Università degli Studi di Milano
Université de Paris-Sud XI

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea Magistrale in Matematica

Mémoire de Master 2 en Mathématiques
Tesi di Laurea Magistrale

The Hodge-Tate decomposition theorem for Abelian Varieties over p-adic fields

following J.M. Fontaine

Candidate:
Federico Binda
Matricola 791067

Thesis advisor:
Prof. Ahmed Abbes
CNRS - IHES

Anno Accademico 2011-2012

Contents

Introduction

0.1. For a smooth complex projective variety X or, more generally, a compact Kähler manifold X, a fundamental result is the so-called "Hodge decomposition" of its singular cohomology with complex coefficients. More precisely, we have a decomposition of the cohomology groups

$$\mathrm{H}^n(X,\mathbb{C}) = \bigoplus_{p+q=n} \mathrm{H}^p(X,\Omega^q_X) \tag{1}$$

where Ω^q_X is the sheaf of holomorphic q-differential forms on X. This decomposition behaves well with respect to the action of the Galois group of $\mathbb{C}$ over $\mathbb{R}$: if we denote by σ the complex conjugation, i.e. the unique non trivial element of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, then σ acts on $\mathrm{H}^n(X,\mathbb{C})$ and transforms a holomorphic q-form in an anti-holomorphic q-form, inducing a map on the cohomology groups that satisfies $\overline{\mathrm{H}^p(X,\Omega^q_X)} = \mathrm{H}^q(X,\Omega^p_X)$.

If X is an abelian variety over $\mathbb{C}$, the Hodge decomposition (1) reduces to give the following canonical isomorphism

$$\mathrm{H}^1(X,\mathbb{C}) = \mathrm{H}^0(X,\mathcal{O}_X) \oplus \mathrm{H}^0(X,\Omega^1_X), \tag{2}$$

since the cup-product pairings identify $\mathrm{H}^r(X,\mathbb{C})$ with the r-th exterior power of $\mathrm{H}^1(X,\mathbb{C})$ and (see [**Ser59**, VII, Th. 10])

$$\mathrm{H}^q(X,\Omega^p_X) = \bigwedge^q \mathrm{H}^1(X,\mathcal{O}_X) \otimes \bigwedge^p \mathrm{H}^0(X,\Omega^1_X).$$

0.2. In the late sixties, Tate asked if a similar result could hold for the p-adic étale cohomology of a proper and smooth variety over a complete discrete valuation field K of characteristic 0 and perfect residue field of characteristic $p > 0$. In [**Tat67**], he established a "Hodge-like" decomposition for an abelian variety with good reduction over K, after extending the scalars to the p-adic completion of an algebraic closure of K.

More precisely, let $\mathcal{O}_K$ be the valuation ring of K, $S = \mathrm{Spec}(\mathcal{O}_K)$, η the generic point of S and $\overline{\eta}$ the geometric point corresponding to an algebraic closure $\overline{K}$ of K. Let $\mathcal{O}_{\mathbf{C}}$ be the p-adic completion of $\mathcal{O}_{\overline{K}}$, $\mathbf{C}$ its fraction field. Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. For every $r \in \mathbb{N}$, we denote by $\mathbf{C}(r)$ the Galois module $\mathbf{C}$ twisted by the action of the r-power of the p-adic cyclotomic character χ_p and by $\mathbf{C}(-r)$ its dual. Let X be an abelian variety over η with good reduction. Tate proved the existence of a canonical G_K-equivariant isomorphism

$$\mathbf{C} \otimes_{\mathbb{Q}_p} \mathrm{H}^1_{\text{ét}}(X_{\overline{\eta}},\mathbb{Q}_p) \xrightarrow{\sim} \mathrm{H}^0(X,\Omega^1_{X/\eta}) \otimes_K \mathbf{C}(-1) \oplus \mathrm{H}^1(X,\mathcal{O}_X) \otimes_K \mathbf{C}, \tag{3}$$

now called the Hodge-Tate decomposition.

We know that there is a canonical isomorphism

$$\mathrm{H}^1_{\text{ét}}(X_{\overline{\eta}},\mathbb{Z}_p) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{T}_p(X_{\overline{\eta}}),\mathbb{Z}_p),$$

where $\mathrm{T}_p(X_{\overline{\eta}})$ is the p-adic Tate module of the abelian variety $X_{\overline{\eta}}$. In this case, (3) is equivalent to the existence of canonical isomorphisms

$$\begin{array}{l} \mathrm{H}^1(X, \mathcal{O}_X) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X_{\overline{\eta}}), \mathbf{C}) \\ \mathrm{H}^0(X, \Omega^1_{X/\eta}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X_{\overline{\eta}}), \mathbf{C}(1)). \end{array} \tag{4}$$

The theorem was proved more generally in [**Tat67**] for p-divisible groups. Using the semi-stable reduction theorem, Raynaud proved in [**SGA 7**] (Exposé 9 Th. 3.6 and Prop. 5.6) the conjecture for all abelian varieties over K, while the proof for the most general statement was established in 1988 by Faltings in [**Fal88**].

In this *mémoire* we present a different proof, due to Fontaine [**Fon82**], of the theorem of Tate and Raynaud as a consequence of a sophisticated, although relatively elementary, analysis of the module of Kähler differentials $\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$. The main advantage of this argument is that it avoids completely the notion of p-divisible group as well as the notion of Néron model and it does not involve the semi-stable reduction theorem.

We give an overview of the content of the different chapters.

0.3. Let K be a complete discrete valuation field of characteristic 0, with perfect residue field of characteristic $p > 0$. In the first chapter, following [**Fon04**], we present some classical results of Tate and Sen: they rely on a fine analysis of the ramification in the cyclotomic $\mathbb{Z}_p$-extension of K, i.e. the unique $\mathbb{Z}_p$-extension K_∞ of K contained in the field generated over K by all the p^n-th roots of 1.

Let $\mathfrak{m}_{K_\infty}$ be the maximal ideal of $\mathcal{O}_{K_\infty}$, $H_K = \mathrm{Gal}(\overline{K}/K_\infty)$, Γ_K the quotient G_K/H_K. Let L be the fraction field of the p-adic completion of $\mathcal{O}_{K_\infty}$. The crucial point is the fundamental theorem of Tate 1.2.6, that states that for every finite extension M of K_∞, we have $\mathrm{Tr}_{M/K_\infty}(\mathcal{O}_M) \supseteq \mathfrak{m}_{K_\infty}$. Using this result, we will show that $L^{\Gamma_K} = \mathbf{C}^{G_K} = K$ and that we have an isomorphism, for every $h \in \mathbb{N}$

$$\mathrm{H}^1_{\mathrm{cont}}(\Gamma_K, \mathrm{GL}_h(K_\infty)) \cong \mathrm{H}^1_{\mathrm{cont}}(G_K, \mathrm{GL}_h(\mathbf{C})).$$

Furthermore, we prove that $\mathrm{H}^0_{\mathrm{cont}}(G_K, \mathbf{C}(1)) = \mathrm{H}^1_{\mathrm{cont}}(G_K, \mathbf{C}(1)) = 0$.

In the next section we study the category of $\mathbf{C}$-representations of G_K, that is the category of finite dimensional $\mathbf{C}$-vector spaces equipped with a continuous and semi-linear action of G_K. They form an abelian category, that we denote by $\mathbf{Rep}_{\mathbf{C}}(G_K)$. In a similar way we define the notion of L-representation and K_∞-representation of Γ_K. According to Sen, we have canonical $\otimes$-equivalences of categories of representations

$$\mathbf{Rep}_{\mathbf{C}}(G_K) \xrightarrow{\sim} \mathbf{Rep}_L(\Gamma_K) \to \mathbf{Rep}_{K_\infty}(\Gamma_K),$$

that can be described as follows.

By a first theorem of Sen, every $\mathbf{C}$-representation of G_K, the $\mathbf{C}$-linear morphism $\mathbf{C} \otimes_L W^{H_K} \to W$ is an isomorphism. Hence the functor $W \mapsto W^{H_K}$ is a $\otimes$-equivalence between $\mathbf{Rep}_{\mathbf{C}}(G_K)$ and $\mathbf{Rep}_L(\Gamma_K)$.

Let $X \in \mathbf{Rep}_L(G_K/H_K)$ and let X_f be the K_∞-vector space obtained by taking the union of all finite dimensional K-subspaces of X that are stable by G_K. A second theorem of Sen proves that the functor $X \mapsto X_f$ defines a $\otimes$-equivalence between $\mathbf{Rep}_{K_\infty}(G_K/H_K)$ and $\mathbf{Rep}_L(G_K/H_K)$, quasi-inverse of the functor $Y \mapsto Y \otimes_{K_\infty} L$.

Let $Y \in \mathbf{Rep}_{K_\infty}(\Gamma_K)$. We will prove that there exists a unique endomorphism s of the K_∞-vector space Y such that, for every $y \in Y$, there exists an open subgroup Γ_y of Γ_K such that

$$\gamma(y) = \exp(\log \chi_p(\gamma) s)(y)$$

for every $\gamma \in \Gamma_y$. The endomowphism s is now called the Sen endomorphism of Y. We will see that s provides enough information to classify the representations up to isomorphisms. We conclude the chapter by giving the abstract definition of Hodge-Tate representations.

0.4. In the second chapter we give the proof of Fontaine of the Theorem of Tate and Raynaud. Let K be as in 0.3. Let $\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$ be the module of $\mathcal{O}_K$-differentials of $\mathcal{O}_{\overline{K}}$. The first part of the chapter is dedicated to the study of this Galois module: we will construct a surjective, G_K-equivariant and $\mathcal{O}_{\overline{K}}$-linear morphism

$$\xi \colon \overline{K} \otimes \mathrm{T}_p(\mathbb{G}_m) \to \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$$

where $\mathrm{T}_p(\mathbb{G}_m)$ denotes the p-adic Tate module of the multiplicative group over $\overline{K}$. The kernel of ξ is given by $\mathfrak{a} \otimes \mathrm{T}_p(\mathbb{G}_m)$, where

$$\mathfrak{a} = \left\{ a \in \overline{K} \mid v(a) \geq -v(\mathcal{D}) - \frac{1}{q-1} \right\}$$

and $\mathcal{D}$ is the absolute different of K. By passing to the limit, we will get a G_K-isomorphism

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) \xrightarrow{\sim} \mathbf{C}(1). \tag{5}$$

This will be obtained as a particular case of more general results on Lubin-Tate formal groups, that hold also when K is a complete discrete valuation field of characteristic $p > 0$ and perfect residue field.

Let X be an abelian variety over η. In section 2.4, we will use the results presented so far to give Fontaine's proof of the decomposition (4). The idea goes as follows: the theorem can be reduced to showing the existence of a K-linear injective morphism

$$\mathrm{H}^0(X, \Omega^1_{X/\eta}) \to \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X), \mathbf{C}(1)). \tag{6}$$

The first step is to consider a proper model $\mathfrak{X}/S$ of finite type for the abelian variety X/η. The group scheme structure on X induces a group structure on the set $\mathfrak{X}(\mathcal{O}_{\overline{K}})$, identified with $X(\overline{K})$, and the translation action of $X(\overline{K})$ induces a morphism

$$\widehat{\varrho} = \widehat{\varrho}_{X,\mathfrak{X},r} \colon p^r \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/S}) \to \mathrm{Hom}_{\mathbb{Z}[G_K]}(X(\overline{K}), \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$$

for a suitable non negative integer r. More precisely, given $\omega \in p^r \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/S})$, we set $\widehat{\varrho}(\omega)$ to be the $\mathbb{Z}[G_K]$-linear morphism

$$\widehat{\varrho}(\omega) \colon u \mapsto u^*(\omega).$$

Let $V_p(X) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], X(\overline{K}))$. By composing with

$$\mathrm{Hom}_{\mathbb{Z}[G_K]}(X(\overline{K}), \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) \to \mathrm{Hom}_{\mathbb{Z}[G_K]}(V_p(X), \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}))$$

and extending the scalars to K, we get a K-linear map that eventually restricts to

$$\varrho = \varrho_{X,\mathfrak{X},r} \colon \mathrm{H}^0(X, \Omega^1_{X/\eta}) \to \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X), \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})).$$

This is the required injective morphism (6), if we take into account the isomorphism (5). It does not depend on the choice of r and of $\mathfrak{X}$.

Acknowledgements

This text would not exist without my supervisor, Ahmed Abbes. I'm deeply grateful to him for the strong support that he provided during the past months, for the valuable remarks and for the countless mathematical explanations. I consider myself honoured to have got a chance of working under him. I would also like to thank Fabrizio Andreatta, who encouraged me to follow this path and has always been a great source of help and precious insights. I could always count on him during the difficulties encountered during the past year.

Un grand merci à tous les amis mathématiciens que j'ai rencontré à Paris: Archibald, Corina, Francesca, Marta, Michaelis, Ramon, Santosh. Un merci tout spécial pour Ziyang "Jerry", pour les longues conversations mathématiques et non.

Non potrei mai dimenticare di ringraziare tutte le persone che mi hanno accompagnato nel corso di questi anni e su cui ho sempre potuto contare. Un enorme grazie agli amici di Via Saldini 50: a Davide, che per quattro anni è stato l'insostituibile compagno di studi e di viaggi. A Riccardo, perché ha condiviso parte di questa follia. A Fiammetta ed Elena, sempre pronte con un sorriso. A Barbara, per l'ironia e gli immancabili pettegolezzi. A Federico, per i suoi paradossi e la sua visione del mondo. Ad Alberto, per il supporto morale e matematico dell'ultimo anno. A Jessica, per avermi sopportato per un anno intero nei cinquanta metri quadri di Rue Censier.

Un grazie agli amici di sempre: Stefano, Corrado, Stefano, Fabrizio, Guido & Nicola. La lontananza geografica non è mai stata un problema per otto anni: perché dovrebbe iniziare ad esserlo ora?

Non avrò mai ringraziato abbastanza la mia famiglia, che mi ha sempre sostenuto nei momenti difficili e mi è stata accanto nei più felici. A mamma Assunta e a papà Fabrizio. Ai nonni Costantino, Franca e Mariuccia. A tutti loro: grazie.

Grazie a Federica. Perché abbiamo condiviso ogni cosa negli ultimi anni e perché senza di lei non ce l'avrei mai fatta. Perché nonostante lei fosse a Madrid, io a Parigi e le nostre famiglie a Milano, siamo riusciti a stare insieme anche quest'anno.
Spero di poterlo fare anche nei prossimi.

Io sono qui
sono venuto a suonare
sono venuto a danzare
e di nascosto ad amare...
(P. Conte)

CHAPTER 1

C-representations: the theory of Tate and Sen

1.1. Review of group cohomology

1.1.1. Let G be a topological group. Let M be a topological G-module, i.e. a topological abelian group endowed with a liner and continuous action of G. Let $\mathcal{C}^n_{\mathrm{cont}}(G,M)$ be the group of continuous n-cochains of G with values in M. Let

$$d_n\colon \mathcal{C}^n_{\mathrm{cont}}(G,M) \to \mathcal{C}^{n+1}_{\mathrm{cont}}(G,M)$$

be the boundary map

$$d_n f(g_1,\dots,g_{n+1}) = g_1 f(g_2,\dots,g_{n+1}) + \sum_{j=1}^{n} (-1)^j f(g_1,\dots,g_j g_{j+1},\dots,g_{n+1}) + (-1)^{n+1} f(g_1,\dots g_n).$$

The sequence $\mathcal{C}^*_{\mathrm{cont}}(G,M)$ is a cochain complex. We denote by $\mathrm{H}^n_{\mathrm{cont}}(G,M)$ the n-th cohomology group of this complex: it is called the n-th continuous cohomology group of G with coefficients in M.

1.1.2. Given a short exact sequence of topological G-modules

$$0 \to M \to M' \to M'' \to 0$$

we have a six-terms-long exact sequence

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

1.1.3. We can still define the groups H^0 and H^1 even when we drop the abelian hypothesis on M, as in [**Ser62**], Appendix to chap. VII. Let M be a topological group, written multiplicatively, endowed with a continuous action of G. $\mathrm{H}^0_{\mathrm{cont}}(G,M)$ is defined as the group M^G of elements of M fixed by G. We denote by $Z^1_{\mathrm{cont}}(G,M)$ the subset of the set of continuous functions of G into M such that

$$f(g_1g_2) = f(g_1)g_1(f(g_2))$$

for $g_1,g_2 \in G$: we call $f \in Z^1_{\mathrm{cont}}(G,M)$ a continuous cocycle. We say that two cocycles f and f' are cohomologous and write $f \sim f'$ if there exists $a \in M$ such that

$$f'(g) = a^{-1} f(g) g(a)$$

for every $g \in G$. This defines an equivalence relation on the set of cocycles. The quotient set has a structure of pointed set: it contains a distinguished element equal to the class of the unit cocycle $f(g) = 1$ for every $g \in G$. We denote its class by 1. We denote $Z^1_{\mathrm{cont}}(G,M)/\sim$ by $\mathrm{H}^1_{\mathrm{cont}}(G,M)$ and we call it the cohomology set of G with values in M. This definition coincides (if we retain just the structure of pointed sets) with the usual one in the abelian case.

1.1.4. Let G be a topological group and let H be a closed normal subgroup of G. Any topological G-module M (abelian or not) can be regarded as H-module, as well as M^H can be regarded as G/H-module. Then we can naturally define the restriction map

$$\mathrm{res}\colon \mathrm{H}^1_{\mathrm{cont}}(G, M) \to \mathrm{H}^1_{\mathrm{cont}}(H, M)$$

and the inflation map

$$\mathrm{Inf}\colon \mathrm{H}^1_{\mathrm{cont}}(G/H, M^H) \to \mathrm{H}^1_{\mathrm{cont}}(G, M).$$

One has the following inflation-restriction exact sequence of pointed sets (resp. of abelian groups if M is abelian):

(1.1.4.1) $$1 \to \mathrm{H}^1_{\mathrm{cont}}(G/H, M^H) \xrightarrow{Inf} \mathrm{H}^1_{\mathrm{cont}}(G, M) \xrightarrow{res} \mathrm{H}^1_{\mathrm{cont}}(H, M).$$

There is a direct proof, valid for the abelian as well as for the non abelian case, in [**Ser62**], chap. VII, §6.

1.2. Statement of the theorems of Tate and Sen

1.2.1. Let K be a complete discrete valuation field of characteristic 0, with perfect residue field of characteristic $p > 0$. We fix an algebraic closure $\overline{K}$ of K and we denote by G_K the Galois group of $\overline{K}$ over K. We denote by $\mathcal{O}_K$ the ring of integers of K and by $\mathcal{O}_{\overline{K}}$ the ring of integers of $\overline{K}$. Let $\mathcal{O}_{\mathbf{C}}$ be the p-adic completion of $\mathcal{O}_{\overline{K}}$, $\mathbf{C}$ its field of fractions. We denote by v_p the valuation of $\mathbf{C}$ extending the valuation of $\overline{K}$ normalized by $v_p(p) = 1$, and by $|.|$ the p-adic absolute value.

For any subfield M of $\mathbf{C}$, we denote by $\mathcal{O}_M$ its valuation ring and by $\mathfrak{m}_M$ the maximal ideal of $\mathcal{O}_M$. If M is a finite extension of K we denote by v_M the unique valuation of $\mathbf{C}$ normalized by $v_M(M^\times) = \mathbb{Z}$ and by $e_M = v_M(p)$ the absolute ramification index of M.

1.2.2. Let χ_p be the cyclotomic character of K, i.e. the continuous homomorphism

$$\chi_p\colon G_K \to \mathbb{Z}_p^\times$$

that gives the action of G_K on the group of units of order a power of p. Let log be the p-adic logarithm, $\log\colon \mathbb{Z}_p^\times \to \mathbb{Z}_p$. We denote by H_K its kernel and by Γ_K the quotient G_K/H_K. Notice that $\Gamma_K \cong \mathbb{Z}_p$ as abelian groups.

Let K_∞ be the cyclotomic $\mathbb{Z}_p$-extension of K: it is the unique $\mathbb{Z}_p$ extension of K contained in the subfield of $\overline{K}$ generated by the roots of unity of order a power of p. By construction we have that $H_K = \mathrm{Gal}(\overline{K}/K_\infty)$ and $\Gamma_K = \mathrm{Gal}(K_\infty/K)$. Let L be the closure of K_∞ in $\mathbf{C}$.

The goal of the first part of this chapter is to present the proof of the following theorems (originally due to Tate and Sen).

1.2.3. Theorem. *We have:*

i) $\mathrm{H}^0_{\mathrm{cont}}(H_K, \mathbf{C}) = \mathbf{C}^{H_K} = L$*;*
ii) *For every* $n \geq 1$, $\mathrm{H}^1_{\mathrm{cont}}(H_K, \mathrm{GL}_h(\mathbf{C})) = 1$.

As a corollary, we have $\mathbf{C}^{G_K} = L^{\Gamma_K}$ and $\mathrm{H}^1_{\mathrm{cont}}(G_K, \mathrm{GL}_h(\mathbf{C})) = \mathrm{H}^1_{\mathrm{cont}}(\Gamma_K, \mathrm{GL}_h(L))$. Indeed, $\mathbf{C}^{G_K} = (\mathbf{C}^{H_K})^{\Gamma_K} = L^{\Gamma_K}$ while the second statement follows from the inflation-restriction exact sequence (1.1.4.1).

1.2.4. Theorem. *We have:*

i) $\mathrm{H}^0_{\mathrm{cont}}(G_K, \mathbf{C}) = \mathrm{H}^0_{\mathrm{cont}}(\Gamma_K, L) = K$;
ii) *For every $h \geq 1$, the map*

$$\mathrm{H}^1_{\mathrm{cont}}(\Gamma_K, \mathrm{GL}_h(K_\infty)) \to \mathrm{H}^1_{\mathrm{cont}}(\Gamma_K, \mathrm{GL}_h(L)) = \mathrm{H}^1_{\mathrm{cont}}(G_K, \mathrm{GL}_h(\mathbf{C}))$$

induced by $\mathrm{GL}_h(K_\infty) \subset \mathrm{GL}_h(\mathbf{C})$ is bijective.

1.2.5. The proof of theorems 1.2.3 and 1.2.4 relies on the following important result of Tate, whose proof is a consequence of a detailed analysis of a ramified $\mathbb{Z}_p$-extension of K (not necessarily the cyclotomic $\mathbb{Z}_p$-extension of 1.2.2).

1.2.6. Theorem (Tate, cf. [**Fon04**], Théorème 1.8). *We keep the notations of 1.2.1. Let K_∞ be a ramified $\mathbb{Z}_p$ extension of K and let M be a finite extension of K_∞. Let $\mathrm{Tr}_{M/K_\infty} : M \to K_\infty$ be the trace map. Then $\mathrm{Tr}_{M/K_\infty}(\mathcal{O}_M) \supseteq \mathfrak{m}_{K_\infty}$.*

1.3. The proof of Tate's Theorem 1.2.6

1.3.1. Let K be as in 1.2.1. Let E be a finite extension of K, J the Galois group $\mathrm{Gal}(E/K)$, $\alpha \in \mathcal{O}_E$ such that $\mathcal{O}_E = \mathcal{O}_K[\alpha]$ [**Ser62**, chap. III, Prop. 12]. We denote by J_i the i-th higher ramification group of K of J [**Ser62**, chap. IV, §1]. We have

$$J_i = \{g \in J \mid i_J(g) \geq i+1\}$$

where $i_J(g) = v_E((g-1)\alpha)$ for every $g \in J$. We call the integers i such that $J_i \neq J_{i+1}$ the ramification numbers of the extension E/K.

1.3.2. Proposition. *Let E be a cyclic ramified extension of K of degree p. Let i be the unique ramification number of the extension E/K. Then we have $i \leq \frac{e_E}{p-1}$ and, for every $x \in E$, $v_E(\mathrm{Tr}_{E/K}(x)) \geq v_E(x) + (p-1)i$.*

Proof. Let τ be a generator of $J = \mathrm{Gal}(E/K)$. We have, for every $x \in E$, $v_E((\tau-1)x) \geq v_E(x) + i$, and the equality holds if an only if $v_E(x)$ is prime to p. Let $P(T) \in \mathbb{Z}[T]$ be a polynomial such that

$$pP(T) = \sum_{j=0}^{p-1} T^j - (T-1)^{p-1}. \tag{1.3.2.1}$$

Hence, for every $x \in E$, we have

$$\mathrm{Tr}_{E/K}(x) = (\tau-1)^{p-1}(x) + pP(\tau)(x) \tag{1.3.2.2}$$

and

$$v_E(pP(\tau)(x)) = e_E + v_E(x), \tag{1.3.2.3}$$

since

$$pP(\tau)(x) = px + \sum_{j=1}^{p-1}(1+\tau+\ldots+\tau^{j-1})(1-\tau)(x) - (1-\tau)^{p-1}(x).$$

Suppose that p divides i and let $\pi \in E$ such that $v_E(\pi) = 1$. We have $v_E((\tau-1)^{p-1}(\pi)) = (p-1)i+1$ and $v_E(pP(\tau)(\pi)) = e_E+1$ (by (1.3.2.3)), that are both prime to p (as e_E is divisible by p). On the other hand, $v_E(\mathrm{Tr}_{E/K}(\pi)) = pv_K(\mathrm{Tr}_{E/K}(\pi))$ is divisible by p. Therefore we have the equality $e_E + 1 = (p-1)i+1$ (using (1.3.2.2)).

Suppose that p does not divide i and let $y \in E$ such that $v_E(y) = i$. We have

$$v_E((\tau - 1)^{p-1}(y)) = (p-1)i + i = pi,$$

while $v_E(pP(\tau)(y)) = e_E + i$ is prime to p. As we have again that $v_E(\mathrm{Tr}_{E/K}(y))$ is divisible by p, we must have $pi < e_E + i$.

