Hodge-Tate decomposition for p-adic abelian varieties with good reduction

Giorgio Navone

A thesis
in the Department of
Mathematics & Statistics

Presented in Partial Fulfillment of the Requirements
For the Degree of
Master of Science (Mathematics)
at Concordia University
Montréal, Québec, Canada

June 2022

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: Giorgio Navone

Entitled: Hodge-Tate decomposition for p-adic abelian varieties with good reduction

and submitted in partial fulfillment of the requirements for the degree of

Master of Science in Mathematics

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

______________________ Chair
Prof. Adrian Iovita

______________________ Examiner
Prof. Denis Benois (Bordeaux University)

______________________ Examiner
Prof. Peter Stevenhagen (Leiden University)

______________________ Thesis Supervisor(s)
Prof. Adrian Iovita

______________________ Thesis Supervisor(s)
Prof. Giovanni Rosso

Approved by ______________________
Prof. Cody Hyndman Chair of Department or Graduate Program Director

____
Prof. Pascale Sicotte Dean of Faculty of Arts and Science

Abstract

Title: "Hodge-Tate decomposition for p-adic abelian varieties with good reduction"
Student: Giorgio Navone
Supervisors: Professor Adrian Iovita and Professor Giovanni Rosso
Thesis Defence: 12 July 2022 at 10:10 AM
Abstract:
The goal of this thesis project is to study the $\mathbb{C}_p$-semilinear representation $\mathbb{C}_p \otimes_{\mathbb{Z}_p} T_p(X)$, where X is an abelian variety over a local field K, following Fontaine's paper “Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux". The main goal is to prove the Hodge-Tate decomposition $T_p(X) \otimes_{\mathbb{Z}_p} \mathbb{C}_p \cong (V_0 \otimes_K \mathbb{C}_p) \oplus (V_1 \otimes_K \mathbb{C}_p(1))$ where V_0, V_1 are K-vector spaces of same dimension of X.
Thus, in the first chapter we compute the continuous cohomology groups of $\mathbb{C}_p(n)$ with respect to $G_K = Gal(\overline{K}, K)$. In the second chapter, Fontaine's work analyse the module of Kähler differentials $\Omega = \Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{\mathbb{Q}}_p})$ using an *integration* of invariant differentials along elements of the Tate module of a $\mathbb{Z}_p$-module Γ. Finally, in the third chapter we prove Tate-Raynaud theorem using the identification $V_p(\Omega) \cong \mathbb{C}_p(1)$ and then the Hodge-Tate decomposition is obtained involving the dual abelian variety and the cohomology groups of $\mathbb{C}_p(n)$.

Acknowledgements

I would like to thoughtfully thank professor Adrian Iovita for his help and supervision and for the proposal of this interesting topic. I also need to express my gratitude to professor Giovanni Rosso that helped me several times during the last months. Both professors were available for issues of any kind during this year in Montreal and they assisted me also in the difficult process of planning my next years.

I would like to thank my family and my girlfriend Anna for their infinite support during the last years. Last but not least, this master program would not have been so exciting without the fun and the collaboration with the fellow students and friends that joined me in these two years: I definitely need to mention Dario, Pier Federico, Stefania, Riccardo, Luca, Laura in Padova and Jeremy, Brendon, Davide and Niccolò in Montreal.

Contents

Introduction

The profinite Galois group $G_K = Gal(\bar{K}, K)$ (for a local field K) is a topic of great interest in algebraic number theory. Therefore arithmetic geometry is keen on understanding the action of G_K on geometric objects, for example on the Tate module $T_p(X)$ of an elliptic curve X or, more in general, of an abelian variety over K. In particular, the aim of this thesis project is to study the $\mathbb{C}_p$-semilinear representation $\mathbb{C}_p \otimes_{\mathbb{Z}_p} T_p(X)$ and to prove that it admits a Hodge–Tate decomposition, i.e. that it decomposes as finite sum of $V_i \otimes_K \mathbb{C}_p(i)$ for some $i \in \mathbb{Z}$, where the V_i's are finite dim. K-vector spaces. These i's are called Hodge–Tate weights and they indicate that the action of G_K is twisted by the i-power of the cyclotomic character $\chi_{\text{cycl}} : G_K \to \mathbb{Z}_p^{\times}$. The main reference of this thesis project is Fontaine's paper "Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux" [Fon82].

We begin with a brief overview of the results on abelian varieties that will be necessary for this project, giving the references for a more detailed dissertation.

In the first chapter we study the continuous cohomology groups of $\mathbb{C}_p(n)$. If $n \neq 0$ then the 0-th and 1-st cohomology group of $\mathbb{C}_p(n)$ are trivial and later this result will be a key algebraic tool for the decomposition. The main idea of the proof is to consider the cyclotomic extension K_∞ given by all p^k-roots of unity and to study the ramification of the intermediate cyclotomic extensions using the upper ramification groups.

The second chapter is dedicated to the study of the module of Kähler differentials $\Omega = \Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{\mathbb{Q}}_p})$. We consider Γ, the $\mathbb{Z}_p$-module structure on $\mathfrak{m}_{\overline{\mathbb{Q}}_p}$ given by the multiplicative formal group $\hat{\mathbb{G}}_m$. An original work of Fontaine studies an *integration* of invariant differentials on Γ along elements of the Tate module of Γ . This allows to identify Ω with $(\overline{\mathbb{Q}}_p/\mathfrak{a})(1)$ for some fractional ideal $\mathfrak{a}$, that implies $V_p(\Omega) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega) \cong \mathbb{C}_p(1)$.

