{-1}(v))$;
- Unit representation: this is F with the trivial action.

We have obvious natural isomorphisms

$$V_1 \otimes (V_2 \otimes V_3) \simeq (V_1 \otimes V_2) \otimes V_3, \quad V_2 \otimes V_1 \simeq V_1 \otimes V_2, \quad V \otimes F \simeq F \otimes V \simeq V.$$

With these additional structures, $\mathbf{Rep}_F(G)$ is a *neutral Tannakian category over F* (ref. e.g. Deligne [Del] in the Grothendieck Festschrift, but we are not going to use the precise definition of Tannakian categories).

Definition 2.10. *A category $\mathscr{C}'$ is 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 $X \in \mathscr{C}'$.*

Definition 2.11. *A* sub-Tannakian category *of $\mathbf{Rep}_F(G)$ is a strictly full sub-category $\mathscr{C}$, such that*

(1) The unit representation F is an object of $\mathscr{C}$;

(2) If $V \in \mathscr{C}$ and V' is a sub-representation of V, then V' and V/V' are all in $\mathscr{C}$;

(3) If V is an object of $\mathscr{C}$, so is V^*;

(4) If $V_1, V_2 \in \mathscr{C}$, so is $V_1 \oplus V_2$;

(5) If $V_1, V_2 \in \mathscr{C}$, so is $V_1 \otimes V_2$.

Definition 2.12. *Let V be a F-representation of G. We say 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

$$\mathbf{D}_B(V) := (B \otimes_F V)^G, \tag{2.5}$$

we get a map

$$\begin{aligned} \alpha_V : B \otimes_E \mathbf{D}_B(V) &\longrightarrow B \otimes_F V \\ \lambda \otimes x \quad &\longmapsto \quad \lambda x \end{aligned} \tag{2.6}$$

for $\lambda \in B$, $x \in \mathbf{D}_B(V)$. 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 2.13. *Assume that B is (F,G)-regular. Then*

(1) For any F-representation V of G, the map α_V is injective and $\dim_E \mathbf{D}_B(V) \le \dim_F V$. We have

$$\begin{aligned} \dim_E \mathbf{D}_B(V) = \dim_F V &\Leftrightarrow \alpha_V \textit{ is an isomorphism} \\ &\Leftrightarrow V \textit{ is } B\textit{-admissible.} \end{aligned} \tag{2.7}$$

(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) to $\mathbf{Rep}_F^B(G)$ is an exact and faithful tensor functor, i.e., it satisfies the following three properties:

(i) Given V_1 and V_2 admissible, there is a natural isomorphism

$$\mathbf{D}_B(V_1) \otimes_E \mathbf{D}_B(V_2) \simeq \mathbf{D}_B(V_1 \otimes V_2). \tag{2.8}$$

(ii) Given V admissible, there is a natural isomorphism

$$\mathbf{D}_B(V^*) \simeq (\mathbf{D}_B(V))^*. \tag{2.9}$$

(iii) $\mathbf{D}_B(F) \simeq E$.

Proof. (1) Let $C = \operatorname{Frac} B$. Since B is (F,G)-regular, $C^G = B^G = E$. We have the following commutative diagram:

$$\begin{tikzcd} B \otimes_E \mathbf{D}_B(V) \arrow[r] \arrow[d, hook] & B \otimes_F V \arrow[dd, hook] \\ B \otimes_E \mathbf{D}_C(V) \arrow[d, hook] & \\ C \otimes_E \mathbf{D}_C(V) \arrow[r] & C \otimes_F V. \end{tikzcd}$$

To prove the injectivity of α_V, we are reduced to show the case when $B = C$ is a field. The injectivity of α_V means that given $h \ge 1$, $x_1, ..., x_h \in \mathbf{D}_B(V)$ linearly independent over E, then they are linearly independent over B. We prove it by induction on h.

The case $h = 1$ is trivial. We may assume $h \ge 2$. 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 $\lambda_i's$ 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 have to prove 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, set $v_i' = 1 \otimes v_i$, 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 $e_j = \sum\limits_{i=1}^{d} b_{ij} v_i$, for $(b_{ij}) \in M_d(B)$. Let $b = \det(b_{ij})$, the injectivity of α_V implies $b \neq 0$.

We need to prove b is invertible in B. Denote $\det V = \bigwedge_F^d V = Fv$, where $v = v_1 \wedge \cdots \wedge v_d$. We have $g(v) = \eta(g) v$ with $\eta : G \to F^\times$. Similarly let $e = e_1 \wedge \cdots \wedge e_d \in \bigwedge_E^d \mathbf{D}_B(V)$, $g(e) = e$ 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 since B is (F, G)-regular.

The second equivalence is easy. The condition that V is B-admissible, is nothing but that there exists a B-basis $\{x_1, \cdots, x_d\}$ of $B \otimes_F V$ such that each $x_i \in \mathbf{D}_B(V)$. Since $\alpha_V(1 \otimes x_i) = x_i$, and α_V is always injective, the 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 exact sequences

$$0 \to V' \to V \to V'' \to 0$$

and

$$0 \to B \otimes_F V' \to B \otimes_F V \to B \otimes_F V\text{”} \to 0.$$

Then we have a sequence

$$0 \to \mathbf{D}_B(V') \to \mathbf{D}_B(V) \to \mathbf{D}_B(V'') \dashrightarrow 0 \tag{2.10}$$

which 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 equality everywhere, and (2.10) is exact at $\mathbf{D}_B(V'')$ too. Then the functor $\mathbf{D}_B$ restricted to $\mathbf{Rep}_F^B(G)$ is exact, and is also faithful because $\mathbf{D}_B(V) \neq 0$ if $V \neq 0$.

Now we prove the second part of the assertion (2). (iii) is trivial. For (i), we have a commutative diagram

$$\begin{tikzcd}
(B \otimes_F V_1) \otimes_B (B \otimes_F V_2) \arrow[r, equal, "\Sigma"] & B \otimes_F (V_1 \otimes_F V_2) \\
\mathbf{D}_B(V_1) \otimes_E \mathbf{D}_B(V_2) \arrow[u, hook] \arrow[r, dotted, "\sigma"] & \mathbf{D}_B(V_1 \otimes_F V_2) \arrow[u]
\end{tikzcd}$$

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 $V = Fv$, $\mathbf{D}_B(V) = E \cdot b \otimes v$, and $V^* = Fv^*$, $\mathbf{D}_B(V^*) = E \cdot b^{-1} \otimes v^*$.

If $\dim_F V = d \geq 2$, we use the isomorphism

$$(\bigwedge\nolimits_F^{d-1} V) \otimes (\det V)^* \simeq V^*.$$

$\bigwedge_F^{d-1} V$ is admissible since it is just a quotient of $\bigotimes_F^{d-1} V$, and $(\det V)^*$ is also admissible since $\dim \det V = 1$, so V^* is admissible.

To show the isomorphism $\mathbf{D}_B(V^*) \simeq \mathbf{D}_B(V)^*$, we have a commutative diagram

$$\begin{tikzcd}
B \otimes_F V^* \arrow[r, "\simeq"] & (B \otimes_F V)^* \\
\mathbf{D}_B(V^*) \arrow[u, hook] \arrow[r, dotted, "\tau"] & \mathbf{D}_B(V)^* \arrow[u]
\end{tikzcd}$$

where the top isomorphism follows by the admissibility of V^*. 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 the induced homomorphism τ. From the diagram τ is clearly injective, and since both $D_B(V)$ and $D_B(V^*)$ have the same dimension as E-vector spaces, τ must be an isomorphism. □

2.2 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 choose a separable closure E^s of E and set $G = G_E = \mathrm{Gal}(E^s/E)$. Set $\varphi = (\lambda \mapsto \lambda^p)$ to be the absolute Frobenius of E.

2.2.1 Étale φ-modules over E.

Definition 2.14. *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, i.e.,*

$$\varphi(x+y) = \varphi(x) + \varphi(y), \quad \textit{for all } x, y \in M; \tag{2.11}$$

$$\varphi(\lambda x) = \varphi(\lambda)\varphi(x) = \lambda^p \varphi(x), \quad \textit{for all } \lambda \in E,\ x \in M. \tag{2.12}$$

If M is an E-vector space, let $M_\varphi = E\ {}_\varphi\!\otimes_E M$, where E is viewed as an E-module by the Frobenius $\varphi : E \to E$, which means for $\lambda, \mu \in E$ and $x \in M$,

$$\lambda(\mu \otimes x) = \lambda\mu \otimes x, \qquad \lambda \otimes \mu x = \mu^p \lambda \otimes x.$$

M_φ is an E-vector space, and if $\{e_1, \cdots, e_d\}$ is a basis of M over E, then $\{1 \otimes e_1, \cdots, 1 \otimes e_d\}$ is a basis of M_φ over E. Hence we have

$$\dim_E M_\varphi = \dim_E M.$$

Our main observation is

Remark 2.15. If M is any E-vector space, giving a semi-linear map $\varphi : M \to M$ is equivalent to giving a linear map

$$\begin{aligned} \Phi : \quad M_\varphi &\longrightarrow M \\ \lambda \otimes x &\longmapsto \lambda\varphi(x). \end{aligned} \tag{2.13}$$

Definition 2.16. *A φ-module M over E is* étale *if $\Phi : M_\varphi \to M$ is an isomorphism and if $\dim_E M$ is finite.*

Let $\{e_1, \cdots, e_d\}$ be a basis of M over E, and assume

$$\varphi e_j = \sum_{i=1}^{d} a_{ij} e_i,$$

then $\Phi(1 \otimes e_j) = \sum_{i=1}^{d} a_{ij} e_i$. Hence

$$\begin{aligned} M \text{ is étale } &\Longleftrightarrow \Phi \text{ is an isomorphism} \Longleftrightarrow \Phi \text{ is injective} \\ &\Longleftrightarrow \Phi \text{ is surjective } \Longleftrightarrow M = E \cdot \varphi(M) \\ &\Longleftrightarrow A = (a_{ij}) \text{ is invertible in E.} \end{aligned} \tag{2.14}$$

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 2.17. *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

$$\begin{tikzcd}
0 \arrow[r] & M'_{\varphi} \arrow[r] \arrow[d, "\Phi'"] & (M_1)_{\varphi} \arrow[r] \arrow[d, "\Phi_1"] & (M_2)_{\varphi} \arrow[r] \arrow[d, "\Phi_2"] & (M'')_{\varphi} \arrow[r] \arrow[d, "\Phi''"] & 0 \\
0 \arrow[r] & M' \arrow[r] & M_1 \arrow[r] & M_2 \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

are exact. By definition, Φ_1 and Φ_2 are isomorphisms, so Φ' is injective and Φ'' is surjective. By comparing the dimensions, both Φ' and Φ'' 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:

- Let M_1, M_2 be two étale φ-modules over E. Let $M_1 \otimes M_2 = M_1 \otimes_E M_2$. It is viewed as a φ-module by
$$\varphi(x_1 \otimes x_2) = \varphi(x_1) \otimes \varphi(x_2).$$
One can easily check that $M_1 \otimes M_2 \in \mathscr{M}_{\varphi}^{\text{ét}}(E)$.
- E is an étale φ-module and for every M étale,
$$M \otimes E = E \otimes M = M.$$
- If M is an étale φ-module, assume that $\Phi : M_{\varphi} \xrightarrow{\sim} M$ corresponds to φ. Set $M^* = \mathscr{L}_E(M, E)$, We have
$${}^t\Phi : M^* \xrightarrow{\sim} (M_{\varphi})^* \simeq (M^*)_{\varphi},$$
where the second isomorphism is the canonical isomorphism since E is a flat E-module. Then
$${}^t\Phi^{-1} : (M^*)_{\varphi} \xrightarrow{\sim} M^*$$
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 and B satisfying $B = {}^tA^{-1}$.

2.2.2 The functor M.

Recall that

Definition 2.18. *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, $\mathbb{F}_p \subset (E^s)^G = E$, and 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

$$\mathbf{M}(V) = \mathbf{D}_{E^s}(V) = (E^s \otimes_{\mathbb{F}_p} V)^G, \tag{2.15}$$

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 $\varphi(x) = x^p$, which commutes with the action of G:

$$\varphi(g(x)) = g(\varphi(x)), \quad \text{for all } g \in G, \ x \in E^s$$

We define the Frobenius on $E^s \otimes_{\mathbb{F}_p} V$ as follows:

$$\varphi(\lambda \otimes v) = \lambda^p \otimes v = \varphi(\lambda) \otimes v.$$

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 is in $\mathbf{M}(V)$, so is $\varphi(x)$. 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 2.19. *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 already know 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 proves that $\mathbf{M}(V)$ is étale and hence the proposition. □

From Proposition 2.19, we thus get an additive functor

$$\mathbf{M} : \mathbf{Rep}_{\mathbb{F}_p}(G) \to \mathscr{M}_{\varphi}^{\text{ét}}(E). \tag{2.16}$$

2.2.3 The inverse functor V.

We now define a functor

$$\mathbf{V} : \mathscr{M}_{\varphi}^{\text{ét}}(E) \longrightarrow \mathbf{Rep}_{\mathbb{F}_p}(G). \tag{2.17}$$

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

$$\mathbf{V}(M) = \{y \in E^s \otimes_E M \mid \varphi(y) = y\} = (E^s \otimes_E M)_{\varphi=1}, \tag{2.18}$$

which is a sub $\mathbb{F}_p$-vector space stable under G.

Lemma 2.20. *The natural map*

$$\begin{array}{rcl} \alpha_M : E^s \otimes_{F_p} \mathbf{V}(M) & \longrightarrow & E^s \otimes_E M \\ \lambda \otimes v & \longmapsto & \lambda v \end{array} \tag{2.19}$$

is injective and therefore $\dim_{\mathbb{F}_p} \mathbf{V}(M) \leq \dim_E M$.

Proof. We want 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 2.21. *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.

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 Frobenius and with the action of G. We use this to identify these two terms. 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 have proved that $\mathbf{V}(\mathbf{M}(V)) = V$. Since $\mathbf{V}(M) \neq 0$ if $M \neq 0$, a formal consequence is that $\mathbf{M}$ is an exact and fully faithful functor inducing an equivalence 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

$$M \simeq \mathbf{M}(V).$$

We take $V = \mathbf{V}(M)$, and prove that $M \simeq \mathbf{M}(\mathbf{V}(M))$.

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 that

$$x_j^p = v\Big(\sum_{i=1}^d b_{ij} e_i^*\Big) = \sum_{i=1}^d b_{ij} x_i.$$

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

$$\mathbf{V}(M) = \mathrm{Hom}_{E-\mathrm{algebra}}(R, E^s). \tag{2.20}$$

Lemma 2.22. *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's 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

$$\mathbf{M}(\mathbf{V}(M)) \simeq M.$$

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 2.22. XX Write 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 $\{x_1^{i_1} x_2^{i_2} \cdots x_d^{i_d}\}$ with $0 \leq i_k \leq p-1$ 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 easily that R_m is a free $E[X_{m+1}, X_{m+2}, \ldots, X_d]$-module with the images of $\{X_1^{i_1} X_2^{i_2} \ldots X_m^{i_m}\}$ with $0 \leq i_q \leq p-1$ 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 $x_j^p = \sum\limits_{i=1}^d b_{ij} x_i + b_j$, we have

$$0 = p x_j^{p-1} dx_j = \sum_{i=1}^d b_{ij} dx_j,$$

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. XX or Illusie's course note) where the E_i's are finite separable extensions of E. Set $n_i = [E_i : E]$, then $p^d = \dim_E R = \sum\limits_{i=1}^r n_i$. On the other hand, we have

$$\mathrm{Hom}_{E-\mathrm{algebra}}(R, E^s) = \coprod_i \mathrm{Hom}_{E-\mathrm{algebra}}(E_i, E^s),$$

and for any i, there are exactly n_i E-embeddings of E_1 into E^s. Therefore the set $\mathrm{Hom}_{E-\mathrm{algebra}}(E, E^s)$ has p^d elements. □

Remark 2.23. 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 $V \simeq \mathbf{V}(M_A)$. 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 $\mathbf{M}(V) \simeq M_A$. Thus $V \simeq \mathbf{V}(M_A)$.

Moreover, if $A, B \in \mathrm{GL}_d(E)$, then

$$\mathbf{V}(M_A) \simeq \mathbf{V}(M_B) \Leftrightarrow \text{there exists } P \in \mathrm{GL}_d(E), \text{ such that } B = P^{-1}A\varphi(P).$$

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.

2.3 p-adic Galois representations of fields of characteristic $p > 0$

2.3.1 Étale φ-modules over $\mathcal{E}$.

Let E be a field of characteristic $p > 0$, and E^s be a separable closure of E with the Galois group $G = \mathrm{Gal}(E^s/E)$. Let $\mathbf{Rep}_{\mathbb{Q}_p}(G)$ denote the category of p-adic representations of G.

From §A.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 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 to the ring $W(E)$ of Witt vectors with coefficients in 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 2.24. *(1) 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 $x, y \in M,\ \lambda \in \mathcal{O}_{\mathcal{E}}$.

(2) A φ-module over $\mathcal{E}$ is an $\mathcal{E}$-vector space D equipped with a semi-linear map $\varphi : D \to D$.

Remark 2.25. A φ-module over $\mathcal{O}_{\mathcal{E}}$ killed by p is just a φ-module over E.

Set

$$M_\varphi = \mathcal{O}_{\mathcal{E}} \ {}_\varphi\!\otimes_{\mathcal{O}_{\mathcal{E}}} M.$$

As before, giving a semi-linear map $\varphi : M \to M$ is equivalent to giving a $\mathcal{O}_{\mathcal{E}}$-linear map $\varPhi : M_\varphi \to M$. 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 $\varPhi : D_\varphi \to D$.

Definition 2.26. *(1) A φ-module over $\mathcal{O}_{\mathcal{E}}$ is* étale *if M is an $\mathcal{O}_{\mathcal{E}}$-module of finite type and $\varPhi : M_\varphi \to M$ is an isomorphism.*

(2) 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 $\mathcal{O}_{\mathcal{E}}$.*

It is easy to check that

Proposition 2.27. *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.*

Recall that an $\mathcal{O}_{\mathcal{E}}$-lattice M is a sub $\mathcal{O}_{\mathcal{E}}$-module of finite type containing a basis. 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

$$\varphi e_j = \sum_{i=1}^{d} a_{ij} e_i, \quad (a_{ij}) \in \mathrm{GL}_d(\mathcal{O}_{\mathcal{E}}).$$

One sees immediately that

Proposition 2.28. *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.*

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. We want to construct equivalences of categories:

$$\mathbf{M} : \mathbf{Rep}_{\mathbb{Q}_p}(G) \to \mathscr{M}_\varphi^{\text{ét}}(\mathcal{E})$$

and

$$\mathbf{M} : \mathbf{Rep}_{\mathbb{Z}_p}(G) \to \mathscr{M}_\varphi^{\text{ét}}(\mathcal{O}_{\mathcal{E}}).$$

2.3.2 The field $\widehat{\mathcal{E}^{\mathbf{ur}}}$

Let $\mathcal{F}$ be a finite extension of $\mathcal{E}$, $\mathcal{O}_{\mathcal{F}}$ be the ring of the integers of $\mathcal{F}$. We say $\mathcal{F}/\mathcal{E}$ is *unramified* if

(1) p is a generator of the maximal ideal of $\mathcal{O}_{\mathcal{F}}$;
(2) $F = \mathcal{O}_{\mathcal{F}}/p$ is a separable extension of E.

For any homomorphism $f : E \to F$ of fields of characteristic p, by Theorem A.45, the functoriality of Cohen rings tells us that there is a unique local homomorphism $\mathcal{C}(E) \to \mathcal{C}(F)$ which induces f on the residue fields. Then for any finite separable extension F of E, there is a *unique* unramified extension $\mathcal{F} = \operatorname{Frac}\mathcal{C}(F)$ of $\mathcal{E}$ whose residue field is F (where *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 on F), and moreover there exists a unique endomorphism $\varphi' : \mathcal{F} \to \mathcal{F}$ such that $\varphi'|_{\mathcal{E}} = \varphi$ 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 A.45, this construction is functorial:

$$\sigma : F \to F', \sigma|_E = \text{Id} \ \text{ induces } \sigma : \mathcal{E}_F \to \mathcal{E}_{F'}, \sigma|_{\mathcal{E}} = \text{Id}$$

and σ commutes with the Frobenius map. In particular, if F/E is Galois, then $\mathcal{E}_F/\mathcal{E}$ is also Galois with Galois group

$$\text{Gal}(\mathcal{E}_F/\mathcal{E}) = \text{Gal}(F/E)$$

and the action of $\text{Gal}(F/E)$ 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

$$\mathcal{E}^{\text{ur}} := \bigcup_{F\in S} \mathcal{E}_F. \tag{2.21}$$

Then $\mathcal{E}^{\text{ur}}/\mathcal{E}$ is a Galois extension with $\text{Gal}(\mathcal{E}^{\text{ur}}/\mathcal{E}) = G$. Let $\widehat{\mathcal{E}^{\text{ur}}}$ be the completion of $\mathcal{E}^{\text{ur}}$, and $\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}}$ be its ring of integers. Then $\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}}$ is a local ring, and

$$\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}} = \varprojlim \mathcal{O}_{\mathcal{E}^{\text{ur}}}/p^n\mathcal{O}_{\mathcal{E}^{\text{ur}}}. \tag{2.22}$$

We have the endomorphism φ on $\mathcal{E}^{\text{ur}}$ such that $\varphi(\mathcal{O}_{\mathcal{E}^{\text{ur}}}) \subset \mathcal{O}_{\mathcal{E}^{\text{ur}}}$. The action of φ extends by continuity to an action on $\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}}$ and $\widehat{\mathcal{E}^{\text{ur}}}$. Similarly we have the action of G on $\mathcal{E}^{\text{ur}}$, $\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}}$ and $\widehat{\mathcal{E}^{\text{ur}}}$. Moreover the action of φ commutes with the action of G. We have the following important facts:

Proposition 2.29. *(1)* $(\widehat{\mathcal{E}^{\text{ur}}})^G = \mathcal{E}$, $(\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}})^G = \mathcal{O}_{\mathcal{E}}$.

(2) $(\widehat{\mathcal{E}^{\text{ur}}})_{\varphi=1} = \mathbb{Q}_p$, $(\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}})_{\varphi=1} = \mathbb{Z}_p$.

2.3.3 $\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}}$ and $\mathbb{Z}_p$ representations.

Proposition 2.30. *For any* $\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}}$*-representation* X *of* G*, the natural map*

$$\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} X^G \to X$$

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 2.7.

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 2.7), i.e. $X' \simeq (E^s)^d$ with the natural action of G. So

$$H^1_{\mathrm{cont}}(G, X') = H^1(G, X') \simeq (H^1(G, E^s))^d = 0.$$

Then we have the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} X'^G \arrow[r] \arrow[d] & \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} X^G \arrow[r] \arrow[d] & \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} X''^G \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & X' \arrow[r] & X \arrow[r] & X'' \arrow[r] & 0.
\end{tikzcd}$$

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 acting on it through

$$\varphi(\lambda \otimes t) = \varphi(\lambda) \otimes t, \quad g(\lambda \otimes t) = g(\lambda) \otimes g(t)$$

for any $g \in G$, $\lambda \in \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$ and $t \in T$. Let

$$\mathbf{M}(T) = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T)^G, \tag{2.23}$$

then by Proposition 2.30,

$$\alpha_T : \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} \mathbf{M}(T) \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T \tag{2.24}$$

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 $0 \to T \to T \to T/pT \to 0$, 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 2.30. Thus $\mathbf{M}(T)$ is étale if and only if $\mathbf{M}(T/pT)$ is étale as a φ-module over E, which is shown in Proposition 2.19.

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

$$\mathbf{V}(M) = \{y \in \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M \mid \varphi(y) = y\} = \left(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M\right)_{\varphi=1}. \tag{2.25}$$

Proposition 2.31. *For any étale φ-module M over $\mathcal{O}_{\mathcal{E}}$, the natural map*

$$\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} \mathbf{V}(M) \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M$$

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 $X'_{\varphi=1} = \mathbf{V}(M')$, $X_{\varphi=1} = \mathbf{V}(M)$, $X''_{\varphi=1} = \mathbf{V}(M'')$. 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 proof 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 extend the analogous result in Theorem 2.21 for mod-p representations.

Theorem 2.32. *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

$$\mathbf{V} : \mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{O}_{\mathcal{E}}) \to \mathbf{Rep}_{\mathbb{Z}_p}(G), \quad M \mapsto \mathbf{V}(M)$$

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 (2.24), then

$$\begin{aligned}\mathbf{V}(\mathbf{M}(T)) =&(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} \mathbf{M}(T))_{\varphi=1} = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T)_{\varphi=1}\\ =&(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}})_{\varphi=1} \otimes_{\mathbb{Z}_p} T = T,\end{aligned}$$

and

$$\begin{aligned}\mathbf{M}(\mathbf{V}(M)) =&(\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} \mathbf{V}(M))^G \simeq (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M)^G\\ =&\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}^G \otimes_{\mathcal{O}_{\mathcal{E}}} M = M.\end{aligned}$$

The theorem is proved.

2.3.4 p-adic representations.

If V is a p-adic representation of G, D is an étale φ-module over $\mathcal{E}$, let

$$\mathbf{M}(V) = (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V)^G,$$

$$\mathbf{V}(D) = (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} D)_{\varphi=1},$$

Theorem 2.33. *(1) For any p-adic representation V of G, $\mathbf{M}(V)$ is an étale φ-module over $\mathcal{E}$, and the natural map:*

$$\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} \mathbf{M}(V) \to \widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V$$

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

$$\mathbf{M} : \mathbf{Rep}_{\mathbb{Q}_p}(G) \to \mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{E})$$

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.

Proof. The proof is a formal consequence of what we did in §2.3.3 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

$$\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} T)[1/p], \quad \mathbf{M}(V) = \mathbf{M}(T)[1/p] = \mathcal{E} \otimes_{\mathcal{O}_{\mathcal{E}}} \mathbf{M}(T).$$

(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

$$\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} D = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M)[1/p], \quad \mathbf{V}(D) = \mathbf{V}(M)[1/p] = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathbf{V}(M).$$

□

Remark 2.34. The category $\mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{E})$ has a natural structure of a Tannakian category, i.e. one may define a tensor product, a duality and the unit object and they have 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 $\mathbf{M}$ is a tensor functor, i.e. we have natural isomorphisms

$$\mathbf{M}(V_1) \otimes \mathbf{M}(V_2) \to \mathbf{M}(V_1 \otimes V_2) \text{ and } \mathbf{M}(V^*) \to \mathbf{M}(V)^*.$$

Similarly, we have a notion of tensor product in the category $\mathscr{M}_{\varphi}^{\text{ét}}(\mathcal{O}_{\mathcal{E}})$, two notion of duality (one for free $\mathcal{O}_{\mathcal{E}}$-modules, the other for p-torsion modules) and similar natural isomorphisms.

2.3.5 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 $\varphi(e_j) = \sum_{i=1}^{d} a_{ij} e_i$. Then M_A is an étale φ-module over $\mathcal{O}_{\mathcal{E}}$ and $T_A = \mathbf{V}(M_A)$ 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 $V \simeq V_A$. 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 2.35. 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 $\mathrm{GL}_d(\mathcal{O}_{\mathcal{E}})$.

3

C-representations and Methods of Sen

3.1 Krasner's Lemma and Ax-Sen's Lemma

3.1.1 Krasner's Lemma.

Proposition 3.1 (Krasner's Lemma). *Let F be a complete nonarchimedean field, and E be a closed subfield of F, let $\alpha, \beta \in F$ with α separable over E. Assume that $|\beta - \alpha| < |\alpha' - \alpha|$ for all conjugates α' of α over E, $\alpha' \neq \alpha$. 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. □

Corollary 3.2. *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. Then $\widehat{K^s} = \widehat{\overline{K}}$ and it is an algebraically closed field.*

Proof. Let $C = \widehat{K^s}$, we shall prove:

(i) If $\mathrm{char}\, K = p$, 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 $m \gg 0$, 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 $P_n'(X) = -\pi^n \neq 0$ and P_n is separable. Let α_n be a root of P_n in K^s, $\alpha_n \in \mathcal{O}_{K^s}$. Then

$$\alpha_{n+1}^p - \alpha_n^p = \pi^{n+1}\alpha_{n+1} - \pi^n\alpha_n + a_{n+1} - a_n,$$

one has $v(\alpha_{n+1}^p - \alpha_n^p) \geq n$. Since $(\alpha_{n+1} - \alpha_n)^p = \alpha_{n+1}^p - \alpha_n^p$, $v(\alpha_{n+1} - \alpha_n) \geq n/p$, which implies $(\alpha_n)_{n \in \mathbb{N}}$ 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

$$P(X) = a_0 + a_1X + a_2X^2 + \cdots + a_{d-1}X^{d-1} + X^d$$

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 decomposition 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'. Let

$$P_1 = b_0 + b_1X + b_2X^2 + \cdots + b_{d-1}X^{d-1} + X^d \in K^s[X]$$

with $b_i \in K^s$, and $v(b_i - a_i) > rd$. 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 $\alpha' \in C'$ and $P(\alpha') = 0$. 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 $v(\beta - \alpha) > r$. Applying Krasner's Lemma, we get $\alpha \in C(\beta) = C$. □

3.1.2 Ax-Sen's Lemma.

Let K be a nonarchimedean field, let E be an algebraic extension of K. For any α containing in any separable extension of E, set

$$\varDelta_E(\alpha) = \min\{v(\alpha' - \alpha)\}, \tag{3.1}$$

where α' are conjugates of α over E. Then

$$\varDelta_E(\alpha) = +\infty \text{ if and only if } \alpha \in E.$$

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 3.3 (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*

$$v(\alpha - a) > \Delta_E(\alpha) - \frac{p}{(p-1)^2} v(p). \tag{3.2}$$

Remark 3.4. If choose $v = v_p$, then $v_p(\alpha - a) > \Delta_E(\alpha) - \frac{p}{(p-1)^2}$, but $\Delta_E(\alpha)$ is dependent of v_p.

We shall follow the proof of Ax ([Ax70]).

Lemma 3.5. *Let $R \in E[X]$ be a monic polynomial of degree $d \geq 2$, such that $v(\lambda) \geq r$ for any root λ of R in $\overline{E}$, the algebraic closure of E. Let $m \in \mathbb{N}$, with $0 < m < d$, then there exists $\mu \in F$, such that μ is a root of $R^{(m)}(X)$, the m-th derivative of $R(X)$, and*

$$v(\mu) \geq r - \frac{1}{d-m} v(\binom{d}{m}).$$

Proof. Let

$$R = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_d) = \sum_{i=0}^{d} b_i X^i,$$

then $b_i \in \mathbb{Z}[\lambda_1, \cdots, \lambda_d]$ are 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 $b_m = \binom{d}{m} (-1)^{d-m} \mu_1 \mu_2 \cdots \mu_{d-m}$. Hence

$$\sum_{i=1}^{d-m} v(\mu_i) = v(b_m) - v(\binom{d}{m}) \geq (d-m)r - v(\binom{d}{m}).$$

There exists i, such that

$$v(\mu_i) \geq r - \frac{1}{d-m} v(\binom{d}{m}).$$

The proof is finished. □

Proof (Proof of Proposition 3.3). For any $d \geq 1$, let $l(d)$ be the biggest integer l such that $p^l \leq d$. Let $\varepsilon(d) = \sum_{i=1}^{l(d)} \frac{1}{p^i - p^{i-1}}$. Then $l(d) = 0$ if and only if $d < p$, or if and only if $\varepsilon(d) = 0$. We want to prove 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 be the monic minimal polynomial of α over E. Let

$$R(X) = P(X + \alpha), \quad R^{(m)}(X) = P^{(m)}(X + \alpha).$$

If d is not a power of P, then $d = p^s n$, with n prime to p, and $n \geq 2$. Otherwise write $d = p^s p$, $s \in \mathbb{N}$. Let $m = p^s$.

Choose μ as in Lemma 3.5. The roots of R are of the form $\alpha' - \alpha$ for α' a conjugate of α. Set $r = \Delta_E(\alpha)$, and $\beta = \mu + \alpha$. Then

$$v(\beta - \alpha) \geq r - \frac{1}{d-m} v\Big(\binom{d}{m}\Big).$$

As $P^{(m)}(\beta) = 0$, and $P^{(m)}(X) \in E[X]$ with degree $d - m$, β is algebraic over E of degree not higher than $d - m$. Either $\beta \in E$, then we choose $a = \beta$, or $\beta \notin E$, then 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 want to check that $v(\alpha - a) > r - \varepsilon(d)$.

Case 1: $d = p^s n$ $(n \geq 2)$, and $m = p^s$. 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: $d = p^s p$, and $m = p^s$. 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 3.6 (Ax-Sen's Lemma, Characteristic$>$ 0 case). *Assume K, E, α as before. Assume K is perfect 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 $r \gg 0$, $v(c^{p^{-r}}) > -\varepsilon$. 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

$$S = \{\sigma \mid \sigma : L \hookrightarrow \overline{E} \text{ be an E-embedding}\},$$

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 $\sum\limits_{\sigma \in S} \sigma(c)\alpha = \mathrm{Tr}_{L/E}(c) = 1$,

$$v(\alpha - a) = v(\sum_{\sigma \in S} \sigma(c)(\alpha - \sigma(\alpha))) \geq \min\{v(\sigma(c)(\alpha - \sigma(\alpha)))\} \geq \varDelta_E(\alpha) - \varepsilon.$$

This completes the proof. □

We give an application of Ax-Sen's Lemma. Let K be a complete nonarchimedean field, K^s be a separable closure of K. Let $G_K = \mathrm{Gal}(K^s/K)$, $C = \widehat{K^s}$. The action of G_K extends by continuity to C. Let H be any closed subgroup of G_K, $L = (K^s)^H$, and $H = \mathrm{Gal}(K^s/L)$. A question arises:

Question 3.7. What is C^H?

If $\mathrm{char}\, K = p$, we have $\overline{K} \subset C$. Let

$$L^{\mathrm{rad}} = \{x \in C \mid \text{there exists } n, \text{ such that } x^{p^n} \in L\}.$$

Then 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 3.8. *For any close subgroup H of G_K, we have*

$$C^H = \begin{cases} \widehat{L}, & \text{if } \mathrm{char}\, K = 0, \\ \widehat{L^{\mathrm{rad}}}, & \text{if } \mathrm{char}\, K = p \end{cases} \tag{3.3}$$

where $L = (K^s)^H$. In particular,

$$C^{G_K} = \begin{cases} \widehat{K} = K, & \text{if } \mathrm{char}\, K = 0, \\ \widehat{K^{\mathrm{rad}}}, & \text{if } \mathrm{char}\, K = p. \end{cases} \tag{3.4}$$

Proof. If $\mathrm{char}\, K = p$, we have a diagram:

$$\begin{tikzcd}
K^s \arrow[r, phantom, "\subset"] \arrow[d, dash, "G_K"'] & (K^{\mathrm{rad}})^s = \overline{K} \arrow[r, phantom, "\subset"] \arrow[d, dash, "G_K"'] & (\widehat{K^{\mathrm{rad}}})^s = \overline{\widehat{K^{\mathrm{rad}}}} \arrow[r, phantom, "\subset"] \arrow[d, dash, "G_K"'] & C \\
K \arrow[r, phantom, "\subset"] & K^{\mathrm{rad}} \arrow[r, phantom, "\subset"] & \widehat{K^{\mathrm{rad}}} &
\end{tikzcd}$$

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 the claim that $C^H = \widehat{L}$.

If $\operatorname{char} K = p$, we choose any $\varepsilon > 0$. If $\operatorname{char} K = 0$, 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 $g \in H$. Thus $\varDelta_L(\alpha_n) \geq n$, which implies that there exists $a_n \in L$, such that $v(\alpha_n - a_n) \geq n - \varepsilon$, and $\lim\limits_{n \to +\infty} a_n = \alpha \in \widehat{L}$. □

3.2 Classification of C-representations

Let K be a p-adic field. Let $G = G_K = \mathrm{Gal}(\overline{K}/K)$. Let $v = v_p$ be the valuation of K and its extensions such that $v(p) = 1$. Let $C = \widehat{\overline{K}}$.

We fix K_∞, a ramified $\mathbb{Z}_p$-extension of K contained in $\overline{K}$. 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 $K_m = K_\infty^{\varGamma_m}$ be the subfield of K_∞ fixed by $\varGamma_m$. Let γ be a topological generator of $\varGamma$ and let $\gamma_m = \gamma^{p^m}$, which is a topological generator of $\varGamma_m$.

For any subfield F of C, let $\widehat{F}$ be its closure in C. We assume the fields considered in this section are equipped with the natural p-adic topology.

3.2.1 The study of $H^1_{\mathrm{cont}}(G, \mathrm{GL}_n(C))$.

We first study the cohomology group $H^1_{\mathrm{cont}}(G, \mathrm{GL}_n(C))$.

Almost étale descent.

Lemma 3.9. *Let H_0 be an open subgroup of H and U be a cocycle $H_0 \to \mathrm{GL}_n(C)$ such that $v(U_\sigma - 1) \geq a$, $a > 0$ for all $\sigma \in H_0$. Then there exists a matrix $M \in \mathrm{GL}_n(C)$, $v(M - 1) \geq a/2$, such that*

$$v(M^{-1} U_\sigma \sigma(M) - 1) \geq a + 1, \quad \textit{for all } \sigma \in H_0.$$

Proof. The proof is imitating the proof of Hilbert's Theorem 90 (Theorem A.108).

Fix $H_1 \subset H_0$ open and normal such that $v(U_\sigma - 1) \geq a + 1 + a/2$ for $\sigma \in H_1$, which is possible by continuity. By Corollary A.89, 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 $S \subset H$ be a set of representatives of H_0/H_1, denote $M_S = \sum\limits_{\sigma \in S} \sigma(\alpha)U_\sigma$, we have $M_S - 1 = \sum\limits_{\sigma \in S} \sigma(\alpha)(U_\sigma - 1)$, this implies $v(M_S - 1) \geqslant a/2$ and moreover

$$M_S^{-1} = \sum_{n=0}^{+\infty}(1 - M_S)^n,$$

so we have $v(M_S^{-1}) \geqslant 0$ and $M_S \in \mathrm{GL}_n(C)$.

If $\tau \in H_1$, then $U_{\sigma\tau} - U_\sigma = U_\sigma(\sigma(U_\tau) - 1)$. Let $S' \subset H_0$ be another set of representatives of H_0/H_1, so for any $\sigma' \in S'$, there exists $\tau \in H_1$ and $\sigma \in S$ such that $\sigma' = \sigma\tau$, so we get

$$M_S - M_{S'} = \sum_{\sigma \in S} \sigma(\alpha)(U_\sigma - U_{\sigma\tau}) = \sum_{\sigma \in S} \sigma(\alpha)U_\sigma(1 - \sigma(U_\tau)),$$

thus

$$v(M_S - M_{S'}) \geqslant a + 1 + a/2 - a/2 = a + 1.$$

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 $v(M_S^{-1}(M_{\tau S} - M_S)) \geq a + 1$. Take $M = M_S$ for any S, we get the result. □

Corollary 3.10. *Under the same hypotheses as the above lemma, there exists $M \in \mathrm{GL}_n(C)$ such that*

$$v(M - 1) \geq a/2, \ \ M^{-1}U_\sigma\sigma(M) = 1, \forall\ \sigma \in \ H_0.$$

Proof. Repeat the lemma ($a \mapsto a+1 \mapsto a+2 \mapsto \cdots$), and take the limits. □

Proposition 3.11. $H^1_{\mathrm{cont}}(H, \mathrm{GL}_n(C)) = 1.$

Proof. We need to show that any given cocycle U on H with values in $\mathrm{GL}_n(C)$ 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 3.10, the restriction of U on H_0 is trivial. By the inflation-restriction sequence

$$1 \to H^1_{\mathrm{cont}}(H/H_0, \mathrm{GL}_n(C^{H_0})) \to H^1_{\mathrm{cont}}(H, \mathrm{GL}_n(C)) \to H^1_{\mathrm{cont}}(H_0, \mathrm{GL}_n(C)),$$

since H/H_0 is finite, by Hilbert Theorem 90, $H^1_{\mathrm{cont}}(H/H_0, \mathrm{GL}_n(C^{H_0}))$ is trivial, as a consequence U is also trivial. □

Proposition 3.12. *The inflation map gives a bijection*

$$j : H^1_{\text{cont}}(\Gamma, \mathrm{GL}_n(\widehat{K}_\infty)) \xrightarrow{\sim} H^1_{\text{cont}}(G, \mathrm{GL}_n(C)). \tag{3.5}$$

Proof. This follows from the exact inflation-restriction sequence

$$1 \to H^1_{\text{cont}}(\Gamma, \mathrm{GL}_n(C^H)) \to H^1_{\text{cont}}(G, \mathrm{GL}_n(C)) \to H^1_{\text{cont}}(H, \mathrm{GL}_n(C)),$$

since the third term is trivial by the previous Proposition, $\widehat{K}_\infty = C^H$, and the inflation map is injective. □

Undo the completion.

Recall by Corollary A.92 and Proposition A.97, for Tate's normalized trace map $R_r(x)$, we have constants c, d independent of r, such that

$$v(R_r(x)) \geq v(x) - c, \quad x \in \widehat{K}_\infty \tag{3.6}$$

and

$$v((\gamma_r - 1)^{-1}x) \geq v(x) - d, \quad x \in X_r = \{x \in \widehat{K}_\infty \mid R_r(x) = 0\}. \tag{3.7}$$

Lemma 3.13. *Given $\delta > 0$, $b \geq 2c + 2d + \delta$. Given $r \geq 0$. Suppose $U = 1 + U_1 + U_2$ with*

$$\begin{aligned} &U_1 \in \mathrm{M}_n(K_r), v(U_1) \geq b - c - d \\ &U_2 \in \mathrm{M}_n(C), v(U_2) \geq b' \geq b. \end{aligned}$$

Then, there exists $M \in \mathrm{GL}_n(C), v(M-1) \geq b - c - d$ such that

$$M^{-1}U\gamma_r(M) = 1 + V_1 + V_2,$$

with

$$\begin{aligned} &V_1 \in \mathrm{M}_n(K_r), \ v(V_1) \geq b - c - d, \\ &V_2 \in \mathrm{M}_n(C), \ v(V_2) \geq b' + \delta. \end{aligned}$$

Proof. One has $U_2 = R_r(U_2) + (1 - \gamma_r)V$ such that

$$v(R_r(U_2)) \geq v(U_2) - c, \quad v(V) \geq v(U_2) - c - d.$$

Thus,

$$\begin{aligned} (1+V)^{-1}U\gamma_r(1+V) &= (1 - V + V^2 - \cdots)(1 + U_1 + U_2)(1 + \gamma_r(V)) \\ &= 1 + U_1 + (\gamma_r - 1)V + U_2 + (\text{terms of degree} \geq 2). \end{aligned}$$

Let $V_1 = U_1 + R_r(U_2) \in \mathrm{M}_n(K_r)$ and W be the terms of degree ≥ 2. Thus $v(W) \geq b + b' - 2c - 2d \geq b' + \delta$. So we can take $M = 1 + V$, $V_2 = W$. □

Corollary 3.14. *Keep the same hypotheses as in Lemma 3.13. Then there exists* $M \in \mathrm{GL}_n(\widehat{K}_\infty)$, $v(M-1) \geq b-c-d$ *such that* $M^{-1}U\gamma_r(M) \in \mathrm{GL}_n(K_r)$.

Proof. Repeat the lemma ($b \mapsto b+\delta \mapsto b+2\delta \mapsto \cdots$), and take the limit. □

Lemma 3.15. *Suppose* $B \in \mathrm{GL}_n(C)$. *If there exist* $V_1, V_2 \in \mathrm{GL}_n(K_i)$ *such that for some* $r \geq i$,

$$v(V_1-1) > d, \quad v(V_2-1) > d, \quad \gamma_r(B) = V_1 B V_2,$$

then $B \in \mathrm{GL}_n(K_i)$.

Proof. Take $C = B - R_i(B)$. We have to show that $C = 0$. Note that C has coefficients in $X_i = (1-R_i)\widehat{K}_\infty$, and R_i is K_i-linear and commutes with γ_r, thus,

$$\gamma_r(C) - C = V_1 C V_2 - C = (V_1-1)CV_2 + V_1 C(V_2-1) - (V_1-1)C(V_2-1)$$

Hence, $v(\gamma_r(C)-C) > v(C)+d$. By Proposition A.97, this implies $v(C) = +\infty$, i.e. $C = 0$. □

Proposition 3.16. *The inclusion* $\mathrm{GL}_n(K_\infty) \hookrightarrow \mathrm{GL}_n(\widehat{K}_\infty)$ *induces a bijection*

$$i : H^1_{\mathrm{cont}}(\Gamma, \mathrm{GL}_n(K_\infty)) \xrightarrow{\sim} H^1_{\mathrm{cont}}(\Gamma, \mathrm{GL}_n(\widehat{K}_\infty)).$$

Moreover, for any $\sigma \to U_\sigma$ *a continuous cocycle of* $H^1_{\mathrm{cont}}(\Gamma, \mathrm{GL}_n(\widehat{K}_\infty))$, *if* $v(U_\sigma - 1) > 2c+2d$ *for* $\sigma \in \Gamma_r$, *then there exists* $M \in \mathrm{GL}_n(K_\infty)$, $v(M-1) > c+d$ *such that*

$$\sigma \longmapsto U'_\sigma = M^{-1}U_\sigma \sigma(M)$$

satisfies $U'_\sigma \in \mathrm{GL}_n(K_r)$.

Proof. We first prove injectivity. Let U, U' be cocycles of Γ in $\mathrm{GL}_n(K_\infty)$ and suppose they become cohomologous in $\mathrm{GL}_n(\widehat{K}_\infty)$, that is, there is an $M \in \mathrm{GL}_n(\widehat{K}_\infty)$ such that $M^{-1}U_\sigma\sigma(M) = U'_\sigma$ for all $\sigma \in \Gamma$. 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 3.15, then $M \in \mathrm{GL}_n(K_r)$. Thus U and U' are cohomologous in $\mathrm{GL}_n(K_\infty)$, and injectivity is proved.

We now prove surjectivity. Given U, a cocycle of Γ in $\mathrm{GL}_n(\widehat{K}_\infty)$, by continuity there exists an r such that for all $\sigma \in \Gamma_r$, we have $v(U_\sigma - 1) > 2c+2d$. By Corollary 3.14, there exists $M \in \mathrm{GL}_r(C)$, $v(M-1) > 2(c+d)$ such that $U'_{\gamma_r} = M^{-1}U_{\gamma_r}\gamma_r(M) \in \mathrm{GL}_n(K_r)$. Moreover, we have $M \in \mathrm{GL}_n(K_\infty)$ by using Lemma 3.15 again.

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 $\gamma_r(U'_\sigma) = U'^{-1}_{\gamma_r} U'_\sigma \sigma(U'_{\gamma_r})$. Apply Lemma 3.15 with $V_1 = U'^{-1}_{\gamma_r}, V_2 = \sigma(U'_{\gamma_r})$, then $U'_\sigma \in \mathrm{GL}_n(K_r)$.

The last part follows from the proof of surjectivity. □

Theorem 3.17. *the map*

$$\eta : H^1_{\mathrm{cont}}(\Gamma, \mathrm{GL}_n(K_\infty)) \longrightarrow H^1_{\mathrm{cont}}(G, \mathrm{GL}_n(C))$$

induced by $G \to \Gamma$ *and* $\mathrm{GL}_n(K_\infty) \hookrightarrow \mathrm{GL}_n(C)$ *is a bijection.*

3.2.2 Study of C-representations.

by Proposition 2.6, if L/K is a Galois extension, we know that there is a one-one correspondence between the elements of $H^1_{\mathrm{cont}}(\mathrm{Gal}(L/K), \mathrm{GL}_n(L))$ and the isomorphism classes of L-representations of dimension n of $\mathrm{Gal}(L/K)$. Thus we can reformulate the results in the previous subsection in the language of C-representations.