By (1.3.2.2) we have, in both cases,

$$v_E(\mathrm{Tr}_{E/K}(x)) \geq v_E(x) + \min\{(p-1)i, e_E\} \geq v_E(x) + (p-1)i$$

for every $x \in E$. □

1.3.3. Lemma. *Let m, n be integers verifying $n \geq m - 1 \geq 0$. Let $i_0, i_1, \ldots, i_{m-1}$ be integers verifying $i_r \equiv i_{r-1} \mod p^r$ for $1 \leq r \leq m-1$. Then the integers $j + i_{v_p(j)}$ for $j \in \mathbb{Z}$ verifying $0 < j < p^n$ and $v_p(j) < m$ are all distinct mod p^n.*

Proof. Suppose, by contradiction, that there exist $j, j' \in \mathbb{Z}$ as above and verifying $j' + i_{v_p(j'} = j + i_{v_p(j)} + p^n a$. Let $s = v_p(j)$, $s' = v_p(j')$. We can suppose $s < s'$, so that $0 \leq s \leq m-2$. But then $v_p(j' - j) = s$, while

$$v_p((i_s - i_{s'}) + p^n a) \geq \min\{s+1, n\} = s+1,$$

which is a contradiction, as $j' - j = (i_s - i_{s'}) + p^n a$. □

1.3.4. Proposition. *Let n be an integer ≥ 1, E a cyclic totally ramified extension of K of degree p^n. Let γ be a generator of the Galois group* $\mathrm{Gal}(E/K)$. *Then*

i) *The extension E/K has exactly n distinct ramification numbers*

$$0 < i_0 < i_1 < \ldots < i_{n-1}.$$

ii) *For $1 \leq r \leq n-1$, we have $i_r \equiv r_{r-1} \mod p^r$.*

iii) *For every $y \in E^\times$ there exists $\lambda \in K$ such that*

$$v_p(y - \lambda) \geq v_p((\gamma - 1)y) - \frac{1}{p-1} \tag{1.3.4.1}$$

Proof. Let K' (resp. E') be the unique extension of degree p (resp. of degree p^{n-1}) of K contained in E. We argue by induction on n. The ramification numbers of E/K' are $i_1, i_2, \ldots, i_{n-1}$, since the lower numbering is compatible with the passage to subgroups. Using [**Ser62**, chap. IV, Prop. 3], we get that for $n \geq 2$, the ramification numbers of E'/K are $i_0, i_1, \ldots i_{n-2}$, and i) follows.

Let π be a uniformizer of E, so that $v_E(\pi) = 1$. Let $J = \mathrm{Gal}(E/K)$. For every $r \in \mathbb{N}$ verifying $1 \leq r < p^n$, we have $i_J(\gamma^r) = i_{v_p(r)}$ and $v_E(\gamma^r - 1)(\pi) = i_{v_p(r)} + 1$. For every $s \in \mathbb{Z}$ verifying $v_p(s) < n$, there exists $\pi_s \in E$ such that $v_E(\pi_s) = s$ and $v_E((\gamma - 1)(\pi_s)) = s + i_{v_p(s)}$. Indeed, set $\pi_0 = 1$ and define, for every $1 \leq r < p^n$, $\pi_r = \pi\gamma(\pi)\ldots\gamma^{r-1}(\pi)$. Then $v_E(\pi_r) = r$ and $(\gamma-1)(\pi_r) = \pi\gamma(\pi)\ldots\gamma^{r-1}(\pi)(\gamma^r(\pi)-\pi)/\pi$, so that $v_E((\gamma-1)(\pi_r)) = r + i_{v_p(r)}$. For $s \geq p^n$, let r be the remainder of the division of s by p^n. Then there exists $\lambda_s \in K$ such that $v_E = s - r$, and we can take $\pi_s = \lambda_s \pi_r$. By substituting K with K', we see that for every $s \in \mathbb{Z}$ verifying $v_p(s) < n-1$, there exists $z_s \in E$ such that $v_E(z_s) = s$ and $v_E((\gamma^p - 1)(z_s)) = s + i_{v_p(s)+1}$.

We show ii) by induction on n. For $n = 1$ there is nothing to prove, so we can assume $n \geq 2$. The induction hypothesis applied to the extension E'/K shows that

$$i_r \equiv i_{r-1} \mod p^r \quad \text{for} \quad 1 \leq r \leq n-2. \tag{1.3.4.2}$$

On the other hand, the induction hypothesis applied to E/K' shows that $i_{n-1} \equiv i_{n-2} \mod p^{n-2}$. Let $s = i_{n-2} - i_{n-1}$. To conclude we need to show that $v_p(s) \neq n-2$.

We argue by contradiction. Let z_s be as above, so that $v_E((\gamma^p - 1)(z_s)) = s + i_{n-1} = i_{n-2}$. Let $x_s = (1 + \gamma + \gamma^2 + \ldots + \gamma^{p-1})(z_s)$. By (1.3.2.1) and (1.3.2.3) we have $v_E(x_s) > s$ and $v_E((\gamma-1)(x_s)) = v_E((\gamma^p - 1)(z_s)) = i_{n-2}$. Since the extension E/K is totally ramified of degree p^n, $\{\pi_r\}_{1 \leq r < p^n}$ is a basis of E over K. Write $x_s = \sum_{r=0}^{p^n-1} b_r \pi_r$ for $b_r \in K$. Hence

$$v_E(x_s) = \min_{0 \leq r < p^n} \{p^n v_K(b_r) + r\}$$

so that $p^n v_K(b_r) + r > s$ for every r. As $(\gamma - 1)(x_s) = \sum_{r=1}^{p^n} b_r(\gamma - 1)(\pi_r)$, if $v_p(r) = n-1$ we have $v_E(b_r(\gamma-1)(\pi_r)) > s + i_{n-1} = i_{n-2}$. By 1.3.3 (for $m = n-1$) we have

$$i_{n-2} = v_E((\gamma - 1)(x_s)) = \min_{0 \leq r < p^n;\, v_p(r) < i_{n-1}} \{p^n v_K(b_r) + r + i_{v_p(r)}\}.$$

Therefore there exists r such that $i_{n-2} \equiv r + i_{v_p(r)} \mod p^r$, which is impossible as

$$v_p(i_{n-2} - i_{v_p(r)}) \geq v_p(r) + 1$$

by (1.3.4.2).

We finally prove iii). For $y \in E^\times$ we have $y = \sum_{r=0}^{p^n-1} b_r \pi_r$, $b_r \in K$ and we can take $\lambda = b_0$. Indeed, there exists a unique r_0, $0 < r_0 < p^n$, such that $v_E(y - \lambda) = v_E(b_{r_0} \pi_{r_0})$. By 1.3.3 (for $m = n$) we have

$$v_E((\gamma - 1)(y)) = \min_{0 < r < p^n} \{v_E(b_r \pi_r + i_{v_p(r)} \leq v_E(y - \lambda) + i_{n-1}$$

so $v_E(y - \lambda) \geq v_E((\gamma - 1)(y)) - i_{n-1}$. Hence

$$v_p(y - \lambda) \geq v_p((\gamma - 1)(y)) - \frac{i_{n-1}}{e_E} \geq v_p((\gamma - 1)(y)) - \frac{1}{p-1}$$

by 1.3.2 applied to the extension E/E'. □

1.3.5. Proposition. *Let n be an integer ≥ 1, E a cyclic totally ramified extension of K of degree p^n. Then for every $x \in E$ we have*

$$v_p(\mathrm{Tr}_{E/K}(x)) \geq v_p(x) + \frac{n(p-1)}{pe_K}$$

Proof. Let $i_0 < i_1 \ldots < i_{n-1}$ be the ramification numbers of the extension E/K. From 1.3.2 we deduce that

$$v_p(\mathrm{Tr}_{E/K}(x)) \geq v_p(x) + \frac{(p-1)}{e_K}\Big(\frac{i_0}{p} + \frac{i_1}{p^2} + \ldots + \frac{i_{n-1}}{p^n}\Big).$$

and the result follows, since by 1.3.4 ii) we have $i_r \geq p^r$ for every r. □

1.3.6. Let K_∞ be a ramified $\mathbb{Z}_p$ extension of K. For every $r \in \mathbb{N}$, we denote by K_r the unique extension of degree p^r of K contained in K_∞. If $\Gamma_K = \mathrm{Gal}(K_\infty/K)$, we denote by Γ_r the Galois group $\mathrm{Gal}(K_\infty/K_r)$. We fix a topological generator γ_0 of Γ_K and we let $\gamma_r = \gamma_0^{p^r}$ be a topological generator of Γ_r.

By 1.3.4, there exists a unique non negative integer $r_0 \geq 0$ and a strictly increasing sequence of positive integers

$$i_0 < i_1 < \ldots < i_{r-1} < i_r < \ldots$$

such that K_{r_0} is the maximal unramified extension of K contained in K_∞ and that, for every $r > r_0$, the ramification numbers of the extension K_r/K_{r_0} are precisely $i_0, i_1, \dots, i_{r-r_0-1}$. Moreover, we have $i_r \equiv i_{r-1} \mod p^r$. The sequence $(i_r)_{r\in\mathbb{N}}$ is called the sequence of ramification numbers of the extension K_∞/K.

1.3.7. Let F be a finite Galois extension of K such that $F \cap K_\infty = K$. For every $r \geq 0$, let $F_r = K_r F$ and $F_\infty = K_\infty F$. Let $J = \mathrm{Gal}(F_\infty/K_\infty)$, $J_r = \mathrm{Gal}(F_r/K_r)$. Let ϖ_r be the canonical isomorphism $J \xrightarrow{\varpi_r} J_r$. For $\tau \in J$, we set $i_r(\tau) = i_{J_r}(\varpi_r(\tau))$.

1.3.8. PROPOSITION. *Under the assumptions of 1.3.7, for every $\tau \in J$ the sequence $\{i_r(\tau)\}$ is stationary.*

PROOF. Up to replacing K with K_m for a sufficiently large m, we can suppose that the extension F_∞/F is totally ramified. Let (j_r) be the sequence of ramification numbers of this extension. Using [**Ser62**, chap. IV, Prop. 3] we have

$$i_r(\tau) = \begin{cases} i_{r+1}(\tau) & \text{if } i_{r+1}(\tau) \leq j_r \\ \frac{1}{p}(i_{r+1}(\tau) + (p-1)j_r) & \text{if } i_{r+1}(\tau) > j_r \end{cases}$$

or, equivalently,

$$i_{r+1}(\tau) = \begin{cases} i_r(\tau) & \text{if } i_r(\tau) \leq j_r \\ p i_r(\tau) - (p-1)j_r & \text{if } i_r(\tau) > j_r. \end{cases} \tag{1.3.8.1}$$

Therefore we have to show that there exists r such that $i_r(\tau) \leq j_r$. Otherwise we would have $i_r(\tau) > j_r$, so that $i_{r+1}(\tau) = p i_r(\tau) - (p-1)j_r$ by (1.3.8.1). Hence, by induction,

$$i_r(\tau) = p^r i_0(\tau) - (p-1)(j_{r-1} + p j_{r-2} + \dots p^{r-1} j_0)$$

so that

$$j_0 + \frac{j_1 - j_0}{p} + \frac{j_2 - j_1}{p^2} + \dots + \frac{j_r - j_{r-1}}{p^r} < i_0(\tau).$$

The right-hand term is independent from r, but the left-hand term is $\geq r+1$, since it is the sum of $r+1$ integers ≥ 1 by 1.3.4, which is a contradiction. ☐

1.3.9. Let E be a finite extension of K. Let r be the unique integer such that $\mathfrak{m}_K^r = \mathcal{D}_{E/K} \cap \mathcal{O}_K$. We have $\mathfrak{m}_K^r \mathcal{D}_{E/K}^{-1} \subset \mathcal{O}_E$. Let $\{a_1, \dots, a_d\}$ be a basis of $\mathcal{O}_E$ over $\mathcal{O}_K$, $\{a_1^*, \dots, a_d^*\}$ the dual basis with respect to the trace form $\mathrm{Tr}\colon E \times E \to K$, b a generator of $\mathfrak{m}_K^r$. Then $(ba_i)a_i^* \in \mathcal{O}_E$ and $\mathrm{Tr}_{E/K}((ba_i)a_i^*) = b$ for every $1 \leq i \leq d$. As $\mathrm{Tr}_{E/K}(\mathcal{O}_E)$ is an ideal of $\mathcal{O}_K$, we deduce that

$$\mathfrak{m}_K^r \subset \mathrm{Tr}_{E/K}(\mathcal{O}_E). \tag{1.3.9.1}$$

PROOF OF 1.2.6. Up to replacing M with a finite extension, we can suppose that M is a Galois extension of K_∞. Up to replacing K with a finite extension contained in K_∞, we can suppose that $M = K_\infty F$, for a finite Galois extension F of K such that $K_\infty \cap F = K$. Using the notations of 1.3.8, we have by [**Ser62**, chap. IV, Prop. 4]

$$v_{F_r}(\mathcal{D}_{F_r/K_r}) = \sum_{\tau \in J,\, \tau \neq 1} i_r(\tau)$$

for every $r \in \mathbb{N}$. By 1.3.8 there exist an integer r_0 and a constant $c \geq 0$ such that $v_{F_r}(\mathcal{D}_{F_r/K_r}) = c$ for $r \geq r_0$.

Let e be the ramification number of F_r/K_r for every $r \geq r_0$. Let $n \in \mathbb{N}$ be the smallest integer such that $en \geq c$. We have

$$\mathfrak{m}_{K_r}^n \subset \mathrm{Tr}_{F_r/K_r}(\mathcal{O}_{F_r}) \subset \mathrm{Tr}_{M/K_\infty}(\mathcal{O}_M).$$

The first inclusion follows from (1.3.9.1). For the second inclusion, notice that $M = FK_\infty$ and that $J = \mathrm{Gal}\,(M/K_\infty)$ is isomorphic to $J_r = \mathrm{Gal}(F_r/K_r)$. Hence, for $x \in \mathcal{O}_F \subset \mathcal{O}_M$, we have $\mathrm{Tr}_{F_r/K_r}(x) = \sum_{g\in J_r} g(x) = \sum_{\tau\in J} \tau(x) = \mathrm{Tr}_{M/K_\infty}(x)$ using the isomorphism ϖ_r.

Since $v_p(\mathfrak{m}_{K_r}^n) = n/e_{K_r}$ goes to 0 as r goes to ∞, we have that $\cup_{r\geq r_0} = \mathfrak{m}_{K_\infty}$ and we conclude that $\mathrm{Tr}_{M/K_\infty}(\mathcal{O}_M) \supseteq \mathfrak{m}_{K_\infty}$. □

1.4. The cohomology of $\mathrm{Gal}(\overline{K}/K_\infty)$: the proof of Theorem 1.2.3

1.4.1. We keep the notations of 1.2.1—1.2.2. Let M be a finite Galois extension of K_∞ and let $J = \mathrm{Gal}(M/K_\infty)$ be the Galois group of M over K_∞.

1.4.2. Lemma. *Let c be a real number > 1. For every $\lambda \in M$ there exists $a \in K_\infty$ such that*

$$|\lambda - a| < c \sup_{g\in J} |(g-1)\lambda|$$

Proof. By 1.2.6 the elements in $\mathrm{Tr}_{M/K_\infty}(\mathcal{O}_M)$ have arbitrary small valuation. Therefore, we can find $y \in \mathcal{O}_M$ such that $x = \mathrm{Tr}_{M/K_\infty}(y)$ satisfies $|x| > \frac{1}{c}$. Let $\mu = \frac{\lambda y}{x}$ and let $a = \mathrm{Tr}_{M/K_\infty}(\mu)$. We have:

$$a = \frac{\mathrm{Tr}(y\lambda)}{x} = \frac{1}{x}\sum_{g\in J} g(y)g(\lambda) = \lambda + \frac{1}{x}\sum_{g\in J} g(y)(g-1)\lambda$$

and

$$|\lambda - a| \leq \sup_{g\in J} |\frac{1}{x} g(y)[(g-1)\lambda]| < c \sup_{g\in J} |(g-1)\lambda|$$

as $|g(y)| \leq 1$, being $y \in \mathcal{O}_M$. □

Proof of part i) of 1.2.3. Let $\lambda \in \mathrm{H}^0_{\mathrm{cont}}(H_K, \mathbf{C}) = C^{H_K}$ and write λ as limit of a sequence $\{\lambda_n\}_{n\in\mathbb{N}} \subset \overline{K}$ such that $|\lambda - \lambda_n| < p^{-n}$. As λ is fixed by H_K we have, for every $h \in H_K$,

$$|(h-1)\lambda_n| = |h(\lambda - \lambda_n) + (\lambda - \lambda_n)| \leq |h(\lambda - \lambda_n)| = |(\lambda - \lambda_n)| < p^{-n}. \tag{1.4.2.1}$$

For every $n \in \mathbb{N}$, let M_n be a finite Galois extension of K_∞ containing λ_n. Let $J_n = \mathrm{Gal}(M_n/K_\infty)$. By (1.4.2.1) we have$|(g-1)\lambda_n| < p^{-n}$ for every $g \in J_n$ (as $J_n \leq H_K$). By 1.4.2 with $c = p$, we have that there exists $a_n \in K_\infty$ such that $|\lambda_n - a_n| < p^{1-n}$. Hence the sequences $\{\lambda_n\}_{n\in\mathbb{N}}$ and $\{a_n\}_{n\in\mathbb{N}}$ have the same limit λ. Hence $\lambda \in L$. □

1.4.3. Let $\mathrm{M}_h(\mathcal{O}_\mathbf{C})$ be the ring of $h \times h$ square matrices with coefficients in $\mathcal{O}_\mathbf{C}$. We equip $\mathrm{M}_h(\mathcal{O}_\mathbf{C})$ with the p-adic topology. Let $|.|$ be the p-adic absolute value on $\mathrm{M}_h(\mathcal{O}_\mathbf{C})$: we have $|A| \leq p^{-r}$ if and only if $A \in p^r\mathrm{M}_h(\mathcal{O}_\mathbf{C})$.

1.4.4. Lemma. *Let H be an open subgroup of H_K and let m be an integer ≥ 2. Let $f_m \in Z^1_{\mathrm{cont}}(H, \mathrm{GL}_h(\mathbf{C}))$ be a continuous cocycle verifying $|f_m(s) - 1| \leq p^{-m}$ for every $s \in H$. Then there exists $b_m \in \mathrm{GL}_h(\mathbf{C})$ with $|b_m - 1| \leq p^{1-m}$ such that the continuous cocycle f_{m+1} defined by*

$$f_{m+1}(s) = (b_m)^{-1} f_m(s) s(b_m)$$

satisfies $|f_{m+1}(s) - 1| \leq p^{-m-1}$ for every $s \in H$.

PROOF. We can reduce to the case $H = H_K$. Indeed, if $K'_\infty = \overline{K}^H$, we can find a finite Galois extension K' of K such that K'_∞ is a ramified $\mathbb{Z}_p$ extension of K'.

Being f_m continuous, we can find an open normal subgroup N of H_K such that $|f_m(g)-1| \leq p^{-m-2}$ for $g \in N$ (it's enough to take for N the pre-image of the open ball of radius p^{-m-2} and center 1). Let $J = H_K/N$ and let $M = \overline{K}^N$ be the corresponding finite Galois extension of K_∞. By Theorem 1.2.6, there exists $y \in \mathcal{O}_M$ such that $\sum_{\tau\in J}\tau(y) = p$. If T is a system of representatives for J in H_K, we let

$$b_m = \frac{1}{p}\sum_{g\in T} f_m(g)g(y).$$

As $f_m(g) \in 1 + p^m\mathrm{M}_h(\mathcal{O}_\mathbf{C})$, we can write $f_m(g) = 1 + p^m a_m(g)$ for $a_m(g) \in \mathrm{M}_h(\mathcal{O}_\mathbf{C})$, so that

$$b_m = \frac{1}{p}\sum_{g\in T}(1+p^m a_m(g))g(y) = \frac{1}{p}\sum_{g\in T} g(y) + p^{m-1}\sum_{g\in T} a_m(g)g(y).$$

Hence $b_m \in 1 + p^{m-1}\mathrm{M}_h(\mathcal{O}_\mathbf{C})$. In particular, $b_m \in \mathrm{GL}_h(\mathcal{O}_\mathbf{C})$. For every $s \in H_K$ we have

$$s(b_m) = \frac{1}{p}\sum_{g\in T} s(f_m(g))((sg)(y)) = \frac{1}{pf_m(s)}\sum_{g\in T} f_m(sg)((sg)(y)). \tag{1.4.4.1}$$

By the cocycle condition we also have $f_m(sg) \equiv f_m(g) \pmod{p^{m+2}}$ when $s \in N$ and $g \in H_K$, and (1.4.4.1) implies

$$s(b_m) \equiv f_m(s)^{-1}b_m \pmod{p^{m+1}}$$

i.e. $f_{m+1} = (b_m)^{-1}f_m(s)s(b_m) \equiv 1 \pmod{p^{m+1}}$. □

PROOF OF PART ii) of 1.2.3. Let $f \in Z^1_{\mathrm{cont}}(H_K, \mathrm{GL}_h(\mathbf{C}))$. Being f continuous, we can find an open normal subgroup N of H_K such that $|f(s) - 1| \leq p^{-2}$ for every $s \in N$ (notice that if f is a cocycle, then $f(1) = 1$, so that the inverse image of an open ball centred in 1 is not empty). Let f_2 be the restriction of f to N. By 1.4.4 we can find a sequence $\{f_m\}_{m\geq 2}$ of continuous cocycles verifying $|f_m(s) - 1| \leq p^{-m}$ for every $s \in N$ and a sequence $\{b_m\}_{m\geq 2} \subseteq \mathrm{GL}_h(\mathbf{C})$ verifying $|b_m - 1| \leq p^{1-m}$ such that

$$f_{m+1}(s) = b_m^{-1}f_m(s)s(b_m)$$

for every $s \in N$. Let $\{\beta_m = \prod_{k=2}^m b_k\}$ the sequence of products. Then, for every $s \in N$,

$$f_{m+1}(s) = \beta_m^{-1}f(s)s(\beta_m).$$

Let b be the limit of the sequence $\{\beta_m\}_{m\geq 2}$; since $\lim_{m\to\infty} f_m = 1$, b is an element of $\mathrm{GL}_h(\mathbf{C})$ satisfying $1 = b^{-1}f(s)s(b)$ for every $s \in N$. In other words, the restriction of f to N is cohomologous to the trivial cocycle. The inflation-restriction exact sequence (1.1.4.1) implies that f is in the image of $\mathrm{H}^1_{\mathrm{cont}}(H_K/N, (\mathrm{GL}_h(\mathbf{C}))^N)$. But H_K/N is the galois group J of the finite Galois extension $\mathbf{C}^N/\mathbf{C}^{H_K}$ and

$$\mathrm{H}^1_{\mathrm{cont}}(J, (\mathrm{GL}_h(\mathbf{C}))^N) = \mathrm{H}^1(J, \mathrm{GL}_h(\mathbf{C}^N))$$

which is trivial by Hilbert's Theorem 90 [**Ser62**, chap. X, Prop. 3]. □

1.5. The cohomology of $\mathrm{Gal}(K_\infty/K)$: the proof of Theorem 1.2.4

1.5.1. Throughout this section, we denote by K_∞ a ramified $\mathbb{Z}_p$ extension of K. We keep the notations of 1.3.6. We say that the $\mathbb{Z}_p$ extension K_∞/K is regular if it is totally ramified and if the sequence $(i_r)_{r\in\mathbb{N}}$ of ramification numbers verifies

$$i_r - i_{r-1} = p^r e_K \quad \text{for every } r \geq 1.$$

We say that the extension K_∞/K is potentially regular if there exists $r_0 \geq 0$ such that K_∞/K_{r_0} is regular. In this case, for every $r \geq r_0$, K_∞/K_r is regular.

1.5.2. Lemma ([**Fon04**, Prop. 1.11]). *The cyclotomic $\mathbb{Z}_p$ extension of K considered in 1.2.2 is potentially regular.*

1.5.3. Lemma ([**Fon04**, Prop. 1.12]). *Let F be a finite extension of K. Then a $\mathbb{Z}_p$ extension K_∞/K is potentially regular if and only if FK_∞/F is potentially regular.*

1.5.4. For every $r \in \mathbb{N}$, let $\mathrm{Tr}_{K_r/K} \colon K_r \to K$ be the trace map. For $x \in K_\infty$, let $r \in \mathbb{N}$ such that $x \in K_r$; let

$$t_K(x) = \frac{1}{p^r}\,\mathrm{Tr}_{K_r/K}(x).$$

The map $t_K \colon K_\infty \to K$ does not depend on the choice of r: it's a projector from the K-vector space K_∞ to its subspace K. Indeed, let $x \in K_r \subseteq K_{r'}$. We have

$$\frac{1}{p^{r'}}\,\mathrm{Tr}_{K_{r'}/K}(x) = \frac{1}{p^r}\Big(\frac{1}{p^{r'-r}}\,\mathrm{Tr}_{K_r/K}(\mathrm{Tr}_{K_{r'}/K_r}(x))\Big) = \frac{1}{p^r}\Big(\frac{1}{p^{r'-r}}\sum_i \mathrm{Tr}_{K_r/K}(\bar{\gamma}^i(x))\Big)$$

where $\bar{\gamma}$ is a generator of $\mathrm{Gal}(K_{r'}/K_r) \leq \mathrm{Gal}(K_{r'}/K)$, so that $\mathrm{Tr}_{K_r/K}(\bar{\gamma}^i(x)) = \mathrm{Tr}_{K_r/K}(x)$, repeated exactly $p^{r'-r}$ times.