Finally, in the third chapter we consider an abelian variety X over K with *good reduction*, i.e. there exists an abelian scheme $\mathfrak{X}$ over $\mathcal{O}_K$ such that $X = \mathfrak{X} \times_{\mathrm{Spec}\mathcal{O}_K} \mathrm{Spec}K$. Assuming the good reduction, we prove Tate-Raynaud theorem: there exists an injective K-linear map

$$\Omega_X(X) \to \mathrm{Hom}_{\mathbb{Z}_p[G]}(T_p(X), V_p(\Omega))$$

where $\Omega_X(X)$ is the K-vector space of global differential forms on X. The G_K-equivariant isomorphisms $V_p(\Omega) \cong \mathbb{C}_p(1)$ and the cohomological results of chapter one lead to the Hodge–Tate decomposition theorem for $T_p(X) \otimes \mathbb{C}_p$, that is a G_K-equivariant $\mathbb{C}_p$-linear isomorphism

$$T_p(X) \otimes_{\mathbb{Z}_p} \mathbb{C}_p \cong (V_0 \otimes_K \mathbb{C}_p) \oplus (V_1 \otimes_K \mathbb{C}_p(1))$$

where V_0, V_1 are K-vector spaces of same dimension of X.

Chapter 0

Generalities on Abelian Varieties

0.1 Definitions

Definition 0.1.1. *A* ***group variety*** *over K is a group object in the category of algebraic varieties over K, i.e. it is an algebraic variety V over K endowed with regular maps $m : V \times V \to V$ and $inv : V \to V$ and an element $e \in V(K)$ such that the following diagrams are commutative:*

$$\begin{tikzcd} V \arrow[r, "{(id,e)}"] \arrow[dr, "id"'] & V \times V \arrow[d, "m"] \\ & V \end{tikzcd} \qquad \begin{tikzcd} V \arrow[r, "{(e,id)}"] \arrow[dr, "id"'] & V \times V \arrow[d, "m"] \\ & V \end{tikzcd}$$

$$\begin{tikzcd} V \arrow[r, "{(id,inv)}"] \arrow[d] & V \times V \arrow[d, "m"] \\ \mathrm{Spec}K \arrow[r, "e"] & V \end{tikzcd} \qquad \begin{tikzcd} V \arrow[r, "{(inv,id)}"] \arrow[d] & V \times V \arrow[d, "m"] \\ \mathrm{Spec}K \arrow[r, "e"] & V \end{tikzcd}$$

$$\begin{tikzcd} V \times V \times V \arrow[r, "id\times m"] \arrow[d, "m\times id"] & V \times V \arrow[d, "m"] \\ V \times V \arrow[r, "m"] & V \end{tikzcd}$$

which represent respectively the properties of the identity element, of the inverse and the associativity rule.

The definition implies a structure of group on $V(\overline{K})$ and on the other hand this structure implies the commutativity of the previous diagrams. In general, for every extension L/K, the set of points $V(L)$ inherits a group structure.
Let a a K-rational point of a group variety V. We define the *right translation* by a to be the map $t_a : V \to V$ given by the composition

$$V \xrightarrow{(id,a)} V \times V \xrightarrow{m} V$$

The map t_a is an isomorphism and its inverse is $t_{inv(a)}$. In particular, a group variety V is always non-singular since we may translate a non-singular open to every point of V.

Definition 0.1.2. *An* ***abelian variety*** *over K is a complete and connected group variety over K.*

We need to introduce also the definition of abelian scheme.

Definition 0.1.3. *An* ***abelian scheme*** *over a ring R is a group scheme $\mathcal{A}$ over R such that the structure morphism $\mathcal{A} \to \mathrm{Spec}R$ is of finite presentation, proper, smooth and with all fibers geometrically connected.*

Notice that a *group scheme* is simply the analogous of a group variety in the settings of schemes.

0.2 Properties

An abelian variety turns out to be projective and commutative (with regard to the group law), thus we will use the additive notation and we may use 0 instead of e. We state the main tools towards these results without any claim to completeness and we also introduce some important notions, such as the Tate module and the sheaf of differentials.

Commutativity

Theorem 0.2.1 (Rigidity theorem). *Let $\alpha : V \times W \to U$ be a regular map and assume V complete and $V \times W$ geometrically irreducible. If there are points $u_0 \in U(K)$, $v_0 \in V(K)$ and $w_0 \in W(K)$ such that*

$$\alpha(V \times \{w_0\}) = \{u_0\} = \alpha(\{v_0\} \times W)$$

then $\alpha(V \times W) = \{u_0\}$.

This implies the important corollary:

Corollary 0.2.2. *Every regular map $\alpha : A \to B$ of abelian varieties is a composition of a homomorphism with a translation.*

Proof. We may translate and assume $\alpha(0) = 0$ so then $\phi : A \times A \to B$ defined as $\phi(a, a') = \alpha(a + a') - \alpha(a) - \alpha(a')$ is a regular map and by the Rigidity Theorem is the zero map, i.e. α is a homomorphism. □

In particular, *inv* is a regular map that maps 0 to 0 and by this corollary it is an homomorphism, hence the operation m of an abelian variety is commutative.

Theorem of the cube/square

The result regarding abelian varieties being projective requires deep work and technicalities, thus for our purposes we may as well define abelian varieties directly as projective group varieties instead of complete.
However, we state two important results on that direction since they will be useful in defining the dual variety in the next section.

Theorem 0.2.3 (Theorem of the cube). *Let U, V , W be complete geometrically irreducible varieties over K, and let $u_0 \in U(K)$, $v_0 \in V(K)$, $w_0 \in W(K)$ be K-rational points. Then an invertible sheaf $\mathcal{L}$ on $U \times V \times W$ is trivial if its restrictions to*

$$U \times V \times \{w_0\}, U \times \{v_0\} \times W, \{u_0\} \times V \times W$$

are all trivial.

Theorem 0.2.4 (Theorem of the square). *For every invertible sheaf $\mathcal{L}$ on an abelian variety A and for every couple of points $a, b \in A(K)$ then*

$$t_{a+b}^*\mathcal{L} \otimes \mathcal{L} \simeq t_a^*\mathcal{L} \otimes t_b^*\mathcal{L}$$

A interesting family of regular maps between abelian varieties are the *isogenies*, i.e. surjective homomorphisms with finite kernel. In particular, for every $n > 0$, the map $n_A : A \to A$ that maps $a \mapsto a + \cdots + a$ (n-times) is an isogeny ([Mil86] section 1.7).