Let W be a C-representation of G of dimension n. Let

$$\widehat{W}_\infty = W^H = \{\omega \mid \omega \in W,\ \sigma(\omega) = \omega \text{ for all } \sigma \in H\}.$$

It is a $\widehat{K}_\infty$-vector space since $C^H = \widehat{K}_\infty$. One has:

Theorem 3.18. *The natural map*

$$\widehat{W}_\infty \otimes_{\widehat{K}_\infty} C \longrightarrow W$$

is an isomorphism.

Proof. This is a reformulation of Proposition 3.11. □

Theorem 3.19. *There exists* $r \in \mathbb{N}$ *and a* K_r*-representation* W_r *of dimension* n*, such that*

$$W_r \otimes_{K_r} \widehat{K}_\infty \xrightarrow{\sim} \widehat{W}_\infty.$$

Proof. This is a reformulation of Proposition 3.16. Let $\{e_1, \cdots, e_n\}$ be a basis of $\widehat{W}_\infty$, the associated cocycle $\sigma \to U_\sigma$ in $H^1_{\mathrm{cont}}(\Gamma, \mathrm{GL}_n(\widehat{K}_\infty))$ is cohomologous to a cocycle with values in $\mathrm{GL}_n(K_r)$ for r sufficiently large. Thus there exists a basis $\{e'_1, \cdots, e'_n\}$ of $\widehat{W}_\infty$, such that $W_r = K_r e'_1 \oplus \cdots \oplus K_r e'_n$ is invariant by Γ_r. □

From now on, we identify $W_r \otimes_{K_r} \widehat{K}_\infty$ with $\widehat{W}_\infty$ and W_r with $W_r \otimes 1$ in $\widehat{W}_\infty$.

Definition 3.20. *We call a vector* $\omega \in \widehat{W}_\infty$ K-finite *if its translate by* Γ *generates a* K*-vector space of finite dimension. Let* W_∞ *be the set of all* K*-finite vectors.*

By definition, one sees easily that W_∞ is a K_∞-subspace of $\widehat{W}_\infty$ on which Γ acts. Moreover, W_r is a subset of W_∞.

Corollary 3.21. *One has* $W_r \otimes_{K_r} K_\infty = W_\infty$*, and hence* $W_\infty \otimes_{K_\infty} \widehat{K}_\infty \cong \widehat{W}_\infty$.

Proof. Certainly $W_r \otimes_{K_r} K_\infty \subset W_\infty$ is a sub K_∞-vector space of W_∞. On the other hand the dimension of $W_r \otimes_{K_r} K_\infty$ is n, and $\dim_{K_\infty} W_\infty \leq \dim_{\widehat{K}_\infty} \widehat{W}_\infty = n$. □

Remark 3.22. The set W_r depends on the choice of basis and is not canonical, but W_∞ is canonical.

3.2.3 Sen's operator ϕ.

Given a C-representation W of G, let W_r, W_∞ be given as above. By Proposition 3.16, there is a basis $\{e_1, \cdots, e_n\}$ of W_r (over K_r) which is also a basis of W_∞ (over K_∞) and of W (over C). We fix this basis. Under this basis, $\rho(\gamma_r) = U_{\gamma_r} \in \mathrm{GL}_n(K_r)$ satisfies $v(U_{\gamma_r} - 1) > c + d$.

We denote by $\log \circ \chi$ the composite map $G \to \Gamma \cong \mathbb{Z}_p$ and its restriction on Γ. This notation seems strange here, but one sees that the composite map $G \to \mathbb{Z}_p \xrightarrow{\exp} \mathbb{Z}_p^*$ is nothing but χ, which will be consistent to the axiomatic setup in § 3.4.

Definition 3.23. *The* operator ϕ of Sen *associated to the C-representation is an endomorphism of W_r whose matrix under the basis $\{e_1, \cdots, e_n\}$ is given by*

$$\Phi = \frac{\log U_{\gamma_r}}{\log \chi(\gamma_r)}. \tag{3.8}$$

One extends ϕ by linearity to an endomorphism of W_∞ and of W.

Theorem 3.24. *Sen's operator ϕ 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*

$$\sigma(\omega) = [\exp(\phi \log \chi(\sigma))]\omega, \quad \textit{for all } \sigma \in \Gamma_\omega. \tag{3.9}$$

Proof. For $\omega = \lambda_1 e_1 + \cdots \lambda_n e_n \in W_\infty$ such that $\lambda_i \in K_\infty$, then λ_i is fixed by some Γ_{r_i} for $r_i \in \mathbb{N}$. Let $\Gamma_\omega = \Gamma_r \cap \Gamma_{r_1} \cap \cdots \cap \Gamma_{r_n}$. Then for any $\sigma \in \Gamma_\omega \subset \Gamma_r$, $\sigma = \gamma_r^a$, $a \in \mathbb{Z}_p$, hence

$$U_\sigma = (U_{\gamma_r})^a \text{ and } \log \chi(\sigma) = a \log \chi(\gamma_r),$$

then

$$\exp(\Phi \log \chi(\sigma)) = \exp\left(a \frac{\log U_{\gamma_r}}{\log \chi(\gamma_r)} \log \chi(\gamma_r)\right) = \exp \log U_\sigma = U_\sigma.$$

Thus

$$\sigma(\omega) = [\exp(\phi \log \chi(\sigma))]\omega, \quad \text{for all } \sigma \in \Gamma_\omega.$$

To prove uniqueness, if (3.9) holds, let $\sigma \in \Gamma_r \cap \Gamma_{e_1} \cap \cdots \cap \Gamma_{e_n}$, write $\sigma = \gamma_r^a$. For $\omega \in W_r$, on one hand, σ acts on ω is given by U_σ under the basis $\{e_1, \cdots, e_n\}$; on the other hand, it is given by $[\exp(\phi \log \chi(\sigma))](\omega)$, so

$$U_{\gamma_r}^a = U_\sigma = \exp(\Phi \log \chi(\sigma)),$$

hence

$$\Phi = \frac{a \log U_{\gamma_r}}{\log \chi(\sigma)} = \frac{\log U_{\gamma_r}}{\log \chi(\gamma_r)}.$$

We have finished the proof. □

We have the following remarks of ϕ:

Remark 3.25. (1) By the proof of the theorem, one sees that

$$\Phi = \frac{\log U_\sigma}{\log \chi(\sigma)}, \quad \text{for any } \sigma \in \Gamma_r, \tag{3.10}$$

thus Sen's operator ϕ does not depend on the choice of γ_r.

(2) By (3.9), one has

$$\phi(\omega) = \frac{1}{\log \chi(\gamma)} \lim_{t \to 0} \frac{\gamma^t(\omega) - \omega}{t}, \quad \text{for } \omega \in W_\infty. \tag{3.11}$$

Thus Γ *commutes with* ϕ on W_∞ and G *commutes with* ϕ on W.

(3) For $\omega \in W_\infty$, $\phi(\omega) = 0$ if and only if the Γ-orbit of ω is *finite* (also equivalent to the stabilizer of ω is an open subgroup of Γ), as is easily seen from (2).

(4) Let W' be another C-representation and ϕ' be the corresponding Sen operator. Then the Sen operator for $W \oplus W'$ is $\phi \oplus \phi'$ and for $W \otimes_C W'$ is $\phi \otimes 1 + 1 \otimes \phi'$. If W' is a subrepresentation of W then the Sen operator ϕ' is the restriction of ϕ to W'. These could be seen from definition or by (2).

(5) The Sen operator of the representation $\mathrm{Hom}_C(W, W')$ is given by $f \mapsto f \circ \phi - \phi' \circ f$ for $f \in \mathrm{Hom}_C(W, W')$. To see this, use the Taylor expansion at $t = 0$:

$$\begin{aligned} \gamma^t f(\gamma^{-t}\omega) - f(w) &= (1 + t \log \gamma) f((1 - t \log \gamma)\omega) + O(t^2) f(\omega) - f(\omega) \\ &= t(\log \gamma) f(\omega) - t f((\log \gamma)\omega) + O(t^2) f(\omega), \end{aligned}$$

now use (2) to conclude.

Example 3.26. Suppose W is of dimension 1 and there is $e \neq 0$ in W such that $\sigma(e) = \chi(\sigma)^i$ for all $\sigma \in G$ (W is called *of Hodge-Tate type of dimension* 1 *and weight* i *in § 5.1*). Then $e \in W_\infty$, and $\gamma^t(e) = \chi(\gamma)^{it} e$, from which we have $(\gamma^t(e) - e)/t \to \log \chi(\gamma) i e$. Therefore the operator ϕ is just *multiplication* by i. This example also shows that K-finite element can has infinite γ-orbit.

Now we study more properties about ϕ.

Proposition 3.27. *There exists a basis of* W_∞ *with respect to which the matrix of* ϕ *has coefficients in* K.

Proof. For any $\sigma \in \Gamma$, we know $\sigma\phi = \phi\sigma$ in W_∞, thus $U_\sigma\sigma(\Phi) = \Phi U_\sigma$ and hence Φ and $\sigma(\Phi)$ are similar to each other. Thus all invariant factors of Φ are inside K. By linear algebra, Φ is similar to a matrix with coefficients in K and we have the proposition. □

Theorem 3.28. *The kernel of ϕ is the C-subspace of W generated by the elements invariant under G, i.e. $W^G \otimes_K C = \operatorname{Ker}\phi$.*

Proof. Obviously every elements invariant under G is killed by ϕ. Now Let X be the kernel of ϕ. It remains to show that X is generated by elements fixed by G. Since ϕ and G commute, X is stable under G, so we can talk about X_∞. Since $X_\infty \otimes_{K_\infty} C = X$ and ϕ is extended to X by linearity, it is enough to find a K_∞-basis $\{e_1, \cdots, e_n\}$ of X_∞ such that $e_i's$ are fixed by Γ. If $\omega \in X_\infty$, then Γ-orbit of ω is finite (by Remark 3.25 (2)). The action of Γ on X_∞ is therefore continuous for the *discrete* topology of X_∞. So by Hilbert's theorem 90, there exists a basis of $\{e_1, \cdots, e_n\}$ of X_∞ fixed by Γ. □

Theorem 3.29. *Let W^1 and W^2 be two C-representations, and ϕ^1 and ϕ^2 be the corresponding operators. For W^1 and W^2 to be isomorphic it is necessary and sufficient that ϕ^1 and ϕ^2 should be similar.*

Proof. Let $W = \operatorname{Hom}_C(W^1, W^2)$ with the usual action of G and ϕ be its Sen operator. W^1 and W^2 are isomorphic means that there is an C-vector space isomorphism $F : W^1 \to W^2$ such that

$$\sigma \circ F = F \circ \sigma$$

for all $\sigma \in G$, so $F \in W^G$. ϕ^1 and ϕ^2 are similar means there is an isomorphism f such that

$$\phi^2 \circ f = f \circ \phi^1,$$

that is $f \in \operatorname{Ker}\phi$. By Theorem 3.28, $W^G \otimes_K C = \operatorname{Ker}\phi$, we see that the necessity is obvious. For sufficiency, it amounts to that given an isomorphism $f \in W^G \otimes_K C$, we have to 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:

$$\det(c_1\bar{f}_1 + \cdots + c_m\bar{f}_m) \neq 0.$$

Here $\bar{f}_i$ is the matrix of f_i with respect to some fixed basis 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 $\lambda_i \in K$ with

$$\det(\lambda_1\bar{f}_1 + \cdots + \lambda_m\bar{f}_m) \neq 0.$$

The homomorphism $F = \lambda_1 f_1 + \cdots + \lambda_m f_m$ then has the required property. □

3.3 Sen's operator ϕ and the Lie algebra of $\rho(G)$.

3.3.1 Main Theorem.

Given a $\mathbb{Q}_p$-representation V, let $\rho : G_K \to \mathrm{Aut}_{\mathbb{Q}_p} V$ be the corresponding homomorphism. Let $W = V \otimes_{\mathbb{Q}_p} C$. Then some connection of the Lie group $\rho(G)$ and the operator ϕ 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 3.30. *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 $\phi \in S \otimes_{\mathbb{Q}_p} C$.*

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. Let $\{e'_1, \cdots, e'_d\}$ be a basis of W_∞ (where $W = V \otimes_{Q_p} C$) such that the K-subspace generated by the e'_i's is stable under an open subgroup $\mathit{\Gamma}_m$ of $\mathit{\Gamma}$ (by Proposition 3.27, 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 $\sigma \in \mathit{\Gamma}_m$. Let M be the matrix transforming the e_i's into the e'_i's, one then has $M^{-1} U_\sigma \sigma(M) = U'_\sigma$ for all $\sigma \in G$.

Let $\mathit{\Phi}$ be the matrix of ϕ with respect to the e'_i's. Put $A = M^{-1} \mathit{\Phi} M$, so that A is the matrix of ϕ with respect to the e_i's. For σ close to 1 in $\mathit{\Gamma}$ one knows that $U'_\sigma = \exp(\mathit{\Phi} \log \chi(\sigma))$, and our assumptions imply that $\mathit{\Phi}$ has coefficients in K.

By duality the Theorem is nothing but the assertion that a $\mathbb{Q}_p$-linear form f vanishes on $\mathfrak{g} \Longleftrightarrow$ the C-extension of f vanishes on ϕ. 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 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: $f(A) = 0 \Longleftrightarrow f(\log U_\sigma) = 0 \quad$ for all $U_\sigma \equiv 1(\bmod p^m)$.

Let

$$G_n = \{\sigma \in G \mid U_\sigma \ \equiv I \text{ and } \mathit{\Phi} \log \chi(\sigma) \equiv 0 (\bmod p^n)\}, \ n \geq 2. \qquad (3.12)$$

Let

$$G_\infty = \bigcap_{n=2}^{\infty} G_n = \{\sigma \in G \mid U_\sigma = I \text{ and } \chi(\sigma) = 1\}. \qquad (3.13)$$

Let $\overset{\vee}{G} = G_1/G_\infty$ 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 $\bar{K}$, by Proposition 3.8, 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 coefficients in $\widehat{L}$, hence A also. 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

$$U'_\sigma = \exp(\varPhi\ \log\chi(\sigma)) \qquad \text{for all } \sigma \in \overset{\vee}{G}_n. \tag{3.14}$$

The statement of our theorem is unchanged if we multiply M by a power of p. We may therefore suppose that M has integral coefficients. After multiplying f by a power of p we may assume that f is "integral", i.e., takes integral values on integral matrices.

For $n > n_0$, $U'_\sigma \equiv I \bmod p^n$, the equation

$$MU_\sigma = U'_\sigma\sigma(M) \tag{3.15}$$

shows then that $\sigma(M) \equiv M(\bmod p^n)$ for $\sigma \in \overset{\vee}{G}_n$. By Ax-Sen's lemma (Proposition 3.3) it follows that for each n there is a matrix M_n such that

$$M_n \equiv M(\bmod\ p^{n-1}),\ \text{and } \sigma(M_n) = M_n \text{ for } \sigma \in \overset{\vee}{G}_n. \tag{3.16}$$

Now suppose $\sigma \in \overset{\vee}{G}_n$, with $n \geqq 2$. We then have

$$U_\sigma \equiv I + \log U_\sigma,\ \text{and } U'_\sigma \equiv I + \log U'_\sigma = I + \log\chi(\sigma)\cdot\varPhi \quad (\bmod p^{2n}).$$

Substituting these congruences in (3.15) we get

$$M + M\log U_\sigma \equiv \sigma(M) + \log\chi(\sigma)\cdot\varPhi\sigma(M)(\bmod p^{2n}).$$

Since $\log U_\sigma$ and $\log\chi(\sigma)$ are divisible by p^n we have by (3.16):

$$M + M_n\log U_\sigma \equiv \sigma(M) + \log\chi(\sigma)\cdot\varPhi M_n(\bmod p^{2n-1}). \tag{3.17}$$

Let r_1 and r_2 be integers such that $p^{r_1-1}M^{-1}$ and $p^{r_2}\varPhi$ have integral coefficients. Let $n > r := 2r_1 + r_2 - 1$. Then M_n is invertible and $p^{r_1-1}M_n^{-1}$ is integral. Multiplying (3.17) on the left by $p^{r_1-1}M_n^{-1}$ and dividing by p^{r_1-1} we get

$$C_n + \log U_\sigma \equiv \sigma(C_n) + \log\chi(\sigma)\cdot M_n^{-1}\varPhi M_n \quad (\bmod p^{2n-r_1}) \tag{3.18}$$

where $C_n = M_n^{-1}M \equiv I(\bmod p^{n-r_1})$. Write $A_n = M_n^{-1}\varPhi M_n$, it is fixed by $\overset{\vee}{G}_n$ and

$$A_n - A = \frac{M - M_n}{M_n^{-1}M^{-1}}\varPhi M_n + M^{-1}\varPhi(M_n - M) \equiv 0 \bmod p^{n-r}.$$

We get

$$\log\chi(\sigma)A_n \equiv \log\chi(\sigma)A(\bmod p^{2n-r}).$$

Then we have

$$(\sigma-1)C_n \equiv \log U_\sigma - \log\chi(\sigma)\cdot A_n(\bmod p^{2n-r_1}).$$

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

$$(\sigma-1)f(C_n) \equiv f(\log U_\sigma) - \log\chi(\sigma)\cdot f(A)(\bmod p^{2n-r}). \tag{3.19}$$

We need the following important lemma, whose proof will be given in next section.

Lemma 3.31. *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

$$\lambda(\sigma) \equiv 0(\bmod p^{m-c-1}), \textit{for all } \sigma \in G(n).$$

Suppose $f(A) = 0$. By (3.19) and Lemma 3.31, we conclude that $f(\log U_\sigma) \equiv 0(\bmod p^{2n-r-c-1})$ for any $\sigma \in \overset{\vee}{G}_n$, where c is the constant of the lemma (which depends only on $\overset{\vee}{G}$). Since $\sigma^{p^{n-2}} \in \overset{\vee}{G}_n$ and $\log U_{\sigma^{p^{n-2}}} = p^{n-2}\log U_\sigma$ for any $\sigma \in \overset{\vee}{G}$. We conclude that $f(\log U_\sigma) \equiv 0(\bmod\ p^{n-r-c+1})$ for all $\sigma \in \overset{\vee}{G}$, hence $f(\log U_\sigma) = 0$ as desired, since n was arbitrary.

Suppose $f(\log U_\sigma) = 0$ for all $\sigma \in \overset{\vee}{G}$: We wish to show $f(A) = 0$. Suppose not, then $f(A_n) \neq 0$ and has constant ordinal for large n, dividing (3.19) by $f(A)$ and using Lemma 3.31, we obtain

$$\log\chi(\sigma) \equiv 0(\bmod p^{2n-r-c-1-s})$$

for large n and all $\sigma \in \overset{\vee}{G}_n$, where s is a constant with $p^s f(A)^{-1}$ integral. Analogous argument as above shows that $\log\chi(\sigma) = 0$ for all $\sigma \in \overset{\vee}{G}$. 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. □

Corollary 3.32. *$\phi = 0$ if and only if $\rho(G)$ is finite.*

Proof. By the theorem $\phi = 0 \Leftrightarrow \mathfrak{g} = 0$. So we only need to show $\mathfrak{g} = 0 \Leftrightarrow \rho(G)$ is finite.

The sufficiency is obvious. For the necessity, we have $\mathfrak{g} = 0$ implies that $\rho(G)$ has a trivial open subgroup which in turn implies that $\rho(G)$ is finite. □

Remark 3.33. In general if k is not algebraically closed, one just needs to replace G by the inertia subgroup and K by the completion of K^{ur}, then the above theorem and corollary still hold.

3.3.2 Application of Sen's filtration Theorem.

We assume k is algebraically closed.

Lemma 3.34. *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 A.80, 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

$$\begin{aligned}
v_p(\mathfrak{D}_{L/K}) =& \frac{1}{e_A}\int_{-1}^{\infty}(1 - |G^v|^{-1})dv \\
\geq& \frac{1}{e_A}\Big(\int_{-1}^{v_r}(1 - |G^v|^{-1})dv + \sum_{j=1}^{r}(1 - \frac{1}{p^j})e_A\Big) \\
\geq& \frac{1}{e_A}\Big((1 - p^{-n})\frac{1}{p-1}e_A + re_A - e_A \cdot \sum_{j=1}^{r}\frac{1}{p^j}\Big) \\
\geq& r.
\end{aligned}$$

Hence p^r divides the different $\mathfrak{D}_{L/K}$. □

Proposition 3.35. *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 $p^{-c}[K : K_n]$.*

Proof. Put $u_n = u_{G/G(n)}, v_n = v_{G/G(n)}$, and $e_n = e_{G(n)} = (G : G(n))e$. From Proposition A.84, 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 A.85), 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 A.83, 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 3.34. The same is trivially true if $s < b+3$. Thus one could take $c = b+3$ for large n, say $n \geq n_1$, and $c = n_1 + b + 3$ would then work for all n. □

Corollary 3.36. $\mathrm{Tr}_{E/K_n}(\mathcal{O}_E) \subset p^{-c}[K:K_n]\mathcal{O}_{K_n}$.

Proof. Let $[K:K_n] = p^s$. The proposition states that $\mathfrak{D}_{E/K_n} \subset p^{s-c}\mathcal{O}_E$, hence $\mathcal{O}_E \subset p^{s-c}\mathfrak{D}_{E/K_n}^{-1}$. On taking the trace the corollary follows. □

We now come to the proof of Lemma 3.31:

Proof (Proof of Lemma 3.31). 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 3.36, 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. □

3.4 Sen's method.

The method of Sen to classify C-representations in § 3.2 actually can be generalized to an axiomatic set-up, as proposed by Colmez.

3.4.1 Tate-Sen's conditions (TS1), (TS2) and (TS3).

Let G_0 be a profinite group and $\chi: \ G_0 \to \mathbb{Z}_p^*$ be a continuous group homomorphism with open image. Set $v(g) = v_p(\log \chi(g))$ and $H_0 = \operatorname{Ker} \chi$.

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) $v(x+y) \geq \inf(v(x), v(y))$;
(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 3.37. *The* Tate-Sen's conditions *for the quadruple* $(G_0, \chi, \tilde{\Lambda}, v)$ *are the following three conditions* ***TS1-TS3***.

(TS1). For all $C_1 > 0$*, for all* $H_1 \subset H_2 \subset H_0$ *open subgroups, there exists an* $\alpha \in \tilde{\Lambda}^{H_1}$ *with*

$$v(\alpha) > -C_1 \ \text{and} \sum_{\tau \in H_2/H_1} \tau(\alpha) = 1. \tag{3.20}$$

(In Faltings' terminology, $\tilde{\Lambda}/\tilde{\Lambda}^{H_0}$ *is called* almost étale.*)*

(TS2). Tate's normalized trace maps*: there exists* $C_2 > 0$ *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 we can find* $\Lambda_{H_2,n} = (\Lambda_{H_1,n})^{H_2}$*, and* $R_{H_1,n} = R_{H_2,n}$ *on* $\tilde{\Lambda}^{H_2}$*;*

(b) for all $g \in G_0$*, we can find* $\Lambda_{gH^{-1}g,n}$ *and* $R_{gH^{-1}g,n}$ *such that*

$$g(\Lambda_{H,n}) = \Lambda_{gHg^{-1},n} \quad g \circ R_{H,n} = R_{gHg^{-1},n} \circ g;$$

(c) $R_{H,n}$ *is* $\Lambda_{H,n}$*-linear and is equal to* Id *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) $\lim\limits_{n \to +\infty} R_{H,n}(x) = x$.

(TS3). There exists 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* $v(\gamma) = v_p(\log \chi(\gamma)) \leq n$*, then* $\gamma - 1$ *is invertible on* $X_{H,n} = (R_{H,n} - 1)\tilde{\Lambda}$ *and*

$$v((\gamma - 1)^{-1}x) \geq v(x) - C_3 \tag{3.21}$$

for $x \in X_{H,n}$.

Remark 3.38. $R_{H,n} \circ R_{H,n} = R_{H,n}$, so $\tilde{\Lambda}^H = \Lambda_{H,n} \oplus X_{H,n}$.

Example 3.39. In § 3.2, we are in the case $\tilde{\Lambda} = C$, $G_0 = G_K$, $v = v_p$, χ being the character $G_0 \to \Gamma \xrightarrow{\exp} \mathbb{Z}_p^*$.

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 § A.4.2.

3.4.2 Almost étale descent

Lemma 3.40. *If $\tilde{\Lambda}$ satisfies (TS1), $a > 0$, and $\sigma \mapsto U_\sigma$ is a 1-cocycle on H, an open subgroup of H_0, 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 3.9, approximating 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, so for any $\sigma' \in S'$, there exists $\tau \in H_1$ and $\sigma \in S$ such that $\sigma' = \sigma\tau$, so we get

$$M_S - M_{S'} = \sum_{\sigma \in S} \sigma(\alpha)(U_\sigma - U_{\sigma\tau}) = \sum_{\sigma \in S} \sigma(\alpha) U_\sigma (1 - \sigma(U_\tau)),$$

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 3.41. *Under the same hypotheses as the above lemma, there exists $M \in \mathrm{GL}_d(\tilde{\Lambda})$ such that*

$$v(M - 1) \geq a/2, \ \ M^{-1} U_\sigma \sigma(M) = 1, \forall \ \sigma \in \ H.$$

Proof. Repeat the lemma ($a \mapsto a + 1 \mapsto a + 2 \mapsto \cdots$), and take the limits. □

3.4.3 Undo the completion

Lemma 3.42. *Assume given $\delta > 0$, $b \geq 2C_2 + 2C_3 + \delta$, and $H \subset H_0$ is open. Suppose $n \geq n(H)$, $\gamma \in G/H$ with $n(\gamma) \leq n$, $U = 1 + U_1 + U_2$ with*

$$\begin{aligned} &U_1 \in \mathrm{M}_d(\Lambda_{H,n}), v(U_1) \geq b - C_2 - C_3 \\ &U_2 \in \mathrm{M}_d(\widetilde{\Lambda}^H), v(U_2) \geq b' \geq b. \end{aligned}$$

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

$$\begin{aligned} &V_1 \in \mathrm{M}_d(\Lambda_{H,n}), \ \ v(V_1) \geq b - C_2 - C_3), \\ &V_2 \in \mathrm{M}_d(\widetilde{\Lambda}^H), \ \ v(V_2) \geq b + \delta. \end{aligned}$$

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 3.43. *Keep the same hypotheses as in Lemma 3.42. 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 3.44. *Suppose* $H \subset H_0$ *is an open subgroup,* $i \geq n(H)$, $\gamma \in G/H$, $n(\gamma) \geq i$ *and* $B \in \mathrm{GL}_d(\widetilde{\Lambda}^H)$. *If there exist* $V_1, V_2 \in \mathrm{GL}_d(\Lambda_{H,i})$ *such that*

$$v(V_1 - 1) > C_3, \quad v(V_2 - 1) > C_3, \quad \gamma(B) = V_1 B V_2,$$

then $B \in \mathrm{GL}_d(\Lambda_{H,i})$.

Proof. Take $C = B - R_{H,i}(B)$. We have to prove $C = 0$. Note that C has coefficients 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. $C = 0$. □

3.4.4 Applications to p-adic representations

Proposition 3.45. *Assume* $\tilde{\Lambda}$ *satisfying (TS1), (TS2) and (TS3). Let* $\sigma \mapsto U_\sigma$ *be 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* $v(U_\sigma - 1) > 2C_2 + 2C_3$ *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

$$\inf_{\sigma \in G} v(U_\sigma - 1) > 2(C_2 + C_3).$$

By Lemma 3.40, 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, it 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:

$$1 \to H_0/H \to G_0/H \to G/H \to 1,$$

$G/H \simeq \mathbb{Z}_p \times$ (finite), and H_0/H is finite. So we are able to choose such an $n(G)$.

Then we have $v(U'_\gamma) > 2(C_2 + C_3)$, and by Corollary 3.43, 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

$$\sigma \mapsto V_\sigma = M^{-1}U_\sigma\sigma(M)$$

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 want 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 $\gamma(V_\tau) = V_\gamma^{-1}V_\tau\tau(V_\gamma)$. Apply Lemma 3.44 with $V_1 = V_\gamma^{-1}, V_2 = \tau(V_\gamma)$, then we obtain what we want. □

Proposition 3.46. *Let T be a free $\mathbb{Z}_p$-representation of G_0, $k \in \mathbb{N}$, $v(p^k) > 2C_2 + 2C_3$, 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;

(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. Translation of Proposition 3.45, by the correspondence

$$\widetilde{\Lambda}\text{-representations of } G_0 \longleftrightarrow H^1(G_0, \mathrm{GL}_d(\widetilde{\Lambda})).$$

For the uniqueness, one uses Lemma 3.44. □

Remark 3.47. 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

$$\Lambda_{H,n} \bigotimes_{\Lambda_{H_0,n}} D_{H_0,n}(T) \xrightarrow{\sim} D_{H,n}(T). \tag{3.22}$$

3.5 C-admissible representations

3.5.1 Notations for the rest of the book.

From now on to the rest of the book, if without further notice, we fix the following notations.

Let K be a p-adic field. Let $\mathcal{O}_K$ be its ring of integers, and $\mathfrak{m}_K$ be the maximal ideal of $\mathcal{O}_K$ and k be its residue field, which is perfect of characteristic $p > 0$. $W = W(k)$ is the ring of Witt vectors and $K_0 = \operatorname{Frac} W = W[1/p]$ is its quotient field. We know that

$$\operatorname{rank}_W \mathcal{O}_K = [K : K_0] = e_K = v_K(p)$$

and if π is a generator of $\mathfrak{m}_K$, then $1, \pi, \cdots, \pi^{e_K-1}$ is a basis of $\mathcal{O}_K$ over W as well as K over K_0. Let σ be the Frobenius map F as in § A.2.1 on K_0, then

$$\sigma(a) = a^p \pmod{pW} \quad \text{if } a \in W.$$

Let $\overline{K}$ be an algebraic closure over K.

For any subfield L of $\overline{K}$ containing K_0, set $G_L = \operatorname{Gal}(\overline{K}/L)$. Let $C = \widehat{\overline{K}}$. By continuity, the Galois group G_{K_0}, hence also G_K, acts on C and

$$C^{G_K} = K.$$

From now on, v will be always the valuation of C or any subfield such that $v(p) = 1$, i.e. $v = v_p$. Then $v(\pi) = \frac{1}{e_K}$.

For any subfield L of C, we denote

- $\mathcal{O}_L = \{x \in L | v(x) \geq 0\}$;
- $\mathfrak{m}_L = \{x \in L | v(x) > 0\}$;
- $k_L = \mathcal{O}_L/\mathfrak{m}_L$.

Denote by $\widehat{L}$ the closure of L in C, that is $\mathcal{O}_{\widehat{L}} = \varprojlim_{n\geq 1} \mathcal{O}_L/p^n\mathcal{O}_L$. We have $\widehat{L} = \mathcal{O}_{\widehat{L}}[\frac{1}{p}]$ and $k_{\widehat{L}} = k_L$. We know that $k_{\overline{K}} = k_C = \bar{k}$, where $\bar{k}$ is an algebraic closure of k. Let $G_k = \operatorname{Gal}(\bar{k}/k)$, I_K be the inertia subgroup of G_K, then

$$1 \to I_K \to G_K \to G_k \to 1$$

is exact.

3.5.2 $\overline{K}$-admissible p-adic representations

Note that $\overline{K}$ is a topological field on which G_K acts continuously.

Definition 3.48. *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 called *trivial* if α_X is an isomorphism.

Proposition 3.49. *X is trivial if and only if the action of G_K is discrete.*

Proof. The sufficiency is 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 $x = \sum\limits_{i=1}^{d} \lambda_i e_i \in X$, we want to prove $G_x = \{g \in G |\ g(x) = x\}$ is an open subgroup of G. Because of the choice of e_i's, $g(x) = \sum\limits_{i=1}^{d} g(\lambda_i) e_i$, so

$$G_x = \bigcap_{i=1}^{d} \{g \in G |\ g(\lambda_i) = \lambda_i\} := \bigcap_{i=1}^{d} G_{\lambda_i},$$

each $\lambda_i \in \overline{K}$ is algebraic over K, so G_{λ_i} is open, then the result follows. □

Definition 3.50. *If V is a p-adic representation 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 $\mathbb{Q}_p$, and write $v_i = 1 \otimes v_i$ also when they are viewed as a basis of $\overline{K} \otimes_{\mathbb{Q}_p} V$ over $\overline{K}$. Then by Proposition 3.49, V is $\overline{K}$-admissible is equivalent to that $G_{v_i} = \{g \in G | g(v_i) = v_i\}$ 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 equals to $\bigcap\limits_{i=1}^{d} G_{v_i}$, is an open subgroup.

We thus get

Proposition 3.51. *A p-adic representation of G_K is $\overline{K}$-admissible if and only if the action of G_K is discrete.*

We can do a little further. Let K^{ur} be 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 $\mathrm{Gal}(\overline{P}/P) = I_K$.

Set $P_0 = \widehat{K_0^{\mathrm{ur}}}$, then $P = KP_0$ and $[P : P_0] = e_K$.

Question 3.52. (1) What does it mean for a $\overline{P}$-representation of G_K to be trivial?

(2) What are the p-adic representations of G_K which are $\overline{P}$-admissible?

Proposition 3.53. (1) *The answer to* Q1, *i.e., a $\overline{P}$-representation of G_K is trivial if and only if the action of I_K is discrete.*

(2) *A p-adic representation of G_K is $\overline{P}$-admissible if and only if the action of I_K is discrete.*

Remark 3.54. By the above two propositions, then if V is a p-adic representation of G_K, and $\rho : G_K \to \mathrm{Aut}_{\mathbb{Q}_p}(V)$, then

$$V \text{ is } \overline{K}\text{-admissible} \Longleftrightarrow \operatorname{Ker}\rho \text{ is open in } G_K,$$

$$V \text{ is } \overline{P}\text{-admissible} \Longleftrightarrow \operatorname{Ker}\rho \cap I_K \text{ is open in } I_K.$$

Proof. Obviously (2) is a consequence of (1), so we only 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 $X^{G_K} = Y^{G_k}$, then $\overline{P} \otimes_K X^{G_k} \to X$ is also an isomorphism. Thus it is enough to prove that any P-representation Y of G_k is trivial, that is, 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 2.30: 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 $P = KP_0$ 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

$$P \otimes_K Y^{G_k} = P_0 \otimes_{K_0} Y^{G_k} \xrightarrow{\sim} Y,$$

so we get the result. □

3.5.3 C-admissible representations.

We can now use Sen's results to study C-admissible representations.

Proposition 3.55. *A p-adic representation V of G_K is C-admissible if and only if the action of I_K on V is discrete.*

Proof. Clearly, the condition is sufficient because as $\overline{P} \subset C$, any representation which is $\overline{P}$-admissible is C-admissible.

For V a p-adic representation of G_K, suppose $\{v_1, \cdots, v_d\}$ is a basis of V over $\mathbb{Q}_p$, V is C-admissible if and only if there exist a C-basis $e_1, \cdots, e_d \in W = C \otimes_{\mathbb{Q}_p} V$, $e_j = \sum_{i=1}^{d} c_{ij} \otimes v_i$, satisfying that $g(e_j) = e_j$ for all $g \in G_K$. Thus W is trivial and Sen's operator ϕ_W of W is 0, by Sen (Corollary 3.32), then $\rho(I_K)$ is finite. □

As a special case of this proposition, we consider any continuous homomorphism $\eta : G_K \to \mathbb{Z}_p^*$, and let $\mathbb{Q}_p(\eta)$ be the $\mathbb{Q}_p$-representation obtained by giving $\mathbb{Q}_p$ the action of G_k via η. Set $C(\eta) = C \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(\eta)$, Tate proved that

Corollary 3.56.

$$C(\eta)^{G_K} \begin{cases} = 0 & \text{\textit{if} } \eta(I_K) \text{ \textit{is not finite},} \\ \cong K & \text{\textit{if} } \eta(I_K) \text{ \textit{is finite.}} \end{cases} \tag{3.23}$$

Proof. One notes that the C-representation $C(\eta)$ is admissible if and only if $C(\eta)^{G_K}$, as a K-vector space of dimension ≤ 1, must be 1-dimensional and hence is isomorphic to K. □

4

The ring $\boldsymbol{R}$ and (φ, Γ)-module

4.1 The ring $\boldsymbol{R}$

4.1.1 The ring $\boldsymbol{R(A)}$.

Let A be a (commutative) ring, and let p be a prime number. We know that A is of characteristic p if the kernel of $\mathbb{Z} \to A$ is generated by p; such a ring can be viewed as an $\mathbb{F}_p$-algebra. If A is of characteristic p, the *absolute Frobenius map* is the homomorphism

$$\varphi : A \to A, \qquad a \mapsto a^p$$

which sometimes is also denoted as σ. If φ is an isomorphism, the ring A is *perfect*. If φ is injective, then A is reduced, that is, there exists no nontrivial nilpotent element, and vice versa.

Definition 4.1. *Assume A is of characteristic p, we define*

$$R(A) := \varprojlim_{n \in \mathbb{N}} A_n, \tag{4.1}$$

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 $x_n \in A$, $x_{n+1}^p = x_n$.

Proposition 4.2. *This ring $R(A)$ is perfect.*

Proof. For any $x = (x_n)_{n \in \mathbb{N}}$, $x = (x_{n+1})_{n \in \mathbb{N}}^p$, and $x^p = 0$ implies $x_n^p = x_{n+1} = 0$ for any $n \geq 1$, then $x = 0$. □

For any n, consider the projection map

$$\begin{aligned} \theta_n : \quad R(A) &\longrightarrow A \\ (x_n)_{n \in \mathbb{N}} &\longmapsto x_n. \end{aligned}$$

If A is perfect, each θ_n is an isomorphism; A is reduced, then θ_0 (hence θ_n) is injective and the image

$$\theta_m(R(A)) = \bigcap_{n\geq m} \varphi^n(A).$$

If A is a topological ring, then we can give to $R(A)$ the topology of the inverse limit. In what follows, we are going to apply this to the case that the topology of A is the discrete topology.

Now let A be a ring, separated and complete for the p-adic topology, that is, $A \to \varprojlim_{n\in\mathbb{N}} A/p^nA$ is an isomorphism. We consider the ring $R(A/pA)$.

Proposition 4.3. *There exists a bijection between $R(A/pA)$ and the set*

$$S = \{(x^{(n)})_{n\in\mathbb{N}} \mid x^{(n)} \in A,\ (x^{(n+1)})^p = x^{(n)}\}.$$

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 $\hat{x}_n$, we have

$$\hat{x}_{n+1}^p \equiv \hat{x}_n \bmod pA.$$

Note that for $m \in \mathbb{N}$, $m \geq 1$, $\alpha \equiv \beta \bmod p^mA$, then

$$\alpha^p \equiv \beta^p \bmod p^{m+1}A,$$

thus for $n, m \in \mathbb{N}$, we have

$$\hat{x}_{n+m+1}^{p^{m+1}} \equiv \hat{x}_{n+m}^{p^m} \bmod p^{m+1}A.$$

Hence for every n, $\lim_{n\to\infty} \hat{x}_{n+m}^{p^m}$ exists in A, and the limit is independent of the choice of the liftings. We denote

$$x^{(n)} = \lim_{n\to\infty} \hat{x}_{n+m}^{p^m}.$$

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

$$R(A/pA) \longrightarrow S.$$

On the other hand the reduction modulo p from $A \to A/pA$ naturally induces the map $S \to R(A/pA)$, $(x^{(n)})_{n\in\mathbb{N}} \mapsto (x^{(n)} \bmod pA)_{n\in\mathbb{N}}$. One can easily check that the two map are inverse to each other. □

Remark 4.4. In the sequel, we shall use the above bijection to identify $R(A/pA)$ to the set S. Then any element $x \in R(A/pA)$ can be written in two ways

$$x = (x_n)_{n\in\mathbb{N}} = (x^{(n)})_{n\in\mathbb{N}},\ x_n \in A/pA,\ x^{(n)} \in A. \tag{4.2}$$

If $x = (x^{(n)})$, $y = (y^{(n)}) \in R(A/pA)$, then

$$(xy)^{(n)} = (x^{(n)}y^{(n)}), \quad (x+y)^{(n)} = \lim_{m\to\infty} (x^{(n+m)} + y^{(n+m)})^{p^m}. \tag{4.3}$$

4.1.2 Basic properties of the ring R.

We have introduced the ring $R(A)$. The most important case for us is that $A = \mathcal{O}_L$ with L being a subfield of $\overline{K}$ containing K_0. Identify $\mathcal{O}_L/p\mathcal{O}_L = \mathcal{O}_{\hat{L}}/p\mathcal{O}_{\hat{L}}$, then the ring

$$R(\mathcal{O}_L/p\mathcal{O}_L) = R(\mathcal{O}_{\widehat{L}}/p\mathcal{O}_{\widehat{L}}) = \{x = (x^{(n)})_{n\in\mathbb{N}} \mid x^{(n)} \in \mathcal{O}_{\widehat{L}}, (x^{(n+1)})^p = x^{(n)}\}.$$

In particular, we set

Definition 4.5. $R := R(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}) = R(\mathcal{O}_C/p\mathcal{O}_C)$.

Recall $v = v_p$ is the valuation on C normalized by $v(p) = 1$. We define $v_R(x) =: v(x) = v(x^{(0)})$ on R.

Proposition 4.6. *The ring R is a complete valuation ring with the valuation given by v. It is perfect of characteristic p. Its maximal ideal $\mathfrak{m}_R = \{x \in R \mid v(x) > 0\}$ and residue field is $\bar{k}$.*

The fraction field $\mathrm{Fr}\, R$ *of R is a complete nonarchimedean perfect field of characteristic p.*

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

$$v(xy) = v(x)v(y).$$

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

$$\{x \in R \mid v(x) \geq p^n\} = \mathrm{Ker}\,(\theta_n : R \to \mathcal{O}_C/p\mathcal{O}_C).$$

So the topology defined by the valuation is the same as the topology of inverse limit, and therefore is complete. Because there is a valuation over R, R is a domain and thus we may consider $\mathrm{Fr}\, R$, the fraction field of R. Then

$$\mathrm{Fr}\, R = \{x = (x^{(n)})_{n\in\mathbb{N}} \mid x^{(n)} \in C, (x^{(n+1)})^p = x^{(n)}\}.$$

The valuation v extends to the fraction field $\mathrm{Fr}\, R$ by the same formula $v(x) = v(x^{(0)})$. $\mathrm{Fr}\, R$ is a complete nonarchimedean perfect field of characteristic $p > 0$ with the ring of integers

$$R = \{x \in \mathrm{Fr}\, R \mid v(x) \geq 0\}$$

whose maximal ideal is $\mathfrak{m}_R = \{x \in \mathrm{Fr}\, R \mid v(x) > 0\}$.

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 $\bar{k}$. □

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 4.7. *The section s is given by*

$$a \in \bar{k} \longrightarrow ([a^{p^{-n}}])_{n\in\mathbb{N}}$$

where $[a^{p^{-n}}] = (a^{p^{-n}}, 0, 0, \cdots) \in \mathcal{O}_{K_0^{\mathrm{ur}}}$ 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 4.8. $\mathrm{Fr}\, R$ *is algebraically closed.*

Proof. As $\mathrm{Fr}\, R$ is perfect, it suffices to prove that it is separably closed, which means that if a monic polynomial $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0 \in R[X]$ is separable, then $P(X)$ has a root in R.

Since P is separable, there exist U_0, $V_0 \in \mathrm{Fr}\, R[X]$ such that

$$U_0P + V_0P' = 1.$$

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 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

$$v(x_{n+1} - x_n) \geq n - m, \quad \text{and} \;\; P(x_n) \in \pi^n R,$$

then $\lim\limits_{n\to\infty} x_n$ exists, and it will be a root of $P(X)$.

We construct (x_n) inductively. We use the claim to construct x_{n_0}. Assume x_n is 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

$$P(x_{n+1}) = P(x_n) + yP'(x_n) + \sum_{j \geq 2} y^j P^{[j]}(x_n). \tag{4.4}$$

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 a y such that

$$v(y) \geq n - m, \quad \text{and} \;\; v(P(x_n) + yP'(x_n)) \geq n+1.$$

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. □

4.1.3 The multiplicative group Fr R^*.

Lemma 4.9. *There is a canonical isomorphism of $\mathbb{Z}$-modules*

$$\operatorname{Fr} R^* \cong \operatorname{Hom}(\mathbb{Z}[1/p], C^*).$$

Proof. Given a homomorphism $f : \mathbb{Z}[1/p] \to C^*$, write $x^{(n)} = f(p^{-n})$, then $(x^{(n+1)})^p = x^{(n)}$, so $x = (x^{(n)})_{n \in \mathbb{N}} \in R$, thus we get a canonical homomorphism

$$\operatorname{Hom}(\mathbb{Z}[1/p], C^*) \longrightarrow \operatorname{Fr} R^*.$$

One can easily check that this is an isomorphism. □

From now on, let us identify $\operatorname{Fr} R^*$ and $\operatorname{Hom}(\mathbb{Z}[1/p], C^*)$ by the canonical isomorphism.

Denote by $U_R \subset \operatorname{Fr} R^*$ the group of the units of R. Since for $x \in R$, $x \in U_R \Leftrightarrow x^{(0)} \in \mathcal{O}_C^*$, we get

$$U_R = \operatorname{Hom}(\mathbb{Z}[1/p], \mathcal{O}_C^*).$$

Let $W(\bar{k})$ be the ring of Witt vectors of $\bar{k}$. Since $W(\bar{k}) \subset \mathcal{O}_C$, we get an inclusion $\bar{k}^* \hookrightarrow \mathcal{O}^*$. Let $U_C^+ = 1 + \mathfrak{m}_C$, then $\mathcal{O}_C^* = \bar{k}^* \times U_C^+$, and therefore

$$\begin{aligned} U_R &= \operatorname{Hom}(\mathbb{Z}[1/p], \mathcal{O}_C^*) \\ &= \operatorname{Hom}(\mathbb{Z}[1/p], \bar{k}^*) \times \operatorname{Hom}(\mathbb{Z}[1/p], U_C^+). \end{aligned}$$

In $\bar{k}$, any element has exactly one p-th root, so $\operatorname{Hom}(\mathbb{Z}[1/p], \bar{k}^*) = \bar{k}^*$. Similarly we have

$$U_R^+ = \{x \in R \mid x^{(n)} \in U_C^+\} = \operatorname{Hom}(\mathbb{Z}[1/p], U_C^+),$$

therefore we get the factorization

$$U_R = \bar{k}^* \times U_R^+.$$

Set $U_R^1 = \{x \in R \mid v(x-1) \geq 1\}$, then $(U_R^1)^{p^n} = \{x \in U_R^1 \mid v(x-1) \geq p^n\}$, and

$$U_R^1 \xrightarrow{\sim} \varprojlim_{n \in \mathbb{N}} U_R^1/(U_R^1)^{p^n}$$

is an isomorphism and a homeomorphism of topological groups. So we may consider U_R^1 as a $\mathbb{Z}_p$-module which is 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.

To summarize, we have

Proposition 4.10. *The sequence*

$$0 \to U_R \to \operatorname{Fr} R^* \xrightarrow{v} \mathbb{Q} \to 0 \tag{4.5}$$

is exact and

(1) $\operatorname{Fr} R^* = \operatorname{Hom}(\mathbb{Z}[1/p], C^*)$*;*

(2) $U_R = \operatorname{Hom}(\mathbb{Z}[1/p], \mathcal{O}_C^*) = \bar{k}^* \times U_R^+$*;*

(3) $U_R^+ = \operatorname{Hom}(\mathbb{Z}[1/p], U_C^+) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} U_R^1$*;*

(4) $U_R^1 = \{x \in R \mid v(x-1) \geq 1\} \xrightarrow{\sim} \varprojlim_{n \in \mathbb{N}} U_R^1/(U_R^1)^{p^n}$.