1.5.5. Proposition ([**Fon04**, Prop. 1.13]). *Suppose that K_∞/K is regular. Then there exists $c \in \mathbb{R}_{>0}$ such that for every $x \in K_\infty$ we have*

$$|t_K(x) - x| \leq c.|(\gamma_0 - 1)x|.$$

1.5.6. Proposition. *Let K_∞/K be a potentially regular $\mathbb{Z}_p$ extension. Then the map $t_K \colon K_\infty \to K$ is continuous. If $\widehat{t}_K \colon L \to K$ denotes the extension of t_K by continuity and L_0 denotes the kernel of $\widehat{t}_K$, we have a decomposition $L = K \oplus L_0$. The operator $\gamma_0 - 1$ is bijective on L_0, with a continuous inverse.*

Proof. Let r_0 be an integer such that the extension K_∞/K_{r_0} is regular. We have

$$t_K = p^{-r_0}\,\mathrm{Tr}_{K_{r_0}/K} \circ t_{K_{r_0}}$$

by transitivity of the norm maps: $p^{-r_0}\,\mathrm{Tr}_{K_{r_0}/K}$ is clearly continuous (being K_{r_0}/K finite) and $t_{K_{r_0}}$ is continuous by 1.5.5.

For the second assertion, suppose firstly that K_∞/K is regular. If $x \in K$, then $\widehat{t}_K(x) = x$, so that $\widehat{t}_K^2 = \widehat{t}_K$ and we can write L as sum $K \oplus L_0$. For every $x \in L$ we clearly have $(\gamma_0 - 1)(x) \in L_0$ and, in particular, $(\gamma_0 - 1)(L_0) \subset L_0$. Let $K_{\infty,0} = K_\infty \cap L_0$ and let, for every $r \in \mathbb{N}$, $K_{r,0} = K_r \cap L_0$: with this notation $K_{\infty,0}$ is the union of $K_{r,0}, r \in \mathbb{N}$ $(K_{r,0} \subset K_{r+1,0} \subset \ldots)$ and L_0 is the closure of $K_{\infty,0}$ in L. As the operator $\gamma_0 - 1$ is injective (hence bijective) on every finite-dimensional K-vector space $K_{r,0}$, it is also bijective on their union $K_{\infty,0}$. Let ϱ be its inverse. For every $y \in K_{\infty,0}$, as $t_K(\varrho(y)) = \widehat{t}_K(\varrho(y)) = 0$, we have by 1.5.5

$$|\varrho(y)| \leq c.|y|$$

and ϱ is continuous. We can extend it to a continuous map, denoted again by ϱ, from L_0 to itself, which is a continuous inverse of $\gamma_0 - 1$.

For the general case, let r_0 be an integer such that the extension K_∞/K_{r_0} is regular and let $\widehat{t}_{K_{r_0}}$ be the continuous extension of $t_{K_{r_0}}$ to L. Let L_{r_0} be its kernel, $\varrho_{r_0} \colon L_{r_0} \to L_{r_0}$ the inverse of the restriction of $\gamma_{r_0} - 1$. We have

$$L = K \oplus L_0 = K_{r_0} \oplus L_{r_0}$$

and, since $L_{r_0} \subset L_0$, we can write

$$L_0 = L_0 \cap K_{r_0} \oplus L_{r_0}.$$

The map $\gamma_0 - 1$ is injective on L_0, as $L_0 \cap K = 0$. Since K_{r_0} is a finite-dimensional K-vector space, $L_0 \cap K_{r_0}$ is of finite dimension over K, so that $\gamma_0 - 1$ is bijective with continuous inverse on it. As

$$\gamma_{r_0} - 1 = \gamma_0^{p_0^r} - 1 = (\gamma_0 - 1)A(\gamma_0)$$

for $A \in \mathbb{Z}[\gamma_0]$, we see that $\gamma_0 - 1$ is bijective on L_{r_0}, with continuous inverse $A(\gamma_0)\varrho_{r_0}$. □

1.5.7. Proposition. *Suppose that K_∞/K is regular. Let λ be a principal unit of $\mathcal{O}_K$ (i.e. $|\lambda - 1| < 1$) but not a root of unity, then $\gamma_0 - \lambda$ is bijective with continuous inverse on L.*

Proof. Since $\gamma_0 - \lambda$ is obviously bijective on K if $\lambda \neq 1$, we can use the decomposition $L = K \oplus L_0$ and prove the statement for L_0. Let ϱ be the inverse of $\gamma_0 - 1$. We have:

$$\varrho \circ (\gamma_0 - \lambda) = \varrho \circ ((\gamma_0 - 1) - \lambda + 1) = 1 - (\lambda - 1)\varrho. \tag{1.5.7.1}$$

Let c be the constant in 1.5.5. If $|\lambda - 1|c < 1$, we have $|(\lambda - 1)\varrho(y)| < |y|$ for all $y \in L_0$ (see the proof of 1.5.6), and consequently $1 - (\lambda - 1)\varrho$ is an automorphism of L_0, with inverse given by the (convergent) geometric series

$$\sum_{r \geq 0} [(\lambda - 1)\varrho]^r.$$

Hence, by (1.5.7.1), $\gamma_0 - \lambda$ has a continuous inverse on L_0. If $|\lambda - 1|c \geq 1$, we replace γ_0 by $\gamma_r = \gamma_0^{p^r}$ and λ by λ^{p^r}, where r is large so large that $|\lambda^{p^r} - 1|c < 1$ (notice that such r exists, since $\lambda = 1 + x$, where $v(x) \geq 1$). We then replace K by K_r, so that $\gamma_r - \lambda^{p^r}$ has a continuous inverse on L_0. Hence the map

$$(\gamma_0 - \lambda)^{p^r} - \gamma_r - \lambda^{p^r}$$

has a continuous inverse, so the same is true for $(\gamma_0 - \lambda)^{p^r}$ and hence for $(\gamma_0 - \lambda)$ too. □

1.5.8. Remark. Using exactly the same argument as in the proof of 1.5.6, we can prove 1.5.7 assuming only that K_∞/K is potentially regular.

1.5.9. From now on, we suppose that the $\mathbb{Z}_p$ extension K_∞/K is potentially regular. We denote by L the closure of K_∞ in $\mathbf{C}$, $\Gamma_K = \mathrm{Gal}(K_\infty/K)$, $H_K = \mathrm{Gal}(\overline{K}/K_\infty)$. We will prove Theorem 1.2.4 as a particular case of the same statement for any potentially regular $\mathbb{Z}_p$-extension.

PROOF OF PART i) of 1.2.4. It's an immediate consequence of 1.5.6. Indeed we have

$$\mathrm{H}^0_{\mathrm{cont}}(\Gamma_K, L) = L^{\Gamma_K} = \{x \in L \mid (\gamma_0 - 1)x = 0\} = \mathrm{Ker}(\gamma_0 - 1),$$

but $L = K \oplus L_0$ and $\gamma_0 - 1$ is bijective on L_0, so that $\mathrm{Ker}(\gamma_0 - 1) = K$. □

1.5.10. THEOREM ([**Sen80**, Prop. 3]). *Let V be a finite dimensional K-vector space, $V \subset L$. If V is stable by γ_0, then $V \subset K_\infty$.*

PROOF. Let $u \in \mathrm{End}_K(V)$ be the restriction of γ_0 to V and let $f_u(T)$ be its characteristic polynomial: we can reduce to the case $f_u(T)$ has all its roots in K. Indeed, let K' be the extension of K obtained by adding the roots of $f_u(T)$ in $\overline{K}$. Let $K'_\infty = K'K_\infty$. Then the extension K'_∞/K' is potentially regular (see Remark 1.5.3) and we can substitute K by K', V by $K' \otimes_K V$ and so on. Moreover, we can suppose that u has only one eigenvalue, say a, by taking the decomposition of V as direct sum of its generalized eigenspaces.

Let v be a non zero eigenvector of u. We have $\gamma_0(v) = av$, so that $\gamma_0^{p^r}(v) = a^{p^r}v$. We have that $|(\gamma_0 - 1)x| \le |x|$, being the action of Γ_K on L is continuous, so that a must be a principal unit (i.e. congruent to 1 mod p). By 1.5.7 a must be a root of unity (cfr [**Tat67**], Prop. 7). Up to replacing K by a finite extension contained in K_∞, we can suppose that $a = 1$. Up to replacing V by $V + K$ (if V does not contain K), we may assume that $V = K \oplus V'$, with $V' \subset L_0 = \mathrm{Ker}\,\widehat{t}_K$. But then $\gamma_0 - 1$ is bijective on L_0, so that $V' = 0$ and $V = K \subset K_\infty$. □

PROOF OF PART ii) of 1.2.4. Let ι be the map

$$\iota\colon \mathrm{H}^1_{\mathrm{cont}}(\Gamma_K, \mathrm{GL}_h(K_\infty)) \to \mathrm{H}^1_{\mathrm{cont}}(\Gamma_K, \mathrm{GL}_h(L))$$

We first prove that ι is injective: let $f, f' \in Z^1_{\mathrm{cont}}(\Gamma_K, \mathrm{GL}_h(K_\infty))$ be two continuous cocycles that become cohomologous in $\mathrm{GL}_h(L)$. Then there exists $b \in \mathrm{GL}_h(L)$ such that

$$f'(\gamma_0) = b^{-1} f(\gamma_0)\gamma_0(b) \tag{1.5.10.1}$$

and it's enough to show that $b \in \mathrm{GL}_h(K_\infty)$. We can rewrite (1.5.10.1) as

$$\gamma_0(b) = f(\gamma_0)^{-1} b f'(\gamma_0). \tag{1.5.10.2}$$

Let K' be the extension of K generated by the coefficients of $f(\gamma_0)$ and $f'(\gamma_0)$: it is a finite extension of K contained in K_∞. Let V be the K'-vector space generated by the coefficients of b: it's a finite dimensional K-vector space, contained in L, and (1.5.10.2) shows that it is stable by γ_0. Being V closed in L, we can apply Theorem 1.5.10 to get $V \subset K_\infty$, so that $b \in \mathrm{GL}_h(K_\infty)$.

To prove the surjectivity we need an auxiliary technical result:

1.5.11. LEMMA. *For every matrix $A \in \mathrm{M}_h(L)$, let $v(A)$ be the minimum of the p-adic valuations of its coefficients. Let r be an integer such that the extension K_∞/K_r is regular and let m be an integer ≥ 5. Let $A_m \in \mathrm{GL}_h(L)$, $X_m \in \mathrm{GL}_h(K_r)$ be matrices verifying*

$$v(A_m - 1) \ge \frac{3p}{p-1}, \quad v(A_m - X_m) \ge \frac{mp}{p-1}.$$

Then there exist $B_m \in \mathrm{GL}_h(L)$ *verifying* $v(B_m - 1) \geq \frac{(m-2)p}{p-1}$ *and* $X_m \in \mathrm{GL}_h(K_r)$ *such that the matrix*

$$A_{m+1} = B_m^{-1} A_m \gamma_r(B_m)$$

verifies $v(A_{m+1} - 1) \geq \frac{3p}{p-1}$ *and* $v(A_{m+1} - X_{m+1}) \geq \frac{p(m+1)}{p-1}$.

The proof of the lemma is a direct computation similar to 1.4.4, using 1.5.6, and we omit it. See [**Fon04**, Lemme 1.17].

We can now prove that ι *is surjective*: let $f \in Z^1_{\mathrm{cont}}(\Gamma_K, \mathrm{GL}_h(L))$. Being f continuous, there exists an integer r — that we can choose big enough so that the extension K_∞/K_r is regular — such that $v(f(\gamma_r) - 1) \geq \frac{5p}{p-1}$. Let $a_5 = f(\gamma_r)$ and let $x_5 = 1$. Using the previous lemma, we can produce three sequences of matrices: $\{a_m\}_{m\geq 5}$ and $\{b_m\}_{m\geq 5}$ in $\mathrm{GL}_h(L)$ and $\{x_m\}_{m\geq 5}$ in $\mathrm{GL}_h(K_r)$ such that, for every $m \geq 5$:

$$\begin{aligned} v(a_m - 1) &\geq \frac{3p}{p-1}; \\ v(a_m - x_m) &\geq \frac{mp}{p-1}; \\ v(b_m - 1) &\geq \frac{(m-2)p}{p-1}; \\ a_{m+1} &= b_m^{-1} a_m \gamma_r(b_m). \end{aligned}$$

The sequence $\{\beta_m = \prod_{k=5}^m b_k\}_{m\geq 5}$ converges to a matrix $b \in \mathrm{GL}_h(L)$ and the sequences $\{a_m\}_{m\geq 5}$ and $\{x_m\}_{m\geq 5}$ both converge to the same limit $x \in \mathrm{GL}_h(K_r)$ and we have

$$x = b^{-1} f(\gamma_r) \gamma_r(b).$$

Let f' be the continuous cocycle, cohomologous to f, defined by $f'(\gamma) = b^{-1} f(\gamma)\gamma(b)$ for every $\gamma \in \Gamma_K$: by construction we have $f'(\gamma_r) = x \in \mathrm{GL}_h(K_r)$. For every $\gamma \in \Gamma_K$, $\gamma_r\gamma = \gamma\gamma_r$, so that

$$f'(\gamma)\gamma(f'(\gamma_r)) = f'(\gamma_r)\gamma_r(f'(\gamma))$$

or, equivalently

$$\gamma_r(f'(\gamma)) = f'(\gamma_r)^{-1} f'(\gamma)\gamma(f'(\gamma_r)) = x^{-1} f'(\gamma)\gamma(x).$$

Hence, the K_r subspace V of L generated by the coefficients of $f'(\gamma)$ is stable by γ_r. Since V is finite dimensional over K we can use again Theorem 1.5.10 to deduce $f'(\gamma) \in \mathrm{GL}_h(K_\infty)$ for every $\gamma \in \Gamma_K$, i.e. f is cohomologous to a cocycle with values in $\mathrm{GL}_h(K_\infty)$ and it is therefore in the image of ι. □

1.5.12. Corollary. *We have* $\mathrm{H}^0_{\mathrm{cont}}(\Gamma_K, L_0) = \mathrm{H}^1_{\mathrm{cont}}(\Gamma_K, L_0) = 0$.

Proof. Indeed, $L_0^{\Gamma_K} = 0$ as we have seen in the proof of part i) of 1.2.4. Let $f \in Z^1_{\mathrm{cont}}(\Gamma_K, L_0)$ be a cocycle. Being f continuous, it is determined by $f(\gamma_0)$ and under this identification the group $B^1_{\mathrm{cont}}(\Gamma_K, L_0)$ of continuous coboundaries is a subgroup of the image of $\gamma_0 - 1$. Hence $\mathrm{H}^1_{\mathrm{cont}}(\Gamma_K, L_0) \subset \mathrm{Coker}(\gamma_0 - 1) = 0$ by 1.5.6. □

1.5.13. Let K_∞/K be the cyclotomic $\mathbb{Z}_p$ extension of K. Let χ be a continuous character of Γ_K into the group of units of $\mathcal{O}_K$. We can define the space L with a twisted action of Γ_K

$$^{s}x = \chi(s)(sx)$$

for all $s \in \Gamma_K$ and all $x \in L$. Following Tate [**Tat67**], we denote this space by $L(\chi)$. Let $\lambda = \chi(\gamma_0)$ and suppose that λ satisfies the assumptions of Prop. 1.5.7: this is the case, for example, when $\chi(L)$ is infinite.

1.5.14. PROPOSITION. *We have* $\mathrm{H}^0(\Gamma_K, L(\chi)) = \mathrm{H}^1_{\mathrm{cont}}(\Gamma_K, L(\chi)) = 0$

PROOF. Indeed, $\mathrm{H}^0(\Gamma_K, L(\chi)) \subset \mathrm{Ker}(\gamma_0 - \lambda) = 0$ by 1.5.7. We can identify $\mathrm{H}^1_{\mathrm{cont}}(\Gamma_K, L(\chi))$ with a subgroup of $\mathrm{Coker}(\gamma_0 - \lambda)$, which is trivial, again by 1.5.7. □

1.5.15. Let χ_p be the cyclotomic character $\chi_p \colon G_K \to \mathbb{Z}_p^\times$ and consider the field $\mathbf{C}$ with the action of G_K twisted by χ_p. We have

$$\mathrm{H}^0_{\mathrm{cont}}(G_K, \mathbf{C}(\chi_p)) = \mathrm{H}^1_{\mathrm{cont}}(G_K, \mathbf{C}(\chi_p)) = 0.$$

Indeed, we have $\mathbf{C}(\chi_p)^{G_K} = (\mathbf{C}(\chi_p)^{H_K})^{\Gamma_K} = L(\chi_p)^{\Gamma_K} = 0$ by Prop 1.5.14, as the kernel of χ_p is contained in H_K by definition. The statement for H^1 follows from 1.5.14 together with the inflation-restriction exact sequence (1.1.4.1).

1.6. Galois Representations

1.6.1. Let G be a topological group and let F be a field endowed with a linear topology and a continuous action of G, compatible with the field structure. A finite-dimensional F-vector space V endowed with a semi-linear action of G is called an F-representation of G. We form a category, denoted $\mathbf{Rep}_F(G)$, with morphisms given by the G-equivariant maps.

We call unit representation the field F with the given action of G. If $V \in \mathbf{Rep}_F(G)$ we call the dual representation of V the F-vector space V^* (dual of V) with the action $g((\varphi)(v)) = g(\varphi(g^{-1}(v)))$ for every $g \in G$, $v \in V$, $\varphi \in V^*$. Finally, given $V_1, V_2 \in \mathbf{Rep}_F(G)$, we can form the tensor product representation $V_1 \otimes V_2$ where the action of G is given by $g(v_1 \otimes v_2) = g(v_1) \otimes g(v_2)$ for every $g \in G, v_i \in V_i$ $(i = 1, 2)$. If $E = F^G$ is the subfield of F fixed by G, the category $\mathbf{Rep}_F(G)$ is a Tannakian category over E.

1.6.2. PROPOSITION. *For every* $V \in \mathbf{Rep}_F(G)$*, the* F*-linear morphism*

$$\varrho_F(V) \colon F \otimes_E V^G \to V$$

induced by the inclusion $V^G \subset V$ *is injective.*

PROOF. By contradiction, let m be the smallest positive integer such that there exist $v_1, v_2, \ldots, v_m \in V^G$ linearly independent over E but not over F. By the minimality of m, there exist $a_1 = 1, \ldots, a_m \in F^\times$ such that $\sum_{i=1}^m a_i v_i = 0$. For every $g \in G$ we have

$$0 = g\Big(\sum_{i=1}^m a_i v_i\Big) = v_1 + \sum_{i=2}^m g(a_i) v_i$$

so that $\sum_{i=2}^m (g(a_i) - a_i) v_i = 0$. Hence, again by the minimality of m, $g(a_i) - a_i = 0$ for every $i = 2, \ldots m$, i.e. $a_i \in E$, that contradicts the independence of the v_i's over E. □

1.6.3. Remark. We can prove in a similar way the following strengthened version of 1.6.2. Let B be an integral E-algebra endowed with a linear topology and a continuous action of G, compatible with the ring structure. Suppose that $B^G = \mathrm{Frac}(B)^G = E$. Then for every $V \in \mathbf{Rep}_F(G)$, the F-linear morphism

$$\varrho_{B,F}(V) \colon B \otimes_E (B \otimes_F V)^G \to B \otimes_F V$$

is injective.

1.6.4. We say that $V \in \mathbf{Rep}_F(G)$ is trivial if $V \cong F^n$ for some $n \in \mathbb{N}$ (isomorphism as F-representations of G). By 1.6.2, we see that V is trivial if and only if the map $\varrho_F(V)$ is bijective or, equivalently, if and only if we have the equality $\dim_E(V^G) = \dim_F V$.

1.6.5. We keep the notations of 1.2.1—1.2.2: K_∞ is the cyclotomic $\mathbb{Z}_p$ extension of K contained in $\overline{K}$, $L = \mathrm{Frac}(\widehat{\mathcal{O}}_{K_\infty})$, the completion taken with respect to the p-adic topology. For every $r \in \mathbb{N}$ we denote by K_r the unique extension of degree p^r over K contained in K_∞. We have $H_K = \mathrm{Gal}(\overline{K}/K_\infty)$ and $\Gamma = \Gamma_K$ is the Galois group $\mathrm{Gal}(K_\infty/K)$. If γ_0 is a topological generator of Γ, $\gamma_r = \gamma_0^{p^r}$ is a topological generator of $\Gamma_r = \mathrm{Gal}(K_\infty/K_r)$.

We naturally have two $\otimes$-functors

$$\begin{aligned} \mathbf{Rep}_{K_\infty}(\Gamma) &\to \mathbf{Rep}_L(\Gamma) \\ V &\mapsto L \otimes_{K_\infty} V \end{aligned} \tag{1.6.5.1}$$

and

$$\begin{aligned} \mathbf{Rep}_L(\Gamma) &\to \mathbf{Rep}_{\mathbf{C}}(G_K) \\ W &\mapsto \mathbf{C} \otimes_L W. \end{aligned} \tag{1.6.5.2}$$

The object of the theory of Sen is to construct two functors in the opposite direction defining $\otimes$-equivalences of categories

$$\mathbf{Rep}_{K_\infty}(\Gamma) \xrightarrow{\sim} \mathbf{Rep}_L(\Gamma) \xrightarrow{\sim} \mathbf{Rep}_{\mathbf{C}}(G_K).$$

1.6.6. Theorem ([**Sen80**, Th. 2]). *Every $\mathbf{C}$-representation of H_K is trivial*

Proof. By 1.6.2 we have to show that, for every $W \in \mathbf{Rep}_{\mathbf{C}}(H_K)$, the map $\varrho_{\mathbf{C}}(W)$ is bijective. Let $\{w_1, \ldots, w_h\}$ be a $\mathbf{C}$-basis of W. We can define a continuous cocycle $f \colon H_K \to \mathrm{GL}_h(\mathbf{C})$ by the assignment $g \mapsto M_g$, where M_g is the matrix representing the action of g on W in the basis $\{w_1, \ldots, w_h\}$, so that the i-th column is given by the coefficients of $g(w_i)$. Let b be the matrix of base-change for another basis of W: the corresponding cocycle is given by the formula $f'(g) = bf(g)b^{-1}$, so that f and f' are cohomologous and the map does not depend on the choice of $\{w_1, \ldots, w_h\}$. By 1.2.3 (ii), $\mathrm{H}^1_{\mathrm{cont}}(H_K, \mathrm{GL}_h(\mathbf{C}))$ is trivial, so that we can choose a basis formed by elements $\{w_i\}_{i=1}^h$ fixed by H_K. Hence, given $w = \sum_{i=1}^h b_i w_i \in W$, we have $w \in W^{H_K}$ if and only $b_i \in \mathbf{C}^{H_K} = L$ (by 1.2.3 (i)). Therefore W^{H_K} is the L-vector space of basis $\{w_i\}_{i=1}^h$ and the statement follows. □

1.6.7. Corollary. *The functor $W \mapsto W^{H_K}$ defines a $\otimes$-equivalence between the category $\mathbf{Rep}_{\mathbf{C}}(G_K)$ and the category $\mathbf{Rep}_L(\Gamma)$, quasi-inverse of the functor* (1.6.5.2).

PROOF. By 1.6.6, the functor $W \mapsto W^{H_K}$ defines a $\otimes$-equivalence between $\mathbf{Rep}_{\mathbf{C}}(H_K)$ and the category of finite-dimensional L-vector spaces, where a quasi inverse given by

$$X \mapsto \mathbf{C} \otimes_L X.$$

If $W \in \mathbf{Rep}_{\mathbf{C}}(G_K)$, W^{H_K} is naturally an L-representation of $\Gamma = G_K/H_K$ and $\mathbf{C} \otimes_L W^{H_K}$ is isomorphic to W as (trivial) representation of H_K, but also as representation of G_K. If $Y \in \mathbf{Rep}_L(\Gamma)$, $(\mathbf{C} \otimes_L Y)^{H_K} \cong C^{H_K} \otimes_L Y = Y$, by definition of the action of G_K on a tensor product. □

1.6.8. Let $V \in \mathbf{Rep}_{K_\infty}(\Gamma)$ and let $\{v_1, \dots, v_h\}$ be a K_∞-basis of V as vectors space. Let M_0 be the matrix representing the action of γ_0 on V in the basis $\{v_i\}$. Let K_r be the field generated over K by the coefficients of M_0: the integer r is called the degree of the basis $\{v_1, \dots, v_h\}$. Since K_r is complete and the action of Γ over V is continuous, the K_r-vector space generated by $\{v_1, \dots, v_h\}$ and contained in V is stable for Γ.

1.6.9. THEOREM ([**Sen80**, Th. 3]). *Let $X \in \mathbf{Rep}_L(\Gamma)$. Let X_f be the union of the sub-K-vector spaces of finite dimension of X that are stable by Γ. The L-linear map*

$$L \otimes_{K_\infty} X_f \to X$$

induced by the inclusion $X_f \subset X$ is bijective.