Proposition 0.2.5. *Let A be an abelian variety of dimension d and let $n > 0$. Then $n_A : A \to A$ is an isogeny of degree n^{2d}, in particular it is surjective and $A_n(\overline{K}) :=$ $\mathrm{Ker}(n_A : A(\overline{K}) \to A(\overline{K}))$ contains n^{2d} points.*

Since this must hold for every $n > 0$, then the finite abelian groups structure theorem implies that $A_n(\overline{K}) \cong (\mathbb{Z}/n\mathbb{Z})^{2d}$ as group.

Moreover, for a prime l we define

$$T_l(A) = \varprojlim A_{l^n}(\overline{K})$$

called the Tate module of A. It is a free $\mathbb{Z}_l$-module of rank $2d$. The action of $\mathrm{Gal}(\overline{K}/K)$ on $A_{l^n}(\overline{K})$ induces an action on $T_l(A)$ which will be the main object of interest in this thesis project.

We conclude this section stating an important proposition regarding the sheaf of differentials $\Omega^1_{V/K}$ for a group variety V, referring to 3.2, 3.3 in [Spr81].

Proposition 0.2.6. *Let V be a smooth algebraic variety over K of dimension d over K, then*

1. *The sheaf of differentials $\Omega^1_{V/K}$ on V is a locally free sheaf of $\mathcal{O}_V$-modules of rank d.*
2. *If V is a group variety, then $\Omega^1_{V/K}$ is free.*

Part 2 derives from the the natural isomorphism

$$\Omega_0 \otimes_K \mathcal{O}_V \cong \Omega^1_{V/K}$$

where Ω_0 is the dual of space of the tangent space $T_{V,0}$ at 0 to V. The map is given by the pullback of $\omega_0 \in \Omega_0$ via the translations. In particular, the everywhere regular forms on an abelian variety A are exactly the invariant forms (see [MRM74] pag. 39-40).

0.3 $\mathrm{Pic}^0(A)$ and the dual variety

Let $\mathcal{L}$ be an invertible sheaf on A; from the theorem of the square we deduce that the map

$$\lambda_{\mathcal{L}} : A(K) \to \mathrm{Pic}(A), a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$$

is a homomorphism for every $\mathcal{L}$. Let define

$$C(\mathcal{L}) = \{a \in A(K) \mid \lambda_{\mathcal{L}}(a) = 0\}.$$

It is a closed subset of A and it is key in the definition of $\mathrm{Pic}^0(A)$, due to the next proposition.

Proposition 0.3.1. *For an invertible sheaf $\mathcal{L}$ on A the following conditions are equivalent:*

- $C(\mathcal{L}) = A(K)$
- $m^*\mathcal{L} \simeq p^*\mathcal{L} \otimes q^*\mathcal{L}$

where p, q are the two projections $A \times A \to A$.

We define $\mathrm{Pic}^0(A)$ as the subgroup of $\mathrm{Pic}(A)$ of the classes of invertible sheaves respecting the equivalent conditions of Proposition 0.3.1.
An important property of invertible sheaf $\mathcal{L} \in \mathrm{Pic}^0(A)$ is that for every couple $\alpha, \beta : V \to A$ of regular maps holds

$$(\alpha + \beta)^*\mathcal{L} \simeq \alpha^*\mathcal{L} \otimes \beta^*\mathcal{L}.$$

The dual abelian variety $A^\vee$ has the goal of parametrizing the elements of $\mathrm{Pic}^0(A)$. We introduce an axiomatic definition of $A^\vee$ and we won't deepen into the actual realization of the variety; for our purposes we assume the existence of the dual abelian variety $A^\vee$ for every abelian variety A over K.
We consider $\mathcal{A}$ the set of pairs $(A^\vee, \mathcal{P})$ where $A^\vee$ is an algebraic variety over K and $\mathcal{P}$ is an invertible sheaf on $A \times A^\vee$ satisfying the following conditions:

- $\mathcal{P}|_{A \times \{b\}} \in \mathrm{Pic}^0(A_b)$ for all $b \in A^\vee$;
- $\mathcal{P}|_{\{0\} \times A^\vee}$ is trivial.

We define the *dual abelian variety* $A^\vee$ and the *Poincare sheaf* $\mathcal{P}$ as a pair $(A^\vee, \mathcal{P}) \in \mathcal{A}$ satisfying the following universal property: for any pair $(T, \mathcal{L}) \in \mathcal{A}$ there exists a unique regular map $\alpha : T \to A^\vee$ such that $(1 \times \alpha)^*\mathcal{P} \simeq \mathcal{L}$.
Some important remarks:
1) Assuming the existence of the dual variety $(A^\vee, \mathcal{P})$, the universal property implies its uniqueness up to a unique isomorphism.
2) The universal property states that

$$\mathrm{Hom}(T, A^\vee) \simeq \{\mathcal{L} \in \mathrm{Pic}(A \times T) \text{ satisfying above conditions}\}$$

and applying to $T = \mathrm{Spec}K$ we obtain

$$A^\vee(K) = \mathrm{Pic}^0(A)$$

3) Finally, by the actual construction of $A^\vee$ as quotient $A/C(\mathcal{L})$ for an ample divisor $\mathcal{L}$ we have that A and $A^\vee$ have the same dimension, since $C(\mathcal{L})$ has dimension zero (see [MRM74] sections 2.7, 2.8).

0.4 Weil pairing

For every $m > 0$, the Weil pairing is a canonical nondegenerate pairing

$$e_m : A_m(\overline{K}) \times A_m^\vee(\overline{K}) \to \mu_m(\overline{K})$$

where $\mu_m(\overline{K})$ is the group of m-th roots of unity in $\overline{K}$.