4.2 The action of Galois group on R

4.2.1 The action of Galois group.

As in previous chapters, we let $W = W(k)$, $K_0 = \operatorname{Frac} W$. The group $G_{K_0} = \operatorname{Gal}(\overline{K}/K_0)$ acts on R and $\operatorname{Fr} R$ in the natural way.

Proposition 4.11. *Let L be an extension of K_0 contained in $\overline{K}$ and let $H = \operatorname{Gal}(\overline{K}/L)$. Then*

$$R^H = R(\mathcal{O}_L/p\mathcal{O}_L), \quad (\operatorname{Fr} R)^H = \operatorname{Frac}(R(\mathcal{O}_L/p\mathcal{O}_L)).$$

The residue field of R^H is $k_L = \bar{k}^H$, the residue field of L.

Proof. Assume $x \in R^H$(resp. $\operatorname{Fr} R^H$), then

$$x = (x^{(n)})_{n\in\mathbb{N}},\ x^{(n)} \in \mathcal{O}_C(\text{resp. } C).$$

For $h \in H$, $h(x) = (h(x^{(n)}))_{n\in\mathbb{N}}$. Hence

$$x \in R^H(\text{resp. } \operatorname{Fr} R^H) \Longleftrightarrow x^{(n)} \in (\mathcal{O}_C)^H(\text{resp. } C^H),\ \forall\, n \in N,$$

then the first assertion follows from the fact

$$C^H = \hat{L}, \quad (\mathcal{O}_C)^H = \mathcal{O}_{C^H} = \mathcal{O}_{\hat{L}} = \varinjlim_{n} \mathcal{O}_L/p^n\mathcal{O}_L.$$

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 4.12. *If $v(L^*)$ 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 last proposition, $k_L \subset R^H = R(\mathcal{O}_L/p\mathcal{O}_L)$, 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 $v(\hat{L}^*) = v(L^*)$ is discrete, so $v(x) = v(x^{(0)}) = +\infty$, which means that $x = 0$. □

4.2.2 $R(K_0^{\mathrm{cyc}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}})$, ε and π.

Let K_0^{cyc} be the subfield of $\overline{K}$ obtained by adjoining to K_0 the p^n-th roots of 1 for all n. Take $(\varepsilon^{(n)})_{n\geq 0}$ such that

$$\varepsilon^{(0)} = 1, \varepsilon^{(1)} \neq 1, \text{ and } (\varepsilon^{(n+1)})^p = \varepsilon^{(n)} \text{ for } n \geq 1.$$

Then

$$K_0^{\mathrm{cyc}} = \bigcup_{n\in\mathbb{N}} K_0(\varepsilon^{(n)}).$$

The question is: what is $R(\mathcal{O}_{K_0^{\mathrm{cyc}}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}})$?

First its residue field is k.

Lemma 4.13. *The element $\varepsilon = (\varepsilon^{(n)})_{n\in\mathbb{N}}$ is a unit of $R(\mathcal{O}_{K_0^{\mathrm{cyc}}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}})$.*

Proof. Write ε_n the image of $\varepsilon^{(n)}$ in $\mathcal{O}_{K_0^{\mathrm{cyc}}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}}$. Put $\pi = \varepsilon - 1$, then $\pi^{(0)} = \lim\limits_{m\to+\infty}(\varepsilon^{(m)}-1)^{p^m}$, 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 $R(\mathcal{O}_{K_0^{\mathrm{cyc}}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}})$. □

Note 4.14. From now on, we set ε and $\pi = \varepsilon - 1$ as in the above Lemma.

Set $H = \mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}})$, then $R^H = R(\mathcal{O}_{K_0^{\mathrm{cyc}}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}})$ by Proposition 4.11. Since $\pi \in R^H$ and $v(\pi) = v_p(\pi^{(0)}) = \frac{p}{p-1} > 1$, $k \subset R^H$, and R^H is complete, then

$$k[[\pi]] \subset R^H \text{ and } k((\pi)) \subset (\mathrm{Fr}\, R)^H.$$

Since for every $x = (x^{(n)})_{n\in\mathbb{N}} \in R^H$, $x = y^p$ with $y = (x^{(n+1)})_{n\in\mathbb{N}}$, R^H and $(\mathrm{Fr}\, R)^H$ are both perfect and complete, we get

$$\widehat{k[[\pi]]^{\mathrm{rad}}} \subset R^H, \quad \widehat{k((\pi))^{\mathrm{rad}}} \subset (\mathrm{Fr}\, R)^H.$$

Theorem 4.15. *We have*

$$\widehat{k[[\pi]]}^{\mathrm{rad}} = R^H, \quad \widehat{k((\pi))}^{\mathrm{rad}} = (\mathrm{Fr}\, R)^H.$$

Moreover, for the projection map

$$\theta_m : R \to O_{\overline{K}}/pO_{\overline{K}}, \ \theta_m((x_n)_{n\in N}) = x_m, \quad (m \in \mathbb{N})$$

then

$$\theta_m(R^H) = \mathcal{O}_{K_0^{\mathrm{cyc}}}/p\mathcal{O}_{K_0^{\mathrm{cyc}}}.$$

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 is enough to check that $\mathcal{O}_{\hat{F}}$ is dense in R^H, and 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 is enough to show that $\mathcal{O}_L/p\mathcal{O}_L \subset \theta_m(\mathcal{O}_F)$, for all m.

Set $\pi_n = \varepsilon^{(n)} - 1$, then

$$\mathcal{O}_{K_0}[\varepsilon^{(n)}] = W[\pi_n], \quad \mathcal{O}_L = \bigcup_{n=0}^{\infty} W[\pi_n].$$

Write $\bar{\pi}_n = \varepsilon_n - 1$, the image of π_n in $\mathcal{O}_L/p\mathcal{O}_L$, then $\mathcal{O}_L/p\mathcal{O}_L$ is generated as a k-algebra by $\bar{\pi}_n$'s. Since $k \subset \mathcal{O}_{E_0}$, we are reduced to prove

$$\bar{\pi}_n \in \theta_m(\mathcal{O}_F) = \theta_m(k[[\pi]]^{\mathrm{rad}}), \quad \text{for all } m, n \in \mathbb{N}.$$

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 $\varepsilon_{n+s} - 1 = \bar{\pi}_{n+s}$ for $n + s \geq 0$, let $s = n - m$, we get

$$\bar{\pi}_n = \theta_m(\pi^{p^{m-n}}) \in \theta_m(k[[\pi]]^{\mathrm{rad}}).$$

This completes the proof. □

4.2.3 A fundamental theorem.

Theorem 4.16. *Let E_0^s be the separable closure of $E_0 = k((\pi))$ in* $\mathrm{Fr}\,R$*, then E_0^s is dense in* $\mathrm{Fr}\,R$*, and is stable under G_{K_0}. Moreover, for any $g \in \mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}})$,*

$$g|_{E_0^s} \in \mathrm{Gal}(E_0^s/E_0),$$

and the map $\mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}}) \to \mathrm{Gal}(E_0^s/E_0)$ is an isomorphism.

Proof. 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 $\mathrm{Fr}\,R$. It is enough to check that $\overline{E}_0$ is dense in $\mathrm{Fr}\,R$ for the first part. In other words, we want 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 is enough 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,

$$\mathcal{O}_L/p\mathcal{O}_L \subset \theta_m(\mathcal{O}_{\overline{E}_0}).$$

Let $K_{0,n} = K_0(\varepsilon^{(n)})$ and $L_n = K_{0,n}L$, then $L/K_{0,n}$ is Galois with Galois group $J_n = \mathrm{Gal}(L_n/K_{0,n})$ and for n large, we have $J_n = J_{n+1} := J$. 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 $\theta_0(\mathcal{O}_{\overline{E}_0}) \subset \mathcal{O}_{K_{0,n}}/p\mathcal{O}_{K_{0,n}}$, 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. Write $P_n(X) = \prod_{g\in J}(X - g(\nu_n))$. We need the following lemma:

Lemma 4.17. *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 (A.23) and the proof of Proposition A.88. □

We will see that the lemma implies the first assertion. 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 $P_n(X)$ (mod p), We choose $Q(X) \in \mathcal{O}_{E_0}[X]$, monic of degree d, a lifting of $\overline{P_n}$. Choose β the image in $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ by θ_0 of a root of Q in $\mathcal{O}_{\overline{E}_0}$ in such a way that

$$v(\beta - \bar{\nu}_n) \geq v(\beta - g(\bar{\nu}_n)), \quad \text{for all } g \in J.$$

We also have $v(\overline{P_n}(\beta)) \geq 1$ since Q is a lifting of $\overline{P_n}$, thus

$$v(\beta - \bar{\nu}_n) \geq \frac{1}{d}.$$

Choose $b \in \mathcal{O}_{\overline{K}}$ a lifting of β such that $v(b) \geq 0$ and b is of degree d as well, then $v(b - \nu_n) \geq \frac{1}{d}$ and hence

$$v(b - \nu_n) > v(\nu_n - g(\nu_n)), \quad \text{for all } g \in J.$$

By Krasner's Lemma, $\nu_n \in \overline{K}(b)$, moreover, $\bar{\nu}_n = \beta \in \theta_0(\mathcal{O}_{\overline{E}_0})$. This proves the first assertion.

For any $a \in E_0^s$, let $P(x) = \sum_{i=1}^{d} \lambda_i X^i \in E_0[X]$ be a separable polynomial such that $P(a) = 0$. Then for any $g \in G_{K_0}$, $g(a)$ is a root of $g(P) = \sum_{i=1}^{d} g(\lambda_i) X^i$. 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 $g \in \mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}}) := H$, $g|_{E_0^s} \in \mathrm{Gal}(E_0^s/E_0)$, in other words, we get a map

$$\mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}}) \longrightarrow \mathrm{Gal}(E_0^s/E_0).$$

We want to prove this 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 $a \in \operatorname{Fr} R$ because E_0^s is dense in $\operatorname{Fr} R$ and the action of g is continuous.

Let $a \in \operatorname{Fr} R$, 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 $\theta_0 : \operatorname{Fr} R \to C$ is surjective, so g acts trivially on C, hence also on $\overline{K}$, we get $g = 1$.

Surjectivity: We identify $H = \mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}}) \hookrightarrow \mathrm{Gal}(E_0^s/E_0)$ a closed subgroup by injectivity. If the above map is not onto, we have

$$E_0 \subsetneqq F = (E_0^s)^H \subset (\mathrm{Fr}\, R)^H = \widehat{E_0^{\mathrm{rad}}},$$

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 4.18. *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 finite separable nontrivial extension E' of E contained in $\widehat{E^{\mathrm{rad}}}$. There are $d = [E' : E]$ distinct embeddings $\sigma_1, \cdots, \sigma_d : E' \to E^s$. We can extend each σ_i to E'^{rad} in the natural way, that is, by setting $\sigma_i(a) = \sigma_i(a^{p^n})^{p^{-n}}$. This map is continuous, hence can be extended to $\widehat{E'^{\mathrm{rad}}} = \widehat{E^{\mathrm{rad}}}$. But σ_i is the identity map on E^{rad}, so it is the identity map on $\widehat{E^{\mathrm{rad}}}$. This is a contradiction. □

4.3 An overview of Galois extensions.

4.3.1 A summary of Galois extensions of K and E.

We first give a summary of the Galois extensions we studied so far.

(1) The field K is a p-adic field with perfect residue field k. The field K_0 is the fraction field of the Witt ring $W(k)$. The extension $K \supset K_0$ is totally ramified. Let $K^{\mathrm{cyc}} = K_0^{\mathrm{cyc}} K = \bigcup_{n\geq 1} K(\varepsilon^{(n)})$, we have the following diagram

$$\begin{array}{ccc} H'_K = \mathrm{Gal}(\overline{K}/K^{\mathrm{cyc}}) & \subset & G_K = \mathrm{Gal}(\overline{K}/K) \\ \cap & & \cap \\ H'_{K_0} = \mathrm{Gal}(\overline{K}/K_0^{\mathrm{cyc}}) & \subset & G_{K_0} = \mathrm{Gal}(\overline{K}/K_0). \end{array}$$

Moreover, $H'_K = H'_{K_0} \cap G_K$, if we set $\Gamma'_K = G_K/H'_K = \mathrm{Gal}(K^{\mathrm{cyc}}/K)$, then $\Gamma'_K \subset \Gamma'_{K_0} = G_{K_0}/H'_{K_0}$, which is isomorphic to an open subgroup of $\mathbb{Z}_p^*$ via the cyclotomic character χ. Since $\mathbb{Z}_p^*$ is of rank 1 over $\mathbb{Z}_p$, with torsion subgroup

$$(\mathbb{Z}_p^*)_{\mathrm{tor}} \simeq \begin{cases} \mathbb{F}_p^* \ (\simeq \mathbb{Z}/(p-1)\mathbb{Z}) & \text{if } p \neq 2, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } p = 2, \end{cases}$$

the group Γ'_K is also rank 1 over $\mathbb{Z}_p$, and we have

$$1 \longrightarrow \Delta_K \longrightarrow \Gamma'_K \longrightarrow \Gamma_K \longrightarrow 1,$$

where $\Gamma_K \simeq \mathbb{Z}_p$, and Δ_K is the torsion subgroup of Γ'_K.

Let $H_K = \mathrm{Gal}(\overline{K}/K^{\infty})$, then we have exact sequences

$$1 \longrightarrow H_K \longrightarrow G_K \longrightarrow \Gamma_K \longrightarrow 1,$$

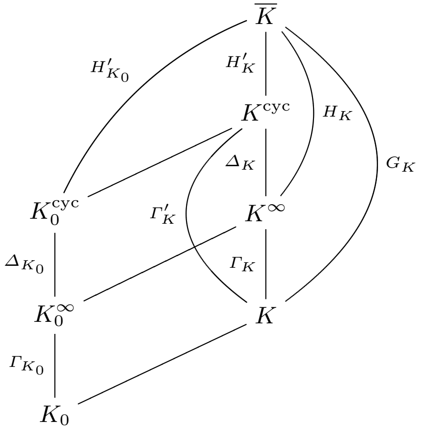


Fig. 4.1. Galois extensions of K and K_0

$$1 \longrightarrow H'_K \longrightarrow H_K \longrightarrow \Delta_K \longrightarrow 1.$$

In conclusion, we have Fig. 5.1.

(2) The field $E_0 = k((\pi))$, moreover, $E_0 \subset E_0^s \subset \operatorname{Fr} R$, and $H'_K \subset H'_{K_0} = \operatorname{Gal}(E_0^s/E_0)$. Set $E'_K = E' = (E_0^s)^{H'_K}$, then E_0^s/E' is a Galois extension with Galois group $\operatorname{Gal}(E_0^s/E') = H'_K$, and E'/E_0 is a finite separable extension. Set

$$E = E_K = (E_0^s)^{H_K} = (E')^{\Delta_K}, \tag{4.6}$$

then E'/E is a Galois extension with Galois group $\operatorname{Gal}(E'/E) = \Delta_K$. We see that E_0^s is also a separable closure of E. Set $E^s = E_0^s$.

In conclusion, we have Fig. 5.2.

Remark 4.19. E is stable under G_K, which acts through Γ_K.

4.3.2 The field $\widetilde{B}$ and its subfields.

Denote by $W(\operatorname{Fr} R)$ the ring of Witt vectors with coefficients in $\operatorname{Fr} R$, which is a complete discrete ring with the maximal ideal generated by p and residue field $W(\operatorname{Fr} R)/p = \operatorname{Fr} R$. Let

$$\widetilde{B} = \operatorname{Frac} W(\operatorname{Fr} R) = W(\operatorname{Fr} R)[\frac{1}{p}]. \tag{4.7}$$

The Galois group G_{K_0} (and therefore G_K) acts naturally on $W(\operatorname{Fr} R)$ and $\widetilde{B}$. Denote by φ the Frobenius map on $W(\operatorname{Fr} R)$ and on $\widetilde{B}$. Then φ commutes with the action of G_{K_0}: $\varphi(ga) = g\varphi(a)$ for any $g \in G_{K_0}$ and $a \in \widetilde{B}$.

$$\begin{tikzcd}
 & & \operatorname{Fr} R = \widehat{E^s} \arrow[d, dash] & & \\
 & & E_0^s = E^s \arrow[d, dash, "H'_K"'] \arrow[ddll, dash, bend right, "H_K"'] \arrow[ddrr, dash, bend left, "H'_{K_0}"] & & \\
 & & E' = E'_K \arrow[dll, dash, "\Delta_K"'] \arrow[drr, dash] & & \\
E = E_K \arrow[drr, dash] & & & & E_0 = E'_{K_0} = k((\pi)) \arrow[dll, dash, "\Delta_{K_0}"'] \\
 & & E_{K_0} & &
\end{tikzcd}$$

Fig. 4.2. Galois extensions of E and E_0

We know that $E_0 = k((\pi)) \subset \operatorname{Fr} R$ and $k[[\pi]] \subset R$. Let $[\varepsilon] = (\varepsilon, 0, 0, \cdots) \in W(R)$ be the Teichmüller representative of ε. Set $\pi_\varepsilon = [\varepsilon] - 1 \in W(R)$, then $\pi_\varepsilon = (\varepsilon, *, *, \cdots)$. Set $W = W(k) \subset W(R)$.

Since

$$W(R) = \varinjlim W_n(R) = \varinjlim W(R)/p^n$$

where $W_n(R) = \{(a_0, \cdots, a_{n-1}) \mid a_i \in R\}$ is a topological ring, the series

$$\sum_{n=0}^{\infty} \lambda_n \pi_\varepsilon^n, \quad \lambda_n \in W, \; n \in \mathbb{N},$$

converges in $W(R)$, we get a continuous embedding

$$W[[\pi_\varepsilon]] \hookrightarrow W(R),$$

and we identify $W[[\pi_\varepsilon]]$ with a closed subring of $W(R)$.

The element π_ε is invertible in $W(\operatorname{Fr} R)$, hence

$$W((\pi_\varepsilon)) = W[[\pi_\varepsilon]][\frac{1}{\pi_\varepsilon}] \subset W(\operatorname{Fr} R)$$

whose elements are of the form

$$\sum_{n=-\infty}^{+\infty} \lambda_n \pi_\varepsilon^n : \; \lambda_n \in W, \; \lambda_n = 0 \text{ for } n \ll 0.$$

Since $W(\operatorname{Fr} R)$ is complete, this inclusion extends by continuity to

$$\mathcal{O}_{\mathcal{E}_0} := \left\{ \sum_{n=-\infty}^{+\infty} \lambda_n \pi_\varepsilon^n | \; \lambda_n \in W, \; \lambda_n \to 0 \text{ when } n \to -\infty \right\}, \tag{4.8}$$

the p-adic completion of $W[[\pi_\varepsilon]][\frac{1}{\pi_\varepsilon}]$.

Note that $\mathcal{O}_{\mathcal{E}_0}$ is a complete discrete ring, whose maximal ideal is generated by p and whose residue field is 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

$$\varphi([\varepsilon]) = (\varepsilon^p, 0, \cdots) = [\varepsilon]^p, \text{ and } \varphi(\pi_\varepsilon) = (1+\pi_\varepsilon)^p - 1. \tag{4.9}$$

The group G_{K_0} acts through Γ'_{K_0}: for $g \in G_{K_0}$,

$$g([\varepsilon]) = (\varepsilon^{\chi(g)}, 0, \cdots) = [\varepsilon]^{\chi(g)},$$

therefore

$$g(\pi_\varepsilon) = (1+\pi_\varepsilon)^{\chi(g)} - 1. \tag{4.10}$$

Proposition 4.20. *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,

$$\mathcal{E}_0^{\mathrm{ur}} = \bigcup_F \mathcal{E}_F \subset \widetilde{B}, \tag{4.11}$$

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.

We have

$$\mathrm{Gal}(\mathcal{E}_0^{\mathrm{ur}}/\mathcal{E}_0) = \mathrm{Gal}(E_0^s/E_0) = H'_{K_0}.$$

Set

$$(\mathcal{E}_0^{\mathrm{ur}})^{H_K} = \mathcal{E}_E := \mathcal{E}, \tag{4.12}$$

then $\mathcal{E}$ is again a complete discrete valuation field whose residue field is E, and $\mathcal{E}_0^{\mathrm{ur}}/\mathcal{E}$ is a Galois extension with the Galois group $\mathrm{Gal}(\mathcal{E}_0^{\mathrm{ur}}/\mathcal{E}) = H_K$. 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 $\mathcal{E}$ is stable under φ, and also stable under G_K, which acts through $\Gamma_K \cong \mathbb{Z}_p$. We have Fig.5.3.

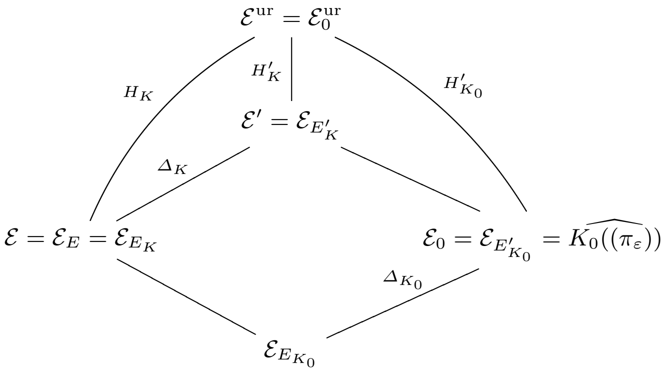

$\mathcal{E}^{\mathrm{ur}} = \mathcal{E}_0^{\mathrm{ur}}$
H_K
H'_K
H'_{K_0}
$\mathcal{E}' = \mathcal{E}_{E'_K}$
Δ_K
$\mathcal{E} = \mathcal{E}_E = \mathcal{E}_{E_K}$
$\mathcal{E}_0 = \mathcal{E}_{E'_{K_0}} = \widehat{K_0((\pi_\varepsilon))}$
Δ_{K_0}
$\mathcal{E}_{E_{K_0}}$

Fig. 4.3. Galois extensions of $\mathcal{E}$ and $\mathcal{E}_0$.

4.4 (φ, Γ)-modules and p-adic Galois representations

4.4.1 (φ, Γ)-modules.

Let V be a $\mathbb{Z}_p$ representation of H_K, where $H_K = \mathrm{Gal}(E^s/E) = \mathrm{Gal}(\mathcal{E}^{\mathrm{ur}}/\mathcal{E})$, then

$$\mathbf{M}(V) = (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} V)^{H_K} \tag{4.13}$$

is an étale φ-module over $\mathcal{O}_{\mathcal{E}}$. By Theorem 2.32, $\mathbf{M}$ 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

$$\mathbf{V} : D \longmapsto (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} D)_{\varphi=1}. \tag{4.14}$$

If instead, suppose V is a p-adic Galois representation of H_K. Then by Theorem 2.33,

$$\mathbf{M} : V \longmapsto (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V)^{H_K} \tag{4.15}$$

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

$$\mathbf{V} : D \longmapsto (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathcal{E}} D)_{\varphi=1}. \tag{4.16}$$

Now assume V is a $\mathbb{Z}_p$ or p-adic Galois representation of G_K, write

$$\mathbf{D}(V) := (\mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \otimes_{\mathbb{Z}_p} V)^{H_K} \text{ or } \mathbf{D}(V) := (\widehat{\mathcal{E}^{\mathrm{ur}}} \otimes_{\mathbb{Q}_p} V)^{H_K}. \tag{4.17}$$

Definition 4.21. *A (φ, Γ)-module D over $\mathcal{O}_{\mathcal{E}}$ (resp. $\mathcal{E}$) is an étale φ-module over $\mathcal{O}_{\mathcal{E}}$ (resp. $\mathcal{E}$) together with an action of Γ_K which is semi-linear, and commutes with φ. D is called* étale *if it is an étale φ-module and the action of Γ_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 2.32 and 2.33, we have

Theorem 4.22. **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* $\mathscr{M}^{\text{ét}}_{\varphi,\Gamma}(\mathcal{O}_{\mathcal{E}})$ *(resp.* $\mathscr{M}^{\text{ét}}_{\varphi,\Gamma}(\mathcal{E})$*), the category of étale* (φ, Γ)*-modules over* $\mathcal{O}_{\mathcal{E}}$ *(resp.* $\mathcal{E}$*), with a quasi-inverse*

$$\mathbf{V}(D) = \big(\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} D\big)_{\varphi=1} \quad (\textit{resp. } \big(\widehat{\mathcal{E}^{\text{ur}}} \otimes_{\mathcal{E}} D\big)_{\varphi=1}) \tag{4.18}$$

and G_K *acting on* $\mathcal{O}_{\widehat{\mathcal{E}^{\text{ur}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} D$ *and* $\widehat{\mathcal{E}^{\text{ur}}} \otimes_{\mathcal{E}} D$ *by*

$$g(\lambda \otimes d) = g(\lambda) \otimes \bar{g}(d)$$

for $\bar{g}$ *the image of* $g \in G_K$ *in* Γ_K*. Actually, this is an equivalence of Tannakian categories.*

Remark 4.23. There is a variant of the above theorem. For V any p-adic representation of G_K, then

$$\mathbf{D}'(V) = (\widehat{\mathcal{E}_0^{\text{ur}}} \otimes_{\mathbb{Q}_p} V)^{H'_K} \tag{4.19}$$

is an étale (φ, Γ')-module over $\mathcal{E}' = (\mathcal{E}^{\text{ur}})^{H'_K}$, and

$$\mathbf{D}(V) = (\mathbf{D}'(V))^{\Delta_K}, \quad \Delta_K = \text{Gal}(\mathcal{E}'/\mathcal{E}).$$

By Hilbert's Theorem 90, the map

$$\mathcal{E}' \otimes_{\mathcal{E}} \mathbf{D}(V) \xrightarrow{\sim} \mathbf{D}'(V)$$

is an isomorphism. Thus the category $\mathscr{M}^{\text{ét}}_{\varphi,\Gamma'}(\mathcal{E}')$ is an equivalence of categories with $\mathbf{Rep}_{\mathbb{Q}_p}(G_K)$ and $\mathscr{M}^{\text{ét}}_{\varphi,\Gamma}(\mathcal{E})$. For $\mathbb{Z}_p$-representations, the correspondent result is also true.

Example 4.24. If $K = K_0 = W(k)[\frac{1}{p}]$, $W = W(k)$, then $\mathcal{E}' = \mathcal{E}_0 = \widehat{K((\pi_\varepsilon))}$. If $V = \mathbb{Z}_p$, then $\mathbf{D}'(V) = \mathcal{O}_{\mathcal{E}_0} = \widehat{W((\pi_\varepsilon))}$ with the (φ, Γ')-action given by

$$\varphi(\pi_\varepsilon) = (1 + pi_\varepsilon)^p - 1, \quad g(\pi_\varepsilon) = (1 + \pi_\varepsilon)^{\chi(g)} - 1. \tag{4.20}$$

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 $A = (a_{ij}) \in \text{GL}_d(\mathcal{E})$. As Γ is isomorphic to $\mathbb{Z}_p$, let γ_0 be a topological generator of Γ,

$$\gamma_0(e_j) = \sum_{i=1}^{d} b_{ij} e_i.$$

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 4.25. (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.

4.4.2 The operator ψ.

Lemma 4.26. *(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 $\varphi(E_{\mathbb{Q}_p}) = k((\pi^p))$;

(2) Use the following diagram of fields, note that all vertical extensions are purely inseparable and horizontal ones are separable:

$$\begin{tikzcd}
E_K \arrow[r] \arrow[d] & E'_K \arrow[d] & E_0 \arrow[l] \arrow[d] \\
\varphi(E_K) \arrow[r] & \varphi(E'_K) & \varphi(E_0) \arrow[l]
\end{tikzcd}$$

We note the statement is still true if replacing F by any finite extension F over K or K_0.

(3) Because $E^s = \cup E_F$.

(4) To show that

$$(x_0, x_1, \cdots, x_{p-1}) \in \mathcal{O}^p_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \xmapsto{\sim} \sum_{i=0}^{p-1} [\varepsilon]^i \varphi(x_i) \in \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$$

is a bijection, it suffices to check it $\bmod p$ and use (3). □

Definition 4.27. *The operator $\psi : \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}} \to \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}$ is defined by*

$$\psi(\sum_{i=0}^{p-1} [\varepsilon]^i \varphi(x_i)) = x_0.$$

Proposition 4.28. *(1)* $\psi\varphi = \mathrm{Id}$*;*

(2) ψ *commutes with* G_K*.*

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 4.29. *(1) If* V *is a* $\mathbb{Z}_p$*-representation of* G_K*, there exists a unique operator* $\psi : \mathbf{D}(V) \to \mathbf{D}(V)$ *with*

$$\psi(\varphi(a)x) = a\psi(x), \quad \psi(a\varphi(x)) = \psi(a)x$$

if $a \in \mathcal{O}_{\mathcal{E}_K}, x \in \mathbf{D}(V)$ *and moreover* ψ *commute with* Γ_K*.*

(2) If D *is an étale* (φ, Γ)*-module over* $\mathcal{O}_{\mathcal{E}_K}$ *or* $\mathcal{E}_K$*, there exists a unique operator* $\psi : D \to D$ *with as in (1). Moreover, for any* $x \in D$*,*

$$x = \sum_{i=0}^{p^n-1}[\varepsilon]^i\varphi^n(x_i)$$

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, use ψ on $\mathcal{O}_{\mathcal{E}} \otimes V \supset \mathbf{D}(V)$. $\mathbf{D}(V)$ is stable under ψ because ψ commutes with H_K, ψ commutes with Γ_K since ψ commutes with G_K.

(2) $D = \mathbf{D}(\mathbf{V}(D))$, thus we have existence and uniqueness of ψ. The rest is by induction on n. □

Example 4.30. For $\mathcal{O}_{\mathcal{E}_0} \supset \mathcal{O}^+_{\mathcal{E}_0} = K_0[[\pi_\varepsilon]]$, $[\varepsilon] = 1 + \pi_\varepsilon$, let $x = F(\pi_\varepsilon) \in \mathcal{O}^+_{\mathcal{E}_0}$, then $\varphi(x) = F((1+\pi_\varepsilon)^p - 1)$. Write

$$F(\pi_\varepsilon) = \sum_{i=0}^{p-1}(1+\pi)^i F_i((1+\pi_\varepsilon)^p - 1),$$

then $\psi(F(\pi_\varepsilon)) = W(k)(\pi_\varepsilon)$. It is easy to see if $F(\pi_\varepsilon)$ belongs to $W(k)[[\pi_\varepsilon]]$, $F_i(\pi_\varepsilon)$ belongs to $W(k)[[\pi_\varepsilon]]$ for all i. Hence $\psi(\mathcal{O}^+_{\mathcal{E}_0}) \subset \mathcal{O}^+_{\mathcal{E}_0} = W(k)[[\pi]]$. Consequently, ψ is continuous on $\mathcal{E}_0$ for the natural topology (the weak topology).

Moreover, we have:

$$\begin{aligned}\varphi(\psi(F)) = F_0((1+\pi_\varepsilon)^p - 1) &= \frac{1}{p}\sum_{z^p=1}\sum_{i=0}^{p-1}(z(1+\pi_\varepsilon))^i F_i((z(1+\pi_\varepsilon))^p - 1) \\ &= \frac{1}{p}\sum_{z^p=1} F(z(1+\pi_\varepsilon) - 1).\end{aligned}$$

Proposition 4.31. *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 $D = \oplus(\mathcal{O}_{\mathcal{E}_0}/p^{n_i})\varphi(e_i)$. Then we have the following diagram:

$$\begin{tikzcd} D \arrow[r, "\psi"] \arrow[d, "\wr"] & D \arrow[d, "\wr"] \\ \oplus(\mathcal{O}_{\mathcal{E}_0}/p^{n_i})\varphi(e_i) \arrow[r] & \oplus(\mathcal{O}_{\mathcal{E}_0}/p^{n_i})e_i \\ \sum x_i\varphi(e_i) \arrow[r, mapsto] & \sum \psi(x_i)e_i \end{tikzcd}$$

Now $x \mapsto \psi(x)$ is continuous in $\mathcal{O}_{\mathcal{E}_0}$, hence ψ is continuous in D.

The second part follows from the fact that $\mathcal{O}_{\mathcal{E}_{E'_K}}$ is a free module of $\mathcal{O}_{\mathcal{E}_0}$ of finite rank, and the remark after Theorem 4.22. $\square$

5

de Rham representations

5.1 Hodge-Tate representations

Recall the Tate module $\mathbb{Z}_p(1) = T_p(\mathbb{G}_m)$ of multiplicative groups, choose a generator t, then G_K acts on $\mathbb{Z}_p(1)$ through 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 acts on it also through χ^i.

Let M be a $\mathbb{Z}_p$-module and $i \in \mathbb{Z}$, Recall 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 5.1. *The* Hodge-Tate ring B_{HT} *is defined to be*

$$B_{\mathrm{HT}} = \bigoplus_{i \in \mathbb{Z}} C(i) = C[t, 1/t]$$

where the element $c \otimes t^i \in C(i) = C \otimes \mathbb{Z}_p(i)$ is denoted by 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 5.2. *The ring B_{HT} is $(\mathbb{Q}_p, G_K)$-regular, which means*

(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. and $B_{\mathrm{HT}}^{G_K} = K$.

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 $b = \sum_{i \in \mathbb{Z}} c_i t^i,\ c_i \in C$, 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 3.56, 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 Sen's theorem, 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 5.3. *We say that a p-adic representation V of G_K is* Hodge-Tate *if it is B_{HT}-admissible.*

Let V be any p-adic representation, define

$$\mathbf{D}_{\mathrm{HT}}(V) = (B_{\mathrm{HT}} \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

It is always true that $\dim_K \mathbf{D}_{\mathrm{HT}}(V) \leqslant \dim_{\mathbb{Q}_p} V$ and

Proposition 5.4. *V is Hodge-Tate if and only if the equality*

$$\dim_K \mathbf{D}_{\mathrm{HT}}(V) = \dim_{\mathbb{Q}_p} V$$

holds.

Proposition 5.5. *For V to be Hodge-Tate, it is necessary and sufficient that the Sen operator ϕ of $W = V \otimes_{\mathbb{Q}_p} C$ be 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 ϕ_{W_i} is just multiplication by i (cf Example 3.26). Therefore the condition is the necessity.

To see it is sufficient, we decompose W into the eigenspaces W_i of ϕ, where ϕ is multiplication by $i \in Z$ in W_i. Then $W_i(-i)$ has $\phi = 0$ and by Theorem 3.28, we have

$$W_i(-i) = (W_i(-i))^{G_K} \otimes_K C.$$

Thus

$$\dim_K \mathbf{D}_{\mathrm{HT}}(V) \geq \sum_i \dim_K (W_i(-i))^{G_K} = \sum_i \dim_C W_i = \dim_{\mathbb{Q}_p} V$$

and hence V is Hodge-Tate. □

For a p-adic representation V, one sees that $\mathbf{D}_{\mathrm{HT}}$ is actually a graded K-vector space since

$$\mathbf{D}_{\mathrm{HT}}(V) = \bigoplus_{i \in \mathbb{Z}} \mathrm{gr}^i \, \mathbf{D}_{\mathrm{HT}}(V), \text{ where } \mathrm{gr}^i \, \mathbf{D}_{\mathrm{HT}}(V) = (C(i) \otimes V)^{G_K}.$$

Definition 5.6. *The* Hodge-Tate number *of V is defined to be $h_i = \dim(C(-i) \otimes V)^{G_K}$.*

Example 5.7. 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

$$\dim(C \otimes_{\mathbb{Q}_p} V_p(E))^{G_K} = \dim(C(-1) \otimes_{\mathbb{Q}_p} V_p(E))^{G_K} = 1.$$

Then the Hodge-Tate number is $(1_0, 1_1)$.

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

$$\mathrm{gr}^i \, \mathbf{D}^*_{\mathrm{HT}} \simeq (\mathrm{gr}^{-i} \, \mathbf{D}_{\mathrm{HT}}(V^*))^*$$

as K-vector spaces.

Remark 5.8. A p-adic representation V of G_K is $\widehat{B_{\mathrm{HT}}}$-admissible if and only if it is B_{HT}-admissible. This is an easy exercise.

5.2 de Rham representations

Recall $\widetilde{B} = W(\mathrm{Fr}\, R)\left[\frac{1}{p}\right] \supset \widehat{\mathcal{E}^{\mathrm{ur}}} \supset \mathcal{E}$ and $W(R) \subset \widetilde{B}$. In this section, we shall define the rings B_{dR}^{+} and B_{dR} such that $W(R) \subset B_{\mathrm{dR}}^{+} \subset B_{\mathrm{dR}}$.

5.2.1 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 see the natural map

$$W(R) = \varprojlim_{f_n} W_n(\mathcal{O}_{\overline{K}}/p)$$

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

$$I = \{(pb_0, pb_1, \cdots, pb_{n-1}, a_n) | b_i, a_n \in \mathcal{O}_C\}.$$

Let $w_{n+1} : W_{n+1}(\mathcal{O}_C) \to \mathcal{O}_C$ be 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

$$\theta_n : W_n(\mathcal{O}_{\overline{K}}/p) \to \mathcal{O}_C/p^n$$

such that the following diagram

$$\begin{tikzcd}
W_{n+1}(\mathcal{O}_C) \arrow[r, "w_{n+1}"] \arrow[d, "\psi_{n+1}"] & \mathcal{O}_C \arrow[d] \\
W_n(\mathcal{O}_{\overline{K}}/p) \arrow[r, "\theta_n"] & \mathcal{O}_C/p^n = \mathcal{O}_{\overline{K}}/p^n
\end{tikzcd}$$

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

$$\theta : W(R) \longrightarrow \mathcal{O}_C.$$

Lemma 5.9. *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*

$$\theta(x) = \sum_{n=0}^{+\infty} p^n x_n^{(n)}.$$

Thus θ *is a homomorphism of* W*-algebras.*

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 5.10. If for $x \in W(R)$, write x as $x = \sum_n p^n [x_n]$ where $x_n \in R$ and $[x_n]$ is its Teichmüller representative, then we have

$$\theta(x) = \sum_{n=0}^{+\infty} p^n x_n^{(0)}.$$

Proposition 5.11. *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 $\varpi^{(0)} = -p$. Let $\xi = [\varpi] + p \in W(R)$. Then $\xi = (\varpi, 1, 0, \cdots)$ and by Lemma 5.9, $\theta(\xi) = \varpi^{(0)} + p = 0$.

Proposition 5.12. *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 $x = \xi y_0 + px_1$, then $\theta(x) = p\theta(x_1)$, hence $x_1 \in \operatorname{Ker}\theta$. We may construct inductively a sequence $x_{n-1} = \xi y_{n-1} + px_n$, then $x = \xi(\sum p^n y_n)$.

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 $(y_i')^p = y_i$.

For the second assertion, if $x \in (\operatorname{Ker}\theta)^n$ for all $n \in \mathbb{N}$, then $v_R(\bar{x}) \geq v_R(\bar{\xi}^n) \geq n$. Hence $\bar{x} = 0$ and $x = py \in pW(R)$. Then $p\theta(y) = \theta(x) = 0$ and $y \in \operatorname{Ker}\theta$. Replaced x by x/ξ^n, we see that $y/\xi^n \in \operatorname{Ker}\theta$ for all n and thus $y \in \bigcap(\operatorname{Ker}\theta)^n$. Repeating this process, $x = py = p(pz) = \cdots = 0$. □

5.2.2 The rings B_{dR}^+ and B_{dR}.

Note that $K_0 = \operatorname{Frac} W = W\left[\frac{1}{p}\right]$, let

$$W(R)\left[\frac{1}{p}\right] = K_0 \otimes_W W(R).$$

We can use the map $x \mapsto 1 \otimes x$ to identify $W(R)$ to a subring of $W(R)\left[\frac{1}{p}\right]$. Note

$$W(R)\left[\frac{1}{p}\right] = \bigcup_{n=0}^{\infty} W(R)p^{-n} = \varinjlim_{n\in\mathbb{N}} W(R)p^{-n}.$$

Then the homomorphism $\theta : W(R) \twoheadrightarrow \mathcal{O}_C$ extends to a homomorphism of K_0-algebras $\theta : W(R)\left[\frac{1}{p}\right] \to C$ which is again surjective and continuous. The kernel is the principal ideal generated by ξ.

Definition 5.13. *The de Rham ring B_{dR}^{+} is*

$$B_{\mathrm{dR}}^{+}=\varprojlim_{n\in\mathbb{N}} W(R)\Big[\frac{1}{p}\Big]/(\operatorname{Ker}\theta)^n=\varprojlim_{n\in\mathbb{N}} W(R)\Big[\frac{1}{p}\Big]/(\xi)^n.$$

Since $\operatorname{Ker}\theta$ is a maximal ideal, which is principal and generated by a non-nilpotent element, B_{dR}^{+} is a complete valuation ring whose residue field is C.

Remark 5.14. Be *careful*: there are at least two different topologies on B_{dR}^{+} that we may consider:

(1). the topology of the discrete valuation ring;

(2). the topology of the inverse limit with the topology induced by the topology of $W(R)\big[\frac{1}{p}\big]$ on each quotient.

We call (2) the *natural topology* of B_{dR}^{+}. The topology (1) is stronger than (2). Actually from(1) the residue field C is endowed with the discrete topology; from (2), the induced topology on C is the natural topology of C.

Definition 5.15.

$$B_{\mathrm{dR}}:=\operatorname{Frac} B_{\mathrm{dR}}^{+}=B_{\mathrm{dR}}^{+}\Big[\frac{1}{\xi}\Big].$$

Since $\bigcap_{n=1}^{\infty}\xi^n W(R)\big[\frac{1}{p}\big]=0$, there is an injection

$$W(R)\Big[\frac{1}{p}\Big]\hookrightarrow B_{\mathrm{dR}}^{+}.$$

We can use it to identify $W(R)$ and $W(R)\big[\frac{1}{p}\big]$ to subrings of B_{dR}^{+}.

We have the following important fact:

Proposition 5.16. *For the homomorphism $\theta: B_{\mathrm{dR}}^{+}\to C$ from a complete discrete valuation ring to the residue field of characteristic 0, there exists a section $s: C\to B_{\mathrm{dR}}^{+}$ which is a homomorphism of rings such that $\theta(s(c))=c$ for all $c\in C$.*

Remark 5.17. The section s is not unique. The proof uses the axiom of choice (Zorn's lemma).

Moreover, one can prove that:

Exercise 5.18. (1). There is no such s which is continuous in the natural topology.

(2). There is no section s which commutes with the action of G_K.

(3). For $\overline{K}\subset C$ an algebraic closure of K inside C, there exists a unique continuous homomorphism $s:\overline{K}\to B_{\mathrm{dR}}^{+}$ commuting with the action of G_K such that $\theta(s(a))=a$, for all $a\in\overline{K}$. We use it to view $\overline{K}$ as a subfield of B_{dR}^{+}, then $\theta: B_{\mathrm{dR}}^{+}\to C$ is a homomorphism of $\overline{K}$-algebras.

Remark 5.19. (1). Assume $\overline{K} \subset B_{\mathrm{dR}}^+$. Note that $\bar{k}$ is the residue field of $\overline{K}$, as well as the residue field of R and $\bar{k} \subset R$. Thus $W(\bar{k}) \subset W(R)$. Let

$$P_0 = W(\overline{k})[\frac{1}{p}] = \mathrm{Frac}\, W(\overline{k})$$

which is the completion of the maximal unramified extension of K_0 in C. We have

$$P_0 \subset W(R)[\frac{1}{p}], \text{ and } P_0 \subset C$$

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 morphism of $\overline{P}$-algebras.

(2). A theorem by Colmez claims that: $\overline{K}$ is dense in B_{dR}^+ with a quite complicated topology in $\bar{K}$ induced by the natural topology of B_{dR}^+. However it is not dense in B_{dR}.

(3). For any $i \in \mathbb{Z}$, let $\mathrm{Fil}^i\, B_{\mathrm{dR}}$ be the i-th power of the maximal ideal of B_{dR}^+. Then if $i \geq 0$, $\mathrm{Fil}^i\, B_{\mathrm{dR}} = \mathfrak{m}^i_{B_{\mathrm{dR}}^+}$. For $i \in \mathbb{Z}$, $\mathrm{Fil}^i\, B_{\mathrm{dR}}$ is the free B_{dR}^+-module generated by ξ^i, i.e.,

$$\mathrm{Fil}^i\, B_{\mathrm{dR}} = B_{\mathrm{dR}}^+\xi^i, \quad \mathrm{Fil}^0\, B_{\mathrm{dR}} = B_{\mathrm{dR}}^+.$$

5.2.3 The element t.

Recall the element $\varepsilon \in R$ given by $\varepsilon^{(0)} = 1$ and $\varepsilon^{(1)} \neq 1$, then $[\varepsilon] - 1 \in W(R)$ and

$$\theta([\varepsilon] - 1) = \varepsilon^{(0)} - 1 = 0.$$

Thus $[\varepsilon] - 1 \in \mathrm{Ker}\,\theta = \mathrm{Fil}^1\, B_{\mathrm{dR}}$. Then $(-1)^{n+1}\frac{([\varepsilon]-1)^n}{n} \in W(R)[\frac{1}{p}]\xi^n$ and

$$\log[\varepsilon] = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{([\varepsilon]-1)^n}{n} \in B_{\mathrm{dR}}^+.$$

We call the above element $t = \log[\varepsilon]$.

Proposition 5.20. *The element*

$$t \in \mathrm{Fil}^1\, B_{\mathrm{dR}}, \textit{ and } t \notin \mathrm{Fil}^2\, B_{\mathrm{dR}}.$$

In other words, t generates the maximal ideal of B_{dR}^+.

Proof. That $t \in \mathrm{Fil}^1\, B_{\mathrm{dR}}$ is because

$$\frac{([\varepsilon]-1)^n}{n} \in \mathrm{Fil}^1\, B_{\mathrm{dR}} \text{ for all } n \geq 1.$$

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 $v(\varepsilon-1)=\frac{p}{p-1}<2$ if $p\neq 2$, contradiction. If $p=2$, compute the next term, we will get a contradiction too. □

Remark 5.21. We should point out that our t is the p-adic analogy 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 $\mathbb{Z}_p(1)=T_p(\mathbb{G}_m)$, viewed additively. Let $\mathbb{Z}_p(1)^*=\mathbb{Z}_p(1)$, viewed multiplicatively. Then $\mathbb{Z}_p(1)^*=\{\varepsilon^\lambda : \lambda \in \mathbb{Z}_p\}$ is a subgroup of U_R^+, and $\mathbb{Z}_P(1)=\mathbb{Z}_p t \subset B_{\mathrm{dR}}^+$. We have

$$\log([\varepsilon]^\lambda)=\lambda\log([\varepsilon])=\lambda t.$$

For any $g \in G_K$, $g(t)=\chi(g)t$ where χ is the cyclotomic character. Recall

$$\operatorname{Fil}^i B_{\mathrm{dR}}=B_{\mathrm{dR}}^+ t^i=B_{\mathrm{dR}}^+(i)$$

and

$$B_{\mathrm{dR}}=B_{\mathrm{dR}}^+[\frac{1}{t}]=B_{\mathrm{dR}}^+[\frac{1}{\xi}],$$

Then

$$\begin{aligned}\operatorname{gr} B_{\mathrm{dR}} &= \bigoplus_{i\in\mathbb{Z}} \operatorname{gr}^i B_{\mathrm{dR}} = \bigoplus_{i\in\mathbb{Z}} \operatorname{Fil}^i B_{\mathrm{dR}}/\operatorname{Fil}^{i+1} B_{\mathrm{dR}} \\ &= \bigoplus_{i\in\mathbb{Z}} B_{\mathrm{dR}}^+(i)/tB_{\mathrm{dR}}^+(i) = \bigoplus_{i\in\mathbb{Z}} C(i).\end{aligned}$$

Hence

Proposition 5.22. $\operatorname{gr} B_{\mathrm{dR}} = B_{\mathrm{HT}} = C(t, \frac{1}{t}) \subset \widehat{B_{\mathrm{HT}}} = C((t))$.