PROOF. As in the proof of 1.6.6, we fix a basis $\{x_1, \dots, x_h\}$ of X over L and we consider the continuous cocycle $f : \Gamma \to \mathrm{GL}_h(L)$ that maps $\gamma \in \Gamma$ to M_γ, where M_γ represents the action of γ on X in the basis $\{x_1, \dots, x_h\}$: f does not depend on the choice of the basis. By 1.2.4 (ii), the map

$$\mathrm{H}^1_{\mathrm{cont}}(\Gamma, \mathrm{GL}_h(K_\infty)) \to \mathrm{H}^1_{\mathrm{cont}}(\Gamma, \mathrm{GL}_h(L))$$

is surjective, so we can suppose that f takes value in $\mathrm{GL}_h(K_\infty)$. In other words, we can choose the x_i's such that the sub-K_∞-vector space Y of X is stable for Γ; in particular $Y \in \mathbf{Rep}_{K_\infty}(\Gamma)$. Since the L-linear map $L \otimes_{K_\infty} Y \to X$ induced by the inclusion $Y \subset X$ is clearly bijective, to complete the proof of the theorem it is enough to show that $Y = X_f$.

First of all, we have $Y \subset X_f$. Indeed, let r be the degree of the basis $\{x_1, \dots, x_h\}$. For every $s \geq r$, the K_s-vector space generated by the x_i's is of finite dimension over K, stable by Γ and Y is clearly equal to the union of those space.

Let $x \in X_f$, $x = \sum_{i=1}^h c_i x_i$ with $c_i \in L$. For every $\gamma \in \Gamma$, $\gamma(x) = \sum_{i=1}^h c_i(\gamma) x_i$, for suitable coefficients $c_i(\gamma) \in L$. Let V be the K_r-subspace of L generated by $c_i(\gamma)$ for $i = 1, \dots, h$ and $\gamma \in \Gamma$ is of finite dimension over K. Write $(a_{i,j}(\gamma))_{1 \leq i,j \leq h}$ for the matrix M_γ. Then $(a_{i,j}(\gamma))_{1 \leq i,j \leq h} \in \mathrm{GL}_h(K_r)$ and

$$\gamma(x) = \sum_{i=1}^h (c_i(\gamma)) x_i = \sum_{i=1}^h \gamma(c_i) a_{i,j}(\gamma) x_i$$

so that V is also the K_r vector space generated by $\gamma(c_i)$ for $i = 1, \dots, h$ and $\gamma \in \Gamma$. It is therefore stable by Γ and, being finite-dimensional, it is contained in K_∞ by 1.5.10. Hence $c_i \in K_\infty$ and $x \in Y$. □

1.6.10. COROLLARY. *The functor $X \mapsto X_f$ defines a $\otimes$-equivalence between the category $\mathbf{Rep}_L(\Gamma)$ and the category $\mathbf{Rep}_{K_\infty}(\Gamma)$, quasi-inverse of the functor* (1.6.5.1).

PROOF. It follows directly from 1.6.9 that the functor defined by the composition $X \mapsto X_f \mapsto X_f \otimes_{K_\infty} L$ is naturally isomorphic to the identity functor. On the other hand, $(L \otimes_{K_\infty} V)_f$ is isomorphic to V for every $V \in \mathbf{Rep}_{K_\infty}(\Gamma)$ by construction, since given a K_∞-basis $\{v_1, \dots, v_h\}$ of V, $\{1 \otimes v_i\}_{i=1}^h$ is an L-basis of $L \otimes_{K_\infty} V$ such that the K_∞ sub-vector space that they generate is stable by Γ. □

1.7. The study of $\mathbf{Rep}_{K_\infty}(\Gamma)$

1.7.1. THEOREM ([**Sen80**, Th. 4]). *Let $Y \in \mathbf{Rep}_{K_\infty}(\Gamma)$. There exists a unique K_∞-linear endomorphism s of Y such that, for every $y \in Y$, there is an open subgroup Γ_y of Γ satisfying*

$$\gamma(y) = \exp\left(\log \chi_p(\gamma).s\right)(y)$$

for every $\gamma \in \Gamma_y$. Moreover, the characteristic polynomial of s has coefficients in K.

PROOF. Let $\{y_1, \dots, y_h\}$ be a K_∞ basis of Y. We first prove the uniqueness of s. Let s, s' be two endomorphisms of Y having the required properties. Then there exists an open subgroup Γ_r of Γ such that for every $\gamma \in \Gamma_r$

$$\gamma(y_i) = \exp\left(\log \chi_p(\gamma).s\right)(y_i) = \exp\left(\log \chi_p(\gamma).s'\right)(y_i)$$

for $i = 1, \dots, h$. Hence $\exp\left(\log \chi_p(\gamma).s\right) = \exp\left(\log \chi_p(\gamma).s'\right)$ for every $\gamma \in \Gamma_r$ and $s = s'$.

Let r_0 be the degree of the basis $\{y_1, \dots, y_h\}$, Y' the K_{r_0}-sub-vector space of Y generated by the y_i's and stable by Γ: Γ_{r_0} acts linearly on Y' (since Γ_{r_0} fixes K_{r_0}) and the action on the y_i's is given by a continuous homomorphism $\Gamma_{r_0} \to \mathrm{GL}_h(K_{r_0})$, $\gamma \mapsto M_\gamma$. For γ sufficiently close to 1 (but different from 1), M_γ is close to I_h in $\mathrm{GL}_h(K_{r_0})$ and the series $\log(M_\gamma)$ converges to an endomorphism $\log(\gamma) \in \mathrm{End}_{K_{r_0}}(Y')$. The endomorphism $s_0 = \frac{\log \gamma}{\log(\chi_p(\gamma))}$ does not depend on the choice of γ. Indeed, let γ_0 be a topological generator of Γ. Let $\gamma = \gamma_0^t$ and let $\gamma' = \gamma_0^{t'}$ be another element in Γ such that $\log \gamma'$ is defined. Then

$$\log(\gamma') = \log(\gamma_0^{\log \chi_p(\gamma')}) = \log \chi_p(\gamma') \log \gamma_0$$

so that the quotient $\frac{\log(\gamma')}{\log \chi_p(\gamma')} = \frac{\log(\gamma)}{\log \chi_p(\gamma)}$ is independent from γ.

Let s be the unique K_∞ endomorphism of Y that restricts to s_0 on Y'.

1.7.2. LEMMA. *There exists $r \geq r_0$ such that the endomorphism $\exp(\log \chi_p(\gamma).s)$ of Y is well defined for every $\gamma \in \Gamma_r$.*

We postpone the proof of the lemma. Writing out the definition of s, for every $y \in Y'$, we have

$$\gamma(y) = \exp\left(\log \chi_p(\gamma).s\right)(y).$$

For a general $y = \sum_{i=1}^h c_i y_i$ with $c_i \in K_\infty$, the formula is satisfied if $\gamma \in \Gamma_y = \Gamma' \cap \Gamma_r$, where Γ' is an open subgroup of Γ which fixes all the c_i's. This proves the existence part of the theorem.

Let M be the matrix of s in the basis $\{y_1, \dots, y_h\}$. For every $\gamma \in \Gamma_r$ we have

$$(\gamma(y_1), \dots, \gamma(y_h)) = \exp(\log \chi_p(\gamma) M)(y_1, \dots, y_h).$$

As $\gamma\gamma_0 = \gamma_0\gamma$ we have, for every $\gamma \in \Gamma_r$

$$(\gamma_0(\gamma(y_1)), \dots, \gamma_0(\gamma(y_h))) = \exp(\log \chi_p(\gamma)\gamma_0(M))(y_1, \dots, y_h)$$

so that M and $\gamma_0(M)$ are similar, that implies that the characteristic polynomial of s is fixed by γ_0, i.e. it's coefficients are in K. □

Proof of Lemma 1.7.2. It's enough to show that there exists an open subgroup Γ_r of Γ such that the series

$$\exp(\log \chi_p(\gamma).s) = \sum_{n\geq 0} \frac{(\log(\chi_p(\gamma)))^n}{n!} s^n$$

converges in the ring $\mathrm{End}_{K_\infty}(Y)$ for every $\gamma \in \Gamma_r$.

Let $\{y_1, \dots, y_h\}$ be a K_∞-basis of Y. For every $b \in \mathbb{Q}$, let Y_b be the $\mathcal{O}_{K_\infty}$-sub module of Y defined by

$$Y_b = \Big\{ \sum_{i=1}^h c_i y_i \in Y \mid v_p(c_i) \geq b \Big\}.$$

Let $a \in \mathbb{Q}$ be such that $s(Y_0) \subseteq Y_a$. Recall that (see [**NS99**, chap. II, Prop. 5.5])

$$\log \mathbb{Z}_p^\times = \begin{cases} p\mathbb{Z}_p & \text{if } p \neq 2 \\ p^2\mathbb{Z}_p & \text{if } p = 2. \end{cases}$$

Let r_K be the unique integer such that $\log \chi_p(\Gamma_K) = p^{r_K}\mathbb{Z}_p$: we have $r_K \geq 1$ if $p \neq 2$ (resp. $r_K \geq 2$ if $p = 2$) and the equality holds if and only if K is absolutely unramified, i.e. $v_K(p) = e_K = 1$ (see [**NS99**, chap. II, Prop. 5.4-5.5]). Let r be the smallest non-negative integer such that $r + r_k + a > \frac{1}{p-1}$. Then for every $n \in \mathbb{N}$ and $\gamma \in \Gamma_r$ we have

$$\frac{(\log(\chi_p(\gamma)))^n}{n!} s^n(Y_0) \subset Y_{n(r+r_K-\frac{1}{p-1}+a)}$$

as $v_p(n!) = \frac{1}{p-1}\sum_{i=1}^r a_i(p^i - 1)$ if $n = \sum_{i=0}^r a_i p^i$, $0 \leq a_i < p$ is the p-adic expansion of n ([**NS99**, chap. II, Lemma 5.6]). Therefore the series $\exp(\log \chi_p(\gamma).s)$ converges. □

1.7.3. Let E be any field. We denote by $\mathcal{S}_E$ the category whose objects are couples (Y, s), where Y is a finite-dimensional E-vector space and $s \in \mathrm{End}_E(Y)$, and morphisms $f\colon (Y_1, s_1) \to (Y_2, s_2)$ are E-linear maps from Y_1 to Y_2 such that $s_2 \circ f = f \circ s_1$.

We set the unit object to be $(E, 0)$ and we define the tensor product $(Y_1, s_1) \otimes (Y_2, s_2)$ by $(Y_1 \otimes_E Y_2, s_1 \otimes id_{Y_2} + id_{y_1} \otimes s_2)$. The dual of (Y, s) is $(Y^*, -s^t)$ where Y^* is the dual vector space of Y and s^t is the transpose homomorphism of s. With these definitions $\mathcal{S}_E$ has a structure of Tannakian category over E.

1.7.4. Let E be a field containing K_∞. Let $Y \in \mathbf{Rep}_{K_\infty}(\Gamma)$. Let $Y_E = E \otimes_{K_\infty} Y$ and let s_E be the E-endomorphism of Y_E deduced by scalar extension from the endomorphism s of 1.7.1. We have therefore defined a $\otimes$-functor

$$Y \mapsto (Y_E, s_E)$$

from $\mathbf{Rep}_{K_\infty}(\Gamma)$ to $\mathcal{S}_E$.

1.7.5. Theorem. *In the notations of 1.7.4, let* $Y_1, Y_2 \in \mathrm{End}_{K_\infty}(\Gamma)$. *The canonical* E*-linear map*

$$E \otimes_K \mathrm{Hom}_{\mathbf{Rep}_{K_\infty}(\Gamma)}(Y_1, Y_2) \to \mathrm{Hom}_{\mathcal{S}_E}((Y_{1,E}, s_{1,E}), (Y_{2,E}, s_{2,E}))$$

is an isomorphism.

PROOF. We can reduce to the case $Y_1 = K_\infty$. Indeed we have the following canonical isomorphisms:

$$\mathrm{Hom}_{\mathbf{Rep}_{K_\infty}(\Gamma)}(Y_1, Y_2) = \mathrm{Hom}_{\mathbf{Rep}_{K_\infty}(\Gamma)}(K_\infty, Y_1^* \otimes Y_2)$$
$$\mathrm{Hom}_{\mathcal{S}_E}(Y_{1,E}, Y_{2,E}) = \mathrm{Hom}_{\mathcal{S}_E}(E, Y_{1,E}^* \otimes Y_{2,E}).$$

We put $Y = Y_2$. For every $\xi \in \mathrm{Hom}_{\mathbf{Rep}_{K_\infty}(\Gamma)}(K_\infty, Y)$, the map $\xi \mapsto \xi(1)$ allow us to identify the K-vector space $\mathrm{Hom}_{\mathbf{Rep}_{K_\infty}(\Gamma)}(K_\infty, Y)$ with $\mathrm{H}^0_{\mathrm{cont}}(\Gamma, Y) = Y^\Gamma$. Moreover, we can identify $\mathrm{Hom}_{\mathcal{S}_E}(E, Y_E)$ with $\mathrm{Ker}\, s_E$. Indeed, if $\varphi\colon (E, 0) \to (Y_E, s_E)$ is a $\mathcal{S}_E$-morphism, then $s_E \circ \varphi = \varphi \circ 0 = 0$, so that $\varphi(1) \in \mathrm{Ker}\, s_E$. We are therefore reduced to prove that the canonical map

$$\varrho\colon E \otimes_K Y^\Gamma \to \mathrm{Ker}\, s_E$$

is bijective. By definition of s_E, we see that it is enough to prove the statement for $E = K_\infty$. Up to replacing Y by $\mathrm{Ker}\, s$ we can assume $s = 0$, $\mathrm{Ker}\, s = Y$. By 1.6.2 ϱ is injective. We fix a K_∞-basis $\{y_1, \ldots, y_h\}$ of Y. Let r_0 be its degree. Being $s = 0$, by 1.7.1, there exists r —that we may assume $r \geq r_0$— such that $\gamma(y_i) = y_i$ for $i = 1, \ldots, h$ and $\gamma \in \Gamma_r$. Let Y_r be the K_r-sub-vector space of Y generated by $y_1, \ldots, y_h$: by construction, Y_r is stable by Γ, that acts on it by means of the finite quotient $\mathrm{Gal}(K_r/K)$. As in the proof of 1.6.6, we can define a 1-cocycle $f\colon \mathrm{Gal}(K_r/K) \to \mathrm{GL}_h(K_r)$ describing the action of $\mathrm{Gal}(K_r/K)$ on Y_r with respect to $\{y_1, \ldots, y_h\}$. By Hilbert's Theorem 90 [**Ser62**, chap. X, Prop. 3], we have

$$\mathrm{H}^1(\mathrm{Gal}(K_r/K), \mathrm{GL}_h(K_r)) = 1.$$

Hence we can assume that $\mathrm{Gal}(K_r/K)$ acts trivially on $y_1, \ldots, y_h$, so that Γ fixes a basis of Y and the map ϱ is therefore surjective. □

1.7.6. LEMMA. *Let E be a field and let Z_1, Z_2 be finite-dimensional E-vector spaces. Let E_0 be an infinite subfield of E, L a sub-E_0-vector space of the E-vector space $\mathcal{L}_E(Z_1, Z_2)$ of E-linear applications from Z_1 to Z_2. The E-vector space $L_E = E \otimes L$ contains an isomorphism if and only if L already contains one.*

PROOF. Let $f \in L_E$ be an isomorphism, $f\colon Z_1 \to Z_2$. Let $\{f_1, \ldots, f_n\}$ be an E-basis of L_E formed by elements of L. Let h be the dimension $\dim_E Z_1 = \dim_E Z_2$ and fix an E-basis of Z_1 and an E-basis of Z_2. For $j = 1, \ldots, n$, let $A_j \in \mathrm{M}_h(E)$ be the matrix of f_j with respect to those basis. Let $P(X_1, \ldots, X_n)$ be the polynomial

$$P(X_1, \ldots, X_n) = \det(X_1 A_1 + X_2 + \ldots + X_n A_n) \in E[X_1, \ldots, X_n].$$

If $f = \sum_{i=1}^n \lambda_i f_i$, $\lambda_i \in E$, we have $P(\lambda_1, \ldots, \lambda_n) \neq 0$, so that P is not identically zero. Being E_0 an infinite field, there exist $\mu_1, \ldots, \mu_n \in E_0$ such that $P(\mu_1, \ldots, \mu_n) \neq 0$ and the element $\sum_{i=1}^n \mu_i f_i$ is an element of L, isomorphism of Z_1 over Z_2. □

1.7.7. COROLLARY. *Two K_∞-representations of Γ, Y_1 and Y_2, are isomorphic in $\mathbf{Rep}_{K_\infty}(\Gamma)$ if and only if $(Y_{1,E}, s_{1,E})$ and $(Y_{2,E}, s_{2,E})$ are isomorphic in $\mathcal{S}_E$.*

1.7.8. Let $W \in \mathbf{Rep}_{\mathbf{C}}(G_K)$. Then we dispose of the L-representation of Γ W^{H_K} and of the K_∞-representation of Γ $(W^{K_K})_f$. We denote by $\Delta_{\mathrm{Sen}}(W)$ the object of $\mathcal{S}_{K_\infty}$ formed by the K_∞-vector space underlying $(W^{K_K})_f$ and by the endomorphism $s_{W,f}$ defined in 1.7.1.

Δ_{Sen} defines a faithful $\otimes$-functor

$$\Delta_{\mathrm{Sen}}\colon \mathbf{Rep}_{\mathbf{C}}(G_K) \to \mathcal{S}_{K_\infty}.$$

By 1.7.7 we see that the knowledge of $\Delta_{\mathrm{Sen}}(W)$ determines — up to isomorphisms — W as $\mathbf{C}$-representation of G_K,

1.8. Classification of C-representations

1.8.1. We keep the notations of 1.2.1—1.2.2. Let W be a $\mathbf{C}$-representation of G_K. In the notations of 1.7.8, we call Sen weights of W the eigenvalues of the endomorphism $s_{W,f}$ in $\overline{K}$. By 1.7.1, the characteristic polynomial of $s_{W,f}$ has coefficients in K. Hence the set of Sen weights of W is stable by G_K.

Let X be a subset of $\overline{K}$ which is stable by G_K. We say that a $\mathbf{C}$-representation W of G_K is of type S_X if its Sen weights are in X. We say that W is of type S_X^m if it is of type S_X and if $s_{W,f}$ is semi-simple.

1.8.2. We denote by $\mathcal{C}(\overline{K})$ the set of the orbists of $\overline{K}$ for the action of G_K. For every indecomposable object W in $\mathbf{Rep_C}(G_K)$, there exists a unique $A \in \mathcal{C}(\overline{K})$ such that W is of type S_A.

Let W be an indecomposable object of type S_A. We can write its Sen endomorphism $s_{W,f}$ as $s_0.s_u = s_u.s_0$, with s_0 semi-simple and s_u unipotent. Let V be the K_∞-vector space underlying $(W^{H_K})_f$, $\overline{V}$ the vector space $V \otimes_{K_\infty} \overline{K}$. We denote again by s_0 the endomorphism of $\overline{V}$ deduced by scalar extension. Then we have:

i) a decomposition of $\overline{V}$ as a direct sum of the eigenspaces of s_0;
ii) a nilpotent endomorphism $\log s_u$ of V.

1.8.3. The $\mathbf{C}$-representations of G_K of type $S_{\{0\}}$ correspond to representations of the additive group $\mathbb{G}_a$. Indeed, to give an action of the additive group $\mathbb{G}_a$ over a K_∞-vector space V comes down to give a nilpotent endomorphism ν of V (so that $\lambda \in K_\infty = \mathbb{G}_a(K_\infty)$ acts over V via $\exp(\lambda\nu)$). Let $K_\infty[\log t]$ be the algebra of polynomials in the variable $\log t$ and coefficients in K_∞. For every $d \geq 1$, we denote by $\mathbb{Z}_p(0;d)$ the sub $\mathbb{Z}_p$-module of $K_\infty[\log t]$ formed by the polynomials in $\log t$ of degree $< d$ with coefficients in $\mathbb{Z}_p$. Hence we see that, up to isomorphisms, there exists a unique indecomposable $\mathbf{C}$-representation of G_K of type $S_{\{0\}}$ of dimension d over $\mathbf{C}$, namely

$$C^K(0;d) = \mathbf{C} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(0;d)$$

where the nilpotent endomorphism ν is $-\frac{\partial}{\partial \log t}$.

Notice that $C^K(0;d)$ is not simple, as $C^K(0;d) \supset C^K(0;d-1) \supset \ldots \supset C^K(0;1)$.

1.8.4. Let W be a simple object of $\mathbf{Rep_C}(G_K)$ and let A be the unique conjugacy class of $\overline{K}$ such that W is of type S_A. Then, for every $d \geq 1$, we can define the indecomposable object of type S_A

$$W \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(0;d).$$

On the other hand, we see that a $\mathbf{C}$-representation W' of G_K is indecomposable of type S_A if and only if there exists $d \in \mathbb{N}^*$ (necessarily unique) such that $W' \cong W \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(0;d)$. Then W' is simple if and only if $d = 1$.

1.8.5. We fix a topological generator γ_0 of Γ. For every $r \in \mathbb{N}$, let $\mathfrak{a}_r$ be the $\mathcal{O}_{\overline{K}}$-sub-module of $\overline{K}$

$$\mathfrak{a}_r = \{\alpha \in \overline{K} \mid v_p(\alpha) > -r - r_K + \frac{1}{p-1}\}$$

where r_K is the integer defined in the proof of 1.7.2. Let $A \in \mathcal{C}(\overline{K})$ and set $P_A(X) = \prod_{\alpha \in A}(X - \alpha) \in K[X]$ be the minimal polynomial of any $\alpha \in A$ over K. Let $K_A \subset \overline{K}$ be the field $K[X]/(P_A(X))$ and denote by β the image of X in K_A. Let d_A be the number of elements in A. Let r_A be the smallest integer r such that an element $\alpha \in A$ belongs to $\mathfrak{a}_r$. By construction, it is the smallest $r \in \mathbb{N}$ such that

$$v_p(\beta \log \chi_p(\gamma)) = v_p(\beta) + v_p(\log(\chi_p(\gamma)) > \frac{1}{p-1}$$

for every $\gamma \in \Gamma_r$. We can therefore define a continuous homomorphism $\varrho_A \colon \Gamma_{r_A} \to K_A^\times$ by

$$\varrho_A(\gamma) = \exp(\beta \log \chi_p(\gamma)).$$

We denote by $M[A]$ the field K_A endowed with the linear and continuous action of Γ_{r_A} given by ϱ_A.

Let $N[A] = K_A[\Gamma] \otimes_{K_A[\Gamma_{r_A}]} M[A]$ be the induced K_A-linear representation of Γ. It is a K_A-vector space of dimension p^{r_A}, since $\{\gamma_0^i \otimes 1\}_{0 \leq i < p^{r_A}}$ is a basis of $N[A]$ over K_A. We denote by $N_\infty[A] = K_\infty \otimes_K N[A]$ the K_∞-representation of Γ deduced by $N[A]$ by scalar extension. We choose a simple sub-object of $N_\infty[A]$ in $\mathbf{Rep}_{K_\infty}(\Gamma)$ and we denote it by $K_\infty[A]$. We set $\mathbf{C}[A]$ to be the $\mathbf{C}$-representation of G_K corresponding to $K_\infty[A]$, i.e.

$$\mathbf{C}[A] = \mathbf{C} \otimes_{K_\infty} K_\infty[A].$$

1.8.6. Theorem. *In the notations 1.8.5, let W be a $\mathbf{C}$-representation of G_K.*

i) *W is simple if and only if there exists $A \in \mathcal{C}(\overline{K})$ such that $W \cong \mathbf{C}[A]$; then W is of type S_A^m and has dimension $d_A p^{s_A}$ over $\mathbf{C}$, where s_A is an integer $0 \leq s_A \leq r_A$ verifying* $\dim_{K_\infty}(K_\infty[A]) = \dim_{\mathbf{C}}(\mathbf{C}[A])$.

ii) *W is indecomposable if and only if there exists $A \in \mathcal{C}(\overline{K})$ such that $W \cong \mathbf{C}[A; d] = \mathbf{C}[A] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(0; d)$; then W is of type S_A and has dimension $d.d_A p^{s_A}$ over $\mathbf{C}$.*

iii) *There exist natural integers $(h_{A,d}(W))_{A \in \mathcal{C}(\overline{K}), d \in \mathbb{N}^*}$, almost all zero, uniquely determined, such that*

$$W \cong \bigoplus_{A \in \mathcal{C}(\overline{K}), d \in \mathbb{N}^*} \mathbf{C}[A; d]^{h_{A,d}(W)}$$

1.8.7. Lemma ([**Fon04**, Prop. 2.12]). *Let F be a field, E a subfield of F, $\overline{E}$ a separable closure of E, $G_E = \mathrm{Gal}(\overline{E}/E)$, $\eta \colon G_E \to \mathbb{Q}/\mathbb{Z}$ a continuous homomorphism and $b \in F$. Let $E' = \overline{E}^{\operatorname{Ker} \eta}$, N the degree of the cyclic extension E'/E, σ the generator of* $\mathrm{Gal}(E'/E)$ *such that $\eta(\sigma) \equiv 1/N \mod \mathbb{Z}$. Let $\Lambda_{E,F}(\eta, b)$ be the associative and unitary $E' \otimes_E F$-algebra generated by an element c satisfying*

$$c^N = 1 \otimes b; \tag{1.8.7.1}$$

$$c(u \otimes x) = (\sigma(u) \otimes x)c \quad \text{if } u \in E' \text{ and } x \in F.$$

Then the algebra $\Lambda_{E,F}(\eta, b)$ is a central simple algebra. The center of $\Lambda_{E,F}(\eta, b)$ is F and of dimension N^2 over its center. $\Lambda_{E,F}(\eta, b)$ isomorphic to an algebra of square matrices with coefficients in a skew field $D_{E,F}(\eta, b)$.