Definition of Weil pairing
For simplicity, let assume K algebraically closed, so let $a \in A_m(\overline{K})$ and $a' \in A^\vee_m(\overline{K}) \subset \mathrm{Pic}^0(A)$. If a' is represented by the divisor D on A, then $m_A^* D$ is linearly equivalent to mD by the property of $\mathrm{Pic}^0(A)$. Since $a' \in A^\vee_m(\overline{K})$ then both $m_A^* D$ and mD are linearly equivalent to 0, i.e. there exist rational functions f and g on A such that $mD = (f)$ and $m_A^* D = (g)$. Since

$$\mathrm{div}(f \circ m_A) = m_A^*(\mathrm{div}(f)) = m_A^*(mD) = m(m_A^* D) = \mathrm{div}(g^m)$$

we deduce that $g^m/(f \circ m_A)$ is a constant function c on A since it has no zeros and poles. Therefore,

$$g(x+a)^m = cf(mx+ma) = cf(mx) = g(x)^m$$

which implies $g/(g \circ t_a)$ to be a function whose m-th power is 1. Since $K(A) = K$ we may identify the function with an element of $\mu_m(K)$ and we define

$$e_m(a, a') = g/(g \circ t_a).$$

From the definition follows the next lemma.

Lemma 0.4.1. *Let m, n be positive integers, then for all $a \in A_{mn}(\overline{K})$ and $a' \in A^\vee_{mn}(\overline{K})$ holds*

$$e_{mn}(a, a')^n = e_m(na, na').$$

This lemma is useful since for every prime l it allows to define a nondegenerate pairing $e_l : T_l(A) \times T_l(A^\vee) \to \mathbb{Z}_l(1)$ as

$$e_l((a_n), (a'_n)) = (e_{l^n}(a_n, a'_n))$$

where $\mathbb{Z}_p(1) = \varprojlim \mu_{l^n}(\overline{K})$ (see paragraph on cyclotomic character in section 1.1).

Chapter 1

Galois cohomology

In this chapter we compute the 0^{th} and 1^{st} Galois cohomology groups of $\mathbb{C}_p(n)$. I personally preferred to follow the exposition on [Jor12], rather than the one in [Tat67], although they are similar in most parts. I will assume the basics of p-adic number theory, whereas I will introduce the upper and lower ramification groups. For further readings on these topics see [Neu13] and [Ser13].

1.1 Generalities on Galois cohomology

We revise the definitions and basic results of Galois group cohomology. We refer to the work of Tate and his definition of continuous cohomology.

Let G be a profinite group, then we consider a topological abelian group M endowed with a continuous G-action, i.e. there is have a continuous map $G \times M \to M$ $(\sigma, m) \mapsto \sigma(m) \in M$ such that for every $m, n \in M$ and for every $\sigma, \tau \in G$

$$1_G(m) = m \qquad \sigma(m+n) = \sigma(m) + \sigma(n) \qquad \sigma(\tau(m)) = (\sigma \cdot \tau)(m)$$

We can directly define the 0^{th} and the 1^{st} cohomology groups of M with respect to G.

Definition 1.1.1. *The* 0^{th} cohomology group *of M with respect to G is the group of G-invariants:*

$$H^0(G, M) = M^G = \{m \in M : \sigma(m) = m \text{ for every } \sigma \in G\}$$

Definition 1.1.2. *The* 1^{st} cohomology group *of M with respect to G is the group*

$$H^1(G, M) = \{f : G \to M : \text{ } f \text{ continuous map s.t. } f(\sigma\tau) = \sigma(f(\tau)) + f(\sigma)\}/\sim$$

where $f \sim g$ if for some $m \in M$ we have $g(\sigma) = f(\sigma) + \sigma(m) - m$.

This definition gives rise to a group indeed, using the standard terminology, it is the group of continuous 1-*cocycles*, i.e. continuous maps $G \to M$ that satisfy the cocycle condition written above, quotient the subgroup of 1-*coboundaries*, i.e. all the maps (that are necessarily continuous) $\sigma \mapsto \sigma(m) - m$ for a certain $m \in M$.

The definition of $H^i(G, M)$ with $i > 1$ is possible in an analogous way and this construction is just a particular case of the right derived functor for the functor $(-)^G$, but this goes beyond our point of interest; Serre's book [Ser13] is recommended for a more general approach.

We know recall some tools very useful when dealing with cohomology groups.

Theorem 1.1.3. *Let $H \subset G$ be a normal subgroup of a profinite group G and let M be a topological abelian group endowed with a continuous $G-$action. Then we have the following exact sequence of groups:*

$$0 \to H^1(G/H, M^H) \xrightarrow{inf} H^1(G, M) \xrightarrow{res} H^1(H, M)^{G/H}$$

Remark 1.1.4. *The map $inf : H^1(G/H, M^H) \to H^1(G, M)$ is defined as follows: if $f \in H^1(G/H, M^H)$, then $inf(f)(g) = f(gH)$ with $g \in G$.*
The map $res : H^1(G, M) \to H^1(H, M)$ is the restriction of the domain and it's possible to define an action of G on $H^1(H, M)$ as $(g(f))(h) = g(f(g^{-1}hg))$. The cocycle condition implies that H acts trivially on $H^1(H, M)$ and moreover the image of res is G (or G/H) invariant in $H^1(H, M)$.

Theorem 1.1.5 (Hilbert 90)**.** *If L/K is a finite Galois extension, then*

$$H^1(G_{L/K}, L^\times) = 0$$
$$H^1(G_{L/K}, L) = 0$$

where $G_{L/K}$ is the Galois group associated to L/K.