Remark 5.23. If we choose a section $s : C \to B_{\mathrm{dR}}^+$ which is a homomorphism of rings and use it to identify C to a subfield of B_{dR}^+, then $B_{\mathrm{dR}} \simeq C((t))$. This is not the right way as s is not continuous. Note there is no such an isomorphism which is compatible with the action of G_K.

Proposition 5.24. $B_{\mathrm{dR}}^{G_K} = K$.

Proof. First as $K \subset \overline{K} \subset B_{\mathrm{dR}}^+ \subset B_{\mathrm{dR}}$, 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 $\bar{b} \in K \subset B_{\mathrm{dR}}^+$. 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 $b - \bar{b} = 0$. □

5.2.4 Galois cohomology of B_{dR}

Suppose K is a finite extension of $\mathbb{Q}_p$. Recall that we have the following:

Proposition 5.25. *For $i \in \mathbb{Z}$, then*

(1) if $i \neq 0$, then $H^n(G_K, C(i)) = 0$ for all n;

(2) if $i = 0$, then $H^n(G_K, C) = 0$ for $n \geq 2$, $H^0(G_K, C) = K$, and $H^1(G_K, C)$ is a 1-dimensional K-vector space generated by $\log \chi \in H^1(G_K, \mathbb{Q}_p)$. (i.e, the cup product $x \mapsto x \cup \log \chi$ gives an isomorphism $H^0(G_K, C) \simeq H^1(G_K, C)$).

Proof. For the case $n = 0$, this is just Corollary 3.56.

We claim that $H^n(H_K, C(i))^{\Gamma_K} = 0$ for $n \geq 0$. Indeed, for any finite Galois extension L/K_∞, let $\alpha \in L$ such that $\operatorname{Tr}_{L/K_\infty}(\alpha) = 1$ and let $c \in H^n(L/K_\infty, C(i)^{G_L})$. Set

$$c'(g_1, \cdots, g_{n-1}) = \sum_{h \in \operatorname{Gal}(L/K_\infty)} g_1 g_2 \cdots g_{n-1} h(\alpha) c(g_1, \cdots, g_{n-1}, h),$$

then $dc' = c$. Thus $H^n(H_K, C(i)) = 1$ by passing to the limit.

For $n = 1$, using the inflation and restriction exact sequence

$$0 \longrightarrow H^1(\Gamma_K, C(i)^{H_K}) \xrightarrow{\inf} H^1(G_K, C(i)) \xrightarrow{\mathrm{res}} H^1(H_K, C(i))^{\Gamma_K}.$$

Then the inflation map is actually an isomorphism. We have $C(i)^{H_K} = \widehat{K}_\infty(i)$. Now $\widehat{K}_\infty = K_n \oplus X_n$ where X_n is the set of all elements whose normalized trace in K_n is 0 by Proposition A.97. Let n be large enough such that $v_K(\chi(\gamma_n) - 1) > d$, then $\chi(\gamma_n)^i\gamma_n - 1$ is invertible in X_n by Proposition A.97. We have

$$H^1(\mathit{\Gamma}_{K_n}, \widehat{K}_\infty(i)) = \frac{\widehat{K}_\infty}{\chi^i(\gamma_n)\gamma_n - 1} = \frac{K_n \oplus X_n}{\chi^i(\gamma_n)\gamma_n - 1} = \frac{K_n}{\chi^i(\gamma_n)\gamma_n - 1}.$$

Thus

$$H^1(\mathit{\Gamma}_{K_n}, \widehat{K}_\infty(i)) = \begin{cases} K_n, & \text{if } i = 0; \\ 0, & \text{if } i \neq 0. \end{cases}$$

Using the same method for computing $H^n(H_K, C(i)) = 1$, as $\widehat{K}_\infty(i)$ is a K-vector space, we have

$$H^i(\mathrm{Gal}(K_n/K), \widehat{K}_\infty(i)^{\mathrm{Gal}(K_n/K)}) = 0, \quad \text{for } i > 0.$$

By inflation-restriction again, $H^1(\mathit{\Gamma}_{K_n}, \widehat{K}_\infty(i)) = 0$ for $i \neq 0$ and for $i = 0$,

$$K = H^1(\mathit{\Gamma}_K, \widehat{K}_\infty) = H^1(\mathit{\Gamma}_K, K) = \mathrm{Hom}(\mathit{\Gamma}, K) = K \cdot \log\chi,$$

the last equality is because $\mathit{\Gamma}_K$ is pro-cyclic.

For $n \geq 2$, $H^n(H_K, C(i)) = 0$. Then just use the exact sequence

$$1 \longrightarrow H_K \longrightarrow G_K \longrightarrow \mathit{\Gamma}_K \longrightarrow 1$$

and Hochschild-Serre spectral sequence to conclude. □

Proposition 5.26. *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. Use the long exact sequence in continuous cohomology attached to the exact sequence

$$0 \longrightarrow t^{i+n}C(\simeq C(i+n)) \longrightarrow t^i B_{\mathrm{dR}}^+/t^{n+i+1}B_{\mathrm{dR}}^+ \longrightarrow t^i B_{\mathrm{dR}}^+/t^{i+n}B_{\mathrm{dR}}^+ \longrightarrow 0,$$

and use induction on $j-i$ (note that in the base step $j = i+1$, $t^i B_{\mathrm{dR}}^+/t^j B_{\mathrm{dR}}^+ \cong C(i)$), and Proposition 5.25 to do the computation. This concludes for the case where i, j are finite. For the general case, one proves it by taking limits. □

5.2.5 de Rham representations.

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. That is, for any p-adic representation V of G_K, let $\mathbf{D}_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K}$, then

$$\alpha_V : B_{\mathrm{dR}} \otimes_K \mathbf{D}_{\mathrm{dR}}(V) \to B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$$

is injective.

Definition 5.27. *A p-adic representation V of G_K is called* de Rham *if it is B_{dR}-admissible, equivalently if α_V is an isomorphism or if* $\dim_K \mathbf{D}_{\mathrm{dR}}(V) = \dim_{\mathbb{Q}_p} V$.

Let $\mathbf{Fil}_K$ be the category of finite dimensional K-vector spaces D equipped with a decreasing filtration indexed by $\mathbb{Z}$ which is exhausted and separated. That is,

- $\operatorname{Fil}^i D$ are sub K-vector spaces of D,
- $\operatorname{Fil}^{i+1} D \subset \operatorname{Fil}^i D$,
- $\operatorname{Fil}^i D = 0$ for $i \gg 0$, and $\operatorname{Fil}^i D = D$ for $i \ll 0$.

A morphism

$$\eta : D_1 \to D_2$$

between two objects of $\mathbf{Fil}_K$ is a K-linear map such that

$$\eta(\operatorname{Fil}^i D_1) \subset \operatorname{Fil}^i D_2 \text{ for all } i \in \mathbb{Z}.$$

We say η is *strict or strictly compatible with the filtration* if for all $i \in \mathbb{Z}$,

$$\eta(\operatorname{Fil}^i D_1) = \operatorname{Fil}^i D_2 \cap \operatorname{Im} \eta.$$

$\mathbf{Fil}_K$ is an additive category.

Definition 5.28. *A short exact sequence in $\mathbf{Fil}_K$ is a sequence*

$$0 \longrightarrow D' \xrightarrow{\alpha} D \xrightarrow{\beta} D'' \longrightarrow 0$$

such that:

(1) α and β are strict morphisms;

(2) α is injective, β is surjective and

$$\alpha(D') = \{x \in D | \beta(x) = 0\}.$$

If D_1 and D_2 are two objects in $\mathbf{Fil}_K$, we can define $D_1 \otimes D_2$ as

- $D_1 \otimes D_2 = D_1 \otimes_K D_2$ as K-vector spaces;
- $\operatorname{Fil}^i (D_1 \otimes D_2) = \sum_{i_1+i_2=i} \operatorname{Fil}^{i_1} D_1 \otimes_K \operatorname{Fil}^{i_2} D_2$.

The unit object is $D = K$ with

$$\operatorname{Fil}^i K = \begin{cases} K, & i \leq 0, \\ 0, & i > 0. \end{cases}$$

If D is an object in $\mathbf{Fil}_K$, we can also define its dual D^* by

- $D^* = \mathscr{L}_K(D, K)$ as a K-vector space;
- $\operatorname{Fil}^i D^* = (\operatorname{Fil}^{-i+1} D)^\perp = \{f : D \to K \mid f(x) = 0, \forall x \in \operatorname{Fil}^{-i+1} D\}$.

If V is any p-adic representation of G_K, then $\mathbf{D}_{\mathrm{dR}}(V)$ is a filtered K-vector space, with

$$\operatorname{Fil}^i \mathbf{D}_{\mathrm{dR}}(V) = (\operatorname{Fil}^i B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

Theorem 5.29. *Denote by $\mathbf{Rep}_{\mathbb{Q}_p}^{\mathrm{dR}}(G_K)$ the category of p-adic representations of G_K which are de Rham. Then $\mathbf{D}_{\mathrm{dR}} : \mathbf{Rep}_{\mathbb{Q}_p}^{\mathrm{dR}}(G_K) \to \mathbf{Fil}_K$ 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.

For the proof of (i), one always has

$$0 \to \mathbf{D}_{\mathrm{dR}}(V') \to \mathbf{D}_{\mathrm{dR}}(V) \to \mathbf{D}_{\mathrm{dR}}(V''),$$

the full exactness follows from the equality

$$\dim_K \mathbf{D}_{\mathrm{dR}}(V) = \dim_K \mathbf{D}_{\mathrm{dR}}(V') + \dim_K \mathbf{D}_{\mathrm{dR}}(V'').$$

For (ii), the injections $V_i \to V_1 \otimes V_2$ induces natural injections $\mathbf{D}_{\mathrm{dR}}(V_i) \to \mathbf{D}_{\mathrm{dR}}(V_1 \otimes V_2)$, thus we have an injection

$$\mathbf{D}_{\mathrm{dR}}(V_1) \otimes \mathbf{D}_{\mathrm{dR}}(V_2) \hookrightarrow \mathbf{D}_{\mathrm{dR}}(V_1 \otimes V_2).$$

By considering the dimension, this injection must also be surjective and $V_1 \otimes V_2$ must be de Rham.

(iii) follows from

$$\begin{aligned}\mathbf{D}_{\mathrm{dR}}(V^*) =&(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} \mathrm{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p))^{G_K} \cong \mathrm{Hom}_{B_{\mathrm{dR}}}(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V, B_{\mathrm{dR}})^{G_K}\\ &\cong \mathrm{Hom}_K((B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K}, K) = \mathbf{D}_{\mathrm{dR}}(V)^*.\end{aligned}$$

□

Let V be a de Rham representation. By the above Theorem, then

$$(\mathrm{Fil}^{i+1} B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K} = \mathrm{Fil}^{i+1} \mathbf{D}_{\mathrm{dR}}(V).$$

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,

$$\bigoplus_{i \in \mathbb{Z}} \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(v) \hookrightarrow \bigoplus_{i \in \mathbb{Z}} (C(i) \otimes_{\mathbb{Q}_p} V)^{G_K} = (B_{\mathrm{HT}} \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

Then

Proposition 5.30. *A p-adic representation V is de Rham implies that V is Hodge-Tate and*

$$\dim_K \mathbf{D}_{\mathrm{dR}}(V) = \sum_{i \in \mathbb{Z}} \dim_K \mathrm{gr}^i \mathbf{D}_{\mathrm{dR}}(V).$$

Proposition 5.31. *(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) is an exercise on Galois cohomology. It is enough to prove it for $K = \mathbb{Q}_p$. In this case $\mathrm{Ext}^1(\mathbb{Q}_p(1), \mathbb{Q}_p) = H^1_{\mathrm{cont}}(K, \mathbb{Q}_p(-1)) \neq 0$ is nontrivial.

(2) is again an exercise on Galois cohomology: $H^1_{\mathrm{cont}}(K, C(i)) = 0$ if $i \neq 0$.

(3) is not so easy! □

Remark 5.32. Any extension of $\mathbb{Q}_p$ by $\mathbb{Q}_p(1)$ is de Rham. (Kummer Theory)

5.2.6 A digression.

Let E be any field of characteristic 0 and X a projective (or proper) smooth algebraic variety over E. Consider the complex

$$\Omega^{\bullet}_{X/E} : \mathcal{O}_{X/E} \to \Omega^1_{X/E} \to \Omega^2_{X/E} \to \cdots,$$

define the de Rham cohomology group $H^m_{\mathrm{dR}}(X/E)$ to be the hyper cohomology $\mathbb{H}^m(\Omega^{\bullet}_{X/E})$ for each $m \in \mathbb{N}$, then it 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 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 5.33 (Tsuji, Faltings). *The 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.

We should point out that our t is the p-adic analogy of $2\pi i \in \mathbb{C}$. Although $\exp(t) = [\varepsilon] \neq 1$ in B^+_{dR}, $\theta([\varepsilon]) = 1$ in $C = \mathbb{C}_p$.

Let ℓ be a prime number. Let $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. For p a prime number, let $G_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and I_p be the inertia group. Choose an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$, then $I_p \subset G_p \hookrightarrow G_{\mathbb{Q}}$.

Definition 5.34. *An ℓ-adic representation V of $G_{\mathbb{Q}}$ is* geometric *if*

(1) It is unramified *away from finitely many p's: let $\rho : G_{\mathbb{Q}} \to Aut_{\mathbb{Q}_l}(V)$ be the representation, it unramified at p means that $\rho(I_p) = 1$ or $I_p \subset \operatorname{Ker} \rho$.*

(2) The representation is de Rham at $p = \ell$.

Conjecture 5.35 (Fontaine-Mazur). Geometric representations are exactly "the representations coming from algebraic geometry".

5.3 Overconvergent (φ, Γ)-modules

In this section, we let

$$A = \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{ur}}}}, \qquad B = \widehat{\mathcal{E}^{\mathrm{ur}}},$$
$$\widetilde{A} = W(\mathrm{Fr}\, R), \qquad \widetilde{B} = \mathrm{Frac}(\widetilde{A}) = W(\mathrm{Fr}\, R)\left[\frac{1}{p}\right].$$

5.3.1 Overconvergent elements.

Definition 5.36. *(1) For $x = \sum_{i=0}^{+\infty} p^i[x_i] \in \widetilde{A}$, $x_i \in \mathrm{Fr}\, R$, $k \in \mathbb{N}$, define*

$$w_k(x) := \inf_{i \leq k} v(x_i).$$

(One checks easily that $w_k(x) \geq v(\alpha)$, $\alpha \in \mathrm{Fr}\, R$, if and only if $[\alpha]x \in W(R) + p^{k+1}\widetilde{A}$).

(2) For a real number $r > 0$, define

$$v^{(0,\, r]}(x) := \inf_{k \in \mathbb{N}} w_k(x) + \frac{k}{r} = \inf_{k \in \mathbb{N}} v(x_k) + \frac{k}{r} \in \mathbb{R} \cup \{\pm\infty\}.$$

(3) Define $\widetilde{A}^{(0,\, r]} := \{x \in \widetilde{A} : \lim_{k \to +\infty} \big(v(x_k) + \frac{k}{r}\big) = \lim_{k \to +\infty} \big(w_k(x) + \frac{k}{r}\big) = +\infty\}$.

Proposition 5.37. *$\widetilde{A}^{(0,\, r]}$ is a ring and $v = v^{(0,\, r]}$ satisfies the following properties:*

(1) $v(x) = +\infty \Leftrightarrow x = 0$;
(2) $v(xy) \geq v(x) + v(y)$;
(3) $v(x+y) \geq \inf(v(x), v(y))$;
(4) $v(px) = v(x) + \frac{1}{r}$;
(5) $v([\alpha]x) = v(\alpha) + v(x)$ if $\alpha \in \mathrm{Fr}\, R$;
(6) $v(g(x)) = v(x)$ if $g \in G_{K_0}$;
(7) $v^{(0,\, p^{-1}r]}(\varphi(x)) = pv^{(0,\, r]}(x)$.

Proof. This is an easy exercise. □

Lemma 5.38. *Given $x = \sum_{k=0}^{+\infty} p^k[x_k] \in \widetilde{A}$, 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) $x \in \widetilde{A}^{(0,\, 1]}$.

Remark 5.39. We first note that if $x \in \operatorname{Fr} R$, then $[x] \in B_{\mathrm{dR}}^{+}$. Indeed, let $v(x) = -m$. Recall $\xi = [\varpi] + p \in W(R)$, where $\varpi \in R$ and $\varpi^{(0)} = -p$, is a generator of $\operatorname{Ker}\theta$. Then $x = \varpi^{-m} y$ for $y \in R$. Thus

$$[x] = [\varpi]^{-m}[y] = p^{-m}(\frac{\xi}{p} - 1)^{-m}[y] \in B_{\mathrm{dR}}^{+}.$$

Proof. (3) ⇔ (4) is by definition of $\widetilde{A}^{(0,\,r]}$. (2) ⇔ (3) is by definition of v. (1) ⇒ (2) is by the continuity of $\theta : B_{\mathrm{dR}}^{+} \to C$. So it remains to show (2) ⇒ (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

$$p^k[x_k] = \left(\frac{p}{[\varpi]}\right)^k [\varpi]^{a_k}[y_k] = p^{a_k}(\frac{\xi}{p} - 1)^{a_k - k}[y_k].$$

By expanding $(1-x)^t$ into power series, we see that

$$p^{a_k}(\frac{\xi}{p} - 1)^{a_k - k} \in p^{a_k - m} W(R) + (\operatorname{Ker}\theta)^{m+1}$$

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}^{+} by the definition of the topology of B_{dR}^{+}. □

Remark 5.40. We just proved that $\widetilde{A}^{(0,1]} = B_{\mathrm{dR}}^{+} \cap \widetilde{A}$, and we can use the isomorphism

$$\varphi^{-n} : \widetilde{A}^{(0,p^{-n}]} \xrightarrow{\sim} \widetilde{A}^{(0,\,1]}$$

to embed $\widetilde{A}^{(0,r]}$ in B_{dR}^{+}, for $r \geq p^{-n}$.

Define

$$\widetilde{A}^{\dagger} := \bigcup_{r>0} \widetilde{A}^{(0,\,r]} = \{x \in \widetilde{A} : \varphi^{-n}(x) \text{ converges in } B_{\mathrm{dR}}^{+} \text{ for } n \gg 0\}.$$

Lemma 5.41. *$x = \sum_{k=0}^{+\infty} p^k[x_k]$ is a unit in $\widetilde{A}^{(0,r]}$ if and only if $x_0 \neq 0$ and $v(\frac{x_k}{x_0}) > -\frac{k}{r}$ for all $k \geq 1$. In this case, $v^{(0,r]}(x) = v(x) = v(x_0)$.*

Proof. The only if part is an easy exercise. Now if $x = \sum_{k=0}^{+\infty} p^k[x_k]$ is a unit in $\widetilde{A}^{(0,r]}$, suppose $y = \sum_{k=0}^{+\infty} p^k[y_k]$ is its inverse. Certainly $x_0 \neq 0$. As

$$\lim_{k\to\infty} v(x_k) + \frac{k}{r} = +\infty, \quad \lim_{k\to\infty} v(y_k) + \frac{k}{r} = +\infty,$$

there are only finite number of x_k and y_j such that $v(x_k) + \frac{k}{r} = v^{(0,r]}(x) = v(x)$ and $v(x_j) + \frac{k}{r} = v^{(0,r]}(y) = v(y)$. Suppose m, n are maximal such that $v(x_m) + \frac{m}{r} = v(x)$ and $v(y_n) + \frac{n}{r} = v(y)$. Compare the coefficients of p^{m+n} in $xy = 1$, if $m + n > 1$, then

$$[x_{m+n}] + \cdots + [x_m y_n] + \cdots [y_{m+n}] = 0.$$

Hence

$$v(x_m y_n) + \frac{m+n}{r} \geq \min_{\substack{i+j=m+n \\ i \neq m}} \{v(x_i y_j) + \frac{m+n}{r}\} > v(x_m y_n) + \frac{m+n}{r},$$

a contradiction. Thus $m = n = 0$ and for $k > 0$, $v(x_k) + \frac{k}{r} > v(x_0)$ or equivalently, $v(\frac{x_k}{x_0}) > -\frac{k}{r}$. □

Set

$$\widetilde{B}^{(0,\, r]} = \widetilde{A}^{(0,r]}[\frac{1}{p}] = \bigcup_{n \in \mathbb{N}} p^{-n} \widetilde{A}^{(0,r]},$$

endowed with the topology of inductive limit, and

$$\widetilde{B}^{\dagger} = \bigcup_{r>0} \widetilde{B}^{(0,\, r]},$$

again with the topology of inductive limit. By the above lemma, we have

Theorem 5.42. *$\widetilde{B}^{\dagger}$ is a subfield of $\widetilde{B}$, stable by φ and G_{K_0}, both acting continuously.*

$\widetilde{B}^{\dagger}$ is called the field of *overconvergent elements.*

Definition 5.43. *(1) $B^{\dagger} = \widetilde{B}^{\dagger} \cap B$, $A^{\dagger} = \widetilde{A}^{\dagger} \cap B$ (so $B^{\dagger}$ is a subfield of B stable by φ and $G_{\mathbb{Q}_p}$), $A^{(0,\, r]} = \widetilde{A}^{(0,\, r]} \cap B$.*

(2) If $\Lambda \in \{A, B, \widetilde{A}^{\dagger}, \widetilde{B}^{\dagger}, A^{\dagger}, B^{\dagger}, A^{(0,\, r]}, B^{(0,\, r]}\}$, define $\Lambda_K = \Lambda^{H'_K}$. For example $A_K = \mathcal{O}_{\mathcal{E}_{E'_K}}$ and $A_K^{(0,\, r]} = \widetilde{A}^{(0,\, r]} \cap \mathcal{O}_{\mathcal{E}_{E'_K}}$.

(3) If $\Lambda \in \{A, B, A^{\dagger}, B^{\dagger}, A^{(0,\, r]}, B^{(0,\, r]}\}$, and $n \in \mathbb{N}$, define $\Lambda_{K,n} = \varphi^{-n}(\Lambda_K) \subset \widetilde{B}$.

We now want to make $A_K^{(0,\, r]}$ more concrete. We know that

$$A_{K_0} = \mathcal{O}_{\mathcal{E}_0} = \widehat{\mathcal{O}_{K_0}((\pi_\varepsilon))} = \left\{ \sum_{n=-\infty}^{+\infty} \lambda_n \pi_\varepsilon^n |\ \lambda_n \in \mathcal{O}_{K_0} = W(k),\ \lambda_n \to 0 \text{ when } n \to -\infty \right\},$$

and $B_{K_0} = \widehat{K_0((\pi_\varepsilon))}$, where $\pi_\varepsilon = [\varepsilon] - 1$.

Consider the extension E'_K/E_0. There are two cases.

(1): If E'_K/E_0 is unramified, then $E'_K = k'((\pi_\varepsilon))$ where k' is a finite Galois extension over k. Then $F' = \operatorname{Frac} W(k') \subset K^{cyc}$ and

$$A_K = \mathcal{O}_{\mathcal{E}_{E'_K}} = \left\{ \sum_{n=-\infty}^{+\infty} \lambda_n \pi_\varepsilon^n | \ \lambda_n \in \mathcal{O}_{F'} = W(k'), \ \lambda_n \to 0 \text{ when } n \to -\infty \right\}.$$

Let $\tilde{\pi}_K = \pi_\varepsilon$ in this case.

(2) In general, let the residue field of $E'_K = k'$ and $F' = \operatorname{Frac} W(k') \subset K^{cyc}$, let π_K be a uniformizer of $E'_K = k'((\pi_K))$, and let $\overline{P}_K(X) \in E'_{F'}[X] = k'((\pi))[X]$ be a minimal polynomial of π_K. Let $P_K(X) \in \mathcal{O}_{F'}[[\pi]][X]$ be a lifting of $\overline{P}_K$. By Hensel's lemma, there exists a unique $\tilde{\pi}_K \in A_K$ such that $P_K(\tilde{\pi}_K) = 0$ and $\pi_K = \tilde{\pi}_K \bmod p$.

Lemma 5.44. *If we define*

$$r_K = \begin{cases} 1, & \textit{if in case (1)}, \\ (2v(\mathfrak{D}_{E'_K/E'_{F'}}))^{-1}, & \textit{otherwise} . \end{cases}$$

where $\mathfrak{D}$ is the different of $E'_K/E'_{F'}$, then π_K and $P'_K(\tilde{\pi}_K)$ are units in $A_K^{(0,\,r]}$ for all $0 < r < r_K$.

Proof. We first show the case (1). We have $\pi_\varepsilon = [\varepsilon - 1] + p[x_1] + p^2[x_2] + \cdots$, 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 $\pi_\varepsilon = [\varepsilon - 1](1 + p[a_1] + p^2[a_2] + \cdots)$, 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 5.41, π_ε is a unit in $A_K^{(0,\,r]}$ for $0 < r < 1$.

In general, we have $\tilde{\pi}_K = [\pi_K] + p[\alpha_1] + p^2[\alpha_2] + \cdots$ and $v(\pi_K) = \frac{1}{e}v(\pi) = \frac{p}{e(p-1)}$ where $e = [E'_K : E'_{F'}]$ is the ramification index. Then $v(\frac{\alpha_i}{\pi_K}) \geq -v(\pi_K) = -\frac{p}{e(p-1)}$. Thus $\tilde{\pi}_K$ is a unit $A_K^{(0,\,r]}$ for $0 < r < \frac{e(p-1)}{p}$. It is easy to check $\frac{e(p-1)}{p} \geq (2v(\mathfrak{D}_{E'_K/E'_{F'}})^{-1}$.

Similarly, $P'_K(\tilde{\pi}_K) = [\overline{P}'_K(\pi_K)] + p[\beta_1] + p^2[\beta_2] + \cdots$, and

$$v(\frac{\beta_i}{\overline{P}'_K(\pi_K)}) \geq -v(\overline{P}'_K(\pi_K)) = -v(\mathfrak{D}_{E'_K/E'_{F'}}),$$

while the last equality follows from Proposition A.73. Thus $P'_K(\tilde{\pi}_K)$ a unit $A_K^{(0,\,r]}$ for $0 < r < (2v(\mathfrak{D}_{E'_K/E'_{F'}})^{-1}$. □

Proposition 5.45. *(1)* $A_K = \{ \sum\limits_{n \in \mathbb{Z}} a_n \tilde{\pi}_K^n : a_n \in \mathcal{O}_{F'}, \lim\limits_{n \to -\infty} v(a_n) = +\infty \}$;

(2) If $0 < r < r_K$, then

$$A_K^{(0,\,r]} = \{ \sum_{n \in \mathbb{Z}} a_n \tilde{\pi}_K^n : a_n \in \mathcal{O}_{F'}, \lim_{n \to -\infty} (v(a_n) + rnv(\pi_K)) = +\infty \}.$$

So $f \mapsto f(\pi_K)$ is an isomorphism from bounded analytic functions on the annulus $0 < v_p(T) \leq rv(\pi_K)$ to the ring $B_K^{(0,\,r]}$.

Proof. (1) follows from the structure of $A_K = \mathcal{O}_{\mathcal{E}_{E'_K}}$ in Chapter 5??.

For (2), we need to show that $\sum\limits_{n<0} a_n\tilde{\pi}_K^n \in A_K^{(0,\, r]}$ if and only if it satisfies the given condition. For $x = \sum\limits_{n<0} a_n\tilde{\pi}_K^n$, for $k \in \mathbb{N}$, let $y_k = p^{-k}\sum_{v(a_n)=k} a_n\tilde{\pi}_K^n$, then $x = \sum\limits_{k\geq 0} p^k y_k$. Let $n_k = \min\{n \mid v(a_n) = k\}$. One has

$$y^k = \frac{a_{n_k}}{p^k}\tilde{\pi}_K^{n_k}\big(1 + \sum_{\substack{n>n_k\\ v(a_n)=k}} \frac{a_n}{a_{n_k}}\tilde{\pi}_K^{n-n_k}\big).$$

Note that the first and the last factor in the above equality are units in A_K, then $w_i(y_k) = w_i(\tilde{\pi}_K^{n_k})$ for $i \in \mathbb{N}$. As a result,

$$w_0(y_k) = n_k v(\pi_K), \quad w_i(y_k) \geq (n_k - i)v(\pi_K) \text{ for } i \geq 1.$$

We now have

$$w_k(x) \geq \min_{0\leq i\leq k} w_k(p^i y_i) = \min_{0\leq i\leq k} w_{k-i}(y_i) \geq \min_{0\leq i\leq k}(n_i - k + i)v(\pi_K)$$

and the equality $w_k(x) = n_k v(\pi_K)$ holds if $w_0(y_k) < w_{k-i}(y_i)$ for all $0 \leq i \leq k-1$. We rewrite the above inequality as

$$w_k(x) + \frac{k}{r} \geq \min_{0\leq i\leq k}(n_i v(\pi_K) + \frac{i}{r}) + (k-i)(\frac{1}{r} - v(\pi_K)).$$

Lemma 5.46. *Suppose $s > 0$, $\{u_k\}$ and $\{v_k\}$ are two sequences in $\mathbb{R}$ satisfying the following two conditions:*

(1) $v_k \geq \min_{0\leq i\leq k} u_i + s(k-i)$;

(2) $u_k = v_k$ if $u_k < u_i + s(k-i)$ for all $0 \leq i \leq k-1$.

Then

$$\lim_{k\to+\infty} u_k = +\infty \quad \textit{if and only if} \quad \lim_{k\to+\infty} u_k = +\infty.$$

Proof (Proof of the lemma). The “only if” part is trivial. Now suppose $\lim_{k\to+\infty} u_k \neq +\infty$. Let $l = \liminf_k u_k$. If $l = -\infty$, we can pick an increasing sequence $\psi(i) \to +\infty$ such that $u_{\psi(i)} < u_k$ for $k < \psi(i)$, thus $u_{\psi(i)} = v_{\psi(i)}$ and $(v_k \nrightarrow +\infty$. If l is finite, pick $u_{\psi(i)} \to l$. Since $s(k-i) \geq s$ for $k \geq i+1$ and $s > 0$, then $u_{\psi(i)} = v_{\psi(i)}$ for i sufficiently large and thus $(v_k \nrightarrow +\infty$. □

We now apply the lemma to the case $u_k = n_k v(\pi_K) + \frac{k}{r}$ and $v_k = w_k(x) + \frac{k}{r}$, note that if $r < r_K$, then $s = \frac{1}{r} - v(\pi_K) > 0$, then $x \in A_K^{(0,r]}$ if and only if $v_k \to +\infty$ as $k \to +\infty$, or if and only if $u_k \to +\infty$, which is equivalent to that $\lim_{n\to-\infty}(v(a_n) + rnv(\pi_K)) = +\infty$. □

Corollary 5.47. *(1) $A_K^{(0,\, r]}$ is a principal ideal domain;*

(2) If L/K is a finite Galois extension, then $A_L^{(0,\, r]}$ is an étale extension of $A_K^{(0,\, r]}$ if $r < r_L$, and the Galois group is nothing but H'_K/H'_L.

Define $\widetilde{\pi}_n = \varphi^{-n}(\pi_\varepsilon)$, $\widetilde{\pi}_{K,n} = \varphi^{-n}(\pi_K)$. Let $K_n = K(\varepsilon^{(n)})$ for $n > 0$.

Proposition 5.48. *(1) If $p^n r_K \geq 1$, $\theta(\widetilde{\pi}_{K,n})$ is a uniformizer of K_n;*
(2) $\widetilde{\pi}_{K,n} \in K_n[[t]] \subset B_{\mathrm{dR}}^+$.

Proof. First by definition

$$\widetilde{\pi}_n = [\varepsilon^{1/p^n}] - 1 = \varepsilon^{(n)} e^{t/p^n} - 1 \in K_{0,n}[[t]] \subset B_{\mathrm{dR}}^+,$$

where $[\varepsilon^{1/p^n}] = \varepsilon^{(n)} e^{t/p^n}$ follows from that the θ value of both sides is $\varepsilon^{(n)}$ and the p^n-th power of both side is $[\varepsilon] = e^t$ (recall $t = \log[\varepsilon]$). This implies the proposition in the unramified case.

For the ramified case, we proceed as follows.

By the definition of E_K', $\pi_{K,n} = \theta(\widetilde{\pi}_{K,n})$ is a uniformizer of $K_n \bmod \mathfrak{a} = \{x : v_p(x) \geq \frac{1}{p}\}$. Let ω_n be the image of $\pi_{K,n}$ in $K_n \bmod \mathfrak{a}$. So we just have to prove $\pi_{K,n} \in K_n$.

Write

$$P_K(x) = \sum_{i=0}^{d} a_i(\pi_\varepsilon) x^i,\ a_i(\pi_\varepsilon) \in \mathcal{O}_{F'}[[\pi_\varepsilon]].$$

Define

$$P_{K,n}(x) = \sum_{i=0}^{d} a_i^{\varphi^{-n}}(\pi_n) x^i,$$

then $P_{K,n}(\pi_{K,n}) = \theta(\varphi(P_K(\widetilde{\pi}_K))) = 0$. Then we have $v(P_{K,n}(\omega_n)) \geq \frac{1}{p}$ and

$$v(P_{K,n}'(\omega_n)) = \frac{1}{p^n} v(P_K'(\overline{\pi}_K)) = \frac{1}{p^n} v(\mathfrak{d}_{E_K'/E_0}) < \frac{1}{2p} \text{ if } p^n r_K > 1.$$

Then one concludes by Hensel's Lemma that $\pi_{K,n} \in K_n$.

For (2), one uses Hensel's Lemma in $K_n[[t]]$ to conclude $\widetilde{\pi}_{K,n} \in K_n[[t]]$. □

Corollary 5.49. *If $0 < r < r_K$ and $p^n r \geq 1$, $\varphi^{-n}(A_K^{(0,\,r]}) \subseteq K_n[[t]] \subseteq B_{\mathrm{dR}}^+$.*

5.3.2 Overconvergent representations

Suppose V is a free $\mathbb{Z}_p$-representation of rank d of G_K. Let

$$\mathbf{D}^{(0,\,r]}(V) := (A^{(0,\,r]} \otimes_{\mathbb{Z}_p} V)^{H_K'} \subset \mathbf{D}(V) = (A \otimes_{\mathbb{Z}_p} V)^{H_K'}.$$

This is a $A_K^{(0,\,r]}$-module stable by Γ_K'. As for φ, we have

$$\varphi : \mathbf{D}^{(0,\,r]}(V) \longrightarrow \mathbf{D}^{(0,\,p^{-1}r]}(V).$$

Definition 5.50. *V is* overconvergent *if there exists an $r_V > 0, r_V \leq r_K$ such that*

$$A_K \bigotimes_{A_K^{(0,\,r_V]}} \mathbf{D}^{(0,\,r_V]}(V) \xrightarrow{\sim} D(V).$$

By definition, it is easy to see for all $0 < r < r_V$,

$$\mathbf{D}^{(0,\,r]}(V) = A_K^{(0,\,r]} \bigotimes_{A_K^{(0,\,r_V]}} \mathbf{D}^{(0,\,r_V]}(V).$$

If V is overconvergent, choose a basis $\{e_1, \cdots, e_d\}$ of $\mathbf{D}^{(0,pr)}(V)$ over $A_K^{(0,pr)}$ for $pr \leq r_V$, then $x \in \mathbf{D}^{(0,r)}(V)$ can be written as $\sum_i x_i \varphi(e_i)$, we define the valuation $v^{(0,r]}$ by

$$v^{(0,r]}(x) = \min_{1 \leq i \leq d} v^{(0,r]}(x_i).$$

One can see that for a different choice of basis, the valuation differs by a bounded constant.

Lemma 5.51. *If $0 < r < p^{-n}$ and $i \in \mathbb{Z}_p^*$, then $[\varepsilon]^{ip^n} - 1$ is a unit in $A_{K_0}^{(0,r]}$ and $v^{(0,r]}([\varepsilon]^{ip^n} - 1) = p^n v(\pi)$.*

Proof. We know that $\pi_\varepsilon = [\varepsilon] - 1$ is a unit in $A_{K_0}^{(0,r]}$ for $0 < r < 1$, then $[\varepsilon]^{p^n} - 1 = \varphi^n(\pi_\varepsilon)$ is a unit in $A_{K_0}^{(0,r]}$ for $0 < r < p^{-n}$. 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 5.52. *Let $\gamma \in \Gamma'_{K_0}$, suppose $\chi(\gamma) = 1 + up^n \in \mathbb{Z}_p^*$ with $u \in \mathbb{Z}_p^*$. Then for $0 < r < p^{-n}$,*

(1) $v^{(0,r]}(\gamma(\pi_\varepsilon) - \pi_\varepsilon) = p^n v(\pi)$.

(2) For $x \in A_{K_0}^{(0,r]}$, $v^{(0,r]}(\gamma(x) - x) \geq v^{(0,r]}(x) + (p^n - 1)v(\pi)$.

Proof. We have $\gamma(\pi_\varepsilon) - \pi_\varepsilon = [\varepsilon]([\varepsilon]^{up^n} - 1)$. By Lemma 5.51, $[\varepsilon]^{up^n} - 1$ is a unit in $A_{K_0}^{(0,r]}$, then $v^{(0,r]}(\gamma(\pi_\varepsilon) - \pi_\varepsilon) = v^{(0,r]}([\varepsilon]^{up^n} - 1) = p^n v(\pi)$. This finishes the proof of (1).

For (2), write $x = \sum_k a_k \pi_\varepsilon^k$ where $v(a_k) + rkv(\pi) \to +\infty$ as $k \to +\infty$. We know, by the proof of Proposition 5.45, that $v^{(0,r]}(x) = \min_k\{n_k v(\pi) + \frac{k}{r}\}$ where $n_k = \min\{n \mid v(a_n) = k\}$. Now

$$\begin{aligned}
\gamma(\pi_\varepsilon^k) - \pi_\varepsilon^k =& \pi_\varepsilon^k \left(\frac{\gamma(\pi_\varepsilon)^k}{\pi_\varepsilon^k} - 1 \right) \\
=& \pi_\varepsilon^k \sum_{j=1}^{\infty} \binom{k}{j} \left(\frac{\gamma(\pi_\varepsilon)}{\pi_\varepsilon} - 1 \right)^j \\
=& \pi_\varepsilon^{k-1} (\gamma(\pi_\varepsilon) - \pi_\varepsilon) \sum_{j=0}^{\infty} \binom{k}{j+1} \left(\frac{\gamma(\pi_\varepsilon)}{\pi_\varepsilon} - 1 \right)^j,
\end{aligned}$$

therefore

$$\gamma(x) - x = (\gamma(\pi_\varepsilon) - \pi_\varepsilon)\sum_k a_k \pi_\varepsilon^{k-1}\left(\frac{\gamma(\pi_\varepsilon)}{\pi_\varepsilon} - 1\right)^j$$

and

$$v^{(0,r]}(\gamma(x) - x) \geq p^n v(\pi) + \min_k\{(n_k - 1)v(\pi) + \frac{k}{r}\} = v^{(0,r]}(x) + (p^n - 1)v(\pi).$$

This finishes the proof of (2). □

Lemma 5.53. *Suppose V is an over-convergent representation. If $\{e_1, \cdots, e_d\}$ is a basis of $\mathbf{D}^{(0,r]}(V)$ and $e_i \in \varphi(D(V))$ for every i, then $x = \sum x_i e_i \in \mathbf{D}^{(0,r]}(V)^{\psi=0}$ if and only if $x_i \in \left(A_K^{(0,r]}\right)^{\psi=0}$ 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 5.54. *If V is overconvergent, then there exists a C_V such that if $\gamma \in \Gamma'_K$, $n(\gamma) = v_p(\log(\chi(\gamma)))$ and $r < \min\{p^{-1}r_V, p^{-n(\gamma)}\}$, then $\gamma - 1$ is invertible in $\mathbf{D}^{(0,\,r]}(V)^{\psi=0}$ and*

$$v^{(0,\,r]}((\gamma - 1)^{-1}x) \geq v^{(0,\,r]}(x) - C_V - p^{n(\gamma)}v(\bar{\pi}).$$

Remark 5.55. (1) Since through different choices of bases, $v^{(0,r]}$ differs by a bounded constant, the result of the above proposition is independent of the choice of bases.

(2) We shall apply the result to $(A_K^{(0,\,r]})^{\psi=0}$.

Proof. First, note that if replace V by $\mathrm{Ind}_{K_0}^K V$, we may assume that $K = K_0$.

Suppose $r < p^{-1}r_V$,pick a basis $\{e_1, \cdots, e_d\}$ of $\mathbf{D}^{(0,pr]}(V)$ over $A_{K_0}^{(0,pr]}$, then $\{\varphi(e_1), \cdots, \varphi(e_d)\}$ is a basis of $\mathbf{D}^{(0,r]}(V)$ over $A_{K_0}^{(0,r]}$. By Lemma 5.53, every $x \in \mathbf{D}^{(0,r]}(V)^{\psi=0}$ can be written uniquely as $x = \sum\limits_{i=1}^{p-1}[\varepsilon]^i\varphi(x_i)$ with $x_i = \sum\limits_{j=1}^{d} x_{ij}e_j \in \mathbf{D}^{(0,pr]}(V)$. Suppose $\chi(\gamma) = 1 + up^n$ for $u \in \mathbb{Z}_p^*$ 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 $\mathbf{D}^{(0,r]}(V)$ for $r < \min\{r_V, p^{-n}\}$, $u \in \mathbb{Z}_p^*$ and n is sufficiently large. Indeed, as the action of γ

is continuous, we may assume $v^{(0,r]}((\gamma-1)e_j) \geq 2v(\pi)$ for every $j = 1, \cdots, d$ for n sufficiently large. Then

$$\frac{f(x)}{[\varepsilon]^{up^n}-1} = \frac{[\varepsilon]^{up^n}}{[\varepsilon]^{up^n}-1}(\gamma(x)-x),$$

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 5.52,

$$v^{(0,r]}\left(\frac{f(x)}{[\varepsilon]^{up^n}-1}\right) \geq v^{(0,r]}(x) + 2v(\pi)$$

for every $x \in \mathbf{D}^{(0,r]}(V)$. Thus

$$g(x) = ([\varepsilon]^{up^n}-1)^{-1}\sum_{k=0}^{+\infty}\left(1-\frac{f}{[\varepsilon]^{up^n}-1}\right)^k$$

is the inverse of f and moreover,

$$v^{(0,r]}\left(g(x)-\frac{x}{[\varepsilon]^{up^n}-1}\right) \geq v^{(0,r]}(x)+v(\pi).$$

By the above claim, we see that if $n \gg 0$, $r > \min\{p^{-1}r_V, p^n\}$, then $\gamma-1$ has a continuous inverse $\sum\limits_{i=1}^{p-1}[\varepsilon]^i\varphi^{-1}\circ f_i^{-1}$ in $\mathbf{D}^{(0,r]}(V)^{\psi=0}$ and

$$v^{(0,r]}((\gamma-1)^{-1}(x)) \geq v^{(0,r]}(x) - p^n v(\pi) - C_V$$

for some constant C_V. In general, if γ^p-1 is invertible in $\mathbf{D}^{(0,r]}(V)^{\psi=0}$ for $r < \min\{p^{-1}r_V, p^{-n-1}\}$, 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 $\mathbf{D}^{(0,r]}(V)^{\psi=0}$ for $r < \min\{p^{-1}r_V, p^{-n}\}$. The proposition follows inductively. □

Theorem 5.56. *All (free $\mathbb{Z}_p$ or $\mathbb{Q}_p$) representations of G_K are overconvergent.*

Proof. One just needs to show the case for $\mathbb{Z}_p$-representations. The $\mathbb{Q}_p$-representation case follows by $\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$.

We shall apply Sen's method to

$$\widetilde{\Lambda} = \widetilde{A}^{(0,\,1]},\ v = v^{(0,\,1]},\ G_0 = G_K, \Lambda_{H'_{K,n}} = \varphi^{-n}(A_K^{(0,\,1]}).$$

Now we show how to check the three conditions.

(TS1). Let $L \supset K \supset K_0$ be finite extensions, for $\alpha = [\bar{\pi}_L](\sum_{\tau\in H'_K/H'_L}\tau([\bar{\pi}_L]))^{-1}$, then for all n,

$$\sum_{\tau \in H'_K/H'_L} \tau(\varphi^{-n}(\alpha)) = 1,$$

and

$$\lim_{n \to +\infty} v^{(0,\,1]}(\varphi^{-n}(\alpha)) = 0.$$

(TS2). First $\Lambda_{H'_K,n} = A^{(0,1]}_{K,n}$. Suppose $p^n r_K \geq 1$. We can define $R_{K,\,n}$ by the following commutative diagram:

$$\begin{tikzcd} R_{K,n}: & \widetilde{A}^{(0,1]}_K \arrow[r] & A^{(0,1]}_{K,n} \\ & A^{(0,1]}_{K,n+k} \arrow[u, hook] \arrow[ur, "\varphi^{-n}\circ\psi^k\circ\varphi^{n+k}"'] & \end{tikzcd}$$

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 $x \in \bigcup_{k\geq 0} A^{(0,1]}_{K,n+k}$, we immediately have: (a). $R_{K,n} \circ R_{K,n+m} = R_{K,n}$; (b). If $x \in A^{(0,1]}_{K,n}$, $R_{K,n}(x) = x$; (c). $R_{K,n}$ is $A^{(0,1]}_{K,n+k}$-linear; (d) $\lim\limits_{n\to+\infty} R_{K,n}(x) = x$.

Furthermore, for $x = \varphi^{-n-k}(y) \in A^{(0,1]}_{K,n+k}$,

$$R_{K,n}(x) = \varphi^{-n}(\psi^k(y)) = \varphi^{-n-k}(\varphi^k \circ \psi^k(y)).$$

Write y uniquely as $\sum_{i=0}^{p^k-1}[\varepsilon]^i \varphi^k(y_i)$, then by Corollary 4.29, $\psi^k(y) = y_0$. Thus

$$v^{(0,1]}(R_{K,n}(x)) = v^{(0,1]}(\varphi^{-n}(y_0)) \geq v^{(0,1]}(\varphi^{-n-k}(y)) = v^{(0,1]}(x).$$

By the above inequality, $R_{K,n}$ is continuous and can be extended to $\widetilde{\Lambda}$ as $\bigcup_{k\geq 0} A^{(0,1]}_{K,n+k}$ is dense in $\widetilde{A}^{(0,1]}$ and the condition (TS2) is satisfied. Let $R^*_{K,n}(x) = R_{K,n+1}(x) - R_{K,n}(x)$, then

$$R^*_{K,n}(x) = \varphi^{-n-1}(1 - \varphi\psi)(\psi^{k-1}(y)) \in \varphi^{-n-1}((A^{(0,1]})^{\psi=0}),$$

thus

$$\begin{aligned} R^*_{K,n}(x) \in \varphi^{-n-1}((A^{(0,1]}_K)^{\psi=0}) \cap \tilde{A}^{(0,1]} =& \varphi^{-n-1}((A^{(0,1]}_K)^{\psi=0} \cap \tilde{A}^{(0,p^{-n-1}]}) \\ =& \varphi^{-(n+1)}((A^{(0,p^{-(n+1)}]}_K)^{\psi=0}). \end{aligned}$$

(TS3). For an element x such that $R_{K,n}(x) = 0$, we have

$$x = \sum_{i=0}^{+\infty} R^*_{K,n+i}(x), \text{ where } R^*_{K,n+i}(x) \in \varphi^{-(n+i+1)}((A^{(0,p^{-(n+i+1)}]}_K)^{\psi=0}).$$

Apply Proposition 5.54 on $(A_K^{(0,p^{-(n+i+1)}]})^{\psi=0}$, then if n is sufficiently large, one can define the inverse of $\gamma - 1$ in $(R_{K,n} - 1)\widetilde{A}$ as

$$(\gamma - 1)^{-1}(x) = \sum_{i=0}^{+\infty} \varphi^{-(n+i+1)}(\gamma - 1)^{-1}(\varphi^{n+i+1} R^*_{K,n+i}(x))$$

and for $x \in (R_{K,n} - 1)\widetilde{A}$,

$$v((\gamma - 1)^{-1}x) \geq v(x) - C,$$

thus (TS3) is satisfied.