Theorem 1.8.6 is then a consequence of the previous discussion and of the following

1.8.8. PROPOSITION. *In the notations of 1.8.5, let* $\eta\colon G_K \to \mathbb{Q}/\mathbb{Z}$ *be the unique character of* G_K *that factors through* Γ *and that maps* γ_0 *to* $\frac{1}{p^{r_A}}$. *Let* $b = \varrho_A(\gamma_0^{p^{r_A}})$. *The* K_A*-algebra*

$$E_A = \mathrm{End}_{\mathbf{Rep}_{K_\infty}(\Gamma)}(N_\infty[A])$$

is identified with $\Lambda_{K,K_A}(\eta, b)$. *The skew field* $D_A = D_{K,K_A}(\eta, b)$ *has rank* p^{2s_A}, *where* s_A *is an integer verifying* $0 \le s_A \le r_A$. *We have*

$$\dim_{K_\infty}(K_\infty[A]) = \dim_{\mathbf{C}} \mathbf{C}[A] = d_A p^{s_A}.$$

Moreover, $\mathbf{C}[A]$ *is a simple object of* $\mathbf{Rep}_{\mathbf{C}}(G_K)$ *of type* S_A *and*

$$\mathrm{End}_{\mathbf{Rep}_{K_\infty}(\Gamma)}(K_\infty[A]) = \mathrm{End}_{\mathbf{Rep}_{\mathbf{C}}(G_K)}(\mathbf{C}[A]) = D_A.$$

PROOF. Let $M_\infty[A] = K_\infty \otimes_K M[A]$. For every $s \in \mathbb{N}$ we set $M_s[A] = K_s \otimes_K M[A]$ and $N_s[A] = K_s \otimes_K N[A]$. We have then the following inclusions:

$$\begin{array}{ccccc} M[A] & \subset & M_s[A] & \subset & M_\infty[A] \\ \cap & & \cap & & \cap \\ N[A] & \subset & N_s[A] & \subset & N_\infty[A]. \end{array}$$

To simplify the notation, we set $r = r_A$. For every $s \ge r$ we have the topological generator $\gamma_s = \gamma_0^{p^s}$ of $\Gamma_s \subset \Gamma_r$. By construction, γ_s acts on $M[A]$ by multiplication with the element $b^{p^{s-r}} = \exp(\beta \log \chi_p(\gamma_0^{p^s}))$.

Let $f \in \mathrm{End}_{\mathbf{Rep}_K(\Gamma_s)}(M[A])$. Then for every $\gamma \in \Gamma_s$, we have $f(\gamma(x)) = \gamma f(x)$ if and only if $f(\gamma_0^{p^s}(x)) = \gamma_0^{p^s} f(x)$, i.e. f satisfies $f(b^{p^{s-r}}x) = b^{p^{s-r}} f(x)$ for every $x \in K[A]$. But we have $K_A = K(b^{p^{s-r}})$, since

$$\beta = \frac{\log b^{p^{s-r}}}{\log(\chi_p(\gamma_0^{p^s}))}$$

and $\log(\chi_p(\gamma_0^{p^s})) \in K^\times$. Hence, the natural injection $K_A \to \mathrm{End}_{\mathbf{Rep}_K(\Gamma_s)}(M[A])$ is an isomorphism.

Let $\{e_1, \ldots, e_d\}$ be a basis of K_A over K, seen as ring of endomorphisms $\mathrm{End}_{\mathbf{Rep}_K(\Gamma_s)}(M[A])$. Let $f \in \mathrm{End}_{\mathbf{Rep}_{K_\infty}(\Gamma_r)}(M_\infty[A])$. Then there exists $s \ge r$ such that $f(M[A]) \subset M_s[A]$. Since f is K_∞-linear, we also have $f(M_s[A]) \subset M_s[A]$, so that the restriction f_s of f to $M_s[A]$ is an element of $\mathrm{End}_{\mathbf{Rep}_{K_s}(\Gamma_r)}(M_s[A])$. Since Γ_s acts trivially on K_s, we have

$$\mathrm{End}_{\mathbf{Rep}_{K_s}(\Gamma_s)}(M_s[A]) = K_s \otimes_K \mathrm{End}_{\mathbf{Rep}_K(\Gamma_s)}(M[A]) = K_s \otimes_K K_A.$$

We can therefore find $\lambda_1, \ldots, \lambda_d \in K_s$ such that f_s, as element of $\mathrm{End}_{\mathbf{Rep}_{K_s}(\Gamma_s)}(M_s[A])$, can be written as $f_s = \sum_{i=1}^d \lambda_i \otimes e_i$. Adding the further condition that f_s commutes with the action of γ_r, we have $\gamma_r(\lambda_i) = \lambda_i$ for every $i = 1, \ldots, d$, i.e. $\lambda_i \in K_r$, so that

$$\mathrm{End}_{\mathbf{Rep}_{K_\infty}(\Gamma_r)}(M_\infty[A]) = K_r \otimes_K K_A. \tag{1.8.8.1}$$

By construction, every element of $N_\infty[A]$ can be written in a unique way as $x = \sum_{i=0}^{p^r-1} \gamma_0^i(x_i)$, with $x_i \in M_\infty[A]$. Let $f \in E_A$. Then $f(x) = \sum_{i=0}^{p^r-1} \gamma_0^i(\varphi(x))$ where φ is the restriction of f to $M_\infty[A]$. Therefore the application

$$E_A \to \mathrm{Hom}_{\mathbf{Rep}_{K_\infty}(\Gamma_r)}(M_\infty[A], N_\infty[A]), \quad f \mapsto \varphi$$

is bijective. Let c be the unique element of E_A defined by $c(x) = \gamma_0(x)$ for every $x \in M[A]$ (so that $c(\lambda x) = \lambda c(x) = \lambda\gamma_0(x)$ for every $\lambda \in K_\infty$, $x \in M[A]$). Then, using (1.8.8.1), every element of E_A can be written in a unique way as $\sum_{i=0}^{p^r-1} c^i f_i$, for $f_i \in K_r \otimes_K K_A$. We see therefore that E_A is an algebra over $K_r \otimes_K K_A$ generated by an element c satisfying the conditions (1.8.7.1) of 1.8.7. As $c^{p^r} = b$, we have that the dimension of E_A over its center K_A is p^{2r}. The skew field D_A has rank p^{2s_A} over K_A for a suitable $0 \leq s_A \leq r$ and for any simple sub-object $K_\infty[A]$ we have therefore

$$\mathrm{End}_{\mathbf{Rep}_{K_\infty}(\Gamma)}(K_\infty[A]) = D_A$$

and $\dim_{K_\infty}(K_\infty[A]) = d_A p^{s_A}$. The statement for $\mathbf{C}[A]$ is clear. □

1.9. Hodge-Tate representations

1.9.1. We keep the notations of 1.8.5. Let $W \in \mathbf{Rep}_{\mathbf{C}}(G_K)$. We say that W is deployed (fr. *déployée*) over K if the Sen weights of W are in K. Let $\mathfrak{a}_0^K = \mathfrak{a}_0 \cap K$ be the fractional ideal of $\mathcal{O}_K$ formed by the elements of p-adic valuation $> -r_K + \frac{1}{p-1}$. Every simple $\mathbf{C}$-representation of G_K of type $S_{\mathfrak{a}_0^K}$ has dimension 1 over $\mathbf{C}$ and the ring of its endomorphisms is reduced to K (see 1.8.8).

Among the representations of type $S_{\mathfrak{a}_0^K}$ we have the representations of type $S_{\mathbb{Z}}^m$. These latter are called $\mathbf{C}$-representation of type Hodge-Tate (or simply $\mathbf{C}$-representation Hodge-Tate). Thus $W \in \mathbf{Rep}_{\mathbf{C}}(G_K)$ is Hodge Tate if it is semi-simple and its Sen weights are in $\mathbb{Z}$.

Let V be a p-adic representation of G_K, i.e. $V \in \mathbf{Rep}_{\mathbb{Q}_p}(G_K)$. By base-change we get the corresponding $\mathbf{C}$-representation, namely

$$\mathbf{C} \otimes_{\mathbb{Q}_p} V \in \mathbf{Rep}_{\mathbf{C}}(G_K).$$

We say that V is Hodge-Tate if $\mathbf{C} \otimes_{\mathbb{Q}_p} V$ is Hodge-Tate.

1.9.2. We fix a generator t of the Tate module $\mathbb{Z}_p(1) = \mathrm{T}_p(\mathbb{G}_m)(\overline{K})$. For every $i \in \mathbb{N}$ we denote by $\mathbb{Z}_p(i)$ the i-th power $\mathbb{Z}_p(1)^{\otimes^i}$ and by $\mathbb{Z}_p(-i)$ its $\mathbb{Z}_p$-dual. For every $\mathbb{Z}_p$-module M, we denote by $M(i)$ the i-th Tate twist of M, i.e. $M(i) = M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(i)$. For $x \in M$ and $u \in \mathbb{Z}_p(i)$, we write xu for $x \otimes u \in M(i)$. The map $x \mapsto xt^i$ is a $\mathbb{Z}_p$-linear bijection between M and $M(i)$, depending on the choice of t.

The group G_K acts over $Z_p(i)$ for every $i \in \mathbb{Z}$: we have $g.u = \chi_p^i(g)u$ for every $g \in G_K$ and $u \in \mathbb{Z}_p(i)$. Similarly, if M is a topological $\mathbb{Z}_p$-module endowed with a linear and continuous action of G_K, we have an induced linear and continuous action on $M(i)$. Namely, we have

$$g(xt^i) = \chi_p^i(g)g(x)t^i \quad \text{for every } g \in G_K, x \in M.$$

We can therefore identify $\mathbf{C}(i) = \mathbf{C} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(i)$ with $\mathbf{C}[\{i\}]$ defined in 1.8.5 for every $i \in \mathbb{Z}$. Indeed, for $A = \{i\}$ we have that Γ acts on $K = K_A$ via ϱ_A, that turns out to be χ_p^i. This identification is not canonical, depending on the choice of a generator t of $\mathbb{Z}_p(1)$, but is G_K-equivariant. Similarly, for every $d \in \mathbb{N}$, $\mathbf{C}[\{i\}; d]$ is isomorphic to $\mathbf{C}(i) \otimes_{\mathbb{Z}_p} Z_p(0; d)$.

Hence, by Fontaine's classification theorem 1.8.6, for any Hodge-Tate object W in $\mathbf{Rep}_{\mathbf{C}}(G_K)$ there exist non negative integers $h_q(W)$, almost always zero and uniquely determined by W, such that

$$W \cong \sum_{q \in \mathbb{Z}} \mathbf{C}(q)^{h_q(W)}.$$

The integer $h_q(W)$ is called the multiplicity of q as a Hodge-Tate weight of W.

1.9.3. Let $B_{\mathrm{HT}} = \mathbf{C}[t^{(1)}, 1/t^{(1)}]$ be the polynomial algebra in the variable $t^{(1)}$. Let t be a generator of $\mathbb{Z}_p(1)$. Then $t = (\varepsilon_n)_{n\in\mathbb{N}}$ where ε_n is a primitive p^n-th root of 1 in $\overline{K}$ and $\varepsilon_{n+1}^p = \varepsilon_n$. For $p \neq 2$, we denote by π_t the unique uniformizer of $\mathbb{Q}_p(\varepsilon_1)$ such that

$$(\pi_t)^{p-1} + p = 0, \quad v_p(\varepsilon_1 - 1 - \pi_t) \geq \frac{2}{p-1}.$$

If $p = 2$ we set $\pi_t = \varepsilon_2 - 1$. Then the map

$$\mathbb{Z}_p(1) = \mathbb{Z}_p t \to B_{\mathrm{HT}}, \quad \lambda t \mapsto \lambda \pi_t t^{(1)}$$

is injective and commutes with the action of G_K. We can identify B_{HT} with $\mathbf{C}[t, t^{-1}] = \bigoplus_{i\in\mathbb{Z}} \mathbf{C}(i)$. By 1.2.4, we have $B_{\mathrm{HT}}^{G_K} = \mathrm{Frac}(B_{\mathrm{HT}})^{G_K} = K$.

1.9.4. For every $\mathbf{C}$-representation W of G_K, we set $D_{\mathrm{HT}}(W) = (B_{\mathrm{HT}} \otimes_{\mathbf{C}} W)^{G_K}$. By 1.6.2—1.6.3, the canonical map

$$\varrho\colon B_{\mathrm{HT}} \otimes_K D_{\mathrm{HT}}(W) \to B_{\mathrm{HT}} \otimes_{\mathbf{C}} W \tag{1.9.4.1}$$

is injective and $\dim_{\mathbf{C}}(D_{\mathrm{HT}}(W)) \leq \dim_{\mathbf{C}}(W)$. Therefore, the representation W is Hodge-Tate if and only if $\dim_{\mathbf{C}}(D_{\mathrm{HT}}(W)) = \dim_{\mathbf{C}}(W)$, that is if and only if (1.9.4.1) is an isomorphism.

1.9.5. Let $V \in \mathbf{Rep}_{Q_p}(G_K)$. Then the dimension inequality in 1.9.4 can be stated as

$$\sum_{i\in\mathbb{Z}} \dim_K(\mathbf{C}(i) \otimes_{\mathbb{Q}_p} V)^{G_K} \leq \dim_{\mathbf{C}}(\mathbf{C} \otimes_{\mathbb{Q}_p} V) = \dim_{\mathbb{Q}_p} V. \tag{1.9.5.1}$$

V is Hodge-Tate if and only if the equality holds in (1.9.5.1).

CHAPTER 2

The Hodge-Tate decomposition Theorem for Abelian Varieties

2.1. Lubin-Tate formal groups and differential modules

2.1.1. Let K be a complete discrete valuation field with perfect residue field k of characteristic $p > 0$, $\mathcal{O}_K$ the ring of integers of K. We fix a separable closure $\overline{K}$ of K and we denote by G_K the absolute Galois group of $\overline{K}$ over K. Let $\mathcal{O}_{\mathbf{C}}$ be the p-adic completion of $\mathcal{O}_{\overline{K}}$ and let $\mathbf{C}$ be its field of fractions.

Let E and K_0 be discrete valuation fields and let $E \to K_0 \to K$ an injective homomorphism such that E has finite residue field k_E, a uniformizer of E is a uniformizer of K_0, K is a finite, separable and totally ramified extension of K_0. Namely,

i) If K has characteristic 0, we take for E any finite extension of $\mathbb{Q}_p$ contained in K. If π is a uniformizer of E, then K_0 is the subfield of K obtained by adjoining π to the fraction field of the ring of Witt vectors $W(k)$.
ii) If K has characteristic p, we have $E = k_E((T)) \subseteq k((T)) = K_0 = K$.

We fix a uniformizer π of E. We denote by v the valuation of $\mathbf{C}$, extending the valuation of $\overline{K}$, normalized by $v(\pi) = 1$. Given any subfield L of $\mathbf{C}$, we denote by $\mathcal{O}_L = \{x \in L \mid v(x) \geq 0\}$ its valuation ring, by $U_L = \{x \in L \mid v(x) = 0\}$ the group of units of $\mathcal{O}_L$ and by $\mathfrak{m}_L = \{x \in L \mid v(x) > 0\}$ the maximal ideal. If I is a sub-$\mathcal{O}_L$-module of L which is free of rank 1, we denote by $v(I)$ the valuation of a generator of I.

2.1.2. Let $\Gamma \in \mathcal{O}_K[[X, Y]]$ be a formal power series in the variables X and Y and coefficients in $\mathcal{O}_K$. We say that Γ is a one-parameter commutative formal group law over $\mathcal{O}_K$ if the following identities are satisfied:

(1) $\Gamma(X, \Gamma(Y, Z)) = \Gamma(\Gamma(X, Y), Z)$ [associativity];
(2) $\Gamma(X, 0) = X$, $\Gamma(Y, 0) = Y$;
(3) $\Gamma(X, Y) = \Gamma(Y, X)$ [commutativity];

It follows immediately that there exist a unique $G(X) \in \mathcal{O}_K[[X]]$ such that $\Gamma(X, G(X)) = 0$ and that $\Gamma(X, Y) = X + Y \mod (X, Y)^2$. If Γ and Γ' are one-parameter commutative formal group laws over $\mathcal{O}_K$, a morphism from Γ to Γ' is a power series f in one variable over $\mathcal{O}_K$ with no constant term such that $f(\Gamma(X, Y)) = \Gamma'(f(X), f(Y))$.

2.1.3. Let Γ be a one-parameter commutative formal group law over $\mathcal{O}_K$ and let $x, y \in \mathfrak{m}_K$. Then the series $\Gamma(x, y)$ converges and its sum belongs to $\mathfrak{m}_K$. Under this composition law, $\mathfrak{m}_K$ is a group which we denote $\Gamma(\mathfrak{m}_K)$. We put

$$\Gamma(\mathfrak{m}_{\overline{K}}) = \varinjlim_{\substack{\overline{K} \supset L \\ L/K \text{ finite}}} \Gamma(\mathfrak{m}_L)$$

If we equip $\mathcal{O}_K[[T]]$ with the T-adic topology and we consider $\mathcal{O}_K$ with the π-adic topology, we have a canonical isomorphism

$$\mathfrak{m}_K \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont},\mathcal{O}_K}(\mathcal{O}_K[[T]], \mathcal{O}_K), \quad x \mapsto \varphi_x(T \mapsto x),$$

the identification being compatible with the group structure induced by Γ. By passage to the inductive limit from the finite case we get

$$\Gamma(\mathfrak{m}_{\overline{K}}) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont},\mathcal{O}_K}(\mathcal{O}_K[[T]], \mathcal{O}_{\overline{K}}). \tag{2.1.3.1}$$

2.1.4. We equip $\mathcal{O}_K[[T]]$ with the T-adic topology. Let $\widehat{\Omega}^1_{\mathcal{O}_K[[T]]/\mathcal{O}_K}$ be the module of continuous $\mathcal{O}_K$-differentials of $\mathcal{O}_K[[T]]$: it is a free $\mathcal{O}_K[[T]]$-module of basis $\mathrm{d}T$. Let Γ be a one-parameter commutative formal group law over $\mathcal{O}_K$. An invariant differential with respect to the formal group law Γ is a differential form

$$\omega = \alpha(T)\mathrm{d}T \in \widehat{\Omega}^1_{\mathcal{O}_K[[T]]/\mathcal{O}_K}$$

satisfying

$$\alpha(\Gamma(X,Y))\mathrm{d}\Gamma(X,Y) = \alpha(X)\mathrm{d}X + \alpha(Y)\mathrm{d}Y \tag{2.1.4.1}$$

or, equivalently,

$$\alpha(\Gamma(X,Y))\Gamma_X(X,Y) = \alpha(X) \tag{2.1.4.2}$$

where $\Gamma_X(X,Y)$ is the partial derivative of Γ with respect to the first variable. We denote by ω_Γ the sub module of $\widehat{\Omega}^1_{\mathcal{O}_K[[T]]/\mathcal{O}_K}$ of the invariant differentials. We say that $\alpha(X)\mathrm{d}T \in \omega_\Gamma$ is normalized if $\alpha(0) = 1$.

2.1.5. PROPOSITION. *We keep the assumptions of 2.1.4. There exists a unique normalized invariant differential with respect to the formal group law Γ, given by the formula*

$$\omega = \frac{\mathrm{d}T}{F_X(0,T)}.$$

ω_Γ is a free $\mathcal{O}_K$-module of rank 1, generated by ω.

PROOF. Suppose $\alpha(T)\mathrm{d}T$ is an invariant differential on Γ. Putting $X = 0$ in (2.1.4.2) gives

$$\alpha(Y)\Gamma_X(0,Y) = \alpha(0)$$

as $\Gamma(0,Y) = Y$. Since $\Gamma_X(0,T) \equiv 1 \mod (T)$, we see that $\Gamma_X(0,T)^{-1} \in \mathcal{O}_K[[T]]$. Hence $\alpha(T)$ is determined by $\alpha(0)$ and every invariant differential is of the form $a\omega$ with $a \in \mathcal{O}_K$ and

$$\omega = \Gamma_X(0,T)^{-1}\mathrm{d}T.$$

Since ω is normalized, it only remains to show that it is invariant. To prove this, we differentiate the relation

$$\Gamma(X, \Gamma(Y,Z)) = \Gamma(\Gamma(X,Y),Z)$$

with respect to X to obtain

$$\Gamma_X(X,\Gamma(Y,Z)) = \Gamma_X(\Gamma(X,Y),Z)\Gamma_X(X,Y).$$

Putting $X = 0$ gives the desired result. □

2.1.6. Let q be the cardinality of the residue field k_E and let $\mathcal{F}_\pi$ be the set of formal power series $f \in \mathcal{O}_E[[T]]$ such that $f(T) \equiv \pi T \mod (T^2)$ and $f(T) \equiv T^q \mod (\pi)$.

2.1.7. THEOREM ([**LT65**, Th. 1 and 2]). (i) *For each $f \in \mathcal{F}_\pi$ there exists a unique $F_f(X,Y) \in \mathcal{O}_E[[X,Y]]$ such that*

$$F_f(X,Y) \equiv X + Y \mod (X,Y)^2,$$
$$f(F_f(X,Y)) = F_f(f(X), f(Y)).$$

The series F_f defines a one-parameter commutative formal group law over $\mathcal{O}_E$.

(ii) *For each $a \in \mathcal{O}_E$ and $f, g \in \mathcal{F}_\pi$ there exists a unique $[a]_{f,g}(T) \in \mathcal{O}_E[[T]]$ such that*

$$[a]_{f,g}(T) \equiv aT \mod (X,Y)^2 \quad \text{and} \quad f([a]_{f,g}(T)) = [a]_{f,g}(g(T)).$$

The series $[a]_{f,g}$ is a formal homomorphism from F_g to F_f.

(ii) *The map $a \mapsto [a]_f = [a]_{f,f}$ defines an isomorphism from $\mathcal{O}_E$ to $\mathrm{End}_{\mathcal{O}_E}(F_f)$, inverse of the morphism $\sum_{i \geq 1} c_i X^i \mapsto c_1$. Under this isomorphism,*

$$[\pi]_f(T) = f(T).$$

The F_f's for $f \in \mathcal{F}_\pi$ are canonically isomorphic by means of the isomorphisms $[1]_{f,g}$. We call any one-parameter commutative formal group law over $\mathcal{O}_E$ of the form F_f, for $f \in \mathcal{F}_\pi$, a Lubin-Tate formal group over $\mathcal{O}_E$.

2.1.8. Let $f \in \mathcal{F}_\pi$ and let $\Gamma = F_f$ be the corresponding Lubin-Tate formal group. By 2.1.7, $\Gamma(\mathfrak{m}_{\overline{K}})$ is canonically equipped with an $\mathcal{O}_E$-module structure. For $a \in \mathcal{O}_E$, $x \in \mathfrak{m}_{\overline{K}}$ we write $a.x = [a]_f(x)$. For every $n \geq 0$, let

$$\Gamma_{\pi^n}(\mathfrak{m}_{\overline{K}}) = \{x \in \Gamma(\mathfrak{m}_{\overline{K}}) \mid \pi^n.x = 0\}$$

be the set of π^n-torsion points of $\Gamma(\mathfrak{m}_{\overline{K}})$. It is naturally an $\mathcal{O}_E/\pi^n\mathcal{O}_E$-module. Moreover, the maps $\Gamma_{\pi^{n+1}}(\mathfrak{m}_{\overline{K}}) \to \Gamma_{\pi^n}(\mathfrak{m}_{\overline{K}})$ given by $x \mapsto \pi.x$ are $\mathcal{O}_E$-linear and $\Gamma_{\pi^0}(\mathcal{O}_{\overline{K}}) = 0$. We call the projective limit

$$\mathrm{T}_\pi(\Gamma) = \varprojlim \Gamma_{\pi^n}(\mathfrak{m}_{\overline{K}})$$

the Tate module of Γ.

2.1.9. PROPOSITION. *Under the assumptions of 2.1.8, $\mathrm{T}_\pi(\Gamma)$ is a free $\mathcal{O}_E$-module of rank* 1.