Proposition 1.1.6. *If the profinite group G is procyclic, i.e. it has a dense subgroup generated by one element g, then*

$$H^0(G, M) = M^g$$
$$H^1(G, M) \cong M/(g-1)M$$

Proof. Of course, $M^G \subset M^g$ and by continuity if $m \in M^g$ then $g'(m) = m$ for every $g' \in G$.
For H^1, using the cocycle condition on $f : G \to M$ we deduce that the value of $f(g^k)$ is determined by $f(g)$. This implies that a continuous cocycle $f : G \to M$ is determined by $f(g) \in M$. A continuous cocycle is then a coboundary if $f(g) = g(m) - m = (g-1)m$ for some $m \in M$, so $H^1(G, M) \cong M/(g-1)M$. □

In general, Galois cohomology is the continuous cohomology with respect to the absolute Galois group $G_K = \mathrm{Gal}(K^{sep}/K)$, which is a profinite group, for a certain field K.

In particular, we are interested in the case K finite extension of $\mathbb{Q}_p$, so K is a complete discrete valuation field of characteristic 0 with finite residue field of characteristic $p > 0$. We consider an algebraic closure $\overline{K} = \overline{\mathbb{Q}}_p$ and its completion $\mathbb{C}_p$. The action of $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ extends by continuity to $\mathbb{C}_p$.

Cyclotomic character

For every $n \in \mathbb{N}$ we fix ζ_n a primitive p^n-adic root of 1 in $\bar{\mathbb{Q}}_p$, in a compatible way, i.e. $\zeta_{n+1}^p = \zeta_n$. Then every $\sigma \in G_K$ maps ζ_n to $\zeta_n^{x_n}$ with $x_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ compatible family, i.e. $x_{n+1} \equiv x_n \pmod{p^n}$; we define the cyclotomic character $\chi_{\text{cycl}} : G_K \to \mathbb{Z}_p^\times$ as $\chi_{\text{cycl}}(\sigma) = \{x_n\}_n \in \mathbb{Z}_p^\times$. Note that every $\{x_n\}_n \in \mathbb{Z}_p^\times$ can be identified with an element of $Gal(F_\infty/\mathbb{Q}_p)$ where F_∞ is given by $\mathbb{Q}_p$ adjoint all the p^n roots of unity.

We can then *twist* $\mathbb{C}_p$ by a power of the cyclotomic character: $\mathbb{C}_p(n)$ is the 1-dimensional $\mathbb{C}_p$ semi-linear representation $\mathbb{C}_p v$ with action of G_K defined as $\sigma(xv) =$

$\sigma(x)\chi_{\mathrm{cycl}}(\sigma)^n v$. Strictly speaking, it means that $\mathbb{C}_p(n)$ is $\mathbb{C}_p$ as vector space but the Galois action of G_K is twisted by the $n-$power of the cyclotomic character. Another way to describe $\mathbb{C}_p(n)$ is $\mathbb{C}_p(n) \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} T^{\otimes n}$ where $T = \varprojlim_{k\in\mathbb{N}} \mu_{p^k}(\overline{K})$ with the convention of taking $T^{\otimes -n}$ the dual of $T^{\otimes n}$ for positive n (remind that $\mu_{p^k}(\overline{K})$ is the group of p^n-roots in $\overline{K}$ and the natural embeddings give a projective system).

The goal of this chapter is to compute $H^0(G_K, \mathbb{C}_p(n))$ and $H^1(G_K, \mathbb{C}_p(n))$ and this computation will be key later combining it with the work of Fontaine.

1.2 Ramification and ramification groups

In this section we introduce the upper and lower ramification groups; they will help us to compute or estimate the ramification of intermediate extensions.

Definition 1.2.1 (Lower ramification groups)**.** *If L/K is a finite Galois extension, then for $u \geq -1$ the lower ramification groups are defined:*

$$G_{L/K,u} = \{\sigma \in G_{L/K} : v_L(\sigma(x) - x) \geq u + 1, \forall x \in \mathcal{O}_L\}$$

Since v_L has only integer values on L, we have $G_{L/K,u} = G_{L/K,\lceil u \rceil}$, so then we can define $G_{L/K,u}$ also as the subgroup of $G_{L/K}$ that acts trivially on $\mathcal{O}_L/\mathfrak{m}_L^{\lceil u \rceil}$ (where $\mathfrak{m}_L$ is the maximal ideal in $\mathcal{O}_L$). An element of $G_{L/K,0}$ is then trivial in $G_{l/k}$ where l, k are the residue fields. Moreover, by Galois correspondence we have that if for every $x \in \mathcal{O}_L$ and for every u we have $v_L(\sigma(x) - x) \geq u$, then it means that σ is the identity on L. We summarize these properties in the next proposition.

Proposition 1.2.2. *1. $G_{L/K,u} = G_{L/K,\lceil u \rceil}$.*

2. $G_{L/K,-1} = G_{L/K}$ and $G_{L/K,0} = I_{L_K}$ (the inertia subgroup).

3. If $u \geq u'$ then $G_{L/K,u'} \subset G_{L/K,u}$ and for $u \gg 0$ we have $G_{L/K,u} = \{1\}$.

For the definition of the upper ramification groups we need the following function.

Definition 1.2.3. *If L/K is a finite Galois extension we define $\phi_{L/K} : [-1, \infty) \to [-1, \infty)$ as*

$$\phi_{L/K}(t) = \int_0^t \frac{1}{[G_{L/K,0} : G_{L/K,u}]} du$$

Remark 1.2.4. *Using the previous proposition we see that $\phi_{L/K}$ is a piece-wise linear function of slope 1 in the interval $[-1, 0]$ and slope $1/e_{L/K} = 1/\#I_{L/K}$ for $t \gg 0$.*

Definition 1.2.5 (Upper ramification groups)**.** *For $u \geq -1$, the upper ramification groups are defined in terms of the lower ramification groups as*

$$G^u_{L/K} = G_{L/K,\phi^{-1}_{L/K}(u)}$$

We will also make use of Herbrand's theorem:

Theorem 1.2.6 (Herbrand)**.** *Let $L/M/K$ be finite Galois extensions, then*

1. $G^u_{M,K} = G^u_{L/K}/(G^u_{L/K} \cap G_{L/M})$

2. $\phi_{L/K} = \phi_{M/K} \circ \phi_{L/M}$

We denote by $\mathcal{D}_{L/K}$ the different of the finite extension L/K; then this final theorem will be the key of our computations later on.