Now Sen's method (§3.4, in particular Proposition 3.45) implies that for any continuous cocycle $\sigma \mapsto U_\sigma$ in $H^1_{\mathrm{cont}}(G_0, \mathrm{GL}_d(\widetilde{A}))$, there exists an $n > 0$, $M \in \mathrm{GL}_d(\widetilde{A})$ such that $V_\sigma \in \mathrm{GL}_d(A_{K,n}^{(0,1]})$ 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 3.44, when n is sufficiently large, $C \in \mathrm{GL}_d(A_{K,n}^{(0,1]})$ and thus $M = NC \in \mathrm{GL}_d(A_{K,n}^{(0,1]})$.

Translate the above results to results about representations, there exists an n and an $A_{K,n}^{(0,1]}$-module $D_{K,n}^{(0,1]} \subset \widetilde{A}^{(0,1]} \bigotimes V$ such that

$$\widetilde{A}^{(0,1]} \otimes_{A_{K,n}^{(0,1]}} D_{K,n}^{(0,1]} \xrightarrow{\sim} \widetilde{A}^{(0,1]} \otimes V.$$

Moreover, one concludes that $D_{K,n}^{(0,1]} \subset \varphi^{-n}(\mathbf{D}(V))$ and $\varphi^n(D_{K,n}^{(0,1]}) \subset \mathbf{D}(V) \cap \varphi^n(\widetilde{A}^{(0,1]} \bigotimes V) = \mathbf{D}^{(0,p^{-n}]}(V)$. We can just take $r_V = p^{-n}$. □

6

Semi-stable *p*-adic representations

In this chapter we shall construct the rings of periods B_{cris} and b_{st}, and introduce the concept of crystalline and semi-stable representations. Let V be a p-adic representation of G_K. Assume it is semi-stable. Let $\mathbf{D}_{\mathrm{st}}(V)$ be the corresponding filtered K-vector space. Then there are two operators φ and N on $\mathbf{D}_{\mathrm{st}}(V)$, giving it additional structures. Furthermore, we will get an equivalence of categories between semi-stable representations and the category of filtered K-vector spaces equipped with two operators φ and N satisfying suitable properties.

6.1 The rings B_{cris} and B_{st}

In this section, we shall define two rings of periods B_{cris} and B_{st} such that

$$\mathbb{Q}_p \subset B_{\mathrm{cris}} \subset B_{\mathrm{st}} \subset B_{\mathrm{dR}}$$

and they are $(G_K, \mathbb{Q}_p)$-regular.

6.1.1 The ring B_{cris}.

Recall

$$\begin{tikzcd} W(R) \arrow[r, "\theta"] \arrow[d, hook] & \mathcal{O}_C \arrow[d, hook] \\ W(R)[\frac{1}{p}] \arrow[r, "\theta"] & C \end{tikzcd}$$

we know $\operatorname{Ker}\theta = (\xi)$ where $\xi = [\varpi] + p = (\varpi, 1, \cdots)$, $\varpi \in R$ such that $\varpi^{(0)} = -p$.

Definition 6.1. *(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 $\frac{a^m}{m!}$ for all $a \in \operatorname{Ker}\theta$.*

(2) The ring A_{cris} is defined to be $\varprojlim\limits_{n\in\mathbb{N}} A^0_{\mathrm{cris}}/p^nA^0_{\mathrm{cris}}$.

(3) The ring B^+_{cris} is defined to be $A_{\mathrm{cris}}\left[\frac{1}{p}\right]$.

Remark 6.2. (1) By definition, A^0_{cris} is just the sub $W(R)$-module of $W(R)\left[\frac{1}{p}\right]$ generated by the $\gamma_m(\xi)=\frac{\xi^m}{m!}, m\in\mathbb{N}$. It is actually a ring, since

$$\gamma_m(\xi)\cdot\gamma_n(\xi)=\binom{m+n}{n}\frac{\xi^{m+n}}{(m+n)!}. \tag{6.1}$$

(2) The module $A_{\mathrm{cris}}/p^nA_{\mathrm{cris}}$ is just the divided power envelop of $W_n(\mathcal{O}_{\overline{K}}/p)$ related to the homomorphism $\theta_n: W_n(\mathcal{O}_{\overline{K}}/p)\to\mathcal{O}_{\overline{K}}/p^n$.

Exercise 6.3. The map $A^0_{\mathrm{cris}}\to A_{\mathrm{cris}}$ is injective. We shall identify A^0_{cris} as a subring of A_{cris}.

Since $A^0_{\mathrm{cris}}\subset W(R)\left[\frac{1}{p}\right]$, by continuity $A_{\mathrm{cris}}\subset B^+_{\mathrm{dR}}$ and $B^+_{\mathrm{cris}}\subset B^+_{\mathrm{dR}}$. We have

$$\begin{tikzcd}
A^0_{\mathrm{cris}} \arrow[r, hook] \arrow[d, hook] & A_{\mathrm{cris}} \arrow[r, hook] \arrow[dr] & B^+_{\mathrm{cris}} \arrow[d, hook] \\
W(R)[\frac{1}{p}] \arrow[rr, hook] & & B^+_{\mathrm{dR}}
\end{tikzcd}$$

The ring homomorphism $\theta: W(R)\to\mathcal{O}_C$ can be extended to A^0_{cris}, and thus to A_{cris}:

$$\begin{tikzcd}
W(R) \arrow[d, hook] \arrow[dr, "\theta"] & \\
A^0_{\mathrm{cris}} \arrow[r, "\theta"'] \arrow[d, hook] & \mathcal{O}_C \\
A_{\mathrm{cris}} \arrow[ur, "\theta"'] &
\end{tikzcd}$$

Proposition 6.4. *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 $a=\sum a_n\gamma_n(\xi)\in A^0_{\mathrm{cris}}$, 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 for $\frac{(ni)!}{(n!)^i i!} \in \mathbb{N}$ for $n \geq 1$ and $i \in N$. 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

$$\frac{a^m}{m!} = \sum_{\text{sum of } i_n = m} \prod_n a_n \cdot \frac{(ni_n)!}{(n!)^{i_n}(i_n)!} \cdot \gamma_{ni_n}(xi) \in A^0_{\text{cris}}$$

and $\theta(\frac{a^m}{m!}) = 0$.

The case for $a \in A_{\text{cris}}$ follows by continuity. □

We then have a ring homomorphism

$$\bar{\theta} : A_{\text{cris}} \xrightarrow{\theta} \mathcal{O}_C \to \mathcal{O}_C/p = \mathcal{O}_{\overline{K}}/p.$$

Proposition 6.5. *The kernel* $\operatorname{Ker}(\bar{\theta}) = (\operatorname{Ker}\theta, p)$ *is again a divided power ideal, which means that, if* $a \in \operatorname{Ker}(\bar{\theta})$*, then for all* $m \in \mathbb{N}$, $m \geq 1$, $\frac{a^m}{m!} \in A_{\text{cris}}$ *and* $\bar{\theta}(\frac{a^m}{m!}) = 0$.

Proof. This is an easy exercise, noting that p divides $\frac{p^m}{m!}$ in $\mathbb{Z}_p$. □

If $\alpha \in A_{\text{cris}}$, α can always be written (not uniquely) as:

$$\alpha = \sum_{n=0} \alpha_n \frac{\xi^n}{n!}, \ \alpha_n \in W(R) \text{ and} \alpha_n \to 0 \ p\text{-adically.}$$

Recall that

$$t = \sum_{n=1}^{+\infty} (-1)^{n+1} \frac{([\varepsilon]-1)^n}{n} \in B^+_{\text{dR}}.$$

Proposition 6.6. *One has* $t \in A_{\text{cris}}$ *and* $t^{p-1} \in pA_{\text{cris}}$.

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, hence $t \in A_{\text{cris}}$.

To show $t^{p-1} \in pA_{\text{cris}}$, we just need to show that $([\varepsilon]-1)^{p-1} \in pA_{\text{cris}}$. 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 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

$$([\varepsilon]-1)^{p-1} \equiv [\varpi^p] \cdot (*) = (\xi - p)^p \cdot (*) \equiv \xi^p \cdot (*) \bmod pA_{\text{cris}},$$

but $\xi^p = p(p-1)!\gamma_p(\xi) \in pA_{\text{cris}}$, we hence have the result. □

Definition 6.7. *We define* $B_{\text{cris}} := B^+_{\text{cris}}[1/t] = A_{\text{cris}}[1/t]$*, then* $B_{\text{cris}} \subset B_{\text{dR}}$.

Remark 6.8. The rings A_{cris}, B^+_{cris}, B_{cris} are all stable under the action of G_K.

The Frobenius map 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

$$\varphi(\gamma_m(\xi)) = \frac{p^m}{m!}(\eta + (p-1)!\gamma_p(\xi))^m \in W(R)[\gamma_p(\xi)] \subset A^0_{\text{cris}}.$$

As a consequence,

$$\varphi(A^0_{\text{cris}}) \subset A^0_{\text{cris}}.$$

By continuity, φ is extended 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 $g \in G_K$, $b \in B_{\text{cris}}$, $\varphi(gb) = g(\varphi b)$.

6.1.2 The logarithm map.

We first recall the construction of the classical p-adic logarithm

$$\log_p : C^* \to C.$$

Using the key fact

$$\log(xy) = \log x + \log y,$$

the construction is processed in four steps:

- For those x satisfying $v(x-1) \geq 1$, set
$$\log x := \sum_{i=0}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}. \qquad (6.2)$$

- In general, for any $x \in 1 + \mathfrak{m}_C = \{x \in C \mid v(x-1) > 0\}$, there exists $m \in \mathbb{N}$ such that $v(x^{p^m} - 1) \geq 1$, then set
$$\log x := \frac{1}{p^m} \log(x^{p^m}). \qquad (6.3)$$

- For any $a \in \mathcal{O}_C^*$, then $\bar{a} \in \bar{k}$ and $\bar{a} \neq 0$. One has a decomposition
$$a = [\bar{a}]x,$$
where $\bar{a} \in \bar{k}^*$, $[\bar{a}] \in W(\bar{k})$ and $x \in 1 + \mathfrak{m}_C$. We let
$$\log a := \log x. \tag{6.4}$$

- Moreover, for any $x \in C$ with $v(x) = \frac{r}{s}, r, s \in \mathbb{Z}, s \geq 1$, we see that $v(x^s) = r = v(p^r)$ and $\frac{x^s}{p^r} = y \in \mathcal{O}_C^*$. 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 let $\log_p p = 0$, then
$$\log_p x := \frac{1}{s} \log_p y = \frac{1}{s} \log y. \tag{6.5}$$

We now define the logarithm map in $(\operatorname{Fr} R)^*$ with values in B_{dR}. Similar to the classical case, one needs the key rule:
$$\log[xy] = \log[x] + \log[y].$$

Recall that
$$U_R^+ = 1 + \mathfrak{m}_R = \{x \in R \mid v(x-1) > 0\},$$
$$U_R^+ \supset U_R^1 = \{x \in R \mid v(x-1) \geq 1\},$$

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) We first define the logarithm map on U_R^1 by
$$\log[x] := \sum_{i=0}^{\infty} (-1)^{n+1} \frac{([x]-1)^n}{n}, \quad x \in U_R^1. \tag{6.6}$$

This series converges in A_{cris}, since
$$\theta([x]-1) = x^{(0)} - 1,$$
which means that $x \in U_R^1$ or equivalently, $\bar{\theta}([x]-1) = 0$. Therefore $\gamma_n([x]-1) = \frac{([x]-1)^n}{n!} \in A_{\text{cris}}$ and
$$\log[x] = \sum_{i=0}^{\infty} (-1)^{n+1} (n-1)! \gamma_n([x]-1)$$
converges since $(n-1)! \to 0$ when $n \to \infty$.

(2) The logarithm map on U_R^1

$$\log:\ U_R^1 \to A_{\mathrm{cris}}, \quad x \mapsto \log[x]$$

extends uniquely to the logarithm map on U_R^+ with values in B_{cris}^+ by

$$\log:\ U_R^+ \to B_{\mathrm{cris}}^+, \quad \log[x] := \frac{1}{p^m}\log[x^{p^m}]\ (m \gg 0). \tag{6.7}$$

By definition, for every $x \in U_R^+$, one can check

$$\varphi(\log[x]) = p\log[x].$$

Furthermore, if denote by U the image of $\log:\ U_R^+ \to B_{\mathrm{cris}}^+$, then we have the following diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Q}_p(1) \arrow[r] \arrow[d, equal] & U_R^+ \arrow[r] \arrow[d, "\cong"] & C \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbb{Q}_p(1) \arrow[r] \arrow[d, hook] & U \arrow[r] \arrow[d, hook] & C \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & B_{\mathrm{dR}}^+(1) \arrow[r] & B_{\mathrm{dR}}^+ \arrow[r] & C &
\end{tikzcd}$$

where the isomorphism $U_R^+ \simeq U$ follows from the fact that for $x = (x^{(n)}) \in U_R^+$, $\log x^{(0)} = 0 \in C$ if and only if $x^{(0)} \in \boldsymbol{\mu}_{p^\infty}(\overline{K})$. As a result, $\varphi u = pu$ for all $u \in U$.

Remark 6.9. One can show that $U = \{u \in B_{\mathrm{cris}}^+ | \varphi u = pu\}$.

(3) For $a \in R^*$, we define

$$\log[a] := \log[x] \tag{6.8}$$

by using the decomposition $R^* = \bar{k}^* \times U_R^+$, $a = a_0 x$ for $a_0 \in \bar{k}^*$, $x \in U_R^+$.

(4) Finally, we can extend the logarithm map to

$$\log:\ (\mathrm{Fr}\,R)^* \to B_{\mathrm{dR}}^+, \quad x \mapsto \log[x].$$

Recall the element $\varpi \in R$ is given by $\varpi^{(0)} = -p, v(\varpi) = 1$. For any $x \in (\mathrm{Fr}\,R)^*$ with $v(x) = \frac{r}{s}$, $r, s \in \mathbb{Z}$, $s \geq 1$, then $\frac{x^s}{\varpi^r} = y \in R^*$. Hence the relation

$$\log(\frac{x^s}{\varpi^r}) = \log y = s\log x - r\log\varpi,$$

implies that

$$\log[x] = \frac{1}{s}(r\log[\varpi] + \log[y]).$$

Thus in order to define $\log[x]$, it suffices to define $\log[\varpi]$.

For $[\varpi] \in W(R) \subset W(R)[\frac{1}{p}] \xrightarrow{\theta} C$, consider $\frac{[\varpi]}{-p}$, note that

$$\theta\left(\frac{[\varpi]}{-p}\right) = \frac{-p}{-p} - 1 = 0,$$

then

$$\log\left(\frac{[\varpi]}{-p}\right) = \sum_{i=0}^{\infty}(-1)^{n+1}\frac{(\frac{[\varpi]}{-p}-1)^n}{n} = -\sum_{i=0}^{\infty}\frac{\xi^n}{np^n} \in B_{\rm dR}^+$$

is well defined. Set

$$\log[\varpi] := \log\left(\frac{[\varpi]}{-p}\right) = \sum_{i=0}^{\infty}(-1)^{n+1}\frac{(\frac{[\varpi]}{-p}-1)^n}{n} \in B_{\rm dR}^+, \qquad (6.9)$$

then we get the desired logarithm map $\log : (\operatorname{Fr} R)^* \rightarrow B_{\rm dR}^+$ for any $x \in (\operatorname{Fr} R)^*$. Note that

- For every $g \in G_K$, $g\varpi = \varpi\varepsilon^{\chi(g)}$, then
$$\log([g\varpi]) = \log[\varpi] + \chi(g)t,$$
as $\log[\varepsilon] = t$.
- The kernel of log is just $\bar{k}^*$. The short exact sequence
$$0 \longrightarrow U_R^+ \longrightarrow (\operatorname{Fr} R)^*/\bar{k}^* \longrightarrow \mathbb{Q} \longrightarrow 0$$
shows that the sub-$\mathbb{Q}_p$-vector space of $B_{\rm dR}^+$ generated by the image of the logarithm map log is $U \oplus \mathbb{Q}_p \log[\varpi]$.

6.1.3 The ring $B_{\rm st}$.

Definition 6.10. *The ring* $B_{\rm st} := B_{\rm cris}[\log[\varpi]]$ *is defined to be the sub* $B_{\rm cris}$*-algebra of* $B_{\rm dR}$ *generated by* $\log[\varpi]$.

Clearly $B_{\rm st}$ is stable under the action of G_K (even of G_{K_0}). Moreover, denote by $C_{\rm cris}$ and $C_{\rm st}$ the fraction fields of $B_{\rm cris}$ and $B_{\rm st}$ respectively, then both $C_{\rm cris}$ and $C_{\rm st}$ are stable under the actions of G_K and G_{K_0}, and the Frobenius map φ on $B_{\rm cris}$ extends to $C_{\rm cris}$.

Proposition 6.11. $\log[\varpi]$ *is transcendental over* $C_{\rm cris}$.

We need a lemma:

Lemma 6.12. *The element* $\log[\varpi]$ *is not contained in* $C_{\rm cris}$.

Proof (Proof of the Lemma). 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 $n \in \mathbb{N}$, 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

$$\theta^i : \mathrm{Fil}^i B_{\mathrm{dR}} \longrightarrow \mathcal{O}_C$$

the map sending $\beta^i\alpha$ to $\theta(\alpha)$. One knows that $\theta^i(\mathrm{Fil}^i S) = \mathcal{O}_C$.

By construction, $A_{\mathrm{cris}} \subset S$ and hence $C_{\mathrm{cris}} = \mathrm{Frac}\, A_{\mathrm{cris}} \subset \mathrm{Frac}(S)$. We show that if $\alpha \in S$ is not zero, then $\alpha \log[\varpi] \notin S$, which is sufficient for the lemma.

Since S is separated by the p-adic topology, it suffices to show that if $r \in \mathbb{N}$ and $\alpha \in S - pS$, then $p^r\alpha u \notin S$. If $a \in W(R)$ satisfies $\theta(a) \in p\mathcal{O}_C$, then $a \in (p,\xi)W(R)$ and hence $a \in pS$. Therefore one can find $i \geq 0$ and $b_n \in W(R)$ such that $\theta(b_i) \notin \mathcal{O}_C$ and

$$\alpha = \underbrace{p\Big(\sum_{0\leq n<i} b_n\beta^n\Big)}_{A} + \underbrace{\sum_{n\geq i} b_n\beta^n}_{B}.$$

Note that $\log[\varpi] = -\sum \beta^n/n$. Suppose $j > r$ is an integer such that $p^j > i$. If $p^r\alpha u \in S$, one has $\alpha \cdot \sum\limits_{n>0} p^{j-1}\beta^n/n \in S$. Note that $\alpha \cdot \sum\limits_{0<n<p^j} p^{j-1}\beta^n/n \in S$, then

$$A \cdot \sum_{n\geq p^j} p^{j-1}\beta^n/n \in \mathrm{Fil}^{p^{j+1}} B_{\mathrm{dR}}, \quad B \cdot \sum_{n>p^j} p^{j-1}\beta^n/n \in \mathrm{Fil}^{i+p^j+1} B_{\mathrm{dR}}$$

and

$$\beta^{p^j}/p \cdot \sum_{n>i} b_n\beta^n \in \mathrm{Fil}^{i+p^j+1} B_{\mathrm{dR}},$$

thus

$$b_i\beta^{i+p^j}/p \in \mathrm{Fil}^{i+p^j} B_{\mathrm{dR}} \cap (S + \mathrm{Fil}^{i+p^j+1} B_{\mathrm{dR}}) = \mathrm{Fil}^{i+p^j} S + \mathrm{Fil}^{i+p^j+1} B_{\mathrm{dR}}.$$

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). If $\log[\varpi]$ is not transcendental, suppose $c_0 + c_1X + \cdots + c_{d-1}X^{d-1} + X^d$ is the minimal polynomial of $\log[\varpi]$ in C_{cris}. For $g \in G_{K_0}$, we have $g([\varpi]/p) = ([\varpi]/p) \cdot [\varepsilon]^{\chi(g)}$ where χ is the cyclotomic character, thus

$$g \log[\varpi] = \log[\varpi] + \chi(g)t.$$

Since C_{cris} is stable by G_{K_0} and for every $g \in G_{K_0}$,

$$g(c_0) + \cdots + g(c_{d-1})(\log[\varpi] + \chi(g)t)^{d-1} + (\log[\varpi] + \chi(g)t)^d = 0.$$

By the uniqueness of minimal polynomial, for every $g \in G_{K_0}$, $g(c_{d-1}) + d \cdot \chi(g)t = c_{d-1}$. If let $c = c_{d-1} + d\log[\varpi]$, one has $g(c) = c$, then $c \in (B_{\mathrm{dR}})^{G_{K_0}} = K_0 \subset B_{\mathrm{cris}}$ and thus $\log[\varpi] = d^{-1}(c - c_{d-1}) \in C_{\mathrm{cris}}$, which contradicts Lemma 6.12. □

As an immediate consequence of Proposition 6.11, we have

Theorem 6.13. *The homomorphism of B_{cris}-algebras*

$$\begin{aligned} B_{\mathrm{cris}}[x] &\longrightarrow B_{\mathrm{st}} \\ x \quad &\longmapsto \log[\varpi] \end{aligned}$$

is an isomorphism.

Theorem 6.14. *(1) $(C_{\mathrm{st}})^{G_K} = K_0$, thus*

$$(B^+_{\mathrm{cris}})^{G_K} = (B_{\mathrm{cris}})^{G_K} = (B_{\mathrm{st}})^{G_K} = K_0.$$

(2) The map

$$\begin{aligned} K \otimes_{K_0} B_{\mathrm{st}} \to &\quad B_{\mathrm{dR}} \\ \lambda \otimes b \mapsto &\quad \lambda b. \end{aligned}$$

is injective.

Proof. Note that $\mathrm{Frac}(K \otimes_{K_0} B_{\mathrm{cris}})$ is a finite extension over C_{cris}, thus $\log[\varpi]$ is transcendental over $\mathrm{Frac}(K \otimes_{K_0} B_{\mathrm{cris}})$. Therefore

$$K \otimes_{K_0} B_{\mathrm{st}} = K \otimes_{K_0} B_{\mathrm{cris}}[\log[\varpi]] = (K \otimes_{K_0} B_{\mathrm{cris}})[\log[\varpi]]$$

and (2) is proved.

For (1), we know that

$$\begin{aligned} &W(R)^{G_K} = W(R^{G_K}) = W(k) = W, \\ &\big(W(R)[\frac{1}{p}]\big)^{G_K} = K_0 = W[\frac{1}{p}], \end{aligned}$$

and

$$W(R)[\frac{1}{p}] \subset B^+_{\mathrm{cris}},$$

then

$$K_0 \subset (B^+_{\mathrm{cris}})^{G_K} \subset (B_{\mathrm{cris}})^{G_K} \subset (B_{\mathrm{st}})^{G_K} \subset (C_{\mathrm{st}})^{G_K} \subset (B_{\mathrm{dR}})^{G_K} = K.$$

Thus (1) follows from (2). □

The operators φ and N on B_{st}.

We extend φ to an endomorphism of B_{st} by requiring

$$\varphi(\log[\varpi]) = p\log[\varpi].$$

Then φ commutes with the action of G_K.

Definition 6.15. *The* monodromy operator

$$\begin{aligned} N : B_{\mathrm{st}} &\longrightarrow B_{\mathrm{st}} \\ \sum_{n\in\mathbb{N}} b_n(\log[\varpi])^n &\longmapsto -\sum_{n\in\mathbb{N}} nb_n(\log[\varpi])^{n-1} \end{aligned}$$

is the unique B_{cris}-derivation such that $N(\log[\varpi]) = -1$.

As a consequence of Theorem 6.13, we have

Proposition 6.16. *The sequence*

$$0 \longrightarrow B_{\mathrm{cris}} \longrightarrow B_{\mathrm{st}} \xrightarrow{N} B_{\mathrm{st}} \longrightarrow 0 \qquad (6.10)$$

is exact.

Proposition 6.17. *The monodromy operator N satisfies:*
(1) $gN = Ng$ for every $g \in G_{K_0}$;
(2) $N\varphi = p\varphi N$.

Proof. Using $g(\log[\varpi]) = \log[\varpi]+\chi(g)t$, and $N(\chi(g)t) = 0$ since $\chi(g)t \in B_{\mathrm{cris}}$, we get that

$$N(gb) = g(Nb), \text{ for all } b \in B_{\mathrm{st}}, g \in G_{K_0}.$$

Since

$$\begin{aligned} N\varphi(\sum_{n\in\mathbb{N}} b_n(\log[\varpi])^n) =& N(\sum_{n\in\mathbb{N}} \varphi(b_n)p^n(\log[\varpi])^n) \\ =& \sum_{n\in\mathbb{N}} n\varphi(b_n)p^n(\log[\varpi])^{n-1} \\ =& p\varphi N(\sum_{n\in\mathbb{N}} b_n(\log[\varpi])^n), \end{aligned}$$

we have $N\varphi = p\varphi N$. □

6.2 Some properties about B_{cris}.

6.2.1 Some ideals of $W(R)$.

For every subring A 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}), and for every $r \in \mathbb{Z}$, we let $\mathrm{Fil}^r A = A \cap$

$\mathrm{Fil}^r B_{\mathrm{dR}}$. In particular, one has $\mathrm{Fil}^0 A = A \cap B^+_{\mathrm{dR}}$ and denotes $\theta : \mathrm{Fil}^0 A \to C$ the restriction of the projection $B^+_{\mathrm{dR}} \to C$.

If A is a subring of B_{cris} stable by φ, and if $r \in \mathbb{Z}$, we let $I^{[r]}A = \{a \in A \mid \varphi^n(A) \in \mathrm{Fil}^r A \text{ for } n \in \mathbb{N}\}$. 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. In this case we also write $I^{[1]}A = IA$.

For any $x \in W(R)$, we write $x' = \varphi^{-1}(x)$, we also denote $\bar{x} \in R$ the reduction of x modulo p. Then for $\pi_\varepsilon = [\varepsilon] - 1$, one has $\pi'_\varepsilon = [\varepsilon'] - 1$. Write $\pi_\varepsilon = \pi'_\varepsilon \cdot \tau$ where $\tau = 1 + [\varepsilon'] + \cdots + [\varepsilon]^{p-1}$. Note that $\theta(\tau) = \sum\limits_{0 \leq i \leq p-1} (\varepsilon^{(1)})^i = 0$ and

$$\bar{\tau} = 1 + \varepsilon' + \cdots + \varepsilon'^{p-1} = \frac{\varepsilon - 1}{\varepsilon' - 1}$$

and $v(\bar{\tau}) = \frac{p}{p-1} - \frac{1}{p-1} = 1$, therefore τ is a generator of $\mathrm{Ker}\,\theta$.

Proposition 6.18. *For every $r \in \mathbb{N}$,*

(1) The ideal $I^{[r]}W(R)$ is the principal ideal generated by π_ε^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 the 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 6.19. *(1) The ideal $IW(R)$ is principal, generated by π_ε.*

(2) For every element $a = (a_0, a_1, \cdots) \in IW(R)$, a generates the ideal if and only if $v(a_0) = \frac{p}{p-1}$ and one has $v(a_n) = \frac{p}{p-1}$ 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 $m \in \mathbb{N}$,

$$\theta(\varphi^m a) = \sum p^n \alpha_n^{p^m} = \alpha_0^{p^m} + \cdots + p^m \alpha_m^{p^m} + p^{m+1}\alpha_{m+1}^{p^m} + \cdots = 0.$$

We claim that for any pair $(r, m) \in \mathbb{N} \times \mathbb{N}$, one has $v(\alpha_m) \geq p^{-m}(1 + p^{-1} + \cdots + p^{-r})$. 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 $v(\alpha_0) \geq 1$;

(b) If $r = 0$, but $m \neq 0$, one has

$$0 = \theta(p^m a) = \sum_{n=0}^{m-1} p^n \alpha_n^{p^m} + p^m \alpha_m^{p^m} \pmod{p^{m+1}};$$

by induction hypothesis, for $0 \leq n \leq m-1$, $v(\alpha_n) \geq p^{-n}$, thus $v(p^n \alpha_n^{p^m}) \geq n + p^{m-n} \geq m+1$, and $v(p^m \alpha_m^{p^m}) \leq m+1$, therefore $v(\alpha_m) \geq p^m$;

(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 $v(\alpha_m) \geq p^{-m}(1+\cdots+p^{-r}$.

Now 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 $n \in \mathbb{N}$, $\theta(\varphi^n \pi_\varepsilon) = \theta([\varepsilon]^{p^n} - 1) = 0$, thus $\pi_\varepsilon \in IW(R)$. As $v(\varepsilon - 1) = \frac{p}{p-1}$, the above claim implies that $IW(R) \subseteq (\pi_\varepsilon, p)$. But the set $(\mathcal{O}_C)^{\mathbb{N}}$ is p-torsion free, thus if $px \in IW(R)$, then $x \in W(R)$. Hence $IW(R) = (\pi_\varepsilon)$ and we have the lemma. □

Proof (Proof of the Proposition). Let $\operatorname{gr}^i W(R) = \operatorname{Fil}^i W(R)/\operatorname{Fil}^{i+1} W(R)$ and let θ^i be the projection from $\operatorname{Fil}^i W(R)$ to $\operatorname{gr}^i W(R)$. As $\operatorname{Fil}^i W(R)$ is the principal ideal generated by τ^i, $\operatorname{gr}^i W(R)$ is a free $\mathcal{O}_C$-module of rank 1 generated by $\theta^i(\tau^i) = \theta^1(\tau)^i$. Note that $\pi_\varepsilon = \pi'_\varepsilon \tau$, then
$$\varphi^n(\pi_\varepsilon) = \pi'_\varepsilon \tau^{1+\varphi+\cdots+\varphi^n} \text{ for every } n \in \mathbb{N}.$$

For $i \geq 1$, $\theta(\varphi^i(\tau)) = p$, hence $\theta^1(\varphi^n(\pi_\varepsilon)) = p^n(\varepsilon^{(1)} - 1) \cdot \theta^1(\tau)$.

Proof of (1): The inclusion $\pi_\varepsilon^r W(R) \subseteq I^{[r]}$ is clear. We show $\pi_\varepsilon^r W(R) \supseteq I^{[r]}$ 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 $a = \pi_\varepsilon^{r-1} b$ with $b \in W(R)$. We know that $\theta^{r-1}(\varphi^n(a)) = 0$ for every $n \in \mathbb{N}$. But
$$\theta^{r-1}(\varphi^n(a)) = \theta(\varphi^n(b)) \cdot (\theta^1(\varphi^n(\pi_\varepsilon)))^{r-1} = (p^n(\varepsilon^{(1)} - 1))^{r-1} \cdot \theta(\varphi^n(b)) \cdot \theta^1(\tau)^{r-1}.$$

Since $\theta^1(\tau)^{r-1}$ is a generator of $\operatorname{gr}^{r-1} W(R)$ 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 $b = \pi_\varepsilon c$. Thus $a \in \pi_\varepsilon^r W(R)$.

Proof of (2): It follows immediately from that $v(\overline{\pi_\varepsilon^r}) = rv(\varepsilon - 1) = \frac{rp}{p-1}$, and that $x \in W(R)$ is a unit if and only if $\bar{x}$ is a unit in R, i.e. if $v(\bar{x}) = 0$. □

6.2.2 A description of A_{cris}.

For every $n \in \mathbb{N}$, we write $n = r(n) + (p-1)q(n)$ with $r(n), q(n) \in \mathbb{N}$ and $0 \leq r(n) < p-1$. Let
$$t^{\{n\}} = t^{r(n)} \gamma_{q(n)}(t^{p-1}/p) = (p^{q(n)} \cdot q(n)!)^{-1} \cdot t^n.$$

Note that if $p = 2$, $t^{\{n\}} = t^n/(2^n n!)$. We have shown that $t^{p-1}/p \in A_{\text{cris}}$, therefore $t^{\{n\}} \in A_{\text{cris}}$. Let Λ_ε be a subring of $K_0[[t]]$ formed by elements of the form $\sum\limits_{n \in \mathbb{N}} a_n t^{\{n\}}$ with $a_n \in W = W(k)$ converging p-adically to 0. Let

$S_\varepsilon = W[[\pi_\varepsilon]]$ be the ring of power series of π_ε with coefficients in W. One can identify S_ε as a sub-W-algebra of Λ_ε, since

$$\pi_\varepsilon = e^t - 1 = \sum_{n\geq 1} \frac{t^n}{n!} = \sum_{n\geq 1} c_n t^{\{n\}},$$

where $c_n = p^{q(n)}q(n)!/n!$, by a simple calculation, c_n tends to 0 as n tends to infinity.

Both S_ε and Λ_ε are subrings of A_{cris}, stable by the actions of φ and of G_{K_0} which factors through $\Gamma'_{K_0} = \text{Gal}(K_0^{cyc}/K_0)$. We see that

$$t = \log([\varepsilon]) = \pi_\varepsilon \cdot \sum_{n\geq 0}(-1)^n \frac{\pi_\varepsilon^n}{n+1} = \pi_\varepsilon \cdot u,$$

where u is a unit in Λ_ε.

Recall Δ_{K_0} is the torsion subgroup of Γ'_{K_0}. Then the subfield of $K_0((t))$ fixed by Δ_{K_0} is $K_0((t^{p-1}))$ (resp. $K((t^2))$ if $p = 2$). As a result, the ring Λ, the subring of Λ_ε fixed by Δ_{K_0}, is formed by $\sum a_n t^{\{n\}}$ with $a_n = 0$ if $p-1 \nmid n$ (resp. if $2 \nmid n$).

Let π_0 be the trace from $K_0((t))$ to $K_0((t^{p-1}))$ (resp. $K_0((t^2))$ if $p = 2$) of π_ε, then

$$\pi_0 = (p-1) \sum_{\substack{n\geq 1\\ p-1|n}} \frac{t^n}{n!} \quad (\text{resp. } 2\sum_{\substack{n\geq 1\\ 2|n}} \frac{t^n}{n!}).$$

One sees that the ring S, the subring of S_ε fixed by Δ_{K_0}, is then the ring of power series $W[[\pi_0]]$. One can easily check that $\pi_0 \in p\Lambda$ (resp. 8Λ), and there exists $v \in \Lambda$ such that $\pi_0/p = v \cdot (t^{p-1}/p)$ (resp. $\pi_0/8 = v \cdot (t^2/8)$). One can also see the evident identification $S_\varepsilon \otimes_S \Lambda = \Lambda_\varepsilon$.

let $q = p + \pi_0$ and let $q' = \varphi^{-1}(q)$. Then $q = \sum_{a\in\mathbb{F}_p} [\varepsilon]^{[a]}$ (resp. $[\varepsilon] + [\varepsilon]^{-1}$) where $[a]$ is the Teichmüller representative of a.

Proposition 6.20. *With the precedent notations,*

(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 $u \in S$ such that

$$\varphi\pi_0 = u\pi_0 q^{p-1} \textit{ if } p \neq 2 \ (\textit{resp. } u\pi_0 q^2 \textit{ if } p = 2).$$

Proof. The case of $p \neq 2$ and $p = 2$ are analogous, we just show the case $p \neq 2$.

Proof of (1): Let π be the norm of π_ε over the field extension $K_0((t))/K_0((t^{p-1}))$. One has

$$\pi_1 = \prod_{h\in\Delta_{K_0}} h(\pi_\varepsilon) = \prod_{a\in\mathbb{F}_p^*} ([\varepsilon]^{[a]} - 1).$$

By Proposition 6.18, since $[\varepsilon]^{[a]} - 1$ is a generator of $IW(R)$, π_1 is a generator of $I^{[p-1]}W(R)$, one has $v(\overline{\pi_1}) = (p-1)\frac{p}{p-1} = p = v(\overline{\pi_0})$. Therefore one has

$W[[\pi_0]] = W[[\pi_1]]$. We can write $\pi_0 = \sum a_m \pi_1^m$ with $a_m \in W$ and a_1 is a unit. Moreover, since $a_0 = \theta(\pi_0) = a_0$, π_0 generates the same ideal as π_1.

Proof of (2): Note that q' and τ are two generators of the kernel of the restriction of θ to $S'_\varepsilon = \varphi^{-1}(S_\varepsilon) = W[[\pi'_\varepsilon]]$, thus

$$\pi_\varepsilon = \varphi\pi'_\varepsilon = \pi'_\varepsilon\tau = u'_1\pi'_\varepsilon q'$$

with u'_1 a unit in S'_ε. Then $\varphi\pi_\varepsilon = u_1\pi_\varepsilon q$ and $\varphi(\pi_\varepsilon^{p-1}) = u_1^{p-1}\pi_\varepsilon^{p-1}q^{p-1}$. Since π_0 and π_ε^{p-1} are two generators of $S_\varepsilon \cap I^{[p-1]}W(R)$, $\varphi(\pi_0) = u\pi_0 q^{p-1}$ with u a unit in S_ε. Now the uniqueness of u and the fact that $S = S_\varepsilon^{\Delta_{K_0}}$ imply that u and $u^{-1} \in S$. □

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 6.21. *One has an isomorphism of $W(R)$-algebras*

$$\alpha : \quad W(R)\widehat{\otimes}_S \Lambda \longrightarrow A_{\mathrm{cris}}$$

which is continuous by p-adic topology, given by

$$\alpha(\sum a_m \otimes \gamma_m(\frac{\pi_0}{p}) = \sum a_m\gamma_m(\frac{\pi_0}{p}).$$

The isomorphism α thus induces an isomorphism

$$\alpha_\varepsilon : \quad W(R)\widehat{\otimes}_{S_\varepsilon}\Lambda_\varepsilon \longrightarrow A_{\mathrm{cris}}.$$

Proof. The isomorphism α_ε comes from

$$W(R)\widehat{\otimes}_{S_\varepsilon}\Lambda_\varepsilon \cong W(R)\widehat{\otimes}_{S_\varepsilon}S_\varepsilon \otimes_s \Lambda \cong W(R)\widehat{\otimes}_S\Lambda$$

and the isomorphism α. We only consider the case $p \neq 2$ ($p = 2$ is analogous).

Certainly the homomorphism α is well defined and continuous as $\frac{\pi_0}{p} \in \mathrm{Fil}^1 A_{\mathrm{cris}}$, 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_{cris} modulo p is the divided power envelope of R relative to an ideal generated by $\overline{q'}$, thus it is the free module over $R/\overline{q'^p}$ with base the images of $\gamma_{pm}(q')$ or $\gamma_m(\frac{q'^p}{p})$. 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_{cris} modulo p is the free module over $R/\overline{\pi_0}$ with base the images of $\gamma_m(\frac{\pi_0}{p})$. It is clear this is also the case for the ring $W(R)\widehat{\otimes}_S\Lambda$ modulo p. □

6.2.3 The filtration by $I^{[r]}$.

Proposition 6.22. *For every $r \in \mathbb{N}$, suppose $I^{[r]} = I^{[r]} A_{\text{cris}}$. 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

$$\varphi(bt^{\{r-1\}}) = p^{(r-1)n} \cdot \varphi^n(b) \cdot t^{\{r-1\}} = c_{r,n} \cdot \varphi^n(b) \cdot t^{r-1}$$

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 π_ε. Thus $bt^{\{r-1\}}$ belongs to an ideal of A_{cris} generated by $\pi_\varepsilon t^{\{r-1\}}$. But in A_{cris}, t and π_ε generate the same ideal as $t = \pi_\varepsilon \times$ (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

$$A^r_{\text{cris}} = A/I^{[r]}, \quad W^r(R) = W(R)/I^{[r]}W(R).$$

Proposition 6.23. *For every $r \in \mathbb{N}$, A^r_{cris} and $W^r(R)$ are of no p-torsion. The natural map*

$$\iota^r : \quad W^r(R) \longrightarrow A^r_{\text{cris}}$$

are injective and its cokernel is p-torsion, annihilated by $p^m m!$ where m is the largest integer such that $(p-1)m < r$.

Proof. For every $r \in \mathbb{N}$, $A_{\text{cris}}/\operatorname{Fil}^r A_{\text{cris}}$ is torsion free. The kernel of the map

$$A_{\text{cris}} \to (A_{\text{cris}}/\operatorname{Fil}^r A_{\text{cris}})^{\mathbb{N}} \quad x \mapsto (\varphi^n x \bmod \operatorname{Fil}^r)_{n\in\mathbb{N}}$$

is nothing by $I^{[r]}$, thus

$$A^r_{\text{cris}} \hookrightarrow (A_{\text{cris}}/\operatorname{Fil}^r A_{\text{cris}})^{\mathbb{N}}$$

is torsion free. As ι^r is injective by definition, $W^r(R)$ is also torsion free.

As $W(R)$-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. □

For every subring A of A_{cris} and for $n \in \mathbb{N}$, write

$$\operatorname{Fil}^r A = A \cap \operatorname{Fil}^r A_{\mathrm{cris}}, \quad \operatorname{Fil}^r_p A = \{a \in \operatorname{Fil}^r A \mid \varphi x \in p^r A\}.$$

Proposition 6.24. *For every $r \in \mathbb{N}$,*

(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) for m the largest integer such that $(q-1)m < r$, 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 $a_n \in W(R)$, it is nothing but to 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 $x \in \operatorname{Fil}^r A_{\mathrm{cris}}$, then by Proposition 6.23, one can write

$$p^m m! x = y + z, \ y \in W(R), \ z \in I^{[r]}.$$

Since $y \in I^{[r]}$, one sees that $y \in \operatorname{Fil}^r W(R) = q'^r W(R) \subseteq N$. The assertion follows since we also have $z \in I^{[r]} \subseteq N$. □

Theorem 6.25. *(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 $n \in \mathbb{N}$, $\varpi^n(x) = p^{-nr-j}t^{-r}\varphi^n(y)$, 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

$$v(c_m) \geq (m+r)(1 - \frac{1}{p-1} - \frac{1}{(p-1)^2}).$$

If $p \neq 2$, it is an 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 6.24.

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. □

Let $B_e = \{b \in B_{\mathrm{cris}}, \varphi b = b\}$, which is a sub-ring of B_{cris} containing $\mathbb{Q}_p$. Note that $u \in U$ means that $u \in B^+_{\mathrm{cris}}, \varphi u = pu$, thus $\frac{u}{t} \in B_e$. One can show that B_e is generated by $\frac{u}{t}$, $u \in U$ as a $\mathbb{Q}_p$-algebra.

Theorem 6.26. *(1) The sequence*

$$0 \longrightarrow \mathbb{Q}_p \longrightarrow B_{\mathrm{cris}} \cap B_{\mathrm{dR}}^+ \xrightarrow{\varphi-1} B_{\mathrm{cris}} \longrightarrow 0$$

is exact.

(2) The sequence

$$0 \longrightarrow B_e \longrightarrow B_{\mathrm{cris}} \xrightarrow{\varphi-1} B_{\mathrm{cris}} \longrightarrow 0$$

is exact.

(3) The sequence

$$0 \longrightarrow \mathbb{Q}_p \hookrightarrow B_e \longrightarrow B_{\mathrm{dR}}/B_{\mathrm{dR}}^+ \longrightarrow 0$$

is exact.

Remark 6.27. The third exact sequence is the so-called *fundamental exact sequence*, which means that

(a) $\mathbb{Q}_p = B_e \cap B_{\mathrm{dR}}^+$,
(b) $B_{\mathrm{dR}} = B_e + B_{\mathrm{dR}}^+$ (not a direct sum).

Proof. The assertion(1) is a special case of Theorem 6.25 (3). By (1), the map $\varphi - 1$ is onto on B_{cris}, i.e., for every $b \in B_{\mathrm{cris}}$, there exists $x \in B_{\mathrm{cris}}$, such that $\varphi x - x = b$. Thus (2) is exact.

For (3), we have the following diagram with exact rows and columns:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathbb{Q}_p \arrow[r] \arrow[d] & B_{\mathrm{dR}}^+ \cap B_{\mathrm{cris}} \arrow[r, "\varphi-1"] \arrow[d] & B_{\mathrm{cris}} \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & B_e \arrow[r] \arrow[d] & B_{\mathrm{cris}} \arrow[r, "\varphi-1"] \arrow[d] & B_{\mathrm{cris}} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \frac{B_e}{\mathbb{Q}_p} \arrow[r] \arrow[d] & \frac{B_{\mathrm{cris}}}{B_{\mathrm{cris}} \cap B_{\mathrm{dR}}^+} \arrow[r] \arrow[d] & 0 & \\
 & 0 & 0 & &
\end{tikzcd}$$

Then

$$B_e/\mathbb{Q}_p \cong \frac{B_{\mathrm{cris}}}{B_{\mathrm{cris}} \cap B_{\mathrm{dR}}^+} \cong \frac{B_{\mathrm{dR}}}{B_{\mathrm{dR}}^+}$$

as $B_{\mathrm{dR}} = B_{\mathrm{cris}} B_{\mathrm{dR}}^+$. □

6.3 Semi-stable p-adic Galois representations

Proposition 6.28. *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 $\mathbb{Q}_p \cdot b$ 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 6.14 (1).

For (3), since $\bar{k}$ is the residue field of R, $W(R)$ contains $W(\bar{k})$ and $W(R)[\frac{1}{p}]$ contains $P_0 := W(\bar{k})[\frac{1}{p}]$. Then B_{cris} contains P_0. 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, by multiplying 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 $g(b) = \chi(g)b$. Let $\bar{b} = \theta(b)$ be the image of $b \in C$. Then $\mathbb{Q}_p\bar{b} \cong \mathbb{Q}_p(\chi)$ is a one-dimensional $\mathbb{Q}_p$-subspace of C stable under G_K, by Sen's theory (Corollary 3.56), this implies that $\chi(I_K)$ is finite and $\bar{b} \in \overline{P} \subset B_{\mathrm{dR}}^+$. Then $b' = b - \bar{b} \in \mathrm{Fil}^i B_{\mathrm{dR}} - \mathrm{Fil}^{i+1} B_{\mathrm{dR}}$ for some $i \geq 1$. Note that $\mathbb{Q}_p b'$ is also stable by G_K whose action is defined by the same χ. Then the G_K-action on $\mathbb{Q}_p\theta(t^{-i}b')$ is defined by $\eta^{-i}\chi$ where η is the cyclotomic character. In this case $\eta^{-i}\chi(I_K)$ is not finite and it is only possible that $b' = 0$ and hence $b = \bar{b} \in \overline{P}$.

Now if $b \in B_{\mathrm{st}}$, then $b \in \overline{P} \cap B_{\mathrm{st}}$. We claim that $\overline{P} \cap B_{\mathrm{st}} = P_0 \subset B_{\mathrm{cris}}$. Indeed, suppose $\overline{P} \cap B_{\mathrm{st}} = Q \supset P_0$. 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 $\mathrm{Frac}(Q)^{G_L} = L$, contradiction! □

For any p-adic representation V, we denote

$$\mathbf{D}_{\mathrm{st}}(V) = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K}, \quad \mathbf{D}_{\mathrm{cris}}(V) = (B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

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 6.29. *A p-adic representation V of G_K is called* semi-stable *if it is B_{st}-admissible, i.e., the map $\alpha_{\mathrm{st}}(V)$ is an isomorphism.*

A p-adic representation V of G_K is called crystalline *if it is B_{cris}-admissible, i.e., the map $\alpha_{\mathrm{cris}}(V)$ is an isomorphism.*

Clearly, for any p-adic representation V, $\mathbf{D}_{\mathrm{cris}}(V)$ is a subspace of $\mathbf{D}_{\mathrm{st}}(V)$ and

$$\dim_{K_0} \mathbf{D}_{\mathrm{cris}}(V) \leq \dim_{K_0} \mathbf{D}_{\mathrm{st}}(V) \leq \dim_{\mathbb{Q}_p} V.$$

Therefore we have

Proposition 6.30. *(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.