PROOF. According to 2.1.7, we may choose $f(X) = \pi X + X^q$. Firstly, we prove that $\Gamma(\mathfrak{m}_{\overline{K}})$ is π-divisible. With this choice of f, the map

$$\Gamma(\mathfrak{m}_{\overline{K}}) \xrightarrow{\pi} \Gamma(\mathfrak{m}_{\overline{K}})$$

is given by $x \mapsto \pi x + x^q$. For every $\alpha \in \mathfrak{m}_{\overline{K}}$, the polynomial $f(X) - \alpha$ is separable and so solvable in $\overline{K}$. All its solutions belong clearly to $\mathfrak{m}_{\overline{K}}$. To prove that $\mathrm{T}_\pi(\Gamma)$ is a free $\mathcal{O}_E$-module of rank 1, it's enough to show that, for every $n \geq 1$, $\Gamma_{\pi^n}(\mathfrak{m}_{\overline{K}})$ is isomorphic to $\mathcal{O}_E/(\pi^n)$ as $\mathcal{O}_E$-module. We proceed by induction on n. For $n = 1$, $\Gamma_\pi(\mathfrak{m}_{\overline{K}})$ is the set of solutions of the equation $f(X) = 0$: it has therefore q elements and it is isomorphic to $\mathcal{O}_E/(\pi)$. Consider the sequence

$$0 \to \Gamma_\pi(\mathfrak{m}_{\overline{K}}) \to \Gamma_{\pi^n}(\mathfrak{m}_{\overline{K}}) \xrightarrow{\pi} \Gamma_{\pi^{n-1}}(\mathfrak{m}_{\overline{K}}) \to 0. \tag{2.1.9.1}$$

Since $\Gamma(\mathfrak{m}_{\overline{K}})$ is π-divisible, (2.1.9.1) is exact. By induction hypothesis, $\Gamma_{\pi^{n-1}}(\mathfrak{m}_{\overline{K}}) \cong \mathcal{O}_E/(\pi^{n-1})$, and the sequence (2.1.9.1) cannot split, since $\Gamma_{\pi^n}(\mathfrak{m}_{\overline{K}})$ contains an element of order exactly π^n: it is enough to divide a generator of $\Gamma_{\pi^{n-1}}(\mathfrak{m}_{\overline{K}})$ by π. $\square$

2.1.10. Let Γ be a Lubin-Tate formal group law over $\mathcal{O}_E$. Let $u \in \Gamma(\mathfrak{m}_{\overline{K}})$: according to 2.1.3.1, u corresponds to $\varphi_u \in \mathrm{Hom}_{\mathrm{cont},\mathcal{O}_E}(\mathcal{O}_E[[T]], \mathcal{O}_{\overline{K}})$. Let

$$\omega = \alpha(T)\mathrm{d}T \in \widehat{\Omega}^1_{\mathcal{O}_E[[T]]/\mathcal{O}_E}$$

be a continuous differential form. We denote by $u^*(\omega)$ the pull-back $\varphi_u(\alpha(T))\mathrm{d}\varphi_u(T)$: it is a well defined element in $\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$. Indeed, by construction, the $\mathcal{O}_E$-linear and continuous morphism φ_u factors through a finite extension L/K

$$\varphi_u \colon \mathcal{O}_E[[T]] \to \mathcal{O}_L$$

where $u = \varphi_u(T) \in \mathfrak{m}_L \subset \mathfrak{m}_{\overline{K}}$. Since L is complete, $\varphi_u(\alpha(T)) = \alpha(u)$ converges in $\mathcal{O}_L$ and we can consider $\alpha(u)\mathrm{d}u$ as an element in $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$. We denote by $u^*(\omega)$ its image by the canonical map

$$\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \to \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}.$$

Restricting to the sub-module of invariant differentials, we have a map:

$$\langle\ ,\ \rangle \colon \Gamma(\mathfrak{m}_{\overline{K}}) \times \omega_\Gamma \to \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K} \quad (u,\omega) \mapsto \langle u,\omega\rangle = u^*(\omega).$$

2.1.11. Proposition. *The pairing $\langle\ ,\rangle$ is $\mathcal{O}_E$-bilinear and it is compatible with the action of G_K, i.e. for any $g \in G_K$, $u \in \Gamma(\mathfrak{m}_{\overline{K}})$, $\omega \in \omega_\Gamma$ we have $\langle g(u),\omega\rangle = g(\langle u,\omega\rangle)$.*

Proof. Indeed, for $u, u' \in \Gamma(\mathfrak{m}_{\overline{K}})$ and $\omega \in \omega_\Gamma$, $\langle u+u',\omega\rangle = \langle u,\omega\rangle + \langle u',\omega\rangle$ by (2.1.4.1). The fact that $\langle au,\omega\rangle = a\langle u,\omega\rangle$ for any $a \in \mathcal{O}_E$, $\omega \in \omega_\Gamma$, $u \in \Gamma(\mathfrak{m}_{\overline{K}})$ follows from the identification of $\mathcal{O}_E$ with $\mathrm{End}_{\mathcal{O}_E}(\Gamma)$ in 2.1.7. The linearity in the second variable and the compatibility with the action of G_K are clear. $\square$

2.1.12. Let Γ be a Lubin-Tate formal group over $\mathcal{O}_E$. Let G_K act trivially on ω_Γ and consider the $\overline{K}$-vector space

$$\overline{K} \otimes_{\mathcal{O}_E} \mathrm{T}_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma.$$

By 2.1.9 and 2.1.5, it is a $\overline{K}$-vector space of dimension 1, endowed with a semilinear continuous action of G_K.

Let $\alpha \in \overline{K} \otimes_{\mathcal{O}_E} \mathrm{T}_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma$. Then α can be written (in a non-unique way) as

$$\alpha = \frac{a}{\pi^r} \otimes u \otimes \omega$$

with $u = (u_n)_{n\in\mathbb{N}} \in \mathrm{T}_\pi(\Gamma)$, $a \in \mathcal{O}_{\overline{K}}$, $r \in \mathbb{N}$ and $\omega \in \omega_\Gamma$. It follows immediately from 2.1.11 and from the definition of $\mathrm{T}_\pi(\Gamma)$ that the element $au_r^*(\omega)$ depends only on α, so that the map

(2.1.12.1)
$$\xi_{K,\Gamma} = \xi \colon \overline{K} \otimes_{\mathcal{O}_E} \mathrm{T}_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma \to \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$$
$$\alpha = \frac{a}{\pi^r} \otimes u \otimes \omega \mapsto au_r^*(\omega)$$

is well defined, $\mathcal{O}_{\overline{K}}$-linear and compatible with the action of G_K.

Let $\mathcal{D}_{K/K_0}$ be the different of the extension K/K_0 and let $\mathfrak{a}_{K,\Gamma}$ be the $\mathcal{O}_{\overline{K}}$-module

$$\mathfrak{a}_{K,\Gamma} = \Big\{a \in \overline{K} \mid v(a) \geq -v(\mathcal{D}_{K/K_0}) - \frac{1}{q-1}\Big\}.$$

2.1.13. THEOREM ([**Fon82**, Thm. 1]). *Under the assumptions of 2.1.12, the map ξ is surjective and*

$$\mathrm{Ker}(\xi) = \mathfrak{a}_{K,\Gamma} \otimes_{\mathcal{O}_E} T_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma.$$

2.2. The proof of Theorem 2.1.13

2.2.1. Let K be as in 2.1. For any field extension L/K, we denote by $\mathcal{D}_{L/K}$ the different of L/K and by $\mathrm{d}_{L/K}\colon \mathcal{O}_L \to \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ the universal derivation.

2.2.2. LEMMA. *Let $K \subseteq M \subseteq L$ be a tower of finite and separable field extensions, u the canonical map $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \xrightarrow{u} \Omega^1_{\mathcal{O}_L/\mathcal{O}_M}$. Then, for any $\omega \in \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$, we have:*

$$v(\mathrm{Ann}(u(\omega))) = \max\{0, v(\mathrm{Ann}(\omega)) - v(\mathcal{D}_{M/K})\}.$$

PROOF. Let b be a generator of $\mathcal{O}_L$ as an $\mathcal{O}_K$-algebra and let $\omega = a\mathrm{d}_{L/K}b \in \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ be a non-zero differential form. Since $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ is generated by $\mathrm{d}_{L/K}b$ and is killed by $\mathcal{D}_{L/K}$, we have $v(\mathrm{Ann}(\omega)) = v(\mathcal{D}_{L/K}) - v(a)$. By definition $u(\omega) = a\mathrm{d}_{L/M}b$, hence

$$v(\mathrm{Ann}(u(\omega))) = \max\{0, v(\mathcal{D}_{L/M}) - v(a)\}.$$

By [**Ser62**, chap. III, Prop. 8], we have

$$v(\mathcal{D}_{L/M}) = v(\mathcal{D}_{L/K}) - v(\mathcal{D}_{M/K})$$

and we can conclude. □

2.2.3. LEMMA. *Let $K \subseteq M \subseteq L$ be a tower of finite and separable field extensions. Let $\iota\colon \Omega^1_{\mathcal{O}_M/\mathcal{O}_K} \to \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ be the map induced by the inclusion $\mathcal{O}_M \subset \mathcal{O}_L$. Then, for every $\omega \in \Omega^1_{\mathcal{O}_M/\mathcal{O}_K}$, we have*

$$\mathrm{Ann}_{\mathcal{O}_L}(\iota(\omega)) = \mathcal{O}_L\,\mathrm{Ann}_{\mathcal{O}_M}(\omega).$$

PROOF. It is enough to consider the case where L/M is unramified or totally ramified. If $\mathcal{O}_L/\mathcal{O}_M$ is étale, then $\Omega^1_{\mathcal{O}_M/\mathcal{O}_K} \otimes_{\mathcal{O}_M} \mathcal{O}_L \cong \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ by [**EGA IV**, 0.20.5.8] and the statement is clear.

Suppose now that L/M is totally ramified. Let b' be a uniformizer for L: it is a root of an Eistenstein polynomial $P(X) = \sum_{i=0}^n a_i X^i \in \mathcal{O}_M[X]$, with $-a_0 = b$ a uniformizer for M. Let $\omega = a\mathrm{d}_{M/K}b \in \Omega^1_{\mathcal{O}_M/\mathcal{O}_K}$ be a non-zero differential and let $\mathfrak{a}$ be its annihilator. Let $\iota(\omega) = a\mathrm{d}_{L/K}b \in \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ be the image of ω. As $b = \sum_{i=1}^n a_i (b')^i$, we have

$$\mathrm{d}_{L/K}b = (a_1 + 2a_2 b' + \ldots + n(b')^{n-1})\mathrm{d}_{L/K}b' = P'(b')\mathrm{d}_{L/K}b',$$

so that $\iota(\omega) = aP'(b')\mathrm{d}_{L/K}b'$. Hence $c \in \mathrm{Ann}_{\mathcal{O}_L}(\iota(\omega))$ if and only if

$$v(caP'(b')) \geq v(\mathcal{D}_{L/K}). \tag{2.2.3.1}$$

Since $\mathcal{D}_{L/M} = (P'(b'))$ by [**Ser62**, chap. III, Cor. 2 to Prop. 11] and since $\mathcal{D}_{L/K} = \mathcal{D}_{L/M}\mathcal{D}_{M/K}$ by [**Ser62**, chap. III, Prop. 8], (2.2.3.1) is equivalent to $v(c) \geq v(\mathcal{D}_{M/K}) - v(a) = v(\mathfrak{a})$, i.e.

$$\mathrm{Ann}_{\mathcal{O}_L}(\iota(\omega)) = \mathcal{O}_L\mathfrak{a}.$$

□

2.2.4. The modules $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ for $K \subseteq L$ varying in the set of finite and separable extensions of K contained in $\overline{K}$ form an inductive system and we have

$$\varinjlim \Omega^1_{\mathcal{O}_L/\mathcal{O}_K} = \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K},$$

that makes clear the fact that $\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$ is a torsion $\mathcal{O}_{\overline{K}}$-module. By 2.2.3, the canonical map $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \to \varinjlim \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$ is injective.

Let $\omega \in \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$, L a finite and separable extension of K such that $\omega \in \Omega^1_{\mathcal{O}_L/\mathcal{O}_K} \subset \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$, $\mathfrak{a}$ the annihilator $\mathrm{Ann}_{\mathcal{O}_L}(\omega) \subset \mathcal{O}_L$. Then the annihilator $\mathrm{Ann}(\omega)$ of ω in $\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$ is simply given by $\mathcal{O}_{\overline{K}}\mathfrak{a}$: in particular $\mathrm{Ann}(\omega)$ is a principal ideal of $\mathcal{O}_{\overline{K}}$ and its valuation is the valuation of $\mathfrak{a}$.

2.2.5. Lemma. *Let $\omega, \omega' \in \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$. Then we have $\mathrm{Ann}(\omega) \subseteq \mathrm{Ann}(\omega')$ if and only if there exists $c \in \mathcal{O}_{\overline{K}}$ such that $\omega' = c\omega$.*

Proof. It is clear that $\omega' = c\omega$ for some $c \in \mathcal{O}_{\overline{K}}$ implies the inclusion between the annihilators.

Assume $\mathrm{Ann}(\omega) \subseteq \mathrm{Ann}(\omega')$. The case $\omega' = 0$ is trivial, so we can assume ω' and ω both non-zero: indeed $\omega' \neq 0$ implies $\mathrm{Ann}(\omega')$ — and a fortiori $\mathrm{Ann}(\omega)$ — different from $\mathcal{O}_{\overline{K}}$, so that also ω is non-zero. Let L be a finite and separable extension such that $\omega, \omega' \in \Omega^1_{\mathcal{O}_L/\mathcal{O}_K}$. If b is a uniformizer of L, we can write $\omega = a\mathrm{d}b$ and $\omega' = a'\mathrm{d}b$, with $a, a' \in \mathcal{O}_L$.

As ω' and ω are both non-zero, we have $v(a) < v(\mathcal{D}_{L/K})$ and $v(a') < v(\mathcal{D}_{L/K})$, while $v(\mathrm{Ann}(\omega)) = v(\mathcal{D}_{L/K}) - v(a)$ and $v(\mathrm{Ann}(\omega')) = v(\mathcal{D}_{L/K}) - v(a')$. The assumption $\mathrm{Ann}(\omega) \subseteq \mathrm{Ann}(\omega')$ implies

$$v(\mathcal{D}_{L/K}) - v(a) \geq v(\mathcal{D}_{L/K}) - v(a') \quad \text{hence} \quad v(a') \geq v(a)$$

so that $a' \in a\mathcal{O}_L$, i.e. there exists a $c \in \mathcal{O}_{\overline{K}}$ such that $\omega' = c\omega$. □

2.2.6. We consider again the notations of 2.1.12: Γ is a Lubin-Tate formal group over $\mathcal{O}_E$ and $\mathrm{T}_\pi(\Gamma)$ is its Tate module. We fix a generator $(\pi_r)_{r\in\mathbb{N}}$ of $\mathrm{T}_\pi(\Gamma)$ over $\mathcal{O}_E$: for every $r \geq 1$, π_r is a generator of the rank one $\mathcal{O}_E/\pi^r$-module $\Gamma_{\pi^r}(\mathfrak{m}_{\overline{K}})$.

Let E_r be the field $E[\pi_r]$. From [**LT65**, Theorem 2] and [**CF67**, VI, §3], we know that the field extensions $E_r = E[\Gamma_{\pi^r}(\mathfrak{m}_{\overline{K}})]$ of E depend only on the uniformizer π of E and are totally ramified, finite, abelian Galois extensions of E. Moreover, π_r is a uniformizer of E_r.

2.2.7. Proposition. *For every $r \geq 1$ we have $v(\mathcal{D}_{E_r/E}) = r - \frac{1}{q-1}$.*

Proof. By [**CF67**, p. 152], we have:

i) the Galois group $\mathrm{Gal}(E_r/E)$ is canonically isomorphic to the quotient

$$U_E/U_E^{(r)} = U_E/(1 + \pi^r\mathcal{O}_E);$$

ii) $e_{E_r/E} = [E_r : E] = q^{r-1}(q-1)$;

Under the isomorphism $U_E/U_E^{(r)} \xrightarrow{\sim} G = \mathrm{Gal}(E_r/E)$, the subgroup $U_E^{(i)}/U_E^{(r)}$ maps onto the ramification group G_{q^i-1}. Hence, from the filtration

$$U_E/U_E^{(r)} \supset U_E^{(1)}/U_E^{(r)} \supset \cdots U_E^{(r)}/U_E^{(r)} = 1,$$

we get that a complete set of ramification groups for the extension E_r/E is given by

$$\begin{aligned} G &= G_0; \\ G_1 = \ldots = G_{q-2} &= G_{q-1}; \\ G_q = \ldots &= G_{q^2-1}; \\ &\ldots \\ 1 &= G_{q^r-1}. \end{aligned}$$

The corresponding upper numbering is $G^i = G_{q^i-1}$ and

$$[G^0 : G^1] = q-1 \quad [G^i : G^{i+1}] = q.$$

By [**Ser62**, chap. IV, Prop. 4], we have

$$v_{E_r}(\mathcal{D}_{E_r/E}) = \sum_{s \neq 1} i_G(s)$$

where $i_G(s) = v_{E_r}(s(\pi_r) - \pi_r)$ for $s \in G$. Moreover:

$$v_{E_r}(\mathcal{D}_{E_r/E}) = \sum_{i=0}^{r-1} \sum_{s \in G^i \setminus G^{i+1}} i_G(s)$$

and the function $i_G(s)$ is constant for $s \in G^i \setminus G^{i+1}$ and equal to q^i for every i. For $i \geq 1$ we have that $\#G^i = q^{r-i}$ and that $\#G^i \setminus G^{i+1} = (q-1)q^{r-i-1}$, where $\#S$ denotes the cardinality of the (finite) set S. Hence:

$$\sum_{i=0}^{r-1} \sum_{s \in G^i \setminus G^{i+1}} i_G(s) = (q-2)q^{r-1} + \sum_{i=1}^{r-1} q^i (q-1) q^{r-i-1} = q^{r-1}(r(q-1)-1).$$

As $v(\mathcal{D}_{E_r/E}) = \frac{1}{e_{E_r/E}} v_{E_r}(\mathcal{D}_{E_r/E})$, we deduce that

$$v(\mathcal{D}_{E_r/E}) = \frac{1}{q^{r-1}(q-1)} q^{r-1}(r(q-1)-1) = r - \frac{1}{q-1}.$$

□

2.2.8. Corollary. *Let ω_0 be a generator of the module of invariant differentials ω_Γ. Then for any non-negative integer r we have:*

(2.2.8.1) $$v(\mathrm{Ann}(\pi_r^*(\omega_0))) = \max\left\{0, r - \frac{1}{q-1} - v(\mathcal{D}_{K/K_0})\right\}$$

Proof. The statement is evident for $r = 0$ (since $u_0 = 0$), so we can assume $r \geq 1$. By passing to the limit in 2.2.2, we have

$$v(\mathrm{Ann}(\nu(\omega))) = \max\{0, v(\mathrm{Ann}(\omega)) - v(\mathcal{D}_{K/K_0})\}$$

where ν is the canonical map $\nu \colon \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_{K_0}} \to \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$. We can therefore assume that $K = K_0$.

Let P_r be the minimal polynomial of π_r over E: it is an Eisenstein polynomial. Since the uniformizer π of E is a uniformizer of K, then $K_r = K[\pi_r] = K \otimes_E E_r$ is a field extension of K, totally ramified, with π_r as uniformizer.

Since $\mathcal{O}_{K_r} = \mathcal{O}_K[\pi_r]$, $\mathrm{d}\pi_r$ generates $\Omega^1_{\mathcal{O}_{K_r}/\mathcal{O}_K}$ and we have:

$$v(\mathrm{Ann}(\mathrm{d}\pi_r)) = v(P_r'(\pi_r)) = v(\mathcal{D}_{E_r/E}).$$

By 2.1.5, we know that ω_0 is of the form $\alpha(T)\mathrm{d}T$ with $\alpha(T)$ invertible in $\mathcal{O}_E[[T]]$. Hence, for every $r \geq 1$,

$$\pi_r^*(\omega_0) = \alpha(\pi_r)\mathrm{d}\pi_r$$

with $\alpha(\pi_r)$ unit. Therefore $v(\mathrm{Ann}(\pi_r^*(\omega_0))) = v(\mathcal{D}_{E_r/E})$ and the statement follows from 2.2.7. □

Proof of Theorem 2.1.13. We first prove the surjectivity of the map ξ. Let ω_0 be a generator of ω_Γ and let $u = (\pi_n)_{n\in\mathbb{N}}$ be a generator of $\mathrm{T}_\pi(\Gamma)$. Let $\omega \in \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$ and let r be an integer such that

$$v(\mathrm{Ann}(\omega)) \leq r - \frac{1}{q-1} - v(\mathcal{D}_{K/K_0}) \leq v(\mathrm{Ann}(\pi_r^*(\omega_0)))$$

by 2.2.8. Hence $\mathrm{Ann}(\omega) \supseteq \mathrm{Ann}(\pi_r^*(\omega_0))$, so that there exists $c \in \mathcal{O}_{\overline{K}}$ such that $\omega = c.\pi_r^*(\omega_0)$ (by 2.2.5) and

$$\omega = \xi\Big(\frac{c}{\pi^r} \otimes u \otimes \omega_0\Big),$$

proving the surjectivity of ξ.

We now determine the kernel: any element $\alpha \in \overline{K} \otimes \mathrm{T}_\pi(\Gamma) \otimes \omega_\Gamma$ can be written in a unique way as $a \otimes u \otimes \omega_0$, with $a \in \overline{K}$. Let $r \in \mathbb{N}$ such that $r \geq \frac{1}{q-1} + v(\mathcal{D}_{K/K_0})$ and such that $\pi^r a \in \mathcal{O}_{\overline{K}}$. The element α is in $\mathrm{Ker}(\xi)$ if and only if $v(\mathrm{Ann}(\xi(\alpha))) \leq 0$ (the annihilator taken in $\overline{K}$). Hence

$$v(\pi^r a) \geq r - \frac{1}{q-1} - v(\mathcal{D}_{K/K_0}),$$

so that $\alpha \in \mathrm{Ker}\,\xi$ if and only if $\alpha \in \mathfrak{a} \otimes \mathrm{T}_\pi(\Gamma) \otimes \omega_\Gamma$. □

2.3. Consequences and corollaries

2.3.1. We keep the assumptions of 2.1.12. Let $\mathrm{T}_\pi(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_E})$ be the π-Tate module of the $\mathcal{O}_E$-module $\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$, i.e.

$$\mathrm{T}_\pi(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_E}) = \mathrm{Hom}_{\mathcal{O}_E}(E/\mathcal{O}_E, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$$

and let $V_\pi(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$ be the E-vector space

$$V_\pi(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) = \mathrm{Hom}_{\mathcal{O}_E}(E, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}).$$

2.3.2. Corollary. *Let $\widehat{\mathfrak{a}}$ be the π-adic completion of $\mathfrak{a}$. We have the following canonical isomorphisms of $\mathcal{O}_{\overline{K}}$-modules (resp. $\mathcal{O}_{\mathbf{C}}$-modules, $\mathbf{C}$-vector spaces)*

$$\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K} \cong (\overline{K}/\mathfrak{a}) \otimes_{\mathcal{O}_E} \mathrm{T}_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma, \tag{2.3.2.1}$$

$$\mathrm{T}_\pi(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_E}) \cong \widehat{\mathfrak{a}} \otimes_{\mathcal{O}_E} \mathrm{T}_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma, \tag{2.3.2.2}$$

$$V_\pi(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) \cong \mathbf{C} \otimes_{\mathcal{O}_E} \mathrm{T}_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma \tag{2.3.2.3}$$

that commute with the action of G_K.

Proof. Isomorphism (2.3.2.1) simply follows from 2.1.13. As $E/\mathcal{O}_E = \varinjlim(\frac{1}{\pi^n}\mathcal{O}_E)/\mathcal{O}_E$ we have:

$$\mathrm{T}_\pi(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_E}) = \varprojlim \mathrm{Hom}_{\mathcal{O}_E}\Big(\frac{1}{\pi^n}\mathcal{O}_E/\mathcal{O}_E, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}\Big).$$

Moreover

$$\mathrm{Hom}_{\mathcal{O}_E}\Big(\frac{1}{\pi^n}\mathcal{O}_E/\mathcal{O}_E, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}\Big) \cong \Big(\frac{1}{\pi^n}\mathfrak{a}/\mathfrak{a}\Big) \otimes_{\mathcal{O}_E} \mathrm{T}_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma$$

using (2.3.2.1) together with the fact that $\mathrm{T}_\pi(\Gamma)$ and ω_Γ are free rank one $\mathcal{O}_E$-modules (hence torsion-free) and that the morphisms are $\mathcal{O}_E$-linear. Therefore

$$\mathrm{T}_\pi(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_E}) = \varprojlim \Big(\frac{1}{\pi^n}\mathfrak{a}/\mathfrak{a}\Big) \otimes_{\mathcal{O}_E} \mathrm{T}_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma = \widehat{\mathfrak{a}} \otimes_{\mathcal{O}_E} \mathrm{T}_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma.$$

Finally, for (2.3.2.3) we write $E = \varinjlim \frac{1}{\pi^n}\mathcal{O}_E$. As above we have:

$$V_\pi(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_E}) = \mathrm{Hom}_{\mathcal{O}_E}(E, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) = \varprojlim \mathrm{Hom}_{\mathcal{O}_E}\Big(\frac{1}{\pi^n}\mathcal{O}_E, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}\Big).$$

To get the isomorphism with $\mathbf{C} \otimes_{\mathcal{O}_E} \mathrm{T}_\pi(\Gamma) \otimes_{\mathcal{O}_E} \omega_\Gamma$, we use again (2.3.2.1). The morphisms ξ of Theorem 2.1.13 is compatible with the action of G_K, so isomorphisms (2.3.2.1), (2.3.2.2) and (2.3.2.3) commute clearly with the action of G_K. □

2.3.3. Assume that K is of characteristic 0, that $E = \mathbb{Q}_p$ and $\pi = p$, so that $q = p$ and $K_0 = \mathrm{Frac}(W(k))$. For this special case (see [**LT65**, §1, p. 380]), the Lubin-Tate formal group Γ over $\mathbb{Q}_p$ is the formal multiplicative group $\widehat{\mathbb{G}}_m$, i.e. the completion along the unit section of the multiplicative group $\mathbb{G}_m$ over $\mathbb{Z}_p$. For $f(T) = (1+T)^p - 1 \in \mathbb{Z}_p[[T]]$, the group law $\Gamma = \Gamma_f(X, Y)$ is the power series $X + Y + XY$. By 2.1.5, we have a canonical generator of ω_Γ, namely the unique normalized invariant differential form $\omega_0 = \frac{\mathrm{d}T}{1+T}$.