Theorem 1.2.7. *Let L/K be a finite extension, then*

1. If I is a (fractional) ideal of L then $v_K(\mathrm{Tr}_{L/K}(I)) = \lfloor v_K(I\mathcal{D}_{L/K})\rfloor$

2. If L/K is Galois,

$$v_L(\mathcal{D}_{L/K}) = \int_{-1}^{\infty}(\#G_{L/K,u} - 1)du \qquad v_K(\mathcal{D}_{L/K}) = \int_{-1}^{\infty}(1 - \frac{1}{\#G^u_{L/K}})du$$

Proof. 1. We prove that $v_K(\mathrm{Tr}_{L/K}(I)) \geq n$ if and only if $v_K(I\mathcal{D}_{L/K}) \geq n$ and the result follows from the fact that $\mathrm{Tr}_{L/K}(I) \subset K$ whereas $I\mathcal{D}_{L/K} \subset L$.

$$v_K(\mathrm{Tr}_{L/K}(I)) \geq n \iff \mathrm{Tr}_{L/K}(I)\mathfrak{m}_K^{-n} \subset \mathcal{O}_K \iff \mathrm{Tr}_{L/K}(I\mathfrak{m}_K^{-n}) \subset \mathcal{O}_K \iff$$
$$\iff I\mathfrak{m}_K^{-n} \subset \mathcal{D}^{-1}_{L/K} \iff v_K(I) - n \geq v_K(\mathcal{D}^{-1}_{L/K}) \iff v_K(I\mathcal{D}_{L/K}) \geq n$$

where we used the definition of the inverse different $\mathcal{D}^{-1}_{L/K} = \{x \in L : \mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subset \mathcal{O}_K\}$.

2. First we observe that the RHS is finite since $\#G_{L/K,u} = 1$ for u big enough. Secondly, the equation on $v_L(\mathcal{D}_{L/K})$ is derived directly from the one on $v_K(\mathcal{D}_{L/K})$ with the substitution $u = \phi^{-1}_{L/K}(t)$, so we are proving only the first equation.

We are in the case K and L finite extensions of $\mathbb{Q}_p$. This means that $\mathcal{O}_L = \mathcal{O}_K(x)$ for some element $x \in \mathcal{O}_L$; if we denote with $f(X)$ the minimal polynomial of x, then $\mathcal{D}_{L/K}$ is generated by $f'(x)$. Now,

$$f(X) = \prod_{\sigma \in G_{L/K}} (X - \sigma(x)) \Longrightarrow f'(x) = \prod_{\sigma \in G_{L/K}, \sigma \neq 1} (x - \sigma(x))$$

So we get $v_L(\mathcal{D}_{L/K}) = \sum_{\sigma \neq 1} v_L(x - \sigma(x))$. The last step is to observe that $\sigma \in G_{L/K,u} \iff v_L(x - \sigma(x)) \geq u + 1$. This implies that

$$\sum_{\sigma : v_L(x-\sigma(x))=n} v_L(x - \sigma(x)) = n(\#G_{L/K,n-1} - \#G_{L/K,n})$$

So denoting with N the maximum of $v_L(x - \sigma(x))$ for $\sigma \neq 1$, we get

$$\begin{aligned}
\sum_{\sigma \neq 1} v_L(x - \sigma(x)) &= \sum_{n=0}^{N} n(\#G_{L/K,n-1} - \#G_{L/K,n}) \\
&= \left(\sum_{n=0}^{N-1} \#G_{L/K,n}\right) - N\#G_{L/K,N} \\
&= \sum_{n=0}^{N-1}(\#G_{L/K,n} - 1) \\
&= \int_{-1}^{\infty}(\#G_{L/K,u} - 1)du
\end{aligned}$$

since $\#G_{L/K,N} = 1$ by assumption on N.

□

1.3 Ax–Sen–Tate Lemma

In this section, we will prove the Ax–Sen–Tate Lemma that will play an important role in computing $H^0(G_K, \mathbb{C}_p(n))$ and $H^1(G_K, \mathbb{C}_p(n))$. We first need a lemma on the valuation of roots of polynomials and thus a lemma on the approximations of algebraic numbers.

Lemma 1.3.1. *Let $f \in \overline{\mathbb{Q}}_p[x]$ be a monic polynomial of degree n such that every root has valuation $\geq u$, then we have:*

1. *If $n = p^k n_0$ with $p \nmid n_0$ then $f^{(p^k)}$ has a root β with $v(\beta) \geq u$.*
2. *If $n = p^{k+1}$ then $f^{(p^k)}$ has a root β with $v(\beta) \geq u - \frac{v(p)}{p^k(p-1)}$*

Proof. We write $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$. We remind that the opposite of the slopes of the Newton polygon associated to f are the valuations of the roots of f (counted with multiplicity). This implies that all slopes are $\leq -u$ so $v(a_n) \geq iu$ for every $0 \leq i \leq n-1$. We write $q = p^k$, then

$$\frac{f^{(q)}}{q!} = \sum_{i=0}^{n-q} \binom{n-i}{q} a_{n-i} X^{n-i-q}$$

So the product of the roots of $f^(q)$ is $\pm a_q / \binom{n}{q}$, thus

$$\sum_{\beta \text{ root of } f^{(q)}} v(\beta) = v(a_q) - v\left(\binom{n}{q}\right)$$

so there exists a root β such that

$$v(\beta) \geq \frac{v(a_q)}{n-q} - \frac{1}{n-q} v\left(\binom{n}{q}\right) \geq u - \frac{1}{n-q} v\left(\binom{n}{q}\right)$$

. To conclude we need to notice that

$$v\left(\binom{n}{q}\right) = \begin{cases} 0 & \text{if } n = p^k n_0 \\ v(p) & \text{if } n = p^{k+1} \end{cases}$$

since $v(n-m) = v(m)$ for every $m < q$ in both cases, whereas $v(q) = v(n)$ in the first case and $v(q) + 1 = v(n)$ in the second case.