Let V be any p-adic representation of G_K, since $K \otimes_{K_0} B_{\mathrm{st}} \to B_{\mathrm{dR}}$ is injective if $[K : K_0] < \infty$ (Theorem 6.14), 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 that V is semi-stable, then $\dim_{K_0} \mathbf{D}_{\mathrm{cris}}(V) = \dim_{\mathbb{Q}_p} V$, thus

$$\dim_K K \otimes_{K_0} \mathbf{D}_{\mathrm{cris}}(V) = \dim_{\mathbb{Q}_p} V \geq \dim \mathbf{D}_{\mathrm{dR}} V,$$

which implies that

$$\dim \mathbf{D}_{\mathrm{dR}} V = \dim_{\mathbb{Q}_p} V,$$

i.e., V is de Rham. Thus we have proved that

Proposition 6.31. *If V is a semi-stable p-adic representation of G_K, then it is de Rham. Moreover,*

$$\mathbf{D}_{\mathrm{dR}}(V) = K \otimes_{K_0} \mathbf{D}_{\mathrm{st}}(V).$$

Let V be any 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 $N\varphi = p\varphi N$. Now one can easily see that the K_0-vector space $D = \mathbf{D}_{\mathrm{st}}(V)$ is stable under φ and N, $\dim_{K_0} D < \infty$ and φ is bijective on D (One can check that φ is injective on B_{st}). Moreover, the K-vector space

$$D_K = K \otimes_{K_0} \mathbf{D}_{\mathrm{st}}(V) \subset \mathbf{D}_{\mathrm{dR}}(V)$$

is equipped with the structure of a filtered K-vector space with the induced filtration

$$\mathrm{Fil}^i D_K = D_K \bigcap \mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(V).$$

In next section, we shall see $\mathbf{D}_{\mathrm{st}}(V)$ is a *filtered* (φ, N)*-module* D over K such that $\dim_{K_0} D < \infty$ and φ is bijective on D.

Remark 6.32. By definition, a crystalline representation is a p-adic representation of G_K which is B_{cris}-admissible. Note that $B_{\mathrm{cris}} = \{b \in B_{\mathrm{st}} \mid Nb = 0\}$. Thus a p-adic representation V of G_K is crystalline if and only if V is semi-stable and $N = 0$ on $D_{\mathrm{st}}(V)$.

6.4 Filtered (φ, N)-modules

6.4.1 Definitions.

Definition 6.33. *A* (φ, N)-module *over k (or equivalently, over K_0) is a K_0-vector space D equipped with two maps*

$$\varphi, N : D \longrightarrow D$$

with the following properties:
(1) φ is semi-linear with respect to the absolute Frobenius σ on K_0.
(2) N is a K_0-linear map.
(3) $N\varphi = p\varphi N$.

A morphism $\eta : D_1 \to D_2$ between two (φ, N)-modules, is a K_0-linear map commuting with φ and N.

Remark 6.34. The map $\varphi : D \to D$ is additive, and

$$\varphi(\lambda d) = \sigma(\lambda)\varphi(d), \text{ for every } \lambda \in K_0,\ d \in D.$$

To give φ is the same as to give a K_0-linear map

$$\Phi : K_0 \,{}_{\sigma}\!\otimes_{K_0} D \to D,$$

by $\Phi(\lambda \otimes d) = \lambda\varphi(d)$.

Remark 6.35. The category of (φ, N)-modules is an abelian category. 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,

(1) There is a tensor product in this category given by

- $D_1 \otimes D_2 = D_1 \otimes_{K_0} D_2$ as K_0-vector space,
- $\varphi(d_1 \otimes d_2) = \varphi d_1 \otimes \varphi d_2$,
- $N(d_1 \otimes d_2) = Nd_1 \otimes d_2 + d_1 \otimes Nd_2$.

(2) K_0 has a structure of (φ, N)-module by $\varphi = \sigma, N = 0$. Moreover

$$K_0 \otimes D = D \otimes K_0 = D,$$

thus it is the *unit object* in the category.

(3) The full sub-category of the category of (φ, N)-modules over k such that

$$\dim_{K_0} D < \infty \text{ and } \varphi \text{ is bijective}$$

is an abelian category and is stable under tensor product.

If D is an object of this sub-category, we may define the *dual object* $D^* = \mathscr{L}(D, K_0)$ of D, the set of linear maps $\eta : D \to K_0$ such that

- $\varphi(\eta) = \sigma \circ \eta \circ \varphi^{-1}$,
- $N(\eta)(d) = -\eta(Nd)$, for all $d \in D$.

Definition 6.36. *A* filtered (φ, N)-module *over K consists of a (φ, N)-module D over K_0 and a filtration on the K-vector space $D_K = K_0 \otimes_{K_0} D$ which is decreasing, separated and exhaustive, i.e., such that* $\operatorname{Fil}^i D_K (i \in \mathbb{Z})$, *the sub K-vector spaces of D_K satisfy*

- $\operatorname{Fil}^{i+1} D_K \subset \operatorname{Fil}^i D_K$,
- $\bigcap_{i \in \mathbb{Z}} \operatorname{Fil}^i D_K = 0, \quad \bigcup_{i \in \mathbb{Z}} \operatorname{Fil}^i D_K = D_K$.

A morphism $\eta : D_1 \to D_2$ of filtered (φ, N)-modules is a morphism of (φ, N)-modules such that the induced K-linear map $\eta_K : K \otimes_{K_0} D_1 \to K \otimes_{K_0} D_2$ satisfies

$$\eta_K(\operatorname{Fil}^i D_{1K}) \subset \operatorname{Fil}^i D_{2K}, \text{ for all } i \in \mathbb{Z}.$$

The set of filtered (φ, N)-modules over K makes a category. We denote it by $\mathbf{MF}_K(\varphi, N)$.

Remark 6.37. The category $\mathbf{MF}_K(\varphi, N)$ is an additive category (but not abelian). Moreover,

(1) There is an tensor product:

$$D_1 \otimes D_2 = D_1 \otimes_{K_0} D_2$$

with φ, N as in Remark 6.35, and 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

$$\operatorname{Fil}^i (D_{1K} \otimes_K D_{2K}) = \sum_{i_1 + i_2 = i} \operatorname{Fil}^{i_1} D_{1K} \otimes_K \operatorname{Fil}^{i_2} D_{2K}.$$

(2) K_0 can be viewed as a filtered (φ, N)-module with $\varphi = \sigma$, $N = 0$ 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.

(3) If $\dim_{K_0} D < \infty$ and if φ is bijective on D, we may define the *dual object* D^* of D by

$$\begin{aligned} (D^*)_K &= K \otimes_{K_0} D^* = (D_K)^* \simeq \mathscr{L}(D_K, K), \\ \mathrm{Fil}^i (D^*)_K &= (\mathrm{Fil}^{-i+1} D_K)^*. \end{aligned}$$

6.4.2 $t_N(D)$ and $t_H(D)$.

Assume D is a (φ, N)-module over k such that $\dim_{K_0} D < \infty$ and φ is bijective. We associate an integer $t_N(D)$ to D here.

(1) 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

$$\varphi d' = \sigma(a) \lambda d = \frac{\sigma(a)}{a} \lambda d',$$

which implies

$$\lambda' = \lambda \frac{\sigma(a)}{a}.$$

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 6.38. *If D is a (φ, N)-module over k of dimension 1 such that φ is bijective, then set*

$$t_N(D) := v_p(\lambda) \tag{6.11}$$

where $\lambda \in \mathrm{GL}_1(K_0) = K_0^*$ is the matrix of φ under some basis.

Remark 6.39. The letter N in the expression $t_N(D)$ stands for the word *Newton*, not for the monodromy map $N : D \to D$.

(2) Assume $\dim_{K_0} D = h$ is arbitrary. The h-th exterior product

$$\bigwedge\nolimits_{K_0}^{h} D \subset D \otimes_{K_0} D \otimes_{K_0} \cdots \otimes_{K_0} D (h \text{ times})$$

is a one-dimensional K_0-vector space. Moreover, φ is injective(resp. surjective, bijective) on D implies that it is also injective(resp. surjective, bijective) on $\bigwedge_{K_0}^{h} D$.

Definition 6.40. *If D is a (φ, N)-module over k of dimension h such that φ is bijective, then set*

$$t_N(D) := t_N(\bigwedge\nolimits_{K_0}^{h} D). \tag{6.12}$$

Choose a basis $\{e_1, \cdots, e_h\}$ of D over K_0, such that $\varphi(e_i) = \sum_{j=1}^{h} a_{ij} e_j$. Write $A = (a_{ij})_{1 \leqslant i,j \leqslant h}$. Given another basis $\{e_1', \cdots, e_h'\}$ with the transformation matrix P, write A' the matrix of φ, then $A = \sigma(P) A' P^{-1}$. Moreover φ is injective if and only if $\det A \neq 0$, and

Proposition 6.41.

$$t_N(D) = v_p(\det A). \tag{6.13}$$

Proposition 6.42. *One has*

(1) If $0 \to D' \to D \to D'' \to 0$ is a short exact sequence of (φ, N)-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 $\{e_1, \cdots, e_{h'}\}$ of D' and extend it to a basis $\{e_1, \cdots, e_h\}$ of D, then $\{\bar{e}_{h'+1}, \cdots, \bar{e}_h\}$ 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 $A \otimes B = (a_{i_1,i_2} B)$. 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 $t_N(D^*) = v_p(\det \sigma(A^{-1})) = -v_p(\det A) = -t_N(D)$. □

Proposition 6.43. *If D is a (φ, N)-module such that $\dim_{K_0} D < \infty$ and φ is bijective, then 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 $D' = N^h(D)$ 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 surjective.

Pick a basis of D' and suppose under this basis, the matrices of φ and N are A and B respectively. By $N\varphi = p\varphi N$ we have $BA = pA\sigma(B)$. Thus $v_p(\det(B)) = 1 + v_p(\det(\sigma(B))) = 1 + v_p(\det(B))$, this is impossible. □

Now let $\mathbf{Fil}_K$ be the category of finite-dimensional filtered K-vector spaces.

Definition 6.44. *Suppose $\Delta \in \mathbf{Fil}_K$ is a finite dimensional filtered K-vector space.*

(1) If $\dim_K \Delta = 1$, define

$$t_H(\Delta) := \max\{i \in \mathbb{Z} : \mathrm{Fil}^i \Delta = \Delta\}. \tag{6.14}$$

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

$$t_H(\Delta) := t_H(\bigwedge\nolimits_K^h \Delta), \tag{6.15}$$

where $\bigwedge_K^h \Delta \subset \Delta \otimes_{K_0} \Delta \otimes_{K_0} \cdots \Delta$ (h times) is the h-th exterior algebra of Δ with the induced filtration.

There is always a basis $\{e_1, \cdots, e_h\}$ of Δ over K which is adapted to the filtration, i.e., there exists $i_1, \cdots, i_h \in \mathbb{Z}$ such that for any integer i,

$$\mathrm{Fil}^i(\Delta) = \bigoplus_{i_j \geqslant i} K e_{i_j}.$$

Then

$$t_H(\Delta) = \sum_{j=1}^{h} i_j.$$

Proposition 6.45. *One has*

$$t_H(\Delta) = \sum_{i \in \mathbb{Z}} i \cdot \dim_K \mathrm{gr}^i \Delta \tag{6.16}$$

with $\mathrm{gr}^i \Delta = \mathrm{Fil}^i \Delta / \mathrm{Fil}^{i+1} \Delta$ by definition.

By the proposition, the definition of $t_H(\Delta)$ is compatible with the filtration, therefore

Corollary 6.46. *If $0 \to \Delta' \to \Delta \to \Delta'' \to 0$ is a short exact sequence of filtered K-vector spaces, then*

$$t_N(\Delta) = t_N(\Delta') + t_N(\Delta'').$$

Remark 6.47. We have a similar formula for $t_N(D)$ like (6.16). Let D be a (φ, N)-module such that $\dim_{K_0} D < \infty$ and φ is bijective on D. In this case D is called a *φ-isocrystal* over K. Then

$$D = \bigoplus_{\alpha \in \mathbb{Q}} D_\alpha,$$

where D_α is the part of slope α. If k is algebraically closed and if $\alpha = \frac{r}{s}$ with $r, s \in \mathbb{Z}, s \geqslant 1$, then D_α is the sub K_0-vector space generated by the $d \in D$'s such that $\varphi^s d = p^r d$. The sum is actually a finite sum. Then

$$t_N(D) = \sum_{\alpha \in \mathbb{Q}} \alpha \dim_{K_0} D_\alpha. \tag{6.17}$$

It is easy to check that $\alpha \dim_{K_0} D_\alpha \in \mathbb{Z}$.

6.4.3 Admissible filtered (φ, N)-modules.

Let D be a filtered (φ, N)-module D over K, we set

$$t_H(D) = t_H(D_K). \tag{6.18}$$

Recall a sub-object D' of D is a sub K_0-vector space stable under (φ, N), and with filtration given by $\mathrm{Fil}^i D'_K = \mathrm{Fil}^i D_K \cap D'_K$.

Definition 6.48. *A filtered (φ, N)-module D over K is called* admissible *if $\dim_{K_0} D < \infty$, φ is bijective on D and*

(1) $t_H(D) = t_N(D)$,

(2) For any sub-object D', $t_H(D') \leq t_N(D')$.

Remark 6.49. 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 admissibility is equivalent to that

(1) $t_H(D) = t_N(D)$,

(2) $t_H(D'') \geq t_N(D'')$, for any quotient 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.

Proposition 6.50. *The category $\mathbf{MF}_K^{ad}(\varphi, N)$ is abelian. More precisely, if D_1 and D_2 are two objects of this category 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). 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, $\mathrm{Im}(\eta) \overset{\sim}{\to} \mathrm{CoIm}(\eta)$ 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 6.51. If D is an object of the category $\mathbf{MF}_K^{ad}(\varphi, N)$, then a sub-object D' is something isomorphic to $\mathrm{Ker}\,(\eta : D \to D_2)$ for another admissible filtered (φ, N)-module D_2. Therefore a sub-object is a sub K_0-vector space D' which is stable under (φ, N) and satisfies $t_H(D') = t_N(D')$.

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 $t_H(D') < t_N(D')$.

6.5 Statement of Theorem A and Theorem B

6.5.1 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 consider the filtered (φ, N)-module $B_{\mathrm{st}} \otimes D$, with the tensor product in the category of filtered (φ, N)-modules. Then

$$\begin{aligned} &B_{\mathrm{st}} \otimes D = B_{\mathrm{st}} \otimes_{K_0} D, \\ &\varphi(b \otimes d) = \varphi b \otimes \varphi d, \\ &N(b \otimes d) = Nb \otimes d + b \otimes Nd. \end{aligned}$$

Since

$$K \otimes_{K_0} (B_{\mathrm{st}} \otimes D) = (K \otimes_{K_0} (B_{\mathrm{st}}) \otimes_K D_K) \subset B_{\mathrm{dR}} \otimes_K D_K,$$

$K \otimes_{K_0} (B_{\mathrm{st}} \otimes D)$ is equipped with the induced filtration from $B_{\mathrm{dR}} \otimes_K D_K$. 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 6.52.

$$\mathbf{V}_{\mathrm{st}}(D) = \{v \in B_{\mathrm{st}} \otimes D \mid \varphi v = v, Nv = 0, 1 \otimes v \in \mathrm{Fil}^0(K \otimes_{K_0} (B_{\mathrm{st}} \otimes D))\}.$$

$\mathbf{V}_{\mathrm{st}}(D)$ is a sub $\mathbb{Q}_p$-vector space of $B_{\mathrm{st}} \otimes D$, stable under G_K.

Theorem A. *(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 $\mathbf{D}_{\mathrm{st}} : \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K) \longrightarrow \mathbf{MF}^{ab}_K(\varphi, N)$ is an equivalence of categories and $\mathbf{V}_{\mathrm{st}} : \mathbf{MF}^{ab}_K(\varphi, N) \longrightarrow \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K)$ is a quasi-inverse of $\mathbf{D}_{\mathrm{st}}$. Moreover, they are compatible with tensor product, dual, etc.

Complements:

(1) $\mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K)$ is a sub-Tannakian category of $\mathbf{Rep}_{\mathbb{Q}_p}(G_K)$.
(2) (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 A, $\mathbf{MF}^{ad}_K(\varphi, N)$ is stable under tensor product and dual.

Remark 6.53. (1) One can prove directly (without using Theorem A) 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 for the case $N = 0$ on D_1 and D_2. Later on, Totaro [Tot96] proved the general case.

(2) 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 A splits into two parts: Proposition A1 and Proposition A2.

Proposition A1. *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 6.54. If Proposition A1 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 $D \simeq \mathbf{D}_{\mathrm{st}}(V)$. 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 A2. *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 $\mathbf{D}_{\mathrm{st}}(V) \simeq D$.*

Remark 6.55. The first proof of Proposition A2 is given by Colmez and Fontaine ([CF00]) in 2000. It was known as the conjecture *weakly admissible implies admissible.* In the old terminology, weakly admissible means admissible in our course, and admissible means ? as in Exercise 6.54.

6.5.2 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 6.56. *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 6.57. 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} are the same.

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.

$$\dim_K \Delta^J = \dim_{K'} \Delta^J = \dim_{\mathbb{Q}_p} V,$$

and hence V is B-admissible. We have the following proposition:

Proposition 6.58. *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 6.59. *(1) A p-adic representation of G_K is K'-*semi-stable *if it is semi-stable as a $G_{K'}$-representation.*

(2) A p-adic representation of G_K is 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.

The converse is also true.

Theorem B. *Any de Rham representation of G_K is potentially semi-stable.*

Remark 6.60. Theorem B 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.

In next chapter we will give parallel proofs of Theorem A and Theorem B relying of the fundamental lemma in p-adic Hodge theory by Colmez and Fontaine.

Comments about Theorem B.

(1) Let K' be a finite Galois extension of K contained in $\overline{K}$, $J = \mathrm{Gal}(K'/K)$. Assume V is a p-adic representation of G_K which is K'-semi-stable. Then

$$\mathbf{D}_{\mathrm{st},K'}(V) = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_{K'}}$$

is an admissible filtered (φ, N)-module over K'.

Write $K_0' = \mathrm{Frac}(W(k'))$, where k' is the residue field of K'. Then $B_{\mathrm{st}}^{G_{K'}} = K_0'$. J acts on $D' = \mathbf{D}_{\mathrm{st},K'}(V)$ semi-linearly with respect to the action of J on K_0', and this action commutes with those of φ and N. In this way, D' is a (φ, N, J)*-module.* The action of J is also semi-linear with respect to the action of J on K_0': for $I(K'/K)$ the inertia subgroup of J, $\mathrm{Gal}(K_0'/K_0) = J/I(K'/K)$, if $\tau \in J$, $\lambda \in K_0'$ and $\delta \in D'$, then $\tau(\lambda\delta) = \tau(\lambda)\tau(\delta)$.

Let $\mathbf{D}_{\mathrm{dR},K'}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_{K'}}$. As an exercise, one can check that

$$\mathbf{D}_{\mathrm{dR},K'}(V) = K' \otimes_{K_0'} D',$$

and hence

$$\mathbf{D}_{\mathrm{dR}}(V) = (K' \otimes_{K_0'} D')^J.$$

The group $J = G_K/G_{K'}$ acts naturally on $(B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p})^{G_{K'}}$, and on $K' \otimes_{K_0'} D'$, J acts by $\tau(\lambda \otimes d') = \tau(\lambda) \otimes \tau(d')$ for $\lambda \in K'$ and $d' \in D'$. These two actions are equivalent.

Definition 6.61. *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 space 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.

Going to the limit over K' and using Theorem B, we get

Proposition 6.62. *There is an equivalence of categories between de Rham representations of G_K and admissible filtered (φ, N, G_K)-modules over K.*

(2) We have analogy with ℓ-adic representations. If $\ell \neq p$, an l-adic representation V of G_K is *potentially semi-stable* if there exists an open subgroup of the inertia subgroup which acts unipotently.

(3) 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 B is equivalent to say that there exists a finite extension K' of K contained in $\overline{K}$ such that $(b_{ij}) \in GL_h(K' \otimes_{K_0'} B_{\mathrm{st}})$.

7

Proof of Theorem A and Theorem B

This chapter is devoted to the proofs of Theorem A and Theorem B.

Theorem A. *(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 $\mathbf{D}_{\mathrm{st}} : \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K) \longrightarrow \mathbf{MF}^{ab}_K(\varphi, N)$ is an equivalence of categories and $\mathbf{V}_{\mathrm{st}} : \mathbf{MF}^{ab}_K(\varphi, N) \longrightarrow \mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_p}(G_K)$ is a quasi-inverse. Moreover, they are compatible with tensor product, dual, etc.

Theorem B. *Any de Rham representation of G_K is potentially semi-stable.*

7.1 Admissible filtered (φ, N)-modules of dimension 1 and 2

7.1.1 Hodge and Newton polygons.

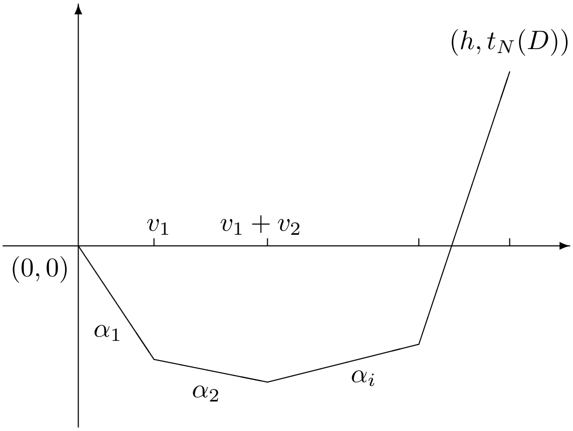
We give an alternative description of the condition of admissibility.

Let D be a filtered (φ, N)-module over K. We have defined $t_N(D)$ which depends only on the map φ on D and $t_H(D)$ which depends only on the filtration on D_K.

To D we can 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.

We know $D = \oplus_{\alpha\in\mathbb{Q}} D_\alpha$, where D_α is the part of D of slope $\alpha \in \mathbb{Q}$. Suppose $\alpha_1 < \alpha_2 < \cdots \alpha_m$ are all α's such that $D_\alpha \neq 0$. Write $v_j = \dim D_{\alpha_j}$.

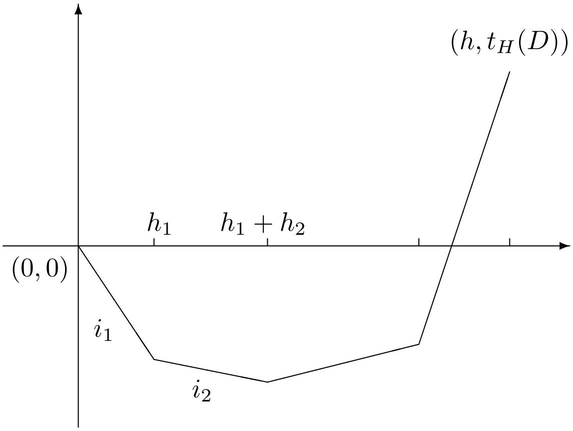
Definition 7.1. *The* Newton polygon *$P_N(D)$ is the polygon with break points $(0,0)$ and $(v_1 + \cdots + v_j, \alpha_1 v_1 + \cdots + \alpha_j v_j)$ for $1 \leq j \leq m$. Thus the end point of $P_N(D)$ is just $(h, t_N(D))$.*



The Newton Polygon $P_N(D)$

The Hodge polygon $P_H(D)$ is defined similarly. Let $i_1 < \cdots < i_m$ be those i's satisfying $\mathrm{Fil}^i D_K / \mathrm{Fil}^{i+1} D_K \neq 0$. Let $h_j = \dim_K(\mathrm{Fil}^{i_j} D_K / \mathrm{Fil}^{i_j+1} D_K)$.

Definition 7.2. *The* Hodge polygon $P_H(D)$ *is the 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* $P_H(D)$ *is just* $(h, t_H(D))$.



The Hodge Polygon $P_H(D)$

Proposition 7.3. *Let D be a filtered (φ, N)-module over K such that* $\dim_{K_0} D < +\infty$ *and φ is bijective on D. Then D is admissible if and only if the following two conditions are satisfied*

(1) For any subobjects D', $P_H(D') \leq P_N(D')$.
(2) $P_H(D)$ and $P_N(D)$ end up at the same point, i.e., $t_N(D) = t_H(D)$.

Remark 7.4. Note that $\alpha \dim_{K_0} D_\alpha \in \mathbb{Z}$. Therefore the break points of $P_H(D)$ and $P_N(D)$ have integer coordinates.

7.1.2 The case when the filtration is trivial.

Let Δ be a filtered K-vector space. We say that the filtration on Δ is *trivial* if

$$\operatorname{Fil}^0 \Delta = \Delta \text{ and } \operatorname{Fil}^1 \Delta = 0.$$

Question 7.5. What are the admissible filtered (φ, N)-modules with trivial filtration?

Let D be a filtered (φ, N)-module over K with dimension $h < \infty$ over K_0 such that φ is bijective.

Assume the filtration on D_K is trivial. Then the Hodge polygon is a straight line from $(0, 0)$ to $(h, 0)$.

Assume in addition that D is admissible. Then $P_H(D) = P_N(D)$, in particular all slopes of D are 0. Therefore there is a lattice M of D such that $\varphi(M) = M$. Since $N\varphi = p\varphi N$, we have $N(D_\alpha) \subset D_{\alpha-1}$, hence $N = 0$.

Conversely, any D of slope 0 and trivial filtration is admissible. If $D' \subset D$, then D' is purely of slope 0, hence $t_N(D') = 0$, therefore $N = 0$.

7.1.3 Tate's twist.

Let D be any filtered (φ, N)-module. For $i \in \mathbb{Z}$, define $D\langle i\rangle$ as follows:

$D\langle i\rangle = D$ as a K_0-vector space,
$\operatorname{Fil}^r(D\langle i\rangle)_K = \operatorname{Fil}^{r+i} D_K$ for $r \in \mathbb{Z}$.

Denote by N' and φ' the N and φ on $D\langle i\rangle$. We just set

$$N' = N, \quad \varphi' = p^{-i}\varphi.$$

Then $D\langle i\rangle$ is a filtered (φ, N)-module. It is easy to check that D is admissible if and only $D\langle i\rangle$ is admissible.

Exercise 7.6. For any p-adic representation V of G_K,

$$\mathbf{D}_{\mathrm{st}}(V(i)) = \mathbf{D}_{\mathrm{st}}(V)\langle i\rangle.$$

The isomorphism 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 $b_n \in B_{\mathrm{st}}$, $v_n \in V$.

7.1.4 Admissible filtered (φ, N)-modules of dimension 1.

Let D be a filtered (φ, N)-module with dimension 1 over K_0 such that φ is bijective on D. Write $D = K_0 d$. Then $\varphi(d) = \lambda d$ for some $\lambda \in K_0^*$ and N must be zero since N is nilpotent.

Since $D_K = D \otimes_{K_0} K = Kd$ is 1-dimensional over K, there exists $i \in \mathbb{Z}$ such that

$$\mathrm{Fil}^r D_K = \begin{cases} D_K, & \text{for } r \leq i, \\ 0, & \text{for } r > i. \end{cases}$$

Note that $t_N(D) = v_p(\lambda)$, and $t_H(D) = i$. Therefore D is admissible if and only if $v_p(\lambda) = i$.

Conversely, given $\lambda \in K_0^*$, we can associate to it D_λ, an admissible filtered (φ, N)-module of dimension 1 given by

$$D_\lambda = K_0,\ \varphi = \lambda\sigma,\ N = 0,$$
$$\mathrm{Fil}^r D_K = \begin{cases} D_K, & \text{for } r \leq v_p(\lambda), \\ 0, & \text{for } r > v_p(\lambda). \end{cases}$$

Exercise 7.7. If λ, $\lambda' \in K_0^*$, then $D_\lambda \cong D_{\lambda'}$ if and only if there exists $u \in W^*$ such that $\lambda' = \lambda \cdot \frac{\sigma(u)}{u}$.

In the special case when $K = \mathbb{Q}_p$, then K_0 is also $\mathbb{Q}_p$, and $\sigma = \mathrm{Id}$. Therefore $D_\lambda \cong D_{\lambda'}$ if and only if $\lambda = \lambda'$.

7.1.5 Admissible filtered (φ, N)-modules of dimension 2.

Let D be a filtered (φ, N)-module with $\dim_{K_0} D = 2$, and φ bijective. Then there exists a unique $i \in \mathbb{Z}$ such that

$$\mathrm{Fil}^i D_K = D_K, \quad \mathrm{Fil}^{i+1} D_K \neq D_K.$$

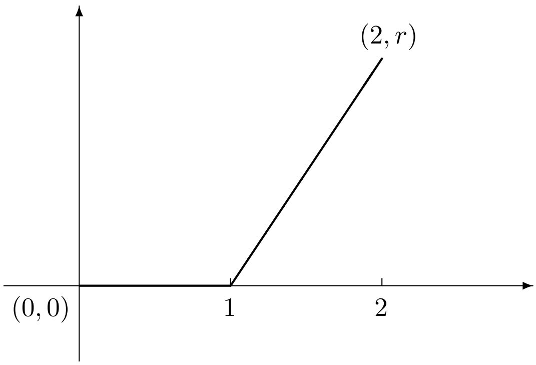
Replacing D with $D\langle i \rangle$, we may assume that $i = 0$. There are two cases.

Case 1: $\mathrm{Fil}^1 D_K = 0$. This means that the filtration is trivial. We have discussed this case in § 7.1.2.

Case 2: $\mathrm{Fil}^1 D_K \neq 0$. Therefore $\mathrm{Fil}^1 D_K = L$ is a 1-dimensional sub K-vector space of D_K. Hence there exists a unique $r \geq 1$ such that

$$\mathrm{Fil}^i D_K = \begin{cases} D_K, & \text{if } i \leq 0, \\ L & \text{if } 1 \leq i \leq r, . \\ 0, & \text{if } i > r \end{cases}$$

So the Hodge polygon $P_H(D)$ is

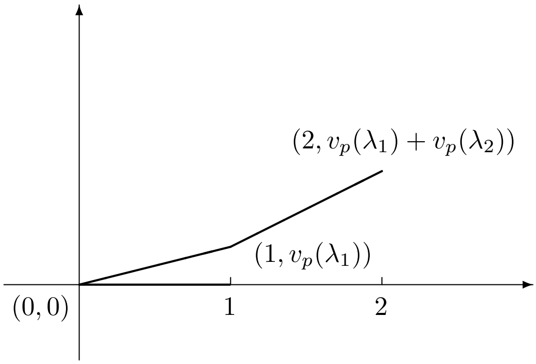


Assume $K = \mathbb{Q}_p$. Then $K_0 = \mathbb{Q}_p$, $D = D_K$, $\sigma = \mathrm{Id}$, φ is bilinear. Let $P_\varphi(X)$ be the characteristic polynomial of φ acting on D. Then

$$P_\varphi(X) = X^2 + aX + b = (X - \lambda_1)(X - \lambda_2)$$

for some a, $b \in \mathbb{Q}_p$, λ_1, $\lambda_2 \in \overline{\mathbb{Q}}_p$.

We may assume $v_p(\lambda_1) \leq v_p(\lambda_2)$. Then $P_N(D)$ is the following



Then the admissibility condition implies that

$$v_p(\lambda_1) \geq 0 \text{ and } v_p(\lambda_1) + v_p(\lambda_2) = r.$$

Case A: $N \neq 0$. Recall that $N(D_\alpha) \subset D_{\alpha-1}$. Therefore

$$v_p(\lambda_2) = v_p(\lambda_1) + 1 \neq v_p(\lambda_1).$$

In particular λ_1, $\lambda_2 \in \mathbb{Q}_p$. 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

$$D = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2, \ \lambda_1 \in \mathbb{Z}_p^*$$

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 question is: What is L?

To obtain the answer, we have to check the admissibility conditions, i.e.

$t_H(D) = t_N(D)$;
$t_H(D') \leq t_N(D')$ for any subobjects D' of D.

We only need to check that for $D' = \mathbb{Q}_p e_1$. We have that

$$t_N(D') = m, \qquad t_H(D') = \begin{cases} r, & \text{if } L = D'; \\ 0, & \text{otherwise.} \end{cases}$$

The admissibility condition implies that $t_H(D') = 0$, i.e. L can be any line $\neq D'$. Therefore there exists a unique $\alpha \in \mathbb{Q}_p$ such that $L = \mathbb{Q}_p(e_2 + \alpha e_1)$.

Conversely, given $\lambda_1 \in \mathbb{Z}_p^*$, $\alpha \in \mathbb{Q}_p$, 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

$$D_{\{\lambda_1,\alpha\}} = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$$

with

$$\begin{aligned} \varphi(e_1) &= \lambda_1 e_1, & N(e_1) &= 0, \\ \varphi(e_2) &= p\lambda_1 e_2, & N(e_2) &= e_1. \end{aligned}$$

$$\mathrm{Fil}^i\, D_{\{\lambda_1,\alpha\}} = \begin{cases} D_{\{\lambda_1,\alpha\}}, & \text{if } i \leq 0, \\ \mathbb{Q}_p(e_2 + \alpha e_1), & \text{if } 1 \leq i \leq 2v_p(\lambda_1) + 1, \\ 0, & \text{otherwise.} \end{cases}$$

Exercise 7.8. $D_{\{\lambda_1,\alpha\}} \cong D_{\{\lambda_1',\alpha'\}}$ if and only if $\lambda_1 = \lambda_1'$ and $\alpha = \alpha'$.

Proposition 7.9. *The map*

$$(i, \lambda_1, \alpha) \longmapsto D_{\{\lambda_1,\alpha\}}\langle i \rangle$$

from $\mathbb{Z} \times \mathbb{Z}_p^* \times \mathbb{Q}_p$ *to the set of isomorphism classes of* 2*-dimensional admissible filtered* (φ, N)*-modules over* $\mathbb{Q}_p$ *with* $N \neq 0$ *is bijective.*

Remark 7.10. When is $D_{\{\lambda_1,\alpha\}}$ irreducible? The answer is: 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 B: $N = 0$. By the admissibility condition, we need to check that for all lines D' of D stable under φ, $t_H(D') \le t_N(D'$. By the filtration of D, the following holds:

$$t_H(D') = \begin{cases} 0, & \text{if } D' \neq L, \\ r, & \text{if } D' = L. \end{cases}$$

Exercise 7.11. 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

$$D_{a,b} = \mathbb{Q}_p e_1 \oplus \mathbb{Q}_p e_2$$

with

$$\begin{cases} \varphi(e_1) = e_2, \\ \varphi(e_2) = -be_1 - ae_2, \end{cases} \qquad N = 0,$$

$$\operatorname{Fil}^i D_{a,b} = \begin{cases} D_{a,b}, & \text{if } i \le 0, \\ \mathbb{Q}_p e_1, & \text{if } 1 \le i \le 2, \\ 0, & \text{otherwise.} \end{cases}$$

Then $D_{a,b}$ is admissible and irreducible.

Exercise 7.12. Let λ_1, $\lambda_2 \in \mathbb{Z}_p$, nonzero, $\lambda_1 \neq \lambda_2$, and $v_p(\lambda_1) \le v_p(\lambda_2)$. 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

$$\begin{cases} \varphi(e_1) = \lambda_1 e_1, \\ \varphi(e_2) = \lambda_2 e_2, \end{cases} \qquad N = 0,$$

$$\operatorname{Fil}^i D'_{\lambda_1,\lambda_2} = \begin{cases} D'_{\lambda_1,\lambda_2}, & \text{if } i \le 0, \\ \mathbb{Q}_p(e_1 + e_2), & \text{if } 1 \le i \le r, \\ 0, & \text{otherwise.} \end{cases}$$

Then D'_{λ_1,λ_2} is admissible. Moreover, it is irreducible if and only if $v_p(\lambda_1) > 0$.

Proposition 7.13. *Assume 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 $\operatorname{Fil}^1 D \neq D, 0$. Assume D is not a direct sum of two admissible (φ, N)-modules of dimension 1. Then either $D \cong D_{a,b}$ for uniquely determined (a, b), or $D \cong D'_{\lambda_1,\lambda_2}$ uniquely determined (λ_1, λ_2).*

7.2 Proof of Proposition A1

We first recall:

Proposition A1. *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*

$$V \longrightarrow \mathbf{V}_{\mathrm{st}}(\mathbf{D}_{\mathrm{st}}(V)).$$

7.2.1 Construction of the natural isomorphism.

Let V be any semi-stable p-adic representation of G_K of dimension h. Let $D = \mathbf{D}_{\mathrm{st}}(V)$. We shall construct the natural isomorphism

$$V \overset{\sim}{\to} \mathbf{V}_{\mathrm{st}}(D) = \mathbf{V}_{\mathrm{st}}(\mathbf{D}_{\mathrm{st}}(V))$$

in this subsection.

The natural map

$$B_{\mathrm{st}} \otimes_{K_0} D \to B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V$$

is an isomorphism. We identify them and call them X.

Let $\{v_1, \cdots, v_h\}$ and $\{\delta_1, \cdots, \delta_h\}$ be bases of V over $\mathbb{Q}_p$ and D over K_0 respectively. Identify v_i with $1 \otimes v_i$ and δ_i with $1 \otimes \delta_i$, and then $\{v_1, \cdots, v_h\}$ and $\{\delta_1, \cdots, \delta_h\}$ are both bases of X over B_{st}.

Any element of X can be written as a sum of $b \otimes \delta$ where $b \in B_{\mathrm{st}}$, $\delta \in D$ and also a sum of $c \otimes v$, 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 X has 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

$$\mathrm{Fil}^i X_{\mathrm{dR}} = \mathrm{Fil}^i B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V = \sum_{r+s=i} \mathrm{Fil}^r B_{\mathrm{dR}} \otimes_K \mathrm{Fil}^s D_K.$$

Then

$$\begin{aligned} \mathbf{V}_{\mathrm{st}}(D) =& \{x \in X | \varphi(x) = x, N(x) = 0, x \in \mathrm{Fil}^0 X\} \\ =& \{x \in X | \varphi(x) = x, N(x) = 0, x \in \mathrm{Fil}^0 X_{\mathrm{dR}}\}. \end{aligned}$$

Note that $V \subset X$ satisfies the above conditions. 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 $b_n \in B_{\mathrm{st}}$.

(1) 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 $1 \leq n \leq h$, which implies that $b_n \in B_{\mathrm{cris}}$ for all n.

(2) 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 $1 \leq n \leq h$.

(3) 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 $1 \leq n \leq h$.

Applying the fundamental exact sequence

$$0 \to \mathbb{Q}_p \to B_e \to B_{\mathrm{dR}}/B_{\mathrm{dR}}^+ \to 0,$$

we have that $b_n \in \mathbb{Q}_p$. Therefore $x \in V$, which implies that $V = \mathbf{V}_{\mathrm{st}}(D)$.

7.2.2 Unramified representations.

Let D be a filtered (φ, N)-module with trivial filtration. Then D is of slope 0 (hence $N = 0$) if and only if there exists a W lattice M such that $\varphi(M) = M$.

Let $K_0 = \mathrm{Frac}\, W(k)$, D be an étale φ-module over K. Let $P_0 = \mathrm{Frac}\, W(\bar{k})$ be the completion of the maximal unramified extension of K_0 in $\overline{K}$. Then $P_0 \subset B_{\mathrm{cris}}^+ \subset B_{\mathrm{st}}$, P_0 is stable under G_K, and G_K acts on P_0 through $G_K/I_K = \mathrm{Gal}(\bar{k}/k)$.

Recall

$$\mathbf{V}_{\mathrm{st}}(D) = (B_{\mathrm{st}} \otimes_{K_0} D)_{\varphi=1, N=0} \cap (B_{\mathrm{dR}}^+ \otimes D_K)$$

with

$$(B_{\mathrm{st}} \otimes_{K_0} D)_{\varphi=1, N=0} = (B_{\mathrm{cris}} \otimes_{K_0} D)_{\varphi=1} \supset (P_0 \otimes_{K_0} D)_{\varphi=1},$$

an unramified representation of G_K of $\mathbb{Q}_p$-dimension $= \dim_{K_0} D$.

If V is an unramified representation of G_K, then

$$\mathbf{D}_{\mathrm{st}}(V) \supset (P_0 \otimes_{\mathbb{Q}_p} V)^{G_K}$$

which is of $\dim_{K_0} = \dim_{\mathbb{Q}_p} V$. Then we get the consequence.

Proposition 7.14. *Any unramified p-adic representation V of G_K is crystalline and $\mathbf{D}_{\mathrm{st}}$ induces an equivalence between $\mathbf{Rep}_{\mathbb{Q}_p}^{\mathrm{ur}}(G_K)$, unramified p-adic representations of G_K (equivalently $\mathbf{Rep}_{\mathbb{Q}_p}(G_k)$) and admissible filtered (φ, N)-modules with trivial filtration (equivalently étale φ-modules over K_0).*

7.2.3 The reductions to an algebraically closed residue field.

Let $\overline{P}$ be an algebraic closure of P inside of C, where

$$K_0^{\mathrm{ur}} \subset P_0 \subset P = P_0 K = \widehat{K}^{\mathrm{ur}}.$$

Then $\overline{P} \subset B_{\mathrm{dR}}^+$. Note that $B_{\mathrm{dR}}(\overline{P}/P) = B_{\mathrm{dR}}(\overline{K}/K) = B_{\mathrm{dR}}$, and same for B_{st} and B_{cris}.

For the exact sequence

$$1 \to I_K \to G_K \to G_k \to 1,$$

we have $I_K = \mathrm{Gal}(\overline{P}/P)$. If V is a p-adic representation of G_K, as $B_{\mathrm{dR}}^{I_K} = P$,

$$D_{\mathrm{dR},P}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{I_K}$$

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.

$D_{\mathrm{dR},P}(V)$ is a P-semilinear representation of G_k. This is trivial:

$$P \otimes_K (D_{\mathrm{dR},P}(V))^{G_k} \to D_{\mathrm{dR},P}(V)$$

is an isomorphism. Now

$$(D_{\mathrm{dR},P}(V))^{G_k} = D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K},$$

Therefore,

Proposition 7.15. *V is de Rham as a representation of G_K if and only if V is de Rham as a representation of I_K.*

Proposition 7.16. *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. 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, then the following is trivial:

$$P_0 \otimes_{K_0} (D_{\mathrm{st},P}(V))^{G_k} \to D_{\mathrm{st},P}(V)$$

is an isomorphism, and $\mathbf{D}_{\mathrm{st}}(V) = (D_{\mathrm{st},P}(V))^{G_k}$. □

7.2.4 A Proposition.

Proposition 7.17. *Let V be a p-adic representation of G_K,*

$$\rho : G_K \to \mathrm{Aut}_{\mathbb{Q}_p}(V)$$

Assume $\rho(I_K)$ is finite, then

(1). V is 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. Since $\overline{P} \subset B_{\mathrm{dR}}$, the only thing to prove is:

V is semi-stable $\Rightarrow \rho(I_K)$ is trivial.

Because of the previous proposition, we may assume $k = \bar{k}$, equivalently $K = P$, or $I_K = G_K$.

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

$$\begin{aligned}\mathbf{D}_{\mathrm{st}}(V) =& (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K} = ((B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^H)^J \\ =& (B_{\mathrm{st}}^H \otimes_{\mathbb{Q}_p} V)^J = (K_0 \otimes_{\mathbb{Q}_p} V)^J = K_0 \otimes_{\mathbb{Q}_p} V^J\end{aligned}$$

because of $B_{\mathrm{st}}^H = K_0$. Thus

$$V \text{ is semi-stable } \Leftrightarrow \dim_{K_0} \mathbf{D}_{\mathrm{st}}(V) = \dim_{\mathbb{Q}_p} V^J = \dim_{\mathbb{Q}_p} V \Leftrightarrow V^J = V,$$

which means $\rho(I_K)$ is trivial. □

7.2.5 Tate's twists.

Recall $V(i) = V \otimes_{\mathbb{Q}_p} \mathbb{Q}_p(i)$, we know that

V is de Rham (resp. semi-stable, crystalline) if and only if $V(i)$ is de Rham (resp. semi-stable crystalline).

We will see that

$$\mathbf{D}_{\mathrm{st}}(V(i)) = \mathbf{D}_{\mathrm{st}}(V)\langle i \rangle.$$

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 $\mathbb{Q}_p(i)$. Then $V(i) = \{v \otimes t^i | v \in V\}$. 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 $b_n \in B_{\mathrm{st}}$, $v_n \in V$.

7.2.6 Representation of dimension 1.

Let V be a p-adic representation of G_K of dimension 1. Write $V = \mathbb{Q}_p v$, then $g(v) = \eta(g)v$ and

$$\eta : G_K \to \mathbb{Q}_p^*$$

is a character(i.e. continuous homomorphism). Moreover, we can make η factors through $\mathbb{Z}^*$. We call

η is *B-admissible* if V is B-admissible.

Then

(1) η is *C-admissible* if and only if η is $\overline{P}$-admissible, or if and only if $\eta(I_K)$ is finite.

(2) If η is Hodge-Tate. Recall

$$\mathbf{D}_{\mathrm{HT}}(V) = \bigoplus_{i\in\mathbb{Z}} (C(-i) \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

Then V is Hodge-Tate if and only if there exists $i \in \mathbb{Z}$ (not unique) 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, or equivalently $\eta\chi^{-i}(I_K)$ is finite where χ is the cyclotomic character. In this case we write $\eta = \eta_0\chi^i$.

Proposition 7.18. *η is Hodge-Tate if and only if it can be written as $\eta = \eta_0\chi^i$ with $i \in \mathbb{Z}$ and η_0 such that $\eta_0(I_K)$ is finite.*

Proposition 7.19. *η is de Rham if and only if η is Hodge-Tate.*

Proof. As 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 de Rham and therefore also is $V = V(-i)(i)$. □

Proposition 7.20. *If $\eta : G_K \to \mathbb{Z}_p^*$ is a continuous homomorphism, then the followings are equivalent:*

(1). η is semi-stable;

(2). η is crystalline;

(3). There exist $\eta_0 : G_K \to \mathbb{Z}_p^*$ unramified and $i \in \mathbb{Z}$ such that $\eta = \eta_0\chi^i$.

Proof. This follows from Proposition 7.17. □

Remark 7.21. Check that if D is an admissible filtered (φ, N)-module over K of dimension 1, then there exists a semi-stable representation V such that $D \simeq \mathbf{D}_{\mathrm{st}}(V)$.

7.2.7 End of the proof of Proposition A1.

Let V be a semi-stable p-adic representation of G_K. We want to prove that $\mathbf{D}_{\mathrm{st}}(V)$ is admissible. We denote by $D = \mathbf{D}_{\mathrm{st}}(V)$.

Let D' be a sub K_0-vector space of D stable under φ and N. We want to prove that

$$t_H(D') \leqslant t_N(D').$$

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

$$\varphi\delta = \lambda\delta,\ \lambda \in K_0,\ \lambda \neq 0.$$

Thus

$$t_N(D') = v_p(\lambda) = r \quad \text{and} \quad N\delta = 0.$$

As $D = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K}$, then $\delta = \sum\limits_{i=1}^{h} b_i \otimes v_i$. Thus

$$\varphi\delta = \sum_{i=1}^{h} \varphi b_i \otimes v_i \text{ and } N\delta = \sum_{i=1}^{h} N b_i \otimes v_i,$$

so $\varphi b_i = \lambda b_i$ and $N b_i = 0$ for all i, 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. Now this case follows from the Lemma below.