We can identify the Tate module $\mathrm{T}_p(\Gamma)$ with the points in $\overline{K}$ of the Tate module of the multiplicative group $\mathbb{G}_m$. More precisely we have, for any $n \in \mathbb{N}$,

$$1 \to \mu_{p^n}(\overline{K}) \to \overline{K}^* \xrightarrow{\cdot p^n} \overline{K}^* \to 1$$

and $\mathrm{T}_p(\mathbb{G}_m)$ is the projective limit $\varprojlim \mu_{p^n}(\overline{K})$, where the transition maps are given by raising to the p-th power. As the map

$$a \mapsto 1 + a \colon \mathfrak{m}_{\overline{K}} \to 1 + \mathfrak{m}_{\overline{K}} \qquad (2.3.3.1)$$

is an isomorphism between the group $\Gamma(\mathfrak{m}_{\overline{K}})$ and $U^{(1)}_{\overline{K}}$ (with standard multiplication), the points of p^n-torsion with respect to the formal group law correspond to the point of p^n-torsion with respect to the standard multiplication in $\overline{K}$. Therefore

$$\mathrm{T}_p(\Gamma) = \mathrm{T}_p(\mathbb{G}_m) = \varprojlim \mu_{p^n}(\overline{K})$$

is the free $\mathbb{Z}_p$-module of rank 1 formed by the sequences $(\varepsilon_n)_{n\in\mathbb{N}}$ of elements of $\mathcal{O}_{\overline{K}}$ such that $\varepsilon_0 = 1$ and $\varepsilon_{n+1}^p = \varepsilon_n$.

Notice that, by definition, the character $\chi\colon G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(\mathrm{T}_p(\Gamma)) \cong \mathbb{Z}_p^\times$ giving the action of G_K on the Tate module of Γ is nothing else but the cyclotomic character χ_p, giving the action of G_K on the group of units of order (a power of) p.

2.3.4. For any $\mathbb{Z}_p$-module M endowed with a linear action of G_K and any $i \in \mathbb{Z}$, we write $M(i)$ for the tensor product

$$M \otimes_{\mathbb{Z}_p} \mathrm{T}_p(\mathbb{G}_m)^{\otimes^i}$$

with the convention $\mathrm{T}_p(\mathbb{G}_m)^{\otimes^0} = \mathbb{Z}_p$ and, for $i > 0$, $\mathrm{T}_p(\mathbb{G}_m)^{\otimes^{-i}}$ is the dual of $\mathrm{T}_p(\mathbb{G}_m)^{\otimes^i}$.

In this setting, we can reformulate Theorem 2.1.13 in the following way:

2.3.5. THEOREM. *The map* $\xi\colon \overline{K}(1) \to \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$ *defined by*

$$p^{-r}a \otimes (\varepsilon_n)_{n\in\mathbb{N}} \mapsto a.\frac{\mathrm{d}\varepsilon_r}{\varepsilon_r}$$

for $a \in \mathcal{O}_{\overline{K}}$, $r \in \mathbb{N}$ *is surjective with kernel* $\mathfrak{a}(1)$ *and induces canonical isomorphisms:*

(2.3.5.1) $$\Omega^1_{\mathcal{O}_{\overline{K}}/K} \cong (\overline{K}/\mathfrak{a})(1),$$

(2.3.5.2) $$\mathrm{T}_p(\Omega^1_{\mathcal{O}_{\overline{K}}/K}) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) \cong \widehat{\mathfrak{a}}(1),$$

(2.3.5.3) $$V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/K}) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) \cong \mathbf{C}(1).$$

2.4. Applications to Abelian Varieties

2.4.1. Let K be a complete discrete valuation field of characteristic 0 with perfect residue field k of characteristic $p > 0$, $\mathcal{O}_K$ the valuation ring of K, $S = \mathrm{Spec}(\mathcal{O}_K)$. We note by η the generic point of S and by $\overline{\eta}$ a geometric point corresponding to an algebraic closure $\overline{K}$ of K. We denote by G_K the absolute Galois group of $\overline{K}$ over K. $f\colon X \to \mathrm{Spec}(K)$ be a morphism of schemes. We call proper $\mathcal{O}_K$-model of X any scheme $\mathfrak{X}$ proper over S such that $\mathfrak{X}_\eta = X$.

2.4.2. PROPOSITION ([**EGA IV**, 2.8.5]). *Let* $f\colon X \to S$ *be a morphism of schemes and let* $X_\eta = f^{-1}(\eta)$ *be the generic fibre of* X. *Let* $\iota\colon X_\eta \to X$ *be the canonical morphism. Let* Z *be a closed subscheme of* X_η. *Then there exists a unique closed subscheme* $\mathfrak{Z}$ *of* X, *flat over* S *and such that* $\iota^{-1}(\mathfrak{Z}) = Z$.

The scheme $\mathfrak{Z}$ is the schematic closure of Z by the composite morphism $Z \to X_\eta \xrightarrow{\iota} X$, where the first arrow is the canonical injection; its underlying space is the closure in X of Z.

2.4.3. From now on, let X be an abelian variety over K and let $\varphi\colon X \to \mathbb{P}^n_K$ be a closed immersion. Let $\iota\colon \mathbb{P}^n_K \to \mathbb{P}^n_{\mathcal{O}_K}$ be the canonical morphism. By 2.4.2, there exists a unique scheme $\mathfrak{X}$, flat and proper over S, such that $i^{-1}(\mathfrak{X}) = X$.

2.4.4. Let $u\colon \mathrm{Spec}(\mathcal{O}_{\overline{K}}) \to \mathfrak{X}$ and let $\omega \in \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_{\overline{K}}})$. We denote by $u^*(\omega) \in \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$ the image of $u^*\omega$ by the canonical $\mathcal{O}_K$-linear map

$$u^*\Omega^1_{\mathfrak{X}/\mathcal{O}_K} \xrightarrow{v} \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}.$$

In this way we obtain a pairing:

(2.4.4.1) $$\mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \times \mathfrak{X}(\mathcal{O}_{\overline{K}}) \to \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$$

by

$$(\omega, u) \mapsto \langle \omega, u\rangle = u^*(\omega).$$

The map (2.4.4.1) is clearly $\mathcal{O}_K$-linear in the first variable and it is compatible with the action of G_K. More precisely, for any $g \in G_K$, $\omega \in \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K})$, $u \in \mathfrak{X}(\mathcal{O}_{\overline{K}})$ we have

$$\langle \omega, g.u\rangle = g(\langle \omega, u\rangle) = g(u^*(\omega)).$$

2.4.5. By construction, we have the fibre product diagram:

$$\begin{array}{ccc} X & \xrightarrow{q_1} & \mathfrak{X} \\ {\scriptstyle q_2}\downarrow & & \downarrow \\ \eta & \longrightarrow & S \end{array}$$

that allow us to identify $\mathrm{H}^0(X, \Omega^1_{X/K})$ with $K \otimes_{\mathcal{O}_K} \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K})$. Indeed, let $(U_i)_{i \in I}$ be an affine open covering of $\mathfrak{X}$ and consider the canonical exact sequence:

$$0 \to \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to \prod_i \mathrm{H}^0(U_i, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to \prod_{i,j} \mathrm{H}^0(U_{i,j}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \tag{2.4.5.1}$$

where $U_{ij} = U_i \cap U_j$. Since K is flat over $\mathcal{O}_K$, the latter induces an exact sequence

$$0 \to \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \otimes_{\mathcal{O}_K} K \to \prod_i \mathrm{H}^0(U_i, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \otimes_{\mathcal{O}_K} K \to \prod_{i,j} \mathrm{H}^0(U_{i,j}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \otimes_{\mathcal{O}_K} K \tag{2.4.5.2}$$

On the other hand, $(U_i \cap X = U_i \otimes_{\mathcal{O}_K} K)_{i \in I}$ is an affine open covering of X and we have, for every $i \in I$,

$$\mathrm{H}^0(U_i, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \otimes_{\mathcal{O}_K} K = \mathrm{H}^0(U_i \otimes_{\mathcal{O}_K} K, \Omega^1_{X/K}).$$

Hence (2.4.5.2) implies that

$$\mathrm{H}^0(X, \Omega^1_{X/K}) = K \otimes_{\mathcal{O}_K} \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}).$$

2.4.6. By the Valuative Criterion of Properness [**EGA II**, 7.3.8] we have a canonical identification of $X(\overline{K})$ with $\mathfrak{X}(\mathcal{O}_{\overline{K}})$: in this way $\mathfrak{X}(\mathcal{O}_{\overline{K}})$ inherits a structure of abelian group, even though $\mathfrak{X}$ is not a group scheme over S.

2.4.7. PROPOSITION. *Under the assumptions of 2.4.4, there exists a non negative integer r_0 such that for every $\omega \in p^{r_0}\mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K})$ and every $u_1, u_2 \in \mathfrak{X}(\mathcal{O}_{\overline{K}}) = X(\overline{K})$ we have:*

$$\langle \omega, u_1 + u_2 \rangle = \langle \omega, u_1 \rangle + \langle \omega, u_2 \rangle$$

PROOF. Let $\mathfrak{Y}$ be an $\mathcal{O}_K$-model of $X \times X$ over K such that the canonical projections $p_1, p_2 \colon X \times_\eta X \rightrightarrows X$ and the group multiplication $m \colon X \times_\eta X \to X$ extend to maps from $\mathfrak{Y}$ to $\mathfrak{X}$. We can construct $\mathfrak{Y}$ as follows: if $\psi \colon X \times_\eta X \to \mathbb{P}^m_K$ is a projective embedding of the product $X \times_\eta X$, we can consider the composite map

$$X \times_\eta X \xrightarrow{id \times m} X \times_\eta X \times_\eta X \to \mathfrak{X} \times_S \mathfrak{X} \times_S \mathfrak{X}.$$

Let $\mathfrak{Y}$ be schematic closure of the composite morphism, so that we have the diagram

$$\begin{array}{ccccccc} X \times_\eta X & \longrightarrow & X \times_\eta X \times_\eta X & \longrightarrow & \mathbb{P}^m_K & \longrightarrow & \eta \\ {\scriptstyle\sigma}\downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathfrak{Y} & \longrightarrow & \mathfrak{X} \times_S \mathfrak{X} \times_S \mathfrak{X} & \longrightarrow & \mathbb{P}^m_{\mathcal{O}_K} & \longrightarrow & S \end{array} \tag{2.4.7.1}$$

We get the required extensions

$$p_{1,\mathfrak{X}}, p_{2,\mathfrak{X}}, m_{\mathfrak{X}} \colon \mathfrak{Y} \to \mathfrak{X}$$

by mean of the other projections.

We know ([**BLR90**, §4.2, Prop.1]) that the everywhere regular differential forms on X are precisely the invariant forms, so that for any $\omega \in \mathrm{H}^0(X, \Omega^1_{X/K})$ we have:

$$m^*\omega - p_1^*\omega - p_2^*\omega = 0$$

in $\mathrm{H}^0(X, \Omega^1_{X\times X/K})$. Let $\omega \in \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K})$ and consider the form $\omega' \in \mathrm{H}^0(\mathfrak{Y}, \Omega^1_{\mathfrak{Y}/\mathcal{O}_K})$ defined by

$$\omega' = m_{\mathfrak{X}}^*\omega - p_{1,\mathfrak{X}}^*\omega - p_{2,\mathfrak{X}}^*\omega.$$

The natural map

$$\mathrm{H}^0(\mathfrak{Y}, \Omega^1_{\mathfrak{Y}/\mathcal{O}_K}) \to \mathrm{H}^0(X\times_K X, \Omega^1_{X\times X/K}) = K \times_{\mathcal{O}_K} \mathrm{H}^0(\mathfrak{Y}, \Omega^1_{\mathfrak{Y}/\mathcal{O}_K}) \tag{2.4.7.2}$$

corresponds to taking the pull-back of a differential form on $\mathfrak{Y}$ via the map σ of (2.4.7.1). Let q_1 be the canonical map $X \to \mathfrak{X}$. Then, by definition, $m_{\mathfrak{X}} \circ \sigma = q_1 \circ m$. Similarly,

$$\begin{aligned} p_{1,\mathfrak{X}} \circ \sigma &= q_1 \circ p_1 \\ p_{2,\mathfrak{X}} \circ \sigma &= q_1 \circ p_2, \end{aligned}$$

so that

$$1 \otimes \omega' = \sigma^*\omega' = m^*(q_1^*\omega) - p_1^*(q_1^*\omega) - p_2^*(q_1^*\omega) = 0.$$

The kernel of (2.4.7.2) is the torsion submodule of the $\mathcal{O}_K$-module $\mathrm{H}^0(\mathfrak{Y}, \Omega^1_{\mathfrak{Y}/\mathcal{O}_K})$. Since $\mathfrak{Y} \to S$ is proper and the sheaf of differentials $\Omega^1_{\mathfrak{Y}/\mathcal{O}_K}$ is coherent, $\mathrm{H}^0(\mathfrak{Y}, \Omega^1_{\mathfrak{Y}/\mathcal{O}_K})$ is of finite type. Therefore there exists an integer $r_0 \geq 0$ such that

$$p^{r_0}[\mathrm{H}^0(\mathfrak{Y}, \Omega^1_{\mathfrak{Y}/\mathcal{O}_K})_{\mathrm{Tors}}] = 0.$$

The restriction

$$p^{r_0}\mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to p^{r_0}\mathrm{H}^0(\mathfrak{Y}, \Omega^1_{\mathfrak{Y}/\mathcal{O}_K}), \quad \omega \mapsto \omega' = m_{\mathfrak{X}}^*\omega - p_{1,\mathfrak{X}}^*\omega - p_{2,\mathfrak{X}}^*\omega \tag{2.4.7.3}$$

vanishes.

Let $u_1, u_2 \in \mathfrak{X}(\mathcal{O}_{\overline{K}})$ and denote by $u_{1,X}$ and $u_{2,X}$ the corresponding $\overline{K}$-points of X. Let v_X

$$v_X\colon \mathrm{Spec}(\overline{K}) \xrightarrow{\Delta} \mathrm{Spec}(\overline{K}) \times \mathrm{Spec}(\overline{K}) \xrightarrow{u_{1,X}\times u_{2,X}} X \times_K X$$

and let $v \in \mathfrak{Y}(\mathcal{O}_{\overline{K}})$ be the corresponding point of $\mathfrak{Y}$. We have:

$$\begin{aligned} &u_1 = p_{1,\mathfrak{X}} \circ v; \quad u_2 = p_{2,\mathfrak{X}} \circ v; \\ &u_{1,X} = p_1 \circ v_X; \quad u_{2,X} = p_2 \circ v_X; \\ &u_1 + u_2 = m_{\mathfrak{X}} \circ v. \end{aligned}$$

By (2.4.7.3), we get for any $\omega \in p^{r_0}\mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K})$,

$$(u_1+u_2)^*\omega = v^*(m_{\mathfrak{X}}^*\omega) = v^*(p_{1,\mathfrak{X}}^*\omega + p_{2,\mathfrak{X}}^*\omega) = u_1^*\omega + u_2^*\omega.$$

□

2.4.8. Let $r \geq r_0$ be a non negative integer such that $p^r \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K})$ is torsion free or, so that the restriction of the canonical map

$$\mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to K \otimes_{\mathcal{O}_K} \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) = \mathrm{H}^0(X, \Omega^1_{X/K})$$

to $p^r \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K})$ is injective. We can restrict the map (2.4.4.1) to

$$p^r \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \times X(\overline{K}) \to \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}.$$

By 2.4.7, this pairing is $\mathbb{Z}[G_K]$-linear in the second variable. The associated homomorphism

$$p^r \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to \mathrm{Hom}_{\mathbb{Z}[G_K]}(X(\overline{K}), \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) \tag{2.4.8.1}$$

is $\mathcal{O}_K$-linear.

2.4.9. Let

$$\mathrm{T}_p(X) = \mathrm{T}_p(X_{\overline{\eta}}) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}_p/\mathbb{Z}_p, X(\overline{K}))$$

be the p-adic Tate module of X. Let $V_p(X) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], X(\overline{K}))$. We have a natural inclusion of $\mathrm{T}_p(X)$ in $V_p(X)$: given any $\alpha = (a_n)_{n\in\mathbb{N}} \in \mathrm{T}_p(X)$ we can define a map $\varphi_\alpha \colon \mathbb{Z}[p^{-1}] \to X(\overline{K})$ by the assignment $p^{-n} \mapsto a_n$ for $n \geq 0$. Let $V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$ be $\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$ as in 2.3. We have the isomorphism

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}). \tag{2.4.9.1}$$

We can compose the $\mathcal{O}_K$-homomorphism (2.4.8.1) with the map:

$$\mathrm{Hom}_{\mathbb{Z}[G_K]}(X(\overline{K}), \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) \xrightarrow{\psi} \mathrm{Hom}_{\mathbb{Z}[G_K]}(V_p(X), V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})) \tag{2.4.9.2}$$

to get

$$p^r \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to \mathrm{Hom}_{\mathbb{Z}[G_K]}(V_p(X), V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}))$$

and then, by extending the scalars to K:

$$\widehat{\varrho} = \widehat{\varrho}^0_{X,\mathfrak{X},r} \colon \mathrm{H}^0(X, \Omega^1_{X/K}) = K \otimes_{\mathcal{O}_K} p^r \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to \mathrm{Hom}_{\mathbb{Z}[G_K]}(V_p(X), V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})).$$

2.4.10. Remark. The map ψ in (2.4.9.2) is injective, as $X(\overline{K})$ is a p-divisible group (in the classical sense).

2.4.11. For any $\omega \in \mathrm{H}^0(X, \Omega^1_{X/K})$ we can take the restriction of the morphism of $\mathbb{Z}[G_K]$-modules

$$\widehat{\varrho}(\omega) \colon V_p(X) \to V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$$

to $\mathrm{T}_p(X) \subset V_p(X) \to V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$. By continuity, $\widehat{\varrho}(\omega)|_{\mathrm{T}_p(X)}$ is $\mathbb{Z}_p$ linear and, in the end, we get a K-linear map:

$$\varrho^0_X = \varrho^0_{X,\mathfrak{X},r} \colon \mathrm{H}^0(X, \Omega^1_{X/K}) \to \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X), V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})) = \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X), \mathbf{C}(1))$$

since $V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$ is $\mathbb{Z}_p[G_K]$-isomorphic to $\mathbf{C}(1)$ by Theorem 2.3.5.

2.4.12. Proposition. *The restriction map*

$$\mathrm{Hom}_{\mathbb{Z}[G_K]}(V_p(X), \mathbf{C}(1)) \to \mathrm{Hom}_{\mathbb{Z}[G_K]}(\mathrm{T}_p(X), \mathbf{C}(1))$$

induced by the inclusion $\mathrm{T}_p(X) \subset V_p(X)$ *is injective*

PROOF. Let $X[p^\infty]$ be the subgroup of p-primary torsion of $X(\overline{K})$. The quotient $D_p(X) = X(\overline{K})/X[p^\infty]$ is a uniquely p-divisible abelian group and we have a canonical isomorphism between $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], D_p(X))$ and $D_p(X)$ given by

$$\varphi \mapsto \varphi(1), \quad x \in D_p(X) \mapsto (\varphi_x \colon 1 \mapsto x).$$

Therefore, the exact sequence

$$0 \to X[p^\infty] \to X(\overline{K}) \to D_p(X) \to 0$$

leads to the exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], X[p^\infty]) \to V_p(X) \to D_p(X) \to 0. \tag{2.4.12.1}$$

Moreover, we have a canonical isomorphism:

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], X[p^\infty]) \cong \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{T}_p(X). \tag{2.4.12.2}$$

Indeed, given any $\mathbb{Z}$-linear map $\varphi \colon \mathbb{Z}[p^{-1}] \to X[p^\infty]$, let $x_0 \in X[p^r]$ be $\varphi(1)$. Then for any $n \in \mathbb{N}$, $x_n = \varphi(1/p^n) \in X[p^{r+n}]$, with $px_n = x_{n-1}$, defining in this way the element $p^{-r} \otimes (p^r x_n)_{n\in\mathbb{N}} \in \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{T}_p(X)$: it is easy to check that the map is an isomorphism.

By applying $\mathrm{Hom}_{\mathbb{Z}[G_K]}(-, \mathbf{C}(1))$ to (2.4.12.1) we get

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G_K]}(D_p(X), \mathbf{C}(1)) \to \mathrm{Hom}_{\mathbb{Z}[G_K]}(V_p(X), \mathbf{C}(1)) \xrightarrow{\alpha} \mathrm{Hom}_{\mathbb{Z}[G_K]}(\mathrm{T}_p(X), \mathbf{C}(1)) \tag{2.4.12.3}$$

as

$$\mathrm{Hom}_{\mathbb{Z}[G_K]}(\mathrm{T}_p(X), \mathbf{C}(1)) = (\mathrm{Hom}_{\mathbb{Z}}(\mathrm{T}_p(X), \mathbf{C}(1)))^{G_K} = \mathrm{Hom}_{\mathbb{Z}[G_K]}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{T}_p(X), \mathbf{C}(1)),$$

so that $\mathrm{Hom}_{\mathbb{Z}[G_K]}(D_p(X), \mathbf{C}(1))$ is identified with the kernel of α.

Since

$$X(\overline{K}) = \bigcup_{\substack{\overline{K} \supset L \supseteq K \\ L \text{ finite, Galois}}} X(L) = \bigcup_{\substack{H \trianglelefteq G_K \\ H \text{ open}}} X(\overline{K})^H,$$

also $D_p(X) = \bigcup (D_p(X))^H$ for H varying in the set of open normal subgroups of G_K. Given $f \in \mathrm{Hom}_{\mathbb{Z}[G_K]}(D_p(X), \mathbf{C}(1))$ we have

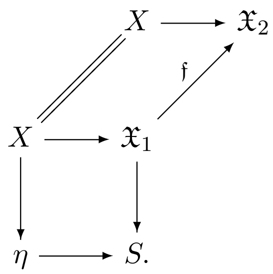
$$f((D_p(X))^H) \subseteq (\mathbf{C}(1))^H = 0$$

by Tate's Theorem (cfr. 1.5.15), for any open normal subgroup H of G_K. Hence $f(D_p(X)) = \bigcup f((D_p(X))^H) = 0$. □

2.4.13. PROPOSITION. *The maps ϱ_X^0 and $\widehat{\varrho}$ do not depend on the choice of r and on the choice of the $\mathcal{O}_K$-model $\mathfrak{X}$.*

PROOF. The K-linearity gives immediately the independence from r. It is clearly enough to check the independence of the map $\widehat{\varrho}$ from the choice of $\mathfrak{X}$. Let $\mathfrak{X}_1$ and $\mathfrak{X}_2$ be two proper

$\mathcal{O}_K$-model of X and suppose that the identity map id_X extends to a morphism $\mathfrak{f}\colon \mathfrak{X}_1 \to \mathfrak{X}_2$:



In this situation we say that $\mathfrak{X}_1$ dominates $\mathfrak{X}_2$. The commutativity of the above diagram implies that

$$\begin{array}{ccccc} \widehat{\varrho}^0_{X,\mathfrak{X}_2}\colon \mathrm{H}^0(X,\Omega^1_{X/K}) & \xrightarrow{\sim} & K\otimes_{\mathcal{O}_K} p^r\mathrm{H}^0(\mathfrak{X}_2,\Omega^1_{\mathfrak{X}_2/\mathcal{O}_K}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G_K]}(V_p(X),V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})) \\ \| & & \Big\downarrow{\scriptstyle \mathfrak{f}^*} & & \| \\ \widehat{\varrho}^0_{X,\mathfrak{X}_1}\colon \mathrm{H}^0(X,\Omega^1_{X/K}) & \xrightarrow{\sim} & K\otimes_{\mathcal{O}_K} p^r\mathrm{H}^0(\mathfrak{X}_1,\Omega^1_{\mathfrak{X}_1/\mathcal{O}_K}) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}[G_K]}(V_p(X),V_p(\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})) \end{array}$$

also commutes, proving that $\widehat{\varrho}^0_{X,\mathfrak{X}_2} = \widehat{\varrho}^0_{X,\mathfrak{X}_1}$. In the general case, if $\mathfrak{X}_1$ and $\mathfrak{X}_2$ are two models of X, we can construct a third $\mathcal{O}_K$-model of X, say $\mathfrak{X}_3$, forcing the existence of maps $\mathfrak{X}_3 \xrightarrow{f_{3,1}} \mathfrak{X}_1$ and $\mathfrak{X}_3 \xrightarrow{f_{3,2}} \mathfrak{X}_2$ extending the identity id_X. Indeed, let $\varphi\colon X \to \mathbb{P}^n_K$ be a projective embedding of X. Arguing as in (2.4.7.1), we can consider the composite map

$$X \xrightarrow{\Delta} \times_K X \times_K X \to \mathfrak{X}_1 \times_{\mathcal{O}_K} \mathfrak{X}_2.$$

and we let $\mathfrak{X}_3$ be the schematic closure of the composite morphism. □

2.4.14. Theorem. *Let X be an abelian variety over K. Then*

$$\varrho^0_X\colon \mathrm{H}^0(X,\Omega^1_{X/K}) \to \mathrm{Hom}_{\mathbb{Z}_p[G]}(T_p(X),\mathbf{C}(1))$$

defined in 2.4.11 is an injective K-linear map, functorial in X.

2.4.15. The same argument used in the proof of 2.4.13 allow us to prove that the map ϱ^0_X just defined is actually functorial in X: given any homomorphism of abelian varieties $f\colon X \to Z$, it's enough to choose two $\mathcal{O}_K$-models for X and Z respectively, say $\mathfrak{X}$ and $\mathfrak{Z}$, such that f extends to a morphism $\mathfrak{f}\colon \mathfrak{X} \to \mathfrak{Z}$.