□

Now we prove a lemma about approximation of algebraic numbers. If $\alpha \in \overline{K}$, we define $\Delta_K(\alpha) = \min v(\sigma(\alpha) - \alpha)$ with $\sigma \in G_{K(\alpha)/K}$.

Lemma 1.3.2. *Let $K/\mathbb{Q}_p$ finite extension and let $\alpha \in \overline{K}$. Then there exists $\beta \in K$ such that*

$$v(\alpha - \beta) \geq \Delta_K(\alpha) - \frac{v(p)}{(p-1)^2}$$

Proof. We will show a stronger statement:

$$v(\alpha - \beta) \geq \Delta_K(\alpha) - \sum_{i=1}^{\lfloor log_p n \rfloor} \frac{v(p)}{(p-1)p^{i-1}}$$

where $n = [K(\alpha) : K] = \deg Q$ with Q minimal polynomial of α over K. We are going to show this by induction on n; the case $n = 1$ is trivial since we can choose $\alpha = \beta$.

The inductive step is the following. Let $P(X) = Q(X + \alpha)$ which has roots $\sigma(\alpha) - \alpha$ for $\sigma \in G_{K(\alpha)/K}$, so we get that all roots of $P(X)$ have valuation $\geq \Delta_K(\alpha)$. We write $n = p^k n_0$ or $n = p^{k+1}$ and $q = p^k$ as in the previous lemma. Thus we get a root $\tilde{\beta}$ of $P^{(q)}$ such that

$$v(\tilde{\beta}) \geq \begin{cases} \Delta_K(\alpha) & n = p^k n_0 \\ \Delta_K(\alpha) - \frac{v(p)}{p^k(p-1)} & n = p^{k+1} \end{cases}$$

Let $\beta = \tilde{\beta} + \alpha$ so that β is a root of $Q^{(q)}$ such that $v(\beta - \alpha) = v(\tilde{\beta})$. Now,

$$\begin{aligned} v(\sigma(\beta) - \beta) =& v(\sigma(\beta) - \sigma(\alpha) + \sigma(\alpha) - \alpha + \alpha - \beta) \geq \\ & \geq \min\{v(\sigma(\beta) - \sigma(\alpha)), v(\sigma(\alpha) - \alpha), v(\alpha - \beta)\} \geq \\ & \geq \min\{\Delta_K(\alpha), v(\alpha - \beta)\} \end{aligned} \tag{1.1}$$

so we get

$$\Delta_K(\beta) \geq \begin{cases} \Delta_K(\alpha) & n = p^k n_0 \\ \Delta_K(\alpha) - \frac{v(p)}{p^k(p-1)} & n = p^{k+1} \end{cases}$$

We can use the inductive hypothesis on $Q^{(q)}$ of degree $n - q$ to find a $\gamma \in K$ such that

$$v(\beta - \gamma) \geq \Delta_K(\beta) - \sum_{i=1}^{\lfloor log_p(n-q) \rfloor} \frac{v(p)}{(p-1)p^{i-1}}$$

Finally we notice that in the case $n = p^k n_0$ we have $\lfloor \log_p(n-q) \rfloor = k + \lfloor \log_p(n_0 - 1) \rfloor = k + \lfloor \log_p n_0 \rfloor = \lfloor \log_p n \rfloor$ so we get

$$v(\beta - \gamma) \geq \Delta_K(\alpha) - \sum_{i=1}^{\lfloor \log_p n \rfloor} \frac{v(p)}{(p-1)p^{i-1}}$$

whereas if $n = p^{k+1}$, then $\lfloor log_p(n - q) \rfloor = k$ while $\lfloor log_p n \rfloor = k + 1$, so

$$v(\beta - \gamma) \geq \Delta_K(\alpha) - \frac{v(p)}{p^k(p-1)} - \sum_{i=1}^{k} \frac{v(p)}{p^{i-1}(p-1)} = \Delta_K(\alpha) - \sum_{i=1}^{k+1} \frac{v(p)}{p^{i-1}(p-1)}$$

We conclude since $v(\alpha - \gamma) = v(\alpha - \beta + \beta - \gamma) \geq \min\{v(\alpha - \beta), v(\beta - \gamma)\} = v(\beta - \gamma)$ □

We can state and prove the Ax–Sen–Tate lemma:

Theorem 1.3.3 (Ax–Sen–Tate). *Let L/K be an algebraic extension. Then $\mathbb{C}_p^{G_L} = \hat{L}$. In particular, if L/K is finite then $\mathbb{C}_p^{G_L} = L$.*

Proof. Let v be a valuation on L and let $x \in \mathbb{C}_p^{G_L}$. We can then choose $\alpha_n \in \overline{\mathbb{Q}_p}$ such that $x = \lim_{n \to \infty} \alpha_n$. For $\sigma \in G_L$ we have

$$v(\sigma(\alpha_n) - \alpha_n) = v(\sigma(\alpha_n - x) - (\alpha_n - x)) \geq \min v(\sigma(\alpha_n - x), v(\alpha_n - x)) = v(\alpha_n - x)$$

so we get $\Delta_L(\alpha_n) \geq v(\alpha_n - x)$. Using Lemma 1.3.2 we can choose $\beta_n \in L$ such that $v(\beta_n - \alpha_n) \geq \Delta_L(\alpha_n) - \frac{v(p)}{(p-1)^2}$; this implies

$$v(x - \beta_n) = v(x - \alpha_n + \alpha_n - \beta_n) \geq \min v(x - \alpha_n), v(\alpha_n - \beta_n) \geq$$

$$\geq \min v(x - \alpha_n), \Delta_L(\alpha_n) - \frac{v(p)}{(p-1)^2} \geq v(x - \alpha_n) - \frac{v(p)}{(p-1)^2}$$

so we deduce that $\lim\limits_{n\to\infty} \beta_n = x$ as well, so $x \in \hat{L}$.