Lemma 7.22. *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 $\Delta = K_0 e$ be an one-dimensional (φ, N)-module with $\varphi e = \frac{1}{\lambda} e$ and $Ne = 0$. Then $t_H(\Delta) = -r$ and

$$\mathrm{Fil}^i \Delta_K = \begin{cases} K, & \text{if } i \leqslant -r, \\ 0, & \text{if } i > -r. \end{cases}$$

$\mathbf{V}_{\mathrm{st}}(\Delta)$ is a $\mathbb{Q}_p$-vector space of dimension 1. Then $\mathbf{V}_{\mathrm{st}}(\Delta) = \mathbb{Q}_p b_0 \otimes e$ for any $\varphi b_0 = \lambda b_0$, $b_0 \neq 0$. Thus $b_0 \in \mathrm{Fil}^r$ but $\notin \mathrm{Fil}^{r+1}$. □

We also see that if $D = D'$ is of dimension 1, then $t_H(D) = t_N(D)$.

General case: let $D = \mathbf{D}_{\mathrm{st}}(V)$, $\dim_{K_0} D = \dim_{\mathbb{Q}_p} V = h$, $\dim_{K_0} D' = m$. We want to prove $t_H(D') \leqslant t_N(D')$ and the equality if $m = h$.

Let $V_1 = \bigwedge^m V$ be 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

$$\mathbf{D}_{\mathrm{st}}(V_1) = \bigwedge^m \mathbf{D}_{\mathrm{st}}(V) = \bigwedge^m_{K_0} D.$$

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.

7.2.8 $\mathbb{Q}_{p^r}$-representations.

Let $r \in \mathbb{N}$, $r \geqslant 1$. Denote by $\mathbb{Q}_{p^r}$ the unique unramified extension of $\mathbb{Q}_p$ of degree r contained in $\overline{K}$. The Galois group $\mathrm{Gal}(\mathbb{Q}_{p^r}/\mathbb{Q})$ is a cyclic group generated by the restriction of φ to $\mathbb{Q}_{p^r}$ ($\varphi|_{\mathbb{Q}_{p^r}} = \sigma$), and

$$\mathbb{Q}_{p^r} \subset P_0 \subset B^+_{\mathrm{cris}} \subset B_{\mathrm{st}}$$

is stable under G_K and φ.

Definition 7.23. *A* $\mathbb{Q}_{p^r}$-representation *of G_K is a finite dimensional $\mathbb{Q}_{p^r}$-vector space such that G_K acts continuously and semi-linearly:*

$$g(v_1 + v_2) = g(v_1) + g(v_2), \quad g(\lambda v) = g(\lambda)g(v).$$

Note that such a representation is also a p-adic representation of G_K with

$$\dim_{\mathbb{Q}_p} V = r \dim_{\mathbb{Q}_{p^r}} V.$$

We say that a $\mathbb{Q}_{p^r}$-representation V of G_K is *de Rham (semi-stable,$\cdots$)* if it is de Rham (semi-stable,$\cdots$) as a p-adic representation.

Let V be a $\mathbb{Q}_{p^r}$-representation V of G_K, recall $\mathbf{D}_{\mathrm{st}}(V) = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K}$. Write

$$\mathbf{D}_{\mathrm{st},r}(V) = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_{p^r}} V)^{G_K}$$

which again is a K_0-vector space.

Proposition 7.24.

$$\dim_{K_0} \mathbf{D}_{\mathrm{st},r}(V) \leqslant \dim_{\mathbb{Q}_{p^r}} V$$

with equality if and only if V is semi-stable.

Proof. One has

$$B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V = \bigoplus_{m=0}^{r-1} B_{\mathrm{st}} \,{}_{\sigma^{-m}}\!\otimes_{\mathbb{Q}_{p^r}} V$$

where ${}_{\sigma^{-m}}\!\otimes_{\mathbb{Q}_{p^r}}$ is the twisted tensor product. Thus

$$\mathbf{D}_{\mathrm{st}}(V) = \bigoplus_{m=0}^{r-1} (B_{\mathrm{st}} \,{}_{\sigma^{-m}}\!\otimes_{\mathbb{Q}_{p^r}} V)^{G_K}.$$

For $d \in \mathbf{D}_{\mathrm{st},r}(V)$, then $\varphi^m d \in (B_{\mathrm{st}\ \sigma^{-m}}\!\otimes_{\mathbb{Q}_{p^r}} V)^{G_K}$, which implies

$$\dim_{K_0}(B_{\mathrm{st}} \otimes_{\mathbb{Q}_{p^r}} V)^{G_K} = \dim_{K_0} \mathbf{D}_{\mathrm{st},r}(V),$$

thus

$$\dim_{K_0} \mathbf{D}_{\mathrm{st}}(V) = r \dim_{K_0} \mathbf{D}_{\mathrm{st},r}(V).$$

We proved the Proposition. □

For a $\mathbb{Q}_{p^r}$-representation V, we have

$$\mathbf{D}_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K} = \bigoplus_{m=0}^{r-1} (B_{\mathrm{dR}\ \sigma^{-m}}\!\otimes_{\mathbb{Q}_{p^r}} V)^{G_K}.$$

If V is semi-stable, then

$$(B_{\mathrm{dR}\ \sigma^{-m}}\!\otimes_{\mathbb{Q}_{p^r}} V)^{G_K} = K\ {}_{\varphi^{-m}}\!\otimes_{K_0} \mathbf{D}_{\mathrm{st},r}(V).$$

Definition 7.25. *A* filtered (φ^r, N)-module *over K is a K_0-vector space Δ with two operators*

$$\varphi^r,\ N:\ \Delta \to \Delta$$

such that N is K_0-linear, φ^r is σ^r-semi-linear, and

$$N\varphi^r = p^r \varphi^r N,$$

and a structure of filtered K vector space on

$$\Delta_{K,m} = K\ {}_{\varphi^{-m}}\!\otimes_{K_0} \Delta$$

for $m = 0, 1, 2, \cdots, r-1$.

If V is a semi-stable $\mathbb{Q}_{p^r}$-representation of G_K, write $\Delta = \mathbf{D}_{\mathrm{st},r}(V)$. Then Δ has a natural structure of a filtered (φ^r, N)-module over K, The inclusion

$$\Delta = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_{p^r}} V)^{G_K} \subset (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K}$$

shows Δ is stable by φ^r and N, and the filtration for $\Delta_{K,m} = K\ {}_{\varphi^{-m}}\!\otimes_{K_0} \Delta$ comes from $B_{\mathrm{dR}\ \sigma^{-m}}\!\otimes_{\mathbb{Q}_{p^r}} V$.

Exercise 7.26. Define a way to associate a filtered (φ, N)-module Δ over K to a (φ, N)-module D over K such that if V is a semi-stable p-adic representation and if $\Delta = \mathbf{D}_{\mathrm{st},r}(V)$, then $D = \mathbf{D}_{\mathrm{st}}(V)$.

Answer: $D = \mathbb{Q}_p[\varphi] \otimes_{\mathbb{Q}_p[\varphi^r]} \Delta$.

Define Δ to be admissible if the associated D is admissible.

Proposition 7.27. *Let $\mathbf{Rep}^{\mathrm{st}}_{\mathbb{Q}_{p^r}}(G_K)$ denote the category of $\mathbb{Q}_{p^r}$ semi-stable 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.

Exercise 7.28. (1) Define $\mathbf{V}_{\mathrm{st},r}$ which has the property that

$$\mathbf{V}_{\mathrm{st},r}(\mathbf{D}_{\mathrm{st},r}(V)) = V.$$

(2) Define tensor products in both categories and check that $\mathbf{D}_{\mathrm{st},r}$ is a $\otimes$ functor.

Examples of $\mathbb{Q}_{p^r}$-representations.

(1) $\mathbb{Q}_{p^r}$ is a $\mathbb{Q}_{p^r}$-representation of dimension 1, $\mathbf{D}_{\mathrm{st},r}(\mathbb{Q}_{p^r}) = K_0$ with $\varphi^r = \sigma^r$, $N = 0$, and all the filtration are trivial.

(2) Let $\pi = p$ or $-p$ be a uniformizing parameter. Consider the Lubin-Tate formal group for $\mathbb{Q}_{p^r}$ associated to π. The fact $\pi \in \mathbb{Q}_p$ implies that this Lubin-Tate formal group is defined over $\mathbb{Z}_p$, and

$$V_p(LT) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(LT).$$

$V_{(r)} = V_p(\Gamma)$ is a one-dimensional $\mathbb{Q}_{p^r}$-vector space, $G_K \to \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ acts semi-linearly on it, so $V_{(r)}$ is a one-dimensional $\mathbb{Q}_{p^r}$-representation of G_K. Moreover, there is a natural injective map

$$V_{(r)} \hookrightarrow \{v \in B^+_{\mathrm{cris}} |\ \varphi^r v = pv\} \cap \mathrm{Fil}^1 B_{\mathrm{dR}}$$

(a fortiori, this is an isomorphism), which implies that $V_{(r)}$ is crystalline.

Write $V_{(r)} = \mathbb{Q}_{p^r} v$, then $e = v^{-1} \otimes v \in \mathbf{D}_{\mathrm{st},r}(V)$, thus

$$\mathbf{D}_{\mathrm{st},r}(V) = K_0 e,\ \varphi^r e = p^{-1} e,\ Ne = 0.$$

Then $\Delta = \mathbf{D}_{\mathrm{st},r}(V_{(r)}) = K_0 e$, and

$$\Delta_{K,m} = K\ {}_{\varphi^{-m}} \otimes_{K_0} K_0 e = K e_m, \quad e_m = 1 \otimes e$$

for $m = 0, 1, \cdots, r-1$. If $m > 0$,

$$\mathrm{Fil}^i \Delta_{K,m} = \begin{cases} K e_m, & \text{if } i \leq 0; \\ 0, & \text{if } i > 0. \end{cases}$$

If $m = 0$,

$$\mathrm{Fil}^i \Delta_{K,0} = \begin{cases} K e_0, & \text{if } i < 0; \\ 0, & \text{if } i \geq 0. \end{cases}$$

7.3 Sketch of a proof of Theorem A and Theorem B

Lemma 7.29. *Let F be a field and J a subgroup of the group of automorphisms of F. Let $E = F^J$. 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. Exercise. □

Proposition 7.30. *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 $\mathbf{D}_{\mathrm{st}}(V) \subset D$ as a subobject.*

Remark 7.31. The above proposition implies that, if D is admissible, the following conditions are equivalent:

(1). $D \simeq \mathbf{D}_{\mathrm{st}}(V)$ where V is some semi-stable p-adic representation.
(2). $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) \geqslant h$.
(3). $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) = h$.

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. By the lemma, there exists a sub K_0-vector space D' of D such that

$$L = C_{\mathrm{st}} \otimes_{K_0} D'.$$

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 $V \subset B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} D$,

$$v_i = \sum_{j=1}^{r} b_{ij} d_j, \quad b_{ij} \in B_{\mathrm{st}}.$$

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 $b = \det(b_{ij}) \in B_{\mathrm{st}}$, then $b \neq 0$. 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 $v_0 = db_0$. Since $v_i \in \mathbf{V}_{\mathrm{st}}(D')$, then $v_0 \in \mathbf{V}_{\mathrm{st}}(\bigwedge^r D')$, which is $\neq 0$ as $v_0 \neq 0$. Now the facts

$$\dim_{K_0} \bigwedge\nolimits^{r} D' = 1 \text{ and } \mathbf{V}_{\mathrm{st}}(\bigwedge\nolimits^{r} D') \neq 0$$

imply that

$$t_H(\bigwedge\nolimits^{r} D') \geqslant t_N(\bigwedge\nolimits^{r} D').$$

Now the admissibility condition implies that $t_H(D') = t_N(D')$, thus $t_H(\bigwedge^r D') = t_N(\bigwedge^r D')$ and

$$\mathbf{V}_{\mathrm{st}}(\bigwedge\nolimits^{r} D') = \mathbb{Q}_p v_0.$$

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 is the $\mathbb{Q}_p$ vector space generated by $v_1, \cdots, v_r$ and

$$r = \dim_{K_0} D' \leqslant \dim_{K_0} D.$$

Because

$$\mathbf{V}_{\mathrm{st}}(D') = V \text{ and } \mathbf{D}_{\mathrm{st}}(V) = D',$$

we get the result that V is semi-stable. □

Proposition 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* $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) = \dim_{K_0} D$.

Proof (Outline of the Proof of Propositions A and B). 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:

$$0 \to \operatorname{Fil}^1 B_{\mathrm{dR}} \to \operatorname{Fil}^0 B_{\mathrm{dR}} = B_{\mathrm{dR}}^+ \to C \to 0,$$

$\otimes V$ and then take the invariant under G_K, we have

$$0 \to \operatorname{Fil}^1 D_K \to \operatorname{Fil}^0 D_K \to (C \otimes_{\mathbb{Q}_p} V)^{G_K}.$$

Because the filtration is trivial, $\operatorname{Fil}^1 D_K = 0$ and $\operatorname{Fil}^0 D_K = D_K$, then we have a monomorphism $D_K = \operatorname{Fil}^0 D_K \to (C \otimes_{\mathbb{Q}_p} V)^{G_K}$, 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). □

Proof (Proposition B in this case). We know that in this case, $D \simeq \mathbf{D}_{\mathrm{st}}(V)$ with

$$V = (P_0 \otimes_{K_0} D)_{\varphi=1}$$

an unramified representation. □

Step 2:

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 $\dim_{\mathbb{Q}_p} \mathbf{V}_{\mathrm{st}}(D) = \dim_{K_0} D$.

By Propositions 2A and 2B, it is enough to prove when V and D are irreducible.

Remark 7.32. Proposition 2A is due to Hyodo when k is finite using Galois cohomology and Tate duality. The proof in the general case is due to Berger and uses the theory of (φ, N)-modules. We won't give the proof of Proposition 2A here.

For Proposition 2B, we need to introduce the so-called *fundamental complex of D*. Write

$$\begin{aligned}
&\mathbf{V}^0_{\mathrm{st}}(D) = \{b \in B_{\mathrm{st}} \otimes_{K_0} D | Nb = 0,\ \varphi b = b\},\\
&\mathbf{V}^1_{\mathrm{st}}(D) = B_{\mathrm{dR}} \otimes_K D_K / Fil^0(B_{\mathrm{dR}} \otimes_K D_K),\\
&\mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D_K) = \sum_{i\in\mathbb{Z}} \mathrm{Fil}^i B_{\mathrm{dR}} \otimes_K \mathrm{Fil}^{-i} D_K.
\end{aligned}$$

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

$$0 \to \mathbf{V}_{\mathrm{st}}(D) \to \mathbf{V}^0_{\mathrm{st}}(D) \to \mathbf{V}^1_{\mathrm{st}}(D).$$

Proposition 7.33. *Under the assumptions of Proposition 2B (not including admissibility condition), then for $i = 0, 1$, the sequence*

$$0 \to \mathbf{V}^i_{\mathrm{st}}(D') \to \mathbf{V}^i_{\mathrm{st}}(D) \to \mathbf{V}^i_{\mathrm{st}}(D'') \to 0$$

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

$$0 \to B_{\mathrm{dR}} \otimes_K D'_K \to B_{\mathrm{dR}} \otimes_K D_K \to B_{\mathrm{dR}} \otimes_K D''_K \to 0.$$

Then we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D'_K) \arrow[r] \arrow[d, hook] & \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D_K) \arrow[r] \arrow[d, hook] & \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K D''_K) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & B_{\mathrm{dR}} \otimes_K D'_K \arrow[r] \arrow[d, two heads] & B_{\mathrm{dR}} \otimes_K D_K \arrow[r] \arrow[d, two heads] & B_{\mathrm{dR}} \otimes_K D''_K \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & \mathbf{V}^1_{\mathrm{st}}(D') \arrow[r] & \mathbf{V}^1_{\mathrm{st}}(D) \arrow[r] & \mathbf{V}^1_{\mathrm{st}}(D'') \arrow[r] & 0
\end{tikzcd}$$

The three columns and the middle row of the above diagram are exact, the top row is exact following from the snake lemma, hence the bottom one is also exact and so we get the result for $i = 1$.

For $i - 0$, note that

$$\mathbf{V}_{\mathrm{st}}^0(D) = \{x \in B_{\mathrm{st}} \otimes_{K_0} D | Nx = 0,\ \varphi x = x\}.$$

Let

$$\mathbf{V}_{\mathrm{cris}}^0(D) = \{y \in B_{\mathrm{cris}} \otimes_{K_0} D | \varphi y = y\}.$$

Let $u = \log[\pi]$ for $\pi^{(0)} = -p$, then

$$B_{\mathrm{st}} = B_{\mathrm{cris}}[u],\ N = -\frac{d}{du} \text{ and } \varphi u = pu.$$

With obvious notation, any $x \in B_{\mathrm{st}} \otimes_{K_0} D$ can be written as

$$x = \sum_{n=0}^{+\infty} x_n u^n,\ x_n \in B_{\mathrm{cris}} \otimes_{K_0} D$$

and almost all $x_n = 0$. The map

$$x \mapsto x_0$$

defines a $\mathbb{Q}_p$-linear bijection between $\mathbf{V}_{\mathrm{st}}^0(D)$ and $\mathbf{V}_{\mathrm{cris}}^0(D)$ which is functorial (however, which is not Galois equivalent).

Enough to prove that

$$0 \to \mathbf{V}_{\mathrm{cris}}^0(D') \to \mathbf{V}_{\mathrm{cris}}^0(D) \to \mathbf{V}_{\mathrm{cris}}^0(D'') \to 0$$

is exact. The only thing which matters is the structure of φ-isocrystals.

a). the case k is algebraically closed. For the exact sequence

$$0 \to D' \to D \to D'' \to 0,$$

it is well known that this sequence splits as a sequence of φ-isocrystals. Thus $D \simeq D' \oplus D''$ and $\mathbf{V}_{\mathrm{cris}}^0(D) = \mathbf{V}_{\mathrm{cris}}^0(D') \oplus \mathbf{V}_{\mathrm{cris}}^0(D'')$.

b). the case k is not algebraically closed. Then

$$\mathbf{V}_{\mathrm{cris}}^0(D) = \{y \in B_{\mathrm{cris}} \otimes_{K_0} D | \varphi y = y\} = \{y \in B_{\mathrm{cris}} \otimes_{P_0} (P_0 \otimes_{K_0} D) | \varphi y = y\}$$

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 7.34. *If V is semi-stable and if $D \cong \mathbf{D}_{\mathrm{st}}(V)$, then the sequence*

$$0 \to \mathbf{V}_{\mathrm{st}}(D) \to \mathbf{V}_{\mathrm{st}}^0(D) \to \mathbf{V}_{\mathrm{st}}^1(D) \to 0$$

is exact.

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

$$\mathbf{V}^0_{\mathrm{st}}(D) = \{x \in B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} D | Nx = 0, \ \varphi x = x\}.$$

As $N(b \otimes v) = Nb \otimes v$ and $\varphi(b \otimes v) = \varphi b \otimes v$, then

$$\mathbf{V}^0_{\mathrm{st}}(D) = B_e \otimes_{\mathbb{Q}_p} V.$$

By definition and the above fact,

$$\mathbf{V}^1_{\mathrm{st}}(D)K) = (B_{\mathrm{dR}}/B^+_{\mathrm{dR}}) \otimes_{\mathbb{Q}_p} V.$$

From the fundamental exact sequence

$$0 \to \mathbb{Q}_p \to B_e \to B_{\mathrm{dR}}/B^+_{\mathrm{dR}} \to 0$$

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 $V = \mathbf{V}_{\mathrm{st}}(D)$, $0 \to \mathbf{V}_{\mathrm{st}}(D) \to \mathbf{V}^0_{\mathrm{st}}(D) \to \mathbf{V}^1_{\mathrm{st}}(D) \to 0$ is exact. □

Proof (Proof of Proposition 2B). Let $0 \to D' \to D \to D'' \to 0$ be the short exact sequence. Then we have a commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathbf{V}_{\mathrm{st}}(D') \arrow[r] \arrow[d] & \mathbf{V}^0_{\mathrm{st}}(D') \arrow[r] \arrow[d] & \mathbf{V}^1_{\mathrm{st}}(D') \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathbf{V}_{\mathrm{st}}(D) \arrow[r] \arrow[d] & \mathbf{V}^0_{\mathrm{st}}(D) \arrow[r] \arrow[d] & \mathbf{V}^1_{\mathrm{st}}(D) \arrow[d] & \\
0 \arrow[r] & \mathbf{V}_{\mathrm{st}}(D'') \arrow[r] & \mathbf{V}^0_{\mathrm{st}}(D'') \arrow[r] \arrow[d] & \mathbf{V}^1_{\mathrm{st}}(D'') \arrow[r] \arrow[d] & 0 \\
 & & 0 & 0 &
\end{tikzcd}$$

which is exact in rows and columns. A diagram chasing shows that $\mathbf{V}_{\mathrm{st}}(D) \to \mathbf{V}_{\mathrm{st}}(D'')$ is onto, thus $\dim_{K_0} \mathbf{V}_{\mathrm{st}}(D) = \dim_{\mathbb{Q}_p} V$. □

Step 3: Reduce the proof to the case when $t_H = 0$.

The Idea for V is the following. In this case $t_H(V) = t_H(D_K)$. For any $i \in \mathbb{Z}$, we have 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 7.35. *If V is a p-adic representation of G_K, let r be the biggest integer $\geqslant 1$ such that we can endow V with the structure of a $\mathbb{Q}_{p^r}$-representation. The* reduced dimension *of V is the integer $\frac{\dim_{\mathbb{Q}_p} V}{r}$.*

For $h \in \mathbb{N},\ h \geqslant 1$, we have

Proposition A'(h). *Any p-adic de Rham representation of G_K of reduced dimension $\leqslant h$ and such that $t_H(V) = 0$ is potentially semi-stable.*

Proposition A(h). *Any p-adic de Rham representation of G_K of reduced dimension $\leqslant h$ is potentially semi-stable.*

Proof (Proof of Proposition A'(h) $\Rightarrow$ Proposition A(h)). 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 $r \geqslant 1$, such that we may consider V as a $\mathbb{Q}_{p^r}$-representation of dimension h. For $s \geqslant 1$ and for any $a \in \mathbb{N}$, define

$$V_{(s)}^a = \mathrm{Sym}^a_{\mathbb{Q}_{p^s}} V_{(s)},$$

then $V_{(s)}^a$ is a $\mathbb{Q}_{p^s}$-representation of dimension 1. Let $V_{(s)}^{-a}$ be the $\mathbb{Q}_{p^s}$-dual of $V_{(s)}^a$. Choose $s = rb$ with $b \geqslant 1$ 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. If $V_{(s)}$ is crystalline, then is also de Rham, thus $V_{(s)}^a$ is de Rham and V' is also de Rham.

An easy exercise shows

$$d = rh = \dim_{\mathbb{Q}_p} V,\ t_H(V') = bt_H(V) - ad.$$

Choose a and b in such a way that $t_H(V') = 0$. Apply Proposition A'(h), 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. □

Exercise 7.36. (1). Define the notion of reduced dimension for a filtered (φ, N)-module.

(2). State Proposition B'(h), Proposition B(h), and prove that B'(h) implies B(h). (Hint: Use $D(V_{(s)}$ instead of $V_{(s)}$).

Last step:

Let $r, h \in \mathbb{N}^*$.

Proposition A(f). *Let V be a $\mathbb{Q}_{p^r}$ de Rham representation of dimension h with $t_H = 0$, then V is potentially semi-stable.*

Proposition B(f). *Let Δ be an admissible filtered (φ^r, N)-module over K_0,* $\dim_{K_0} = h$*, D be the associated filtered (φ, N)-module with $t_H = 0$. Then*

$$\dim_{\mathbb{Q}_{p^r}} \mathbf{D}_{\mathrm{st}}(V) = h.$$

Proof (Sketch of Proof). We prove it by induction on h. Suppose it is known for (r', h') with $h' < h$ and r' arbitrary, we want to prove it is OK for (r, h). By induction, we may assume the result is known for V' or D' with the same (r, h), $t_H = 0$ but $P_H(V')$ or $P_H(D')$ is strictly above P_H $(> P_H)$.

The initial step is known.

Idea of the proof: For V, we want to find V', $V' \subset B_e \otimes_{\mathbb{Q}_p} V \subset B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V$, such that

(i) $B_e \otimes_{\mathbb{Q}_p} V' \xrightarrow{\sim} B_e \otimes_{\mathbb{Q}_p} V$ is an isomorphism;
(ii) V' is de Rham with $t_H = 0$ and $P_H(V') > P_H(V)$.

Then it is OK. As $B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V' = B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V$ implies that

$$(B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V')^{G_K} = (B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} V)^{G_K},$$

hence $\mathbf{D}_{\mathrm{st}}(V') = \mathbf{D}_{\mathrm{st}}(V)$.

For Proposition B_f: We have D and Δ, we want to construct D' and Δ'. Take $D' = D$ as a (φ, N)-module, then $D'_K = D_K$. Change the filtration a little bit. Construct V' for D' and $V \subset B_e \otimes_{\mathbb{Q}_p} V'$. Recall $U = \{u \in B^+_{\mathrm{cris}} | \varphi u = pu\}$ and the exact sequence:

$$0 \to \mathbb{Q}_p(1) \to U \to C \to 0.$$

Choose $t \in \mathbb{Q}_p(1) \subset B^+_{\mathrm{cris}}$ such that $\varphi t = pt$. Then

$$U(-1) = \{\frac{u}{t} | u \in U\} \subset B_{\mathrm{cris}}$$

and we have the exact sequence

$$0 \to \mathbb{Q}_p \to U(-1) \to C(-1) \to 0.$$

Tensor V over $\mathbb{Q}_p$, we get the following exact sequence

$$0 \to V \to U(-1) \otimes_{\mathbb{Q}_p} V \to C(-1) \otimes_{\mathbb{Q}_p} V \to 0.$$

Looks for $V' \subset U(-1) \otimes_{\mathbb{Q}_p} V \subset B_e \otimes_{\mathbb{Q}_p} V$. □

A

Preliminary

A.1 Inverse limits and Galois theory

A.1.1 Inverse limits.

In this subsection, we always assume that $\mathscr{A}$ is an abelian category with infinite products. In particular, one can let $\mathscr{A}$ be the category of sets, of (topological) groups, of (topological) rings, of left (topological) module over a ring A.

Definition A.1. *A partially ordered set I is called a* directed set *if for any $i, j \in I$, there exists $k \in I$ such that $i \leq k$ and $j \leq k$.*

Definition A.2. *Let I be a directed set. Let $(A_i)_{i\in I}$ be a family of objects in $\mathscr{A}$. This family is called an* inverse system *(or a* projective system*) of $\mathscr{A}$ over the index set I if for every 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:*

(1). $\varphi_{ii} = \mathrm{Id}$;

(2). For every $i \leq j \leq k$, $\varphi_{ki} = \varphi_{ji}\varphi_{kj}$.

Definition A.3. *The* inverse limit *(or* projective limit*) of a given inverse system $A_\bullet = (A_i)$ is defined to be an object in $\mathscr{A}$*

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

such that the natural projection $\varphi_i : A \to A_i$, $a = (a_j)_{j\in I} \mapsto a_i$ is a morphism for each $i \in I$.

Remark A.4. One doesn't need the set I to be a directed set but only to be a partially ordered set to define an inverse system. For example, let I be 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 $\varphi_i = \varphi_{ji}\varphi_j$ for every pair $i \leq j$. Actually, A is the solution of the *universal problem*:

Proposition A.5. *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 $f_j = \varphi_j \circ f$.*

Proof. This is an easy exercise. □

By definition, if $\mathscr{A}$ is the category of topological spaces, i.e., if X_i is a topological space for every $i \in I$ and φ_{ij}'s are continuous maps, then $X = \varprojlim_{i\in I} X_i$ is a topological space equipped with a natural topology, the *weakest topology* such that all the φ_i's are continuous. Recall that the product topology of the topological space $\prod_{i\in I} X_i$ is the *weakest topology* such that the projection $\mathrm{pr}_j : \prod_{i\in I} X_i \to X_j$ is continuous for every $j \in I$. Thus the natural topology of 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 given the discrete topology, then X is associated with the topology of the inverse limit of discrete topological spaces. In particular, if each X_i is a finite set with discrete topology, then we will get a *profinite set* (inverse limit of finite sets). In this case, as $\varprojlim X_i \subset \prod_{i\in I} X_i$ is closed, and $\prod_{i\in I} X_i$ is compact, therefore $\varprojlim X_i$ is compact. Easily 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 group with $\varphi_i : \varprojlim_j X_j \to X_i$ a (continuous) homomorphism of groups.

If the X_i's are finite groups with discrete topology, we get a *profinite group* for the inverse limit in this case. 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 A.6. (1) For the set of positive integers $\mathbb{N}^*$, we define an ordering $n \leq m$ 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

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

.

(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

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

induces an isomorphism of topological rings

$$\widehat{\mathbb{Z}} \simeq \prod_{\ell \text{ prime number}} \mathbb{Z}_\ell.$$

A.1.2 Galois theory.

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

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

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

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

Galois theory tells us that the following restriction map is an isomorphism

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

From now on, we identify the two groups through the above isomorphism. Put the topology of the inverse limit with the discrete topology on each $\mathrm{Gal}(E/K)$, the group $G = \mathrm{Gal}(L/K)$ is then a profinite group, equipped with a compact and totally disconnected topology, which is called the *Krull topology.* We have

Theorem A.7 (Fundamental Theorem of Galois Theory). *There is a one-one correspondence between intermediate field extensions $K \subset K' \subset L$*

and closed subgroups H of $\mathrm{Gal}(L/K)$ *given by* $K' \to \mathrm{Gal}(L/K')$ *and* $H \to L^H$ *where* $L^H = \{x \in L \mid g(x) = x$ *for all* $g \in H\}$ *is the invariant field of* H.

Moreover, the above correspondence gives one-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 A.8. (1) 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 $E \in \mathcal{E}$, there exists $n_E \in \mathbb{N}$ such that if $n \geq n_E$, then $g_n|_E = g|_E$.

(2) The open normal subgroups of G are the groups $\mathrm{Gal}(L/E)$ for $E \in \mathcal{E}$, and there is an exact sequence

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

(3) A subgroup of G is open if and only if it contains an open normal subgroup. That is, for any subset X of G, X is an open subgroup if and only if for all $x \in X$, there exists an open normal subgroup H_x such that $xH_x \in X$.

(4) 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 first give an easy example:

Example A.9. Let K be a finite field with q 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 K^s. The extension K_n/K is cyclic with Galois group $\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/n\mathbb{Z} = \langle \varphi_n \rangle$ 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 $G \simeq \widehat{\mathbb{Z}}$ is topologically generated by $\varphi \in G$: $\varphi(x) = x^q$ for $x \in K^s$, i.e. with obvious notations, any elements of G can be written uniquely as $g = \varphi^a$ with $a \in \widehat{\mathbb{Z}}$. φ is called the *arithmetic Frobenius* and φ^{-1} is called the *geometric Frobenius* of G.

In the case $K = \mathbb{Q}$, let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The structure of $G_{\mathbb{Q}}$ is far from being completely understood. An open question is: Let J be a finite groups. Is it true that 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).

For each place p of $\mathbb{Q}$ (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

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

one can identify $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ to 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 know properties about each G_p.

This phenomenon is not unique. There is a generalization of the above to number fields, i.e., a finite extension of $\mathbb{Q}$, whose completions are finite extensions of $\mathbb{Q}_p$. There is also an analogue for global function fields, i.e., finite extensions of $k(x)$ with k a finite field, whose completions are of the type $k'((y))$, where k' is a finite extension of k. As a consequence, we are led to study the properties of local fields.

A.2 Witt vectors and complete discrete valuation rings

A.2.1 Nonarchimedean fields and local fields.

First let us recall the definition of valuation.

Definition A.10. *Let A be a ring. If $v : A \to \mathbb{R} \cup \{+\infty\}$ is a function such that*

(1) $v(a) = +\infty$ if and only if $a = 0$,
(2) $v(ab) = v(a) + v(b)$,
(3) $v(a + b) \geq \min\{v(a), v(b)\}$,

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

The above definition of valuation is usually called *a valuation of height* 1.

For a ring A with a valuation v, one can always define a topology to A with a neighborhood basis of 0 given by $\{x : v(x) > n\}$, then A becomes a topological ring. The valuation v on A defines an *absolute value*: $|a| = e^{-v(a)}$. For any $a \in A$, then

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

If v_1 and v_2 are valuations on A, then v_1 and v_2 are *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 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 $v(a/b) = v(a) - v(b)$. Then the *ring of valuations* (often called the *ring of integers*)

$$\mathcal{O}_K = \{a \in K \mid v(a) \geq 0\} \tag{A.1}$$

is a local ring, with the maximal ideal $\mathfrak{m}_K$ given by

$$\mathfrak{m}_K = \{a \in K \mid v(a) > 0\}, \tag{A.2}$$

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

Definition A.11. *A field K with a valuation v is called a* valuation field*.*

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. Choose $\pi \in \mathcal{O}_K$, $\pi \neq 0$, and $v(\pi) > 0$, let

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

Then $\mathcal{O}_{\widehat{K}}$ is again a domain and $\widehat{K} = \mathcal{O}_{\widehat{K}}[1/\pi]$.

Remark A.12. The ring $\mathcal{O}_{\widehat{K}}$ does not depend on the choice of π. Indeed, if $v(\pi) = r > 0$, $v(\pi') = s > 0$, for any $n \in \mathbb{N}$, there exists $m_n \in \mathbb{N}$, such that $\pi^{m_n} \in \pi'^n \mathcal{O}_K$, so

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

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

Remark A.15. By abuse of notations, we will set the extended valuation $v' = v$.

Let F be a complete field with respect to a discrete valuation, let F' be any algebraic extension of F. We denote by v_F the unique valuation of F' extending the given valuation of F such that $v_F(F^*) = \mathbb{Z}$. v_F is called the normalized valuation of F.

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

Definition A.16. *A* local field *is a complete discrete valuation field whose residue field is perfect of characteristic $p > 0$. Thus a local field is always a complete nonarchimedean field.*

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

Example A.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 the normalized valuation and perfect residue field k, $\operatorname{char} k = p > 0$. Let π be a uniformizing parameter of K. Then $v_K(\pi) = 1$ and $\mathfrak{m}_K = (\pi)$. One has an isomorphism

$$\mathcal{O}_K \xrightarrow{\sim} \varprojlim_n \mathcal{O}_K/\mathfrak{m}_K^n = \varprojlim_n \mathcal{O}_K/(\pi^n),$$

the topology defined by the valuation for $\mathcal{O}_K$ is the same as the topology of the inverse limit with the discrete topology in each $\mathcal{O}_K/\mathfrak{m}_K^n$. Thus we have the following propositions:

Proposition A.18. *The local field K is locally compact (equivalently, $\mathcal{O}_K$ is compact) if and only if the residue field k is finite.*

Proposition A.19. *Let S be a set of representatives of k in $\mathcal{O}_K$. Then every element $x \in \mathcal{O}_K$ can be uniquely written as*

$$x = \sum_{\substack{i \geq 0 \\ s_i \in S}} s_i \pi^i \tag{A.3}$$

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

$$x = \sum_{\substack{i \geq -n \\ s_i \in S}} s_i \pi^i. \tag{A.4}$$

As $p \in \mathfrak{m}_K$, by the binomial theorem, for $a, b \in \mathcal{O}_K$, we have the following fact:

$$a \equiv b \bmod \mathfrak{m}_K \quad \Longrightarrow \quad a^{p^n} \equiv b^{p^n} \bmod \mathfrak{m}_K^{n+1} \text{ for } n \geq 0. \tag{A.5}$$

Proposition A.20. *For the natural map $\mathcal{O}_K \to k$, there is a natural section $r : k \to \mathcal{O}_K$ which is unique and multiplicative.*

Proof. Let $a \in k$. For any $n \in \mathbb{N}$, there exists a unique $a_n \in k$ such that $a_n^{p^n} = a$, $a_{n+1}^p = a_n$. Let $\widehat{a}_n$ be a lifting of a_n in $\mathcal{O}_K$.

By (A.5), $\widehat{a}_{n+1}^p \equiv \widehat{a}_n \bmod \mathfrak{m}_K$ implies that $\widehat{a}_{n+1}^{p^{n+1}} \equiv \widehat{a}_n^{p^n} \bmod \mathfrak{m}_K^{n+1}$. Therefore $r(a) := \lim\limits_{n \to \infty} \widehat{a}_n^{p^n}$ exists. By (A.5) again, $r(a)$ is found to be independent of the choice of the liftings of the $\widehat{a}_n$'s. It is easy to check that r is a section of ρ and is multiplicative. Moreover, if t is another section, we can always choose $\widehat{a}_n = t(a_n)$, then

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

hence the uniqueness follows. □

Remark A.21. This element $r(a)$ is usually called the *Teichmüller representative* of a, often denoted as $[a]$.

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

Theorem A.22. *If K is a local field of characteristic p, then*

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

Remark A.23. This theorem is true for K with residue field k of equal characteristic. See Serre [Ser80], Chap. II for the proof.

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

A.2.2 Witt vectors.

Let p be a prime number, A be a commutative ring. Let X_i, Y_i, $i\in\mathbb{N}$ be indeterminates and let

$$A[\underline{X},\underline{Y}]=A[X_0,X_1,\cdots,X_n,\cdots;Y_0,Y_1,\cdots,Y_n,\cdots].$$

Lemma A.24. *For all $\Phi\in\mathbb{Z}[X,Y]$, there exists a unique sequence $\{\Phi_n\}_{n\in\mathbb{N}}$ in $\mathbb{Z}[\underline{X},\underline{Y}]$ such that*

$$\begin{aligned}&\Phi(X_0^{p^n}+pX_1^{p^{n-1}}+\cdots+p^nX_n,Y_0^{p^n}+Y_1^{p^{n-1}}+\cdots+p^nY_n)\\&=(\Phi_0(\underline{X},\underline{Y}))^{p^n}+p\,(\Phi_1(\underline{X},\underline{Y}))^{p^{n-1}}+\cdots+p^n\,\Phi_n(\underline{X},\underline{Y}).\end{aligned}\tag{A.6}$$

Moreover,

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

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

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

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 Φ_{n+1} has coefficients in $\mathbb{Z}$, we need to prove that

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

It is verified 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, we get the lemma. □

Remark A.25. The polynomials $W_n = \sum\limits_{i=0}^{n} p^i X_i^{p^{n-i}}$, $n \in \mathbb{N}$, are called the *Witt polynomials* for the sequence $(X_0, \cdots, X_n, \cdots)$. One can easily see that $X_n \in \mathbb{Z}[p^{-1}][W_0, \cdots, W_n]$ for each n.

For $n \geq 1$, let $W_n(A) = A^n$ as a set. Applying the above lemma, if $\Phi = X + Y$, we set $S_i := \Phi_i \in \mathbb{Z}[X_0, X_1, \cdots, X_i; Y_0, Y_1, \cdots, Y_i]$; if $\Phi = XY$, we set $P_i := \Phi_i \in \mathbb{Z}[X_0, X_1, \cdots, X_i; Y_0, Y_1, \cdots, Y_i]$.

For two vectors $a = (a_0, a_1, \cdots, a_{n-1}), b = (b_0, b_1, \cdots, b_{n-1}) \in W_n(A)$, put

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

where

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

Remark A.26. It is clear that

$$S_0 = X_0 + Y_0, P_0 = X_0 Y_0. \tag{A.7}$$

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

$$S_1 = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_0^i\, Y_0^{p-i}. \tag{A.8}$$

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

$$P_1 = X_1\,Y_0^p + X_0^p\,Y_1 + p\,X_1\,Y_1. \tag{A.9}$$

But for general n, it is too complicated to write down S_n and P_n explicitly.

Consider the map

$$\begin{array}{ccc} W_n(A) & \xrightarrow{\rho} & A^n \\ (a_0, a_1, \cdots, a_{n-1}) & \longmapsto & (w_0, w_1, \cdots, w_{n-1}) \end{array}$$

where $w_i = W_i(a) = a_0^{p^i} + p\,a_1^{p^{i-1}} + \cdots + p^i\,a_i$. Then

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

We notice the following facts:

(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 $W_n(A) \subset W_n(A[\frac{1}{p}])$. Thus $W_n(A)$ is a subring with the identity $1 = (1, 0, 0, \cdots)$, as $a, b \in W_n(A)$ implies that $a - b \in W_n(A)$, when applying Lemma A.24 to $\Phi = X - Y$.

(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

$$W_n(I) = \{(a_0, a_1, \cdots, a_n) \mid a_i \in I\}$$

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.

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

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

This is a surjective homomorphism of rings for each n. Define

$$W(A) = \varprojlim_{n \in \mathbb{N}^*} W_n(A).$$

Put the topology of the inverse limit with the discrete topology on each $W_n(A)$, then $W(A)$ can be viewed as a topological ring. The elements in $W(A)$ can be written as $(a_0, a_1, \cdots, a_i, \cdots)$.

Definition A.27. *The ring $W_n(A)$ is called the* ring of Witt vectors of length n *of A, an element of it 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 it 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

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

The map

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

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

Example A.28. One has $W(\mathbb{F}_p) = \mathbb{Z}_p$.

W_n and W are actually functorial: let $h : A \longrightarrow B$ 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 similarly the homomorphism $W(h) : W(A) \to W(A)$.

Remark A.29. In fact, W_n is represented by an affine group scheme over $\mathbb{Z}$:

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

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 A.30. 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. Similarly $\rho : W(A) \to A^{\mathbb{N}}$ is not an isomorphism either.

Maps related to the ring of Witt vectors.

Let A be a commutative ring. We can define the maps $\mathcal{V}$, r and φ related to $W(A)$.

(1) The shift map $\mathcal{V}$.
We define

$$\mathcal{V} : W(A) \to W(A), \quad (a_0, \cdots, a_n, \cdots) \mapsto (0, a_0, \cdots, a_n, \cdots),$$

which is called the *shift map*. It is additive: it suffices to verify this fact when p is invertible in A, and in that case the homomorphism $\rho : W(A) \to A^{\mathbb{N}}$ transforms V into the map which sends $(w_0, w_1, \cdots)$ to $(0, pw_0, \cdots)$.

By passage to the quotient, one deduces from $\mathcal{V}$ an additive map of $W_n(A)$ into $W_{n+1}(A)$. There are exact sequences

$$0 \to W_k(A) \overset{\mathcal{V}^r}{\to} W_{k+r}(A) \to W_r(A) \to 0.$$

(2) The Teichmüller map r.

We define a map

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

When p is invertible in A, ρ transforms r into the mapping that sends x to $(x, x^p, \cdots, x^{p^n}, \cdots)$. One deduces by the same reasoning as in (1) the following formulas:

$$r(xy) = r(x)r(y), \quad x, y \in A$$

$$(a_0, a_1, \cdots) = \sum_{n=0}^{\infty} \mathcal{V}^n(r(a_n)), \quad a_i \in A$$

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

(3) The Frobenius map φ.

Suppose k is a ring of characteristic p. The homomorphism

$$k \to k, \quad x \mapsto x^p$$

induces a ring homomorphism:

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

which is called the *Frobenius map.*

A.2.3 Structure of complete discrete valuation rings with unequal characteristic.

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

Definition A.31. *We say that a ring A of characteristic p is* perfect *if the endomorphism $x \to x^p$ of A is an automorphism, i.e., every element of $x \in A$ has a unique p-th root, denoted $x^{p^{-1}}$. When A is a field, this is the usual definition of a perfect field.*

Definition A.32. *If A is a ring which is Hausdorff and complete for a decreasing filtration of ideals $\mathfrak{a}_1 \supset \mathfrak{a}_2 \cdots$ such that $\mathfrak{a}_m \cdot \mathfrak{a}_n \subset \mathfrak{a}_{m+n}$, and if the ring $A/\mathfrak{a}_1$ is perfect of characteristic p, then A is called a* p-ring. *If furthermore the filtration is the p-adic filtration $\{p^n A\}_{n \in \mathbb{N}}$, with the residue ring $k = A/pA$ perfect, and if p is not a zero-divisor in A, then A is called a* strict p-ring.

Proposition A.33. *Let A be a p-ring, then:*

(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) In order that $a \in A$ belong to $S = f(k)$, it is necessary and sufficient that a be 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. The proof is very similar to the proof of Proposition A.20. We omit it here. See [Ser80] for details. □

Proposition A.33 implies that when A is a p-ring, it always has the system of multiplicative representatives $f : A/\mathfrak{a}_1 \to A$, and for every sequence $\alpha_0, \cdots, \alpha_n, \cdots$, of elements of $A/\mathfrak{a}_1$, the series

$$\sum_{i=0}^{\infty} f(\alpha_i)p^i \tag{A.10}$$

converges to an element $a \in A$. If furthermore A is a strict p-ring, every element $a \in A$ can be uniquely expressed in the form of a series of type (A.10). 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 A.34. Let X_α be a family of indeterminates, and let S be the ring of $p^{-\infty}$-polynomials in the X_α with integer coefficients, i.e., $S = \bigcup\limits_{n\geq 0} \mathbb{Z}[X_\alpha^{p^{-n}}]$ If one provides S with the p-adic filtration $\{p^nS\}_{n\geq 0}$ and completes it, one obtains a strict p-ring that will be denoted $\widehat{S} = \widehat{\mathbb{Z}[X_\alpha^{p^{-\infty}}]}$. The 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 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 A.35. *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 $\theta : \mathbb{Z}[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}] \to A$ 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 θ induces, on the residue rings, a homomorphism $\bar{\theta} : \mathbb{F}_p[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}] \to k$ which sends X_i to α_i and Y_i to β_i. Since θ commutes with the multiplicative representatives, one thus has

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

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

Definition A.36. *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 $e = v(p)$ is called the* absolute ramification index *of A. A is called* absolutely unramified *if $e = 1$, i.e., if p is a local uniformizer of A.*

Remark A.37. If A is a strict p-ring, and its residue ring A/pA is a field, then A is a complete discrete valuation ring, absolutely unramified.

Proposition A.38. *Suppose A and A' are two p-rings with residue rings k and k', suppose A is also strict. For every homomorphism $h : k \to k'$, there exists exactly one homomorphism $g : A \to A'$ such that the diagram*

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

is commutative. As a consequence, two strict p-rings with the same residue ring are canonically isomorphic.

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

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

hence the uniqueness. But by Proposition A.35, g defined by the above way is indeed a homomorphism. □

Theorem A.39. *For every perfect ring k of characteristic p, there exists a unique strict p-ring H with residue ring k. In fact $H = W(k)$.*

Proof. The uniqueness follows from Proposition A.38. For the existence, if $k = \mathbb{F}_p[X_\alpha^{p^{-\infty}}]$, then $H = \widehat{S}$ satisfies the condition. In general, as every perfect ring is a quotient of a ring of the type $\mathbb{F}_p[X_\alpha^{p^{-\infty}}]$, we just need to show if $h : k \to k'$ is a surjective homomorphism and if there exists a strict p-ring H_k with residue ring k, then there exists a strict p-ring $H_{k'}$ with residue ring k'.

Indeed, for $a, b \in H_k$, we say $a \equiv b$ if the images of their coordinates by h are equal. This is an equivalence relation, and if $a \equiv b, a' \equiv b'$, then $a * a' \equiv b * b'$ by Proposition A.35. Let $H_{k'}$ be the quotient of H_k modulo this equivalence relation. It is routine to check $H_{k'}$ is a strict p-ring with residue ring k'.