2.4.16. The map ϱ^0_X is K linear by construction and functorial by 2.4.15. Since the restriction map $\mathrm{Hom}_{\mathbb{Z}[G_K]}(V_p(X),\mathbf{C}(1)) \to \mathrm{Hom}_{\mathbb{Z}[G_K]}(\mathrm{T}_p(X),\mathbf{C}(1))$ is injective by 2.4.12, it's enough to prove that $\widehat{\varrho}$ defined in (2.4.9) is injective. On the other hand, $\widehat{\varrho}$ is the scalar extension to K of the composition between the map (2.4.8.1) and the injective map ψ of (2.4.9.2). Hence, we are reduced to prove the following

2.4.17. Proposition. *The map*

$$p^r\mathrm{H}^0(\mathfrak{X},\Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to \mathrm{Hom}_{\mathbb{Z}[G_K]}(X(\overline{K}),\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$$

defined in (2.4.8.1) *is injective.*

We dedicate section 2.5 to the proof of this result.

2.5. The Proof of Proposition 2.4.17

The independence from the choice of the $\mathcal{O}_K$-model $\mathfrak{X}$ given by 2.4.13, allow us to use the following desingularization lemma:

2.5.1. Lemma. *Let X be a projective variety over K, of dimension d. Let $u \in X(K)$ be a regular point of X. Then there exists a proper $\mathcal{O}_K$-model $\mathfrak{X}$ of X such that if $\overline{u}$ denotes the closed point in the closure of u in $\mathfrak{X}$, the $\mathfrak{m}_{\overline{u}}$-adic completion of $\mathcal{O}_{\mathfrak{X},\overline{u}}$ is isomorphic to the ring of formal powers series in d variables over $\mathcal{O}_K$.*

Proof. Let φ be a closed immersion $\varphi\colon X \to \mathbb{P}^n_K$, so that:

$$X = \mathrm{Proj}(K[X_0, \dots, X_n]/I)$$

for a homogeneous ideal I of $K[X_0, \dots, X_n]$. We choose homogeneous coordinates $(X_0; \dots; X_n)$ of $\mathbb{P}^n_K$ so that u is the point $(1 : 0 \dots : 0)$: being u a regular point of X, the Jacobian criterion implies — up to a variable reordering — that we can find homogeneous polynomials $F_1, \dots, F_{n-d}$ in I, locally defining X, such that the $(n-d) \times (n-d)$ minor

$$\left(\frac{\partial F_i}{\partial X_{d+j}}(u)\right)_{1 \le i,j \le n-d} \tag{2.5.1.1}$$

of the Jacobian matrix at u is invertible. By a linear change of variables we can further assume that such minor is the identity matrix I_{n-d}.

Let J be the homogeneous ideal of $K[X_0, \dots, X_n]$ generated by

$$\begin{array}{ll} X_i & \text{for } 1 \le i \le d \\ X_i X_j & \text{for } i, j \ge 1. \end{array} \tag{2.5.1.2}$$

If $r_i = \deg F_i$, $1 \le i \le n-d$, we have

$$F_i \equiv X_0^{r_i - 1} X_{d+i} \pmod{J}, \qquad \text{for } 1 \le i \le n-d. \tag{2.5.1.3}$$

by (2.5.1.1) and (2.5.1.2). Let π be a uniformizer of $\mathcal{O}_K$. We choose non negative integers s_i such that

$$\pi^{s_i} F_i \in \mathcal{O}_K[X_0, \dots, X_n], \qquad \text{for } 1 \le i \le n-d.$$

Let $s \in \mathbb{N}$ such that $s \ge s_i$ for every $1 \le i \le n-d$ and we set:

$$\begin{array}{ll} X_0 = X_0', & \\ X_i = \pi^{2s} X_i' & \text{for } 1 \le i \le d, \\ X_i = \pi^s X_i' & \text{for } d+1 \le i \le n. \end{array} \tag{2.5.1.4}$$

With this choice, a straightforward computation shows that we can find $(n-d)$ homogeneous polynomials G_i in the variables X_i' such that:

$$\begin{array}{l} F_i = \pi^s G_i \\ G_i \equiv (X_0')^{r_i - 1} X_{d+i}' \pmod{\pi \mathcal{O}_K[X_0', \dots X_n']} \end{array} \qquad \text{for } 1 \le i \le n-d. \tag{2.5.1.5}$$

We adopt the linear change of coordinates (2.5.1.4) in $\mathbb{P}^n_K$ and consider the open immersion

$$\mathbb{P}^n_K = \mathrm{Proj}(K[X_0', \dots X_n']) \to \mathrm{Proj}(\mathcal{O}_K[X_0', \dots X_n']) = \mathbb{P}^n_{\mathcal{O}_K} \tag{2.5.1.6}$$

Let $\mathfrak{X}$ be the schematic closure of $X \to \mathbb{P}^n_{\mathcal{O}_K}$ via (2.5.1.6). Let $\overline{u}$ be the closed point of the closure of u in $\mathfrak{X}$. We place ourselves in the principal affine open neighbourhood of $\overline{u}$ (resp. u) $D_+(X_0') = \mathbb{P}^n_{\mathcal{O}_K} \setminus V_+(X_0')$ (resp. $D_+(X_0') \cap \mathbb{P}^n_K$), so to have affine coordinates $x_i = X_i'/X_0'$.

Let $\mathfrak{m}_u \subset \mathcal{O}_{X,u}$ be the maximal ideal of the local ring of X at u. The ring $\mathcal{O}_{X,u}$ is regular and local of dimension d. By construction, the K-vector space $\mathfrak{m}_u/\mathfrak{m}_u^2$ is generated by $x_1, \ldots, x_d$.

Let $\mathfrak{m}_{\overline{u}} \subset \mathcal{O}_{\mathfrak{X},u}$ be the maximal ideal of the local ring of $\mathfrak{X}$ at $\overline{u}$. Let $I_{0,\mathcal{O}_K}$ be the ideal of $\mathcal{O}_K[x_1, \ldots, x_n]$ defining $\mathfrak{X}$ in $D_+(X_0') = \mathbb{A}^n_{\mathcal{O}_K}$. It is generated locally at $\overline{u}$ by the de-homogenized polynomials ${X_0'}^{-r_i} G(X_i')$, written in the variables x_i. Then $\mathfrak{m}_{\overline{u}}$ is generated by π together with the images of $x_1, \ldots, x_n$ modulo $I_{0,\mathcal{O}_K}$. The local ring $\mathcal{O}_{\mathfrak{X},\overline{\mathrm{u}}}$ is a regular local ring of dimension $d+1$. Indeed, $\mathcal{O}_{\mathfrak{X},\overline{\mathrm{u}}}$ has dimension at least $d+1$, since when we invert π we obtain a ring of dimension d. The equality in the dimension and the regularity follow from the fact that $\mathfrak{m}_{\overline{u}}/\mathfrak{m}_{\overline{u}}^2$ is generated by $\pi, x_1, \ldots, x_d$ by (2.5.1.5).

We have

$$\widehat{\mathcal{O}}_{\mathfrak{X},\overline{u}} \cong \mathcal{O}_K[[x_1, \ldots, x_d]]$$

Indeed, any element of $\widehat{\mathcal{O}}_{\mathfrak{X},\overline{u}}$ can be expanded as a power series in the x_i with coefficients in $\mathcal{O}_K$, so we have a surjective map

$$\mathcal{O}_K[[x_1, \ldots, x_d]] \to \widehat{\mathcal{O}}_{\mathfrak{X},\overline{u}}$$

and we conclude by [**EGA IV**, 0.17.3.5 (ii)], being $\mathcal{O}_K[[x_1, \ldots, x_d]]$ a regular local ring of dimension $d+1 = \dim \mathcal{O}_{\mathfrak{X},\overline{\mathrm{u}}} = \dim \widehat{\mathcal{O}}_{\mathfrak{X},\overline{\mathrm{u}}}$. □

2.5.2. Let $e \in X(K)$ be the unit section of X and let $\mathfrak{X}$ be the proper $\mathcal{O}_K$-model of X provided by Lemma 2.5.1, so that

$$\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}} = \mathcal{O}_K[[T_1, \ldots, T_g]]$$

where $g = \dim X$ and $\overline{e}$ is the closed point of the closure of e in $\mathfrak{X}$. Let $\widehat{\Omega}^1_{\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}}/\mathcal{O}_K}$ be the module of continuous $\mathcal{O}_K$-differentials of $\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}}$, i.e. the separated completion of the $\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}}$-module of $\mathcal{O}_K$-differentials $\Omega^1_{\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}}/\mathcal{O}_K}$ (see [**EGA IV**, 0.20.7.14.2]). By [**EGA IV**, 0.20.4.5], we have the canonical isomorphism

$$\widehat{\Omega}^1_{\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}}/\mathcal{O}_K} = \varprojlim \Omega^1_{\mathcal{O}_{\mathfrak{X},\overline{e}}/\mathcal{O}_K}/\mathfrak{m}_{\overline{e}}^n \Omega^1_{\mathcal{O}_{\mathfrak{X},\overline{e}}/\mathcal{O}_K}.$$

If we take the composition with the (injective) canonical map

$$\Omega^1_{\mathcal{O}_{\mathfrak{X},\overline{e}}/\mathcal{O}_K} \to \widehat{\Omega}^1_{\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}}/\mathcal{O}_K} \tag{2.5.2.1}$$

we have an injective $\mathcal{O}_K$-linear morphism

$$p^r \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to \widehat{\Omega}^1_{\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}}/\mathcal{O}_K}. \tag{2.5.2.2}$$

Indeed, a global section $\omega \in p^r \mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \subset \mathrm{H}^0(X, \Omega^1_{X/K})$ is mapped to 0 in the stalk $\Omega^1_{\mathcal{O}_{\mathfrak{X},\overline{e}}/\mathcal{O}_K}$ if and only if it is mapped to 0 in $\Omega^1_{\mathcal{O}_{X,e}/K}$, that implies $\omega = 0$, since the everywhere defined 1-form over an abelian variety are determined by the value in e.

2.5.3. We equip $\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}}$ with the $\mathfrak{m} = (T_1, \ldots, T_g)$-adic topology and $\mathcal{O}_{\overline{K}}$ with the p-adic topology. To give a continuous $\mathcal{O}_K$-linear map $f \colon \widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}} \to \mathcal{O}_{\overline{K}}$ amounts to give g elements $x_{f,1}, \ldots, x_{f,g}$ in the maximal ideal $\mathfrak{m}_{\overline{K}}$ of $\mathcal{O}_{\overline{K}}$. Therefore we have a canonical map

$$\widehat{\Omega}^1_{\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}}/\mathcal{O}_K} \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathrm{cont},\mathcal{O}_K}(\widehat{\mathcal{O}}_{\mathfrak{X},\overline{e}}, \mathcal{O}_{\overline{K}}), \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}) \tag{2.5.3.1}$$

given by

$$\omega = \sum_{i=1}^{d} \alpha_i(T_1, \ldots, T_g)\mathrm{d}T_i \in \widehat{\Omega}^1_{\widehat{\mathcal{O}}_{\mathfrak{X},\bar{e}}/\mathcal{O}_K} \mapsto (f \mapsto \sum_{i=1}^{d} \alpha_i(x_{f,1}, \ldots, x_{f,g})\mathrm{d}x_{f,i})$$

as $\alpha_i(x_{f,1}, \ldots, x_{f,g})$ converges in $\mathcal{O}_{\overline{K}}$ for every i and f.

Let ϑ be the composition of (2.5.2.2) with (2.5.3.1):

$$\vartheta\colon p^r\mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathrm{cont},\mathcal{O}_K}(\widehat{\mathcal{O}}_{\mathfrak{X},\bar{e}}, \mathcal{O}_{\overline{K}}), \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$$

Using the natural inclusion

$$\mathrm{Hom}_{\mathrm{cont},\mathcal{O}_K}(\widehat{\mathcal{O}}_{\mathfrak{X},\bar{e}}, \mathcal{O}_{\overline{K}}) \subset \mathfrak{X}(\mathcal{O}_{\overline{K}}) = X(\overline{K})$$

we see that for every $\omega \in p^r\mathrm{H}^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K})$, $\vartheta(\omega)$ corresponds to the restriction to the subset $\mathrm{Hom}_{\mathrm{cont},\mathcal{O}_K}(\widehat{\mathcal{O}}_{\mathfrak{X},\bar{e}}, \mathcal{O}_{\overline{K}})$ of $\langle \omega, - \rangle \in \mathrm{Hom}_{\mathbb{Z}[G_K]}(X(\overline{K}), \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$, image of ω through (2.4.8.1). To complete the proof of 2.4.17 is therefore enough to establish the following

2.5.4. Lemma. *The canonical map*

$$\widehat{\Omega}^1_{\widehat{\mathcal{O}}_{\mathfrak{X},\bar{e}}/\mathcal{O}_K} \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathrm{cont},\mathcal{O}_K}(\widehat{\mathcal{O}}_{\mathfrak{X},\bar{e}}, \mathcal{O}_{\overline{K}}), \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K})$$

is injective.

2.5.4 can be restated in the following purely algebraic form:

2.5.5. Lemma. *Let $\omega = \sum_{i=1}^{d} \alpha_i(T_1, \ldots, T_g)\mathrm{d}T_i$ be a formal power series in d variables with coefficients in $\mathcal{O}_K$. be a non-zero continuous differential form. Then there exist $x_1, \ldots, x_g \in \mathfrak{m}_{\overline{K}}$ such that*

$$\sum_{i=1}^{d} \alpha_i(x_1, \ldots, x_g)\mathrm{d}x_i$$

is a non-zero element of $\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$.

Proof. We first verify the statement for $g = 1$. Let $\omega = \alpha(T)\mathrm{d}T = \sum_{i\geq 0} a_i T^i \mathrm{d}T$ with $a_i \in \mathcal{O}_K$. Let v be the valuation of $\overline{K}$ normalized by $v(K^\times) = \mathbb{Z}$ and let

$$s = \inf_{i\in\mathbb{N}} v(a_i) \in \mathbb{N}.$$

As $s \in \mathbb{N}$, there exists a smallest non negative integer i_0 satisfying $v(a_{i_0}) = s$. Then, for any $x \in \mathfrak{m}_{\overline{K}}$ such that $v(x) < \frac{1}{i_0}$ we have:

$$v(\alpha(x)) = s + i_0 v(x) < s + 1.$$

It's enough to choose x to be a uniformizer for a finite (ramified) extension L of K, contained in $\overline{K}$ such that $v(\mathcal{D}_{L/K}) \geq s+1$. Then by 2.2.3 the annihilator of $\mathrm{d}x$ in $\mathcal{O}_{\overline{K}}$ is $\mathcal{O}_{\overline{K}}\mathcal{D}_{L/K}$, so that $\alpha(x)\mathrm{d}x$ is not zero as element of $\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$. □

The general case is a consequence of the following statement:

2.5.6. LEMMA. *Let $\alpha_1, \dots, \alpha_g$ be g formal power series in g variables, $\alpha_i \in \mathcal{O}_K[[T_1, \dots, T_g]]$ and suppose that at least one of them is non zero. Then there exist g formal power series $\varphi_1, \dots, \varphi_g$ in one variable T over $\mathcal{O}_K$ with no constant terms such that*

$$\sum_{i=1}^{g} \alpha_i(\varphi_1, \dots, \varphi_g)\varphi_i'$$

is a non zero element of $\mathcal{O}_K[[T]]$, where φ_i' denotes the formal derivative of φ_i with respect to the variable T.

PROOF. We look for the φ_i's of the form $\varphi_i = a_iT + b_iT^2$ with $a_i, b_i \in \mathcal{O}_K$. Let $\lambda = \sum_{i=1}^{g} \alpha_i(\varphi_1, \dots, \varphi_g)\varphi_i'$; we have

$$\lambda = \sum_{i=1}^{g} \alpha_i(a_1T + b_1T^2, \dots, a_gT + b_gT^2)(a_i + 2b_iT).$$

Write α_i in the form $\alpha_i = \sum_{m \geq 0} \alpha_{i,m}$ with $\alpha_{i,m}$ homogeneous of degree m in the variables $T_1, \dots, T_g$. If r is the smallest integer such that there exists j with $\alpha_{j,r} \neq 0$, we have the following expansion for λ:

$$\lambda = \Big(\sum_{i=1}^{g} a_i\alpha_{i,r}(a_1, \dots, a_g)\Big)T^r + \Big(\sum_{i=1}^{g} a_i\alpha_{i,r+1}(a_1, \dots, a_g) + \\ + \sum_{j=1}^{g} 2b_j\alpha_{j,r}(a_1, \dots, a_g) + \sum_{i,j} a_ib_j\frac{\partial\alpha_{i,r}}{\partial T_j}(a_1, \dots, a_g)\Big)T^{r+1} + \dots$$

We now have three possibilities:

i) If $F = \sum_{i=1}^{g} T_i\alpha_{i,r}(T_1, \dots, T_g) \neq 0$, being $\mathcal{O}_K$ infinite, we can find $a_1, \dots, a_g$ in $\mathcal{O}_K$ such that $F(a_1, \dots, a_g) \neq 0$. For this choice of the a_i's, $\lambda \neq 0$ for any choice of the b_j's.

ii) If $F = 0$ we look at the next term in the expansion of λ: if

$$G = \sum_{i=1}^{g} T_i\alpha_{i,r+1}(T_1, \dots, T_g) \neq 0,$$

we can use again the fact that $\mathcal{O}_K$ is infinite to find a_i's such that $G(a_1, \dots, a_g) \neq 0$. If we set $b_j = 0$ for every j we see that $\lambda \neq 0$.

iii) If $F = G = 0$, we have, by taking the derivative of F with respect to T_j:

$$\alpha_{j,r}(T_1, \dots, T_g) + \sum_{i=1}^{g} T_i\frac{\partial\alpha_{i,r}}{\partial T_j}(T_1, \dots, T_g) = 0 \qquad (2.5.6.1)$$

for every $1 \leq j \leq g$. Moreover

$$\lambda = \Big(\sum_{j=1}^{g} b_j\Big(2\alpha_{j,r}(a_1, \dots, a_g) + \sum_{i=1}^{g} a_i\frac{\partial\alpha_{i,r}}{\partial T_j}(a_1, \dots, a_g)\Big)\Big)T^{r+1} + \dots$$

so that if we substitute (2.5.6.1), we get

$$\lambda = \Big(\sum_{j=1}^{g} b_j\alpha_{j,r}(a_1, \dots, a_d)\Big)T^{r+1} + \dots$$

It is enough to choose a j such that $\alpha_{j,r} \neq 0$ to find a_i's in $\mathcal{O}_K$ such that $\alpha_{j,r}(a_1, \dots, a_g) \neq 0$. If we set $b_j = 1$ and $b_i = 0$ for $i \neq j$ we see that $\lambda \neq 0$.

□

2.6. Connections with Tate's conjecture

2.6.1. Let K be as in 2.4.1, X an abelian variety over K, $\mathrm{T}_p(X) = \mathrm{T}_p(X_{\overline{\eta}})$ the p-adic Tate module of X.

2.6.2. THEOREM (Tate-Raynaud). *Under the assumptions 2.6.1, there exist canonical, bijective, K-linear homomorphisms*

$$\varrho^1_X : \mathrm{H}^1(X, \mathcal{O}_X) \to \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X), \mathbf{C}),$$
$$\varrho^0_X : \mathrm{H}^0(X, \Omega^1_{X/K}) \to \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X), \mathbf{C}(1))$$

where ϱ^0_X is the homomorphism defined in 2.4.11.

PROOF. Let g be the dimension of X. By 2.4.14 we have:

$$d = \dim_K(\mathrm{Hom}_{\mathbb{Z}_p[G_K]}(T_p(X), \mathbf{C}(1))) \geq \dim_K \mathrm{H}^0(X, \Omega^1_{X/K}) = g. \tag{2.6.2.1}$$

Equality holds in (2.6.2.1) if and only if ϱ^0_X is an isomorphism. Let $\hat{X}$ be the dual abelian variety of X. If we interchange the roles of X and $\hat{X}$, we get from the injection

$$\varrho^0_{\hat{X}} : \mathrm{H}^0(\hat{X}, \Omega^1_{\hat{X}/K}) \to \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(\hat{X}), \mathbf{C}(1))$$

the inequality

$$d' = \dim_K(\mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(\hat{X}), \mathbf{C}(1))) \geq g.$$

The Weil pairing

$$\mathrm{T}_p(X) \times \mathrm{T}_p(\hat{X}) \to \mathbb{Z}_p(1)$$

is a perfect $\mathbb{Z}_p$-linear pairing, compatible with the action of G_K (see [**Mum70**, p. 186]). It induces a canonical isomorphism

$$\mathrm{T}_p(X) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{T}_p(\hat{X}), \mathbb{Z}_p(1)). \tag{2.6.2.2}$$

Let $W = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{T}_p(X), \mathbf{C}(1))$ and $\hat{W} = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{T}_p(\hat{X}), \mathbf{C}(1))$. By (2.6.2.2) we have $W \cong \mathrm{T}_p(\hat{X}) \otimes_{\mathbb{Z}_p} \mathbf{C}$ and $\hat{W} \cong \mathrm{T}_p(X) \otimes_{\mathbb{Z}_p} \mathbf{C}$, so that there is a canonical non-degenerate G_K-pairing

$$W \times \hat{W} \to \mathbf{C}(1). \tag{2.6.2.3}$$

By (1.5.15), we have $\mathrm{H}^0_{\mathrm{cont}}(G_K, \mathbf{C}(1)) = \mathrm{H}^1_{\mathrm{cont}}(G_K, \mathbf{C}(1)) = 0$. By 1.6.2, $\hat{W}^{G_K} \otimes_K \mathbf{C}$ and $W^{G_K} \otimes_K \mathbf{C}$ are $\mathbf{C}$-subspaces of $\hat{W}$ and W. Since they are paired into $\mathbf{C}(1)^{G_K}$, they are orthogonal with respect to the pairing (2.6.2.3). Their dimensions are d' and d respectively, and by (1.9.5.1) we have $d + d' \leq 2g = \dim_{\mathbf{C}}(T_p(X) \otimes_{\mathbb{Z}_p} \mathbf{C})$, as required.

In order to get the morphism ϱ^1_X we use again duality for abelian varieties. First of all, recall that there is a canonical isomorphism between the tangent space at 0 to the dual abelian variety $\hat{X}$ and $\mathrm{H}^1(X, \mathcal{O}_X)$ ([**Mum70**], Corollary 3, p. 130). Hence

$$\mathrm{H}^1(X, \mathcal{O}_X) = \mathrm{Hom}_K(\mathrm{H}^0(\hat{X}, \Omega^1_{\hat{X}/K}), K).$$

The spaces $\mathrm{H}^0(X, \Omega^1_{X/K})$ and $\mathrm{H}^0(\hat{X}, \Omega^1_{\hat{X}/K})$ are mapped injectively onto subspaces of W and $\hat{W}$ which are orthogonal with respect to the pairing to $\mathbf{C}(1)$. Hence we have

$$\mathrm{Hom}_{\mathbf{C}}(\mathrm{H}^0(\hat{X}, \Omega^1_{\hat{X}/K}), \mathbf{C}(1)) = W^{G_K},$$

so that $\mathrm{H}^1(X, \mathcal{O}_X) = W^{G_K} \otimes_K \mathbf{C}(-1)$. But then

$$W^{G_K} \otimes_K \mathbf{C}(-1) = \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X), \mathbf{C}(1)) \otimes_K \mathbf{C}(-1) \cong \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X), \mathbf{C})$$

providing the required isomorphism

$$\varrho^1_X \colon \mathrm{H}^1(X, \mathcal{O}_X) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p[G_K]}(\mathrm{T}_p(X), \mathbf{C}).$$

$\square$

Bibliography

[BLR90] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*, volume 21. Springer-Verlag, 1990.

[CF67] J.W.S. Cassels and A. Frölich. *Algebraic number theory: proceedings of an instructional conference*. Academic Pr., 1967.

[Fal88] G. Faltings. p-adic Hodge Theory. *J. Amer. Math. Soc*, 1(1):255–299, 1988.

[Fon82] J.M. Fontaine. Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux. *Inventiones mathematicae*, 65(3):379–409, 1982.

[Fon04] J.M. Fontaine. Arithmétique des représentations galoisiennes p-adiques. *Astérisque*, 295:1–115, 2004.

[EGA II] A. Grothendieck. *Éléments de géométrie algébrique (rédigés avec la collaboration de Jean Dieudonné): II. Étude globale élémentaire de quelques classes de morphismes*, volume 8 of *Pub. Math.* IHES, 1961.

[EGA IV] A. Grothendieck. *Éléments de géométrie algébrique (rédigés avec la collaboration de Jean Dieudonné): IV. Étude locale des schémas et des morphismes de schémas*, volume 20 of *Pub. Math.* IHES, 1964.

[SGA 7] A. Grothendieck, M. Raynaud, DS Rim, P. Deligne, and N.M. Katz. *Groupes de monodromie en géométrie algébrique*. Springer, 1972.

[LT65] J. Lubin and J. Tate. Formal complex multiplication in local fields. *The Annals of Mathematics*, 81(2), 1965.

[Mum70] D. Mumford. *Abelian varieties*, volume 2. Oxford Univ Press, 1970.

[NS99] J. Neukirch and N. Schappacher. *Algebraic number theory*, volume 322 of *Die Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1999.

[Sen80] S. Sen. Continuous cohomology and p-adic galois representations. *Inventiones mathematicae*, 62(1):89–116, 1980.

[Ser59] J.P. Serre. *Groupes algébriques et corps de classes. Publications de l'Institut de Mathématique de l'Université de Nancago, VII*, volume 1264. Hermann, 1959.

[Ser62] J.P. Serre. *Corps locaux. Publications de l'Institut de Mathématique de l'Université de Nancago, VIII*, volume 1296. Hermann, 1962.

[Tat67] J. Tate. p-divisible groups. In *Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin*, pages 158–183, 1967.