On the other hand, if $x \in \hat{L}$, then $x = \lim \beta_n$ for some $\beta_n \in L$. The action of G_L is continuous so for $\sigma \in G_L$ we get $\sigma(x) = \sigma(\lim \beta_n) = \lim \sigma(\beta_n) = \lim \beta_n = x$ since β_n are invariant under the action of G_L. □

1.4 Cyclotomic extensions and ramification estimates

Let $F = \mathbb{Q}_p$ and K/F a finite extension; we define $K_n = K(\zeta_n)$ (where ζ_n is a primitive p^n-adic root of unity over K) and K_∞ the minimal field that contains every K_n. Analogously we define $F_n = \mathbb{Q}_p(\zeta_n)$ and F_∞. We call $\Gamma_K = G_{K_\infty/K}$, $\Gamma_{K_n} = G_{K_\infty/K_n}$, $H_K = G_{K_\infty}$, that is kerχ_{cycl}. We use the similar notation for F recalling that $\Gamma_F \cong \mathbb{Z}_p^\times$, $\Gamma_{F_n} \cong 1 + p^n\mathbb{Z}_p$ with $G_{F_n/F} \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$. This is summarized in the following diagram of Galois extensions:

$$\begin{tikzcd}
\overline{\mathbb{Q}_p} \arrow[r, dash] \arrow[d, dash, "H_K"'] & \overline{\mathbb{Q}_p} \arrow[d, dash, "H_F"] \\
K_\infty \arrow[r, dash] \arrow[d, dash, "\Gamma_{K_n}"'] \arrow[dd, dash, bend right=60, "\Gamma_K"'] & F_\infty \arrow[d, dash, "1+p^n\mathbb{Z}_p"] \arrow[dd, dash, bend left=60, "\mathbb{Z}_p^\times"] \\
K_n \arrow[r, dash] \arrow[d, dash] & F_n \arrow[d, dash, "(\mathbb{Z}/p^n\mathbb{Z})^\times"] \\
K \arrow[r, dash] & F
\end{tikzcd}$$

In this section our goal is to study the relation between the cyclotomic extension of K and the cyclotomic extension of $F = \mathbb{Q}_p$ and this will provide us some estimates of the ramification of K_n/F_n with the help of the upper ramification filtration groups.

We begin with a lemma on the cyclotomic extensions.

Lemma 1.4.1. *1. The cyclotomic character factors as $G_K \twoheadrightarrow \Gamma_K \hookrightarrow \Gamma_F \cong \mathbb{Z}_p^\times$, so we just think χ_{cycl} as the embedding $\Gamma_K \hookrightarrow \Gamma_F$.*

2. There exists an integer n_K such that $1 + p^{n_K}\mathbb{Z}_p \subset \chi_{\text{cycl}}(\Gamma_K)$

3. For $n \geq n_K$ we have $\chi_{\text{cycl}}(\Gamma_{K_n}) \cong 1 + p^n\mathbb{Z}_p$ and $K_n \cap F_\infty = F_n$.

Proof. 1. We have already mentioned that ker$\chi_{\text{cycl}} = H_K$, so we consider $\chi_{\text{cycl}} : \Gamma_K \to \mathbb{Z}_p^\times$ and notice that this is compatible with the isomorphism $\Gamma_F \cong \mathbb{Z}_p^\times$, i.e. $\chi_{\text{cycl}} : \Gamma_K \to \Gamma_F$ is given by the restriction to F_∞. Now this map is injective since if $g \in \Gamma_K$ is nontrivial, then g doesn't map ζ_n to itself for some $n \in \mathbb{N}$. This implies that $g|_{F_\infty}$ is not trivial. So we have the embedding $\chi_{\text{cycl}} : \Gamma_K \to \Gamma_F$.

2. First, χ_{cycl} is continuous since maps $\Gamma_{K_n} \to \Gamma_{F_n}$ and since Γ_K is a profinite group, we get $\chi_{\text{cycl}}(\Gamma_K)$ is compact. We consider the logarithm $log : 1 + p^2\mathbb{Z}_p \to p^2\mathbb{Z}_p$, which is a continuous homomorphism so by continuity we get $log(\chi_{\text{cycl}}(\Gamma_K) \cap (1+p^2\mathbb{Z}_p))$ is the image of a compact inside the closed $p^2\mathbb{Z}_p$, so it is closed and thus open as well (again because working in $\mathbb{Z}_p$ that is profinite). The logarithm is also invertible so $\chi_{\text{cycl}}(\Gamma_K) \cap (1 + p^2\mathbb{Z}_p)$ is an open subgroup in $\mathbb{Z}_p^\times$ so it contains some $1 + p^{n_K}\mathbb{Z}_p$.

3. We want to prove that for $n \geq n_K$ we have $\chi_{\text{cycl}}(\Gamma_{K_n}) = 1 + p^n\mathbb{Z}_p \cong \Gamma_{F_n}$. Indeed, the injection $\Gamma_K \hookrightarrow \Gamma_F$ gives an injection $\Gamma_{K_n} \hookrightarrow \Gamma_{F_n}$; moreover, Γ_K surjects onto Γ_{F_n} by part two. To conclude we notice that if $g \in \Gamma_K$ is mapped to an element of Γ_{F_n} it must fix ζ_{p^n}, so $g \in \Gamma_{K_n}$, so $\Gamma_{K_n} \cong \Gamma_{F_n}$ since we have surjectivity and injectivity, both given by χ_{cycl}.

   Finally