Now for the second part, let H be the strict p-ring with residue ring k, and let $f : k \to H$ be the multiplicative system of representatives of H. Define

$$\theta : W(k) \to H, \quad (a_0, \cdots, a_n, \cdots) \mapsto \sum_{i=0}^{\infty} f(a_i^{p^{-i}})p^i.$$

It is a bijection. When $H = \widehat{S}$, $\mathfrak{a} = (X_0, \cdots)$, $\mathfrak{b} = (Y_0, \cdots)$, we have

$$\begin{aligned}\sum_{i=0}^{n} f(X_i^{p^{-i}})p^i + \sum_{i=0}^{n} f(Y_i^{p^{-i}})p^i &= W_n(\underline{X}^{p^{-n}}) + W_n(\underline{Y}^{p^{-n}}) \\ &= W_n(S_0(\underline{X}^{p^{-n}}, \underline{Y}^{p^{-n}}), \cdots),\end{aligned}$$

$$\sum_{i=0}^{n} f(S_i(\mathfrak{a}, \mathfrak{b})^{p^{-i}})p^i = W_n(f(S_i(\mathfrak{a}, \mathfrak{b})^{p^{-n}})).$$

Since

$$S_i(X^{p^{-n}}, Y^{p^{-n}}) \equiv f(S_i(\underline{X}^{p^{-n}}, \underline{Y}^{p^{-n}})) = f(S_i(\mathfrak{a}, \mathfrak{b})^{p^{-n}}) \mod p,$$

we get $\theta(\mathfrak{a}) + \theta(\mathfrak{b}) \equiv \theta(\mathfrak{a} + \mathfrak{b}) \bmod p^{n+1}$, for any $n \geq 0$. Therefore, $\theta(\mathfrak{a}) + \theta(\mathfrak{b}) = \theta(\mathfrak{a} + \mathfrak{b})$. Similarly, $\theta(\mathfrak{a})\theta(\mathfrak{b}) = \theta(\mathfrak{a}\mathfrak{b})$. It follows that the formulas are valid without any restriction on H, $\mathfrak{a}$ and $\mathfrak{b}$. So θ is an isomorphism. □

By the above theorem and Proposition A.38, we immediately have:

Corollary A.40. *For k, k' perfect rings of characteristic p,* $\mathrm{Hom}(k, k') = \mathrm{Hom}(W(k), W(k'))$.

Corollary A.41. *If k is a field, perfect or not, then $\mathcal{V}\varphi = p = \varphi\mathcal{V}$.*

Proof. It suffices to check this when k is perfect; in that case, applying the isomorphism θ above, one finds:

$$\theta(\varphi\mathcal{V}\mathfrak{a}) = \sum_{i=0}^{\infty} f(a_i^{p^{-i}})p^{i+1} = p\theta(\mathfrak{a}) = \theta(p\mathfrak{a}),$$

which gives the identity. □

Now we can state the main theorems of the unequal characteristic case.

Theorem A.42. *(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 $\psi : W(k) \to A$ which makes the diagram

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

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

Proof. (1) is a special case of Theorem A.39.

For (2), the existence and uniqueness of ψ follow from Proposition A.38, since A is a p-ring. As A is of characteristic 0, ψ is injective. If π is a uniformizer of A, then every $a \in A$ can be uniquely written as $a = \sum\limits_{i=0}^{\infty} f(\alpha_i)\pi^i$ for $\alpha_i \in k$. Replaced π^e by $p \times$ (unit), then a is uniquely written as

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

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

Remark A.43. From now on, we denote the Teichmüller representative $r(a)$ of $a \in k$ by $[a]$, then by the proof of Theorem A.39, the homomorphism $\psi : W(k) \to A$ in the above theorem is given by

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

For the case $A = W(k)$, for $a \in k$, the Teichmüller representative $r(a)$ is the same as the element $r(a) = (a, 0, \cdots)$, we have

$$(a_0, a_1, \cdots) = \sum_{n=0}^{\infty} p^n [a_n^{p^{-n}}]. \tag{A.11}$$

A.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 more complicated. We first quote two theorems without proof from commutative algebra (cf. Matsumura [Mat86], § 29, pp 223-225):

Theorem A.44 (Theorem 29.1, [Mat86]). *Let $(A, \pi A, k)$ be a discrete valuation ring and K an extension of k; then there exists a discrete valuation ring $(B, \pi B, K)$ containing A.*

Theorem A.45 (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 A.46. The above theorem is a generalization of Proposition A.38.

Applying $A = \mathbb{Z}_p$ to Theorem A.44, then if K is a given field of characteristic p, there exists an absolutely unramified discrete valuation ring R of characteristic 0 with residue field K. By Theorem A.45, this ring R is unique up to isomorphism.

Definition A.47. *Let k be a field of characteristic $p > 0$, the* Cohen ring $\mathcal{C}(k)$ *is the unique (up to isomorphism) absolutely unramified discrete valuation ring of characteristic 0 with residue field 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

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

If k is perfect, only the empty set is a p-basis of k; if k is imperfect, there always exists nonempty sets satisfying condition (1), then any maximal such set (which must exist, by Zorn's Lemmma) must also satisfy (2) 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 $I_n = \prod_B \{0, \cdots, p^n - 1\}$, 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

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

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 Corollary A.41, 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. Hence we proved

Proposition A.48. *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 A.49. *The canonical projection* $\mathrm{pr} : W_{n+1}(k) \to W_n(k)$ *induces a surjection $\pi : \mathcal{C}_{n+1}(k) \to \mathcal{C}_n(k)$.*

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 π 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 π is surjective, it suffices to show that the associate graded map is surjective. But for $r < n$, we have the following commutative diagram

$$\begin{tikzcd}
p^r\mathcal{C}_{n+1}(k)/p^{r+1}\mathcal{C}_{n+1}(k) \arrow[r, "\mathrm{gr}\,\pi"] \arrow[d, "j"'] & p^r\mathcal{C}_n(k)/p^{r+1}\mathcal{C}_n(k) \arrow[d, "j'"'] \\
V^rW_{n+1}(k)/V^{r+1}W_{n+1}(k) \simeq k \arrow[r, "\mathrm{gr\,pr}=\mathrm{Id}"] & V^rW_n(k)/V^{r+1}W_n(k) \simeq k
\end{tikzcd}$$

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 $\mathrm{gr}\,\pi$ is surjective for $r < n$. For $r = n$, $p^n\mathcal{C}_n(k) = 0$. Then $\mathrm{gr}\,\pi$ is surjective at every grade and hence π is surjective. □

By Proposition A.48, we thus have

Theorem A.50. *The ring* $\varprojlim_n \mathcal{C}_n(k)$ *is the Cohen ring* $\mathcal{C}_n(k)$ *of* k.

Remark A.51. (1) By construction, $\mathcal{C}(k)$ is identified as a subring of $W(k)$; moreover, for $k_0 = \cap_{n\in N} k^{p^n}$ the largest perfect subfield of k, $\mathcal{C}(k)$ contains $W(k_0)$.

(2) 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 $\alpha \in I_n$.

A.3 Galois groups of local fields

In this section, we let K be a local field with the residue field $k = k_K$ perfect of characteristic p and the normalized valuation v_K. Let $\mathcal{O}_K$ be the ring of integers of K, whose maximal ideal is $\mathfrak{m}_K$. Let $U_K = \mathcal{O}_K^* = \mathcal{O}_K - \mathfrak{m}_K$ 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:

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

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

A.3.1 Ramification groups of finite Galois extension.

Let L/K be a 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.

Lemma A.52. *Let* $\sigma \in G$, *and let* i *be an integer* ≥ -1. *Then the following three conditions are equivalent:*

(1) σ *operates trivially on the quotient ring* $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$.

(2) $v_L(\sigma(a) - a) \geq i + 1$ *for all* $a \in \mathcal{O}_L$.

(3) $v_L(\sigma(x) - x) \geq i + 1$.

Proof. This is a trivial exercise. □

Proposition A.53. *For each integer $i \geq -1$, let G_i be the set of $\sigma \in G$ satisfying conditions (1), (2), (3) of Lemma A.52. 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 $\sigma \in G$ and every $\tau \in G_i$, since G_i acts trivially on the quotient ring $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$, we have $\sigma\tau\sigma^{-1}(x) \equiv x \bmod \mathfrak{m}_L^{i+1}$, namely, $\sigma\tau\sigma^{-1} \subseteq G_i$. Thus, G_i is a normal subgroup for all i. The remaining part follows just by definition. □

Definition A.54. *The group G_i is called the i-th* ramification group *of G (or of L/K).*

We denote the inertia subgroup G_0 by $I(L/K)$ and its invariant field by $L_0 = (L/K)^{\mathrm{ur}}$; we denote by $G_1 = P(L/K)$ and call it the wild inertia subgroup *of G, and denote its invariant field by $L_1 = (L/K)^{\mathrm{tame}}$.*

Remark A.55. The ramification groups define a filtration of G. The quotient G/G_0 is isomorphic to the Galois group $\mathrm{Gal}(k_L/k)$ of the residue extension.

The field L_0 is the maximal unramified subextension inside L. In Proposition A.59, we shall see that L_1 is the maximal tamely ramified subextension inside L.

Remark A.56. 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 $H_i = G_i \cap H$. 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.

We shall describe the quotient G_i/G_{i+1} in the following.

Let π be a uniformizer of L.

Proposition A.57. *Let i be a non-negative integer. In order that an element σ of the inertia group G_0 belongs to G_i, it is necessary and sufficient that $\sigma(\pi)/\pi = 1 \bmod \mathfrak{m}_L^i$.*

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

We recall the following result:

Proposition A.58. *(1) $U_L^0/U_L^1 = k_L^*$;*

(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.

Back to the ramification groups, then the equivalence in Proposition A.57 can be translated to

$$\sigma \in G_i \Leftrightarrow \sigma(\pi)/\pi \in U_L^i.$$

We have a more precise description of G_i/G_{i+1} following Proposition A.58:

Proposition A.59. *The map which to $s \in G_i$, assigns $s(\pi)/\pi$, induces by passage to the quotient an isomorphism θ_i of the quotient group G_i/G_{i+1} onto a subgroup of the group U_L^i/U_L^{i+1}. This isomorphism is independent of the choice of the uniformizer π.*

(1) The group G_0/G_1 is cyclic, and is mapped isomorphically by θ_0 onto a subgroup of $\boldsymbol{\mu}(k_L)$, the group of roots of unity contained in k_L. Its order is prime to p, the characteristic of the residue field k_L.

(2) If the characteristic of k_L is $p \neq 0$, the quotients G_i/G_{i+1}, $i \geq 1$, are abelian groups, and are direct products of cyclic groups of order p. The group G_1 is a p-group, the inertia group G_0 has the following property: it 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 A.60. The group G_0 is solvable. If k is a finite field, then G is also solvable.

In fact, we can write 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^* 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

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

The homomorphism θ_0 is the canonical isomorphism

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

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

By the short exact sequence

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

hence $\mathrm{Gal}(L_1/K)$ 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 $\mathrm{Gal}(k_L/k)$.

A.3.2 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

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

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 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 $v_K((K^s)^*) = \mathbb{Q}$, 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 an algebraic closure of k. We use the notations

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

Note that P_K is a pro-p-group, an 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

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

If N divides N', then $N' = N\,m$, and the transition map is

$$\begin{aligned} \boldsymbol{\mu}_{N'}(\bar{k}) &\longrightarrow \boldsymbol{\mu}_N(\bar{k}) \\ \varepsilon &\longmapsto \varepsilon^m. \end{aligned}$$

Therefore we get

Proposition A.61. *If we write* $\boldsymbol{\mu}_{\ell^\infty} = \mathbb{Z}_\ell(1)$ *(which is the Tate twist of* $\mathbb{Z}_\ell$*, which we shall introduce in §1.1.4), then*

$$I_K/P_K \xrightarrow[\textit{canonically}]{\simeq} \prod_{\ell\neq p} \mathbb{Z}_\ell(1). \tag{A.12}$$

We denote

$$\widehat{\mathbb{Z}}' = \prod_{\ell \neq p} \mathbb{Z}_\ell, \qquad \widehat{\mathbb{Z}}'(1) = \prod_{\ell \neq p} \mathbb{Z}_\ell(1),$$

where $\widehat{\mathbb{Z}}'(1)$ is isomorphic, but not canonically to $\widehat{\mathbb{Z}}'$. Then

$$I_K/P_K \simeq \widehat{\mathbb{Z}}'(1) = \prod_{\ell \neq p} \mathbb{Z}_\ell(1).$$

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

A.3.3 The functions $\boldsymbol{\Phi}$ and $\boldsymbol{\Psi}$.

Assume $G = \mathrm{Gal}(L/K)$ finite. Set

$$i_G : \quad G \to \mathbb{N}, \quad \sigma \mapsto v_L(\sigma(x) - x). \tag{A.13}$$

The function i_G has the following properties:

(1) $i_G(\sigma) \geq 0$ and $i_G(1) = +\infty$;
(2) $i_G(\sigma) \geq i + 1 \Leftrightarrow \sigma \in G_i$;
(3) $i_G(\tau\sigma\tau^{-1}) = i_G(\sigma)$;
(4) $i_G(\sigma\tau) \geq \min(i_G(\tau), i_G(\sigma))$.

Let H be a subgroup of G. Let K' be the subextension of L fixed by H. Following Remark A.56, we have

Proposition A.62. *For every $\sigma \in H$, $i_H(\sigma) = i_G(\sigma)$, and $H_i = G_i \cap H$.*

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

Proposition A.63. *For every $\delta \in G/H$,*

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

where $e' = e_{L/K'}$.

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

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

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

Let $f \in \mathcal{O}_{K'}[X]$ be the minimal polynomial of x over the intermediate field K'. Then $f(X) = \prod_{\tau \in H}(X - \tau(x))$. Denote by $\sigma(f)$ the polynomial obtained from f by transforming each of its coefficients by σ. Clearly $\sigma(f)(X) = \prod(X - \sigma\tau(x))$. As $\sigma(f) - f$ has coefficients divisible by $\sigma(y) - y$, one sees that $a = \sigma(y) - y$ divides $\sigma(f)(x) - f(x) = \sigma(f)(x) = \pm b$.

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 $g(X) - y$ has x as root and has all its coefficients in $\mathcal{O}_{K'}$; it is therefore divisible by the minimal polynomial f: $g(X) - y = f(X)h(X)$ with $h \in \mathcal{O}_{K'}[X]$. Transform this equation by σ and substitute x for X in the result; ones gets $y - \sigma(y) = \sigma(f)(x)\sigma(h)(x)$, which shows that $b = \pm\sigma(f)(x)$ divides a. □

Let u be a real number ≥ 1. Define $G_u = G_i$ where i is the smallest integer $\geq u$. Thus

$$\sigma \in G_u \Leftrightarrow i_G(\sigma) \geq u + 1.$$

Put

$$\Phi(u) = \int_0^u (G_0 : G_t)^{-1} dt, \tag{A.14}$$

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

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

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

$$\Phi(u) = \frac{1}{g_0}(g_1 + g_2 + ... + g_m + (u - m)g_{m+1}), \text{ with } g_i = |G_i|. \tag{A.15}$$

In particular,

$$\Phi(m) + 1 = \frac{1}{g_0} \sum_{i=0}^{m} g_i. \tag{A.16}$$

Immediately one can verify

Proposition A.64. *(1) The function Φ is continuous, piecewise linear, increasing and concave.*

(2) $\Phi(0) = 0$.

(3) If we denote by Φ'_r and Φ'_l the right and left derivatives of Φ, then $\Phi'_l = \Phi'_r = \frac{1}{(G_0:G_u)}$, if u is not an integer; $\Phi'_l = \frac{1}{(G_0:G_u)}$ and $\Phi'_r = \frac{1}{(G_0:G_{u+1})}$, if u is an integer.

Moreover, the proposition above characterizes the function Φ.

Proposition A.65. $\Phi(u) = \frac{1}{g_0} \sum\limits_{\sigma \in G} \min\{i_G(\sigma), u + 1\} - 1.$

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

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

Hence $\theta = \varPhi$. □

Theorem A.66 (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 $v = \varPhi_{L/K'}(u)$.*

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

$$i_{G/H}(\sigma') - 1 = \varPhi_{L/K'}(i_G(\sigma) - 1). \tag{A.17}$$

Let $m = i_G(\sigma)$. If $\tau \in H$ belongs to $H_{m-1} = G_{m-1}(L/K')$, then $i_G(\tau) \geq m$, and $i_G(\sigma\tau) \geq m$ and so that $i_G(\sigma\tau) = m$. If $\tau \notin H_{m-1}$, then $i_G(\tau) < m$ and $i_G(\sigma\tau) = i_G(\tau)$. In both cases we therefore find that $i_G(\sigma\tau) = \min\{i_G(\tau), m\}$. Applying Proposition A.63, since $i_G(\tau) = i_H(\tau)$ and $e' = e_{L/K'} = |H_0|$, this gives

$$i_{G/H}(\sigma') = \frac{1}{e'}\sum_{\tau \in H} i_G(\sigma\tau) = \frac{1}{e'}\sum_{\tau \in H} \min\{i_G(\tau), m\}.$$

Proposition A.65 gives the formula (A.17), which in turn yields

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

Herbrand's Theorem is proved. □

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

Proposition A.67. *If K'/K is a Galois subextension of L/K, then*

$$\varPhi_{L/K} = \varPhi_{K'/K} \circ \varPhi_{L/K'} \quad \textit{and}\ \varPsi_{L/K} = \varPsi_{L/K'} \circ \varPsi_{K'/K}.$$

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 $G_u/H_u = (G/H)_v, v = \varPhi_{L/K'}(u)$. 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

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

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

We define the *upper numbering* of the ramification groups by

$$G^v := G_u, \text{ where } u = \Psi(v). \tag{A.18}$$

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

$$\Psi(v) = \int_0^v [G^0 : G^w] dw. \tag{A.19}$$

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

Proposition A.68. *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 the Herbrand theorem and Proposition A.67, 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. □

A.3.4 Different and discriminant.

Let L/K be a finite separable field extension. The ring of integers $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of finite rank.

Definition A.69. *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., an ideal of L given by*

$$\mathfrak{D}_{L/K} := \{x \in L \mid \mathrm{Tr}(x^{-1}y) \in \mathcal{O}_K \textit{ for } y \in \mathcal{O}_L\}. \tag{A.20}$$

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

$$[\mathfrak{D}^{-1}_{L/K} : \mathcal{O}_L] := (\det(\rho)) \tag{A.21}$$

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

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

Suppose $\{e_i\}$ is a basis of $\mathcal{O}_L/\mathcal{O}_K$, let $\{e_i^*\}$ be a dual basis of $\mathfrak{D}_{L/K}^{-1}$. Let $e_i = \rho(e_i^*)$, 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

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

where σ runs through K-monomorphisms of L into K^s. Note that $(\det \rho^{-1})$ is the norm of the fractional ideal $\mathfrak{D}_{L/K}^{-1}$, thus $\delta_{L/K} = N_{L/K}(\mathfrak{D}_{L/K})$.

Proposition A.70. *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 $\mathfrak{a} \neq 0$,

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

□

Corollary A.71. *Let $M/L/K$ be separable extensions of finite degrees. 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 A.70 to show that

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

□

Corollary A.72. *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 $n \geq 0$, $\mathrm{Tr}(\mathfrak{m}_L^n) = \mathfrak{m}_K^r$ where $r = [(m+n)/e]$.*

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 shows 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 A.73. *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 need the following formula of Euler:

Lemma A.74 (Euler).

$$\mathrm{Tr}(x^i/f'(x)) = \begin{cases} 0, & \text{if } i = 0, \cdots, n-2; \\ 1, & \text{if } i = n-1 \end{cases} \tag{A.22}$$

where $n = \deg f$.

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

Proof (Proof of Proposition A.73). 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 $(-1)^{n(n-1)}$. Hence $x^j/f'(x)$, $0 \leq j \leq n-1$ is a basis of $\mathfrak{D}_{L/K}^{-1}$. □

Proposition A.75. *Let L/K be a finite Galois extension of local fields with Galois group G. Then*

$$\begin{aligned} v_L(\mathfrak{D}_{L/K}) &= \sum_{s \neq 1} i_G(s) = \sum_{i=0}^{\infty} (|G_i| - 1) \\ &= \int_{-1}^{\infty} (|G_u| - 1) du = |G_0| \int_{-1}^{\infty} (1 - |G^v|^{-1}) dv. \end{aligned} \tag{A.23}$$

Thus

$$v_K(\mathfrak{D}_{L/K}) = \int_{-1}^{\infty} (1 - |G^v|^{-1}) dv. \tag{A.24}$$

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 (A.23) are easy. For the last equality,

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

(A.24) follows easily from (A.23), since $v_K = \frac{1}{|G_0|} v_L$. □

Corollary A.76. *Let $L/M/K$ be finite Galois extensions of local fields. Then*

$$v_K(\mathfrak{D}_{L/M}) = \int_{-1}^{\infty} \left(\frac{1}{|\operatorname{Gal}(M/K)|^v} - \frac{1}{|\operatorname{Gal}(L/K)|^v} \right) dv. \tag{A.25}$$

Proof. This follows from the transitive relation $\mathfrak{D}_{L/K} = \mathfrak{D}_{L/M}\mathfrak{D}_{M/K}$ and (A.24). □

A.4 Ramification in p-adic Lie extensions

A.4.1 Sen's filtration Theorem.

In this subsection, we shall give the proof of Sen's theorem about the Lie filtration and the ramification filtration agree in 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. Put

$$v_G = \inf\{v \mid v \geq 0, G^{v+\varepsilon} = 1 \text{ for } \varepsilon > 0\}$$

and

$$u_G = \inf\{u \mid u \geq 0, G_{u+\varepsilon} = 1 \text{ for } \varepsilon > 0\}.$$

Then

$$u_G = \Psi_G(v_G) \leq |G| v_G. \tag{A.26}$$

Lemma A.77. *One can always find 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 $\operatorname{Gal}(L'/K') = \operatorname{Gal}(L/K)$. 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. □

We first suppose $G = A$ is a finite abelian p-group.

Proposition A.78. *If $v \leq \frac{e_A}{p-1}$, then $(A^v)^p \subseteq A^{pv}$; if $v > \frac{e_A}{p-1}$, then $(A^v)^p = A^{v+e_A}$.*

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 $K_0 = W(k_0)[\frac{1}{p}]$ 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 fact that

$$\begin{aligned} U_v^p &\subset U_{pv}, \qquad \text{if } v \le \frac{e_A}{p-1} \\ U_v^p &= U_{v+e}, \qquad \text{if } v > \frac{e_A}{p-1}. \end{aligned}$$

and the following lemma. □

Lemma A.79. *Suppose K is a complete discrete valuation field with quasi-finite residue field. Let L/K be an abelian extension with Galois group A. Then the image of U_K^n under the reciprocity map $K^* \to G$ is dense in A^n.*

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

Corollary A.80. *For $n \in \mathbb{N}$, let $A_{(n)}$ be the n-torsion subgroup of A. If $v_A \le \frac{p}{p-1}e_A$, then $v_A \ge p^m v_{A/A_{(p^m)}}$ for all $m \ge 1$; if $v_A > \frac{p}{p-1}e_A$, then $v_A = v_{A/A_{(p)}} + e_A$.*

Proof. If $v_A \le \frac{p}{p-1}e_A$, then $t_m = p^{-m}v_A \le \frac{1}{p-1}e_A$, and $(A^{t_m+\varepsilon})^{p^m} = A^{p^m t_m+\varepsilon} = A^{v_A+\varepsilon} = 1$ for $\varepsilon > 0$, then $A^{t_m+\varepsilon} \subset A_{(p^m)}$ and thus $v_{A/A_{(p^m)}} \le p^{-m}v_A$.

If $v_A > \frac{p}{p-1}e_A$, then $t = v_A - e_A > \frac{1}{p-1}e_A$, and $(A^{t+\varepsilon})^p = A(t+\varepsilon+e_A) = A(v_A+\varepsilon)$ for $\varepsilon \ge 0$. Thus $v_A = v_{A/A_{(p)}} + e_A$. □

Definition A.81. *We call A* small *if $v_A \le \frac{p}{p-1}e_A$, or equivalently, if $(A^x)^p \subseteq A^{px}$ for all $x \ge 0$.*

Lemma A.82. *If A is small, then for every $m \ge 1$,*

$$u_A \ge p^{m-1}(p-1)(A_{(p^m)} : A_{(p)})u_{A/A_{(p^m)}}. \tag{A.27}$$

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

$$\begin{aligned} u_A =&\Psi_A(v_A) = \int_0^{v_A}(A : A^t)dt \ge \Psi_A(v_A) \ge \int_{p^{-1}v_A+\varepsilon}^{v_A}(A : A^t)dt \\ \ge&(v_A - p^{-1}v_A - \varepsilon)(A : A^{p^{-1}v_A+\varepsilon}) \ge \left(v_A \cdot \frac{p-1}{p} - \varepsilon\right)(A : A_{(p)}). \end{aligned}$$

The last inequality holds since $(A^{p^{-1}v_A+\varepsilon})^p = 1$ by Proposition A.78. Then by Corollary A.80,

$$u_A \ge v_A(A : A_{(p)}) \cdot \frac{p}{p-1} \ge p^{m-1}(p-1)v_{A/A_{(p^m)}}(A : A_{(p)}).$$

Since $u_{A/A_{(p^m)}} \le v_{A/A_{(p^m)}}(A : A_{(p^m)})$ by (A.26), we have the desired result.

We now suppose G is a p-adic Lie group of dimension $d > 0$ with a Lie filtration $\{G(n)\}$. We suppose $G(1)$ 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

$$\Psi_n = \Psi_{G/G(n)},\ v_n = v_{G/G(n)}, \quad u_n = u_{G/G(n)} = \Psi_n(v_n),\ e_n = e_{G(n)}. \quad \text{(A.28)}$$

Proposition A.83. *For each $n \geq 1$ we have $G^v \cap G(n) = G(n)^{\Psi_n(v)}$ for $v \geq 0$. In particular,*

$$G^v = G(n)^{u_n + (v - v_n)(G:G(n))}, \quad \text{for } v > v_n, \quad \text{(A.29)}$$

i.e.,

$$G^{v_n + te} = G(n)^{u_n + te_n}, \quad \text{for } t > 0. \quad \text{(A.30)}$$

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

$$v_{G(n)/G(n+r)} = u_n + (v_{n+r} - v_n)(G : G(n)). \quad \text{(A.31)}$$

Proof. We have

$$G^v \cap G(n) = G_{\Psi_G(v)} \cap G(n) = G(n)_{\Psi_G(v)} = G(n)^{\Phi_{G(n)}\Psi_G(v)} = G(n)^{\Psi_n(v)}$$

since $\Psi_G = \Psi_{G(n)}\Psi_n$. 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 (A.31) follows from (A.29). □

Proposition A.84. *There exists an integer n_1 and a constant c such that for all $n \geq n_1$,*

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

Proof. By (A.30), 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

$$G(n)/G(n+r) \xrightarrow{\log} p^n\mathscr{L}/p^{n+r}\mathscr{L} \xrightarrow{p^{-n}} \mathscr{L}/p^r\mathscr{L} \cong (\mathbb{Z}/p^r\mathbb{Z})^d. \quad \text{(A.32)}$$

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 A.82 with $A = G(n)/G(n+r)$, $m = r-1$. 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 A.80,

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

and by (A.31), 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 A.85. *There is a constant c such that*

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

for all n.

Remark A.86. The above theorem means that the filtration of G by ramification subgroups with the upper numbering agrees with the Lie filtration.

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 A.84 and (A.32) hold. We assume $n \geq n_1 > 1$.

Let c_1 be the constant given in Proposition A.84. Let $c_0 = c_1 + \frac{\alpha e}{p-1}$ for some constant $\alpha \geq 1$. By Proposition A.84, $G^{ne+c_0} \subset G_n$ for large n.

By (A.30),

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

Apply Proposition A.78 to $A = G(n)/G(2n+1)$, since $u_n + \frac{\alpha e_n}{p-1} > \frac{e_n}{p-1}$, we have

$$(G^{ne+c_0})^p G(2n+1) = G^{(n+1)e+c_0} G(2n+1). \tag{A.33}$$

Put

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

Then (A.33) 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 $\bar{G} = G/N$. Then $\bar{G}$ is a p-adic Lie group filtered by $\bar{G}(n) = \exp p^n \bar{\mathscr{L}}$ where $\bar{\mathscr{L}} = \mathscr{L}/I$.

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

Lemma A.87. $\dim \bar{G} = 0$, *i.e.,* $\bar{G} = 1$.

Proof (Proof of the Lemma). If not, we can apply the proceeding theory to $\bar{G}$ 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

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

since

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

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. □

A.4.2 Totally ramified $\mathbb{Z}_p$-extensions.

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

For the higher ramification groups Γ^v of Γ with the upper numbering, suppose $\Gamma^v = \Gamma(i)$ for $v_i < v \leq v_{i+1}$, then by Proposition A.84 or by Wyman's result [Wym69], we have $v_{n+1} = v_n + e$ for $n \gg 0$. By Herbrand's Theorem (Theorem A.66),

$$\operatorname{Gal}(K_n/K)^v = \Gamma^v \Gamma(n)/\Gamma(n) = \begin{cases} \Gamma(i)/\Gamma(n), & \text{if } v_i < v \le v_{i+1},\ i \le n; \\ 1, & \text{otherwise.} \end{cases} \tag{A.34}$$

Proposition A.88. *Let 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 $L = L_0 K_\infty$ 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 $L_n = L_0 K_n$. Then by (A.25),

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

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

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

as $n \to \infty$ by (A.34). Now the proposition follows from Corollary A.72. □

Corollary A.89. *For any $a > 0$, there exists $x \in L$, such that*

$$v_K(x) > -a \text{ and } \operatorname{Tr}_{L/K_\infty}(x) = 1. \tag{A.35}$$

Proof. For any $a > 0$, find $\alpha \in \mathcal{O}_L$ such that $v_K(\operatorname{Tr}_{L/K_\infty}(\alpha))$ is less than a. Let $x = \frac{\alpha}{\operatorname{Tr}_{L/K_\infty}(\alpha)}$, then x satisfies (A.35). □

Remark A.90. Clearly the proposition and the corollary are still true if replacing K_∞ by any field M such that $K_\infty \subset M \subset L$. (A.35) is called the *almost étale condition.*

Proposition A.91. *There is a constant c such that*

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

where a_n is bounded.

Proof. We apply (A.34) and (A.24), 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 A.92. *There is a constant c which is independent of n such that for $x \in K_n$, we have*

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

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

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

where $j = \left[\frac{i+d}{p}\right]$ (cf. Corollary A.72). Thus

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

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

Definition A.93. *For $x \in K_\infty$, if $x \in K_{n+m}$, we define*

$$R_n(x) = p^{-m} \operatorname{Tr}_{K_{n+m}/K_n}(x), \qquad R_{n+i}^*(x) = R_{n+i}(x) - R_{n+i-1}(x).$$

$R_n(x)$ is called Tate's normalized trace map*.*

Remark A.94. Use the transitive properties of the trace map and the fact $[K_{n+m} : K_n] = p^m$, one can easily see that $p^{-m} \operatorname{Tr}_{K_{n+m}/K_n}(x)$ does not depend on m such that $x \in K_{n+m}$.

For $n = 0$, we write $R_0(x) = R(x)$.

Proposition A.95. *There exists a constant $d > 0$ such that for all $x \in K_\infty$,*

$$v_K(x - R(x)) \geq v_K(\gamma x - x) - d.$$

Proof. We prove by induction on n an inequality

$$v_K(x - R(x)) \geq v_K(\gamma x - x) - c_n, \text{ if } x \in K_n \tag{A.36}$$

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

For $x \in K_{n+1}$, let $\gamma_n = \gamma^{p^n}$, then

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

thus

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

In particular, let $c_1 = e$, (A.36) 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 (A.36) for $n + 1$. □

Remark A.96. If we take K_n as a ground field instead of K and replace $R(x)$ by $R_n(x)$, from the proof we have a corresponding inequality with the same d.

By Corollary A.92, the linear operator R_n is continuous on K_∞ for each n and therefore extends to $\widehat{K}_\infty$ by continuity. As K_n is complete, $R_n(K_\infty) = K_n$ for each n. Denote

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

Then X_n is a closed subspace of $\widehat{K}_\infty$.

Proposition A.97. *(1) $\widehat{K}_\infty = K_n \oplus X_n$ for each 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, or if $v_K(\lambda - 1) > d$, then $\gamma - \lambda$ 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) Let $K_{n,0} = K_n \cap X_0$, then $K_n = K \oplus K_{n,0}$ and X_0 is the completion of $K_{\infty,0} = \cup K_{n,0}$. Note that $K_{n,0}$ is a finite dimensional K-vector, the operator $\gamma - 1$ is injective on $K_{n,0}$, and hence bijective on $K_{n,0}$ and on $K_{\infty,0}$. By Proposition A.95, then

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

for $y = (\gamma - 1)x \in K_{n,0}$. 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 con 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 A.95, 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 unchanged 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 $\gamma-\lambda$. □

A.5 Continuous Cohomology

A.5.1 Abelian cohomology.

Definition A.98. *Let G be a group. 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 the group 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 may be viewed as a *left $\mathbb{Z}[G]$-module* by setting

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

The G-modules form an *abelian category.*

Let M be a topological G-module. For any $n\in\mathbb{N}$, 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 for $n=0$, $C^0_{\text{cont}}(G,M):=M$. Let

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

be given by

$$\begin{aligned}
&(d_0a)(g)=g(a)-a;\\
&(d_1f)(g_1,g_2)=g_1(f(g_2))-f(g_1g_2)+f(g_1);\\
&(d_nf)(g_1,g_2,\cdots,g_n,g_{n+1})=g_1(f(g_2,\cdots,g_n,g_{n+1}))\\
&\qquad\qquad+\sum_{i=1}^{n}(-1)^i f(g_1,g_2,\cdots,g_{i-1},g_ig_{i+1},\cdots,g_n,g_{n+1})\\
&\qquad\qquad+(-1)^{n+1}f(g_1,g_2,\cdots,g_n).
\end{aligned}$$

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 A.99. *Set*

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

and call them as the group of continuous n-cocycles*, the group of* continuous n-coboundaries *and the* n-th continuous cohomology group *of M respectively.*

Clearly we have

Proposition A.100. *(1) $H^0_{\text{cont}}(G,M)=Z^0=M^G=\{a\in M\mid g(a)=a, \text{for all } g\in G\}$.*

(2)

$$H^1_{\text{cont}}(G,M)=\frac{Z^1}{B^1}=\frac{\{f:G\to M\mid f \textit{ continuous},\ f(g_1g_2)=g_1f(g_2)+f(g_1)\}}{\{\sigma_a=(g\mapsto g\cdot a-a):a\in M\}}.$$

Corollary A.101. *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 then induces morphism from $Z^n_{\text{cont}}(G,M_1)$ (resp. $B^n_{\text{cont}}(G,M_1)$ or $H^n_{\text{cont}}(G,M_1)$) to $Z^n_{\text{cont}}(G,M_2)$ (resp. $B^n_{\text{cont}}(G,M_2)$ or $H^n_{\text{cont}}(G,M_2)$).

Proposition A.102. *For a short exact sequence of topological G-modules*

$$0\longrightarrow M'\xrightarrow{\alpha} M\xrightarrow{\beta} M''\longrightarrow 0,$$

then there is an exact sequence

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

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

Proof. Note that for any $g\in G$, $\beta(g(x)-x)=\beta(g(x))-\beta(x)=g(\beta(x))-\beta(x)=g(a)-a=0$, Thus $g(x)-x\in\operatorname{Im}\alpha$, so that $\alpha^{-1}(g(x)-x)$ is meaningful.

The proof is routine. We omit it here. □

Remark A.103. From the above proposition, the functor $H^0(G,-)$ is left exact. In general, the category of topological G-modules *does not* have sufficiently many injective objects, and it is not possible to have a long exact sequence.

However, if β admits a continuous set theoretic section $s:M''\to M$, one can define a map

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

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

Two special cases.

(1). If G is a group with the discrete topology,

$$H^n(G,M) = H^n_{\text{cont}}(G,M)$$

and one has a long exact sequence.
(2). If G is a profinite group and M is equipped with the discrete topology, we also have a long exact sequence. In this situation, to say that G acts *continuously* means that, for all $a \in M$, the group $G_a = \{g \in G | g(a) = a\}$ is open in G. In this case, M is called a *discrete G-module.* We set

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

Denote by $\mathcal{H}$ the set of normal open subgroups of G, then one sees that the natural map

$$\varinjlim_{H\in\mathcal{H}} H^n(G/H, M^H) \xrightarrow{\sim} H^n(G,M)$$

is an isomorphism.

Example A.104. If G is a field and L is a Galois extension of K, then $G = \text{Gal}(L/K)$ is a profinite group and $H^n(G,M) = H^n(L/K,M)$ is the *Galois cohomology.* In particular, if $L = K^s$ is a separable closure of K, we write $H^n(G,M) = H^n(K,M)$.

A.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 $g \in G$, $x, y \in M$. We can define

$$H^0_{\text{cont}}(G,M) = M^G = \{x \in M \mid g(x) = x, \forall g \in G\}$$

and

$$Z^1_{\text{cont}}(G,M) = \{f : G \to M \text{ continuous} \mid f(g_1g_2) = f(g_1)\cdot g_1f(g_2)\}.$$

If $f, f' \in Z^1_{\text{cont}}(G,M')$, we say that f and f' are *cohomologous* if there exists $a \in M$ such that $f'(g) = a^{-1}f(g)g(a)$ for all $g \in G$. This defines an equivalence relation for the set of cocycles and $H^1_{\text{cont}}(G,M)$ is the set of equivalence classes. $H^1_{\text{cont}}(G,M)$ is actually a *pointed set* with the *distinguished point* being the trivial class $f(g) \equiv 1$ for all $g \in G$.

Definition A.105. *$H^1_{\text{cont}}(G,M)$ is* trivial *if it has only one 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

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

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

Proposition A.106. *Let* $1 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 1$ *be an exact sequence of continuous topological G-groups. Then there exists a long exact sequence of pointed sets:*

$$1 \to M'^G \overset{\alpha_0}{\to} M^G \overset{\beta_0}{\to} M''^G \overset{\delta}{\to} H^1(G, M') \overset{\alpha_1}{\to} H^1(G, M) \overset{\beta_1}{\to} H^1(G, M''),$$

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

$$\delta(c) = (\sigma \mapsto \alpha^{-1}(b^{-1}\sigma b)).$$

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

$$a_{\sigma\tau} = b^{-1}\sigma\tau(b) = b^{-1}\sigma(b) \cdot \sigma(b^{-1}\tau(b)) = a_\sigma\sigma(a_\tau),$$

thus a_σ satisfies the cocycle condition. If we choose b' other than b such that $\beta(b') = \beta(b) = c$, then $b' = ba$ for some $a \in A$, and

$$a'_\sigma = b'^{-1}\sigma(b') = a^{-1}b^{-1}\sigma(b)\sigma(a) = a^{-1}a_\sigma\sigma(a)$$

is cohomologous to a_σ.

Now we check the exactness:

(1). Exactness at M'^G. Trivial.

(2). Exactness at M^G. By functoriality, $\beta_0\alpha_0 = 1$, thus $\operatorname{Im}\alpha_0 \subseteq \operatorname{Ker}\beta_0$. On the other hand, if $\beta_0(b) = 1$ and $b \in M^G$, then $\beta(b) = 1$ and $b \in M' \cap M^G = M'^G$.

(3). Exactness at M''^G. If $c \in \beta_0(B^G)$, then c can be lifted to an element in M^G and $\delta(c) = 1$. On the other hand, if $\delta(c) = 1$, then $1 = a_\sigma = b^{-1}\sigma(b)$ for some $b \in \beta^{-1}(c)$ and for all $\sigma \in G$, hence $b = \sigma(b) \in M^G$.

(4). Exactness at $H^1(G, M')$. A cocycle a_σ maps to 1 in $H^1(G, M)$ is equivalent to say that $a_\sigma = b^{-1}\sigma(b)$ for some $b \in M$. From the definition of δ, one then see $\alpha_1\delta = 1$. On the other hand, if $a_\sigma = b^{-1}\sigma(b)$ for every $\sigma \in G$, then $\beta(b^{-1}\sigma(b)) = \beta(a_\sigma) = 1$ and $\beta(b) \in M''^G$ and $\delta(\beta(b)) = a_\sigma$.

(5). Exactness at $H^1(G,M)$. By functoriality, $\beta_1\alpha_1 = 1$, thus $\operatorname{Im}\alpha_1 \subseteq \operatorname{Ker}\beta_1$. Now if b_σ maps to $1 \in H^1(G,M'')$, then there exists $c \in M''$, $c^{-1}\beta(b_\sigma)\sigma(c) = 1$. Pick $b' \in M$ such that $\beta(b') = c$, then $\beta(b'^{-1}b_\sigma\sigma(b')) = 1$ and $b'^{-1}b_\sigma\sigma(b') = a_\sigma$ is a cocycle of M'. □

We use the same conventions of notations as the abelian case: if we use the discrete topology, $H^n(G,M) = H^n_{\mathrm{cont}}(G,M)$, and same kind of conventions for profinite groups and 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

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

Given a cocycle $a_{\overline{\sigma}} : G/H \to M^H$, for any $\sigma \in G$, just set $a_\sigma = a_{\overline{\sigma}} : G \to M^H \subseteq M$, thus we have the inflation map

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

Proposition A.107 (Inflation-restriction sequence). *One has the following exact sequence*

$$1 \longrightarrow H^1_{\mathrm{cont}}(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1_{\mathrm{cont}}(G,M) \xrightarrow{\mathrm{res}} H^1_{\mathrm{cont}}(H,M). \tag{A.37}$$

Proof. By definition, its is clear that $\mathrm{res}\circ\mathrm{Inf}$ maps 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 $a_\sigma = a_{\overline{\sigma}}$ is equivalent to the distinguished element in $H^1(G,M)$, then $a_\sigma = a^{-1}\sigma(a)$ for some $a \in M$, but for any $\tau \in H$, $a_\sigma = a_{\sigma\tau}$, thus $\sigma(a) = \sigma(\tau(a))$, i.e., $a = \tau(a)$ and hence $a \in M^H$, so $a_{\overline{\sigma}}$ is cohomologous to the trivial cocycle from $G/H \to A^H$.

(2) Exactness at $H^1_{\mathrm{cont}}(G,M)$: If $a_\sigma : G \to M$ is a cocycle whose restriction to H is cohomologous to 0, then $a_\tau = a^{-1}\tau(a)$ for some $a \in M$ and all $\tau \in H$. Let $a'_\sigma = a \cdot a_\sigma\sigma(a^{-1})$, then a'_σ is cohomologous to a_σ and $a'_\tau = 1$ for all $\tau \in H$. By the cocycle condition, then $a'_{\sigma\tau} = a'_\sigma\sigma(a'_\tau) = a'_\sigma$ if $\tau \in H$. Thus a'_σ is constant on the cosets of H. Again using the cocycle condition, we get $a'_{\tau\sigma} = \tau a'_\sigma$ for all $\tau \in H$, but $\tau\sigma = \sigma\tau'$ for some $\tau' \in H$, thus $a'_\sigma = \tau a'_\sigma$ for all $\tau \in H$. We therefore get a cocycle $a_{\overline{\sigma}} = a'_\sigma : G/H \to A^H$ which maps to a_σ. □

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

Theorem A.108 (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) For all $n \geq 1$, $H^1(L/K,\mathrm{GL}_n(L))$ is trivial.

Proof. It suffices to show the case that L/K is a finite extension. (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 K^n, we form $b(x) = \sum\limits_{\sigma \in \mathrm{Gal}(L/K)} c_\sigma(\sigma(x))$. Then $b(x)$, $x \in K^n$ generates K^n as a K-vector space. In fact, if u is a linear form which is 0 at all $b(x)$, then for every $h \in K$,

$$0 = u(b(hx)) = \sum c_\sigma \cdot u(\sigma(h)\sigma(x)) = \sum \sigma(h)u(a_\sigma(\sigma(x))).$$

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

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

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.

[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.

[BB05a] D. Benois and L. Berger, *Théorie d'Iwasawa des représentations cristallines ii*, Prépulications (2005).

[BB05b] L. Berger and C. Breuil, *Sur quelques représentations potentiellement cristallines de* $\mathrm{GL}_2(\mathbb{Q}_p)$, Prépublication (2005).

[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).

[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.

[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.

[Ber02] L. Berger, *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] ———, *Équations différentielle p-adique et (φ, N)-modules filtrés*, Prépublication (2004).

[Ber04b] ———, *An introduction to the theory of p-adic representations*, Geometric Aspects of Dwork Theory, Walter de Gruyter, Berlin, 2004, pp. 255–292.

[Ber04c] ———, *Limites de repésentations cristallines*, Compositio Math. **140** (2004), no. 6, 1473–1498.

[Ber04d] ———, *Représentations de de rham et normes universelles*, Bull. Soc. Math. France **133** (2004), no. 4, 601–618.

[Ber05] ———, *Représentations modulaire de* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et représentations galoisiennes de dimension 2*, Habitation (2005).

[Ber06] ———, *Représentations galoisiennes et analyse p-adique*, Habilitation (2006).

[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* $\mathrm{Gal}(\bar{\shortparallel}_p/\mathbb{Q}_p)$ *en* $\ell = p$, Duke Math. J. **115** (2002), no. 2, 205–310, Avec un appendice par Guy Henniart.

[BM05] ———, *Représentations semi-stables de* $\mathrm{GL}_2(\mathbb{Q}_p)$, Prépulication (2005).

[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.

[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] ———, *Série spéciale p-adiques et cohomologie éale complétée*, Prépublication (2003).

[Bre03b] ———, *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathbb{Q}_p)$, Compositio Math. **138** (2003), no. 2, 165–188.

[Bre03c] ———, *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.

[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.

[CF00] P. Colmez and J.-M. Fontaine, *Construction des représentations p-adiques semi-stables*, Invent. Math. **140** (2000), 1–43.

[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.

[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, 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, 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, 2003, pp. 53–101.

[Col04a] ______, *La conjecture de Birch et Swinnerton-Dyer p-adiques*, Séminaire Bourbaki. Vol 2002/2003, Astérisque, vol. 294, 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] ______, *Fonctions d'une variable p-adique*, Prépublication (2005).

[Col05b] ______, *Fontaine's rings and p-adic L-functions*, 2005, Lecture Notes of a course given in Fall 2004 at Tsinghua University, Beijing, China.

[Col05c] ______, *Série principale unitaire pour* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et représentations triangulines de dimension* 2, Prépublication (2005).

[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.

[Del] P. Deligne, *Catégories tannakiennes*, The Grothendieck Festschrift (P. Cartier et al., ed.), vol. II, Progress in Math., no. 87, Birkhaüser, Boston, pp. 111–195.

[Del70] ———, *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, vol. II, 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.

[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.

[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.

[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.

[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.

[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.

[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.

[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).

[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., Warsawa, 1983.

[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, no. 295, 2004, pp. 1–115.

[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), 1994.

[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.

[GD60] A. Grothendieck and J. Dieudonné, *Le language des schémas*, Publ. Math. IHES **4** (1960).

[GD61a] ———, *Étude cohomologique des faisceaux cohérents*, Publ. Math. IHES **11, 17** (1961).

[GD61b] ———, *Étude globale élémentaire de quelques classes de morphismes*, Publ. Math. IHES **8** (1961).

[GD67] ______, *Étude locale des schémas et des morphismes des schémas*, Publ. Math. IHES **20,24,28,32** (1964,1965,1966,1967).

[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*, 589 ed., Lecture Notes in Math., 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.

[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),, Geom. Topol. Monogr. (electronic), no. 3, 2000, pp. 263–272.

[Her01] ______, *Une approche nouvelle de la dualité locale de tate*, Math. Ann. **320** (2001), 307–337.

[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.

[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, 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.

[Ill03] ———, *Grothendieck's existence theorem in formal geometry*, 2003.

[Ill04] ———, *Algebraic geometry*, 2004, Lecture Notes in Spring 2004, Tsinghua University, Beijing, China.

[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.

[Kat93c] ———, *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via b_{dr}, part II*, preprint (1993).

[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.

[Ked04] K. Kedlaya, *A p-adic local monodromy theorem*, Ann. of Math. (2) **160** (2004), no. 1, 93–184.

[KKT96] K. Kato, M. Kurihara, and T. Tsuji, *Local Iwasawa theory of Perrin-Riou and syntomic complexes*, preprint (1996).

[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.

[Lub95] J. Lubin, *Sen's theorem on iteration of power series*, Proc. Amer. Math. Soc. **123** (1995), 63–66.

[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.

[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.

[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.

[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.

[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.

List of Notation

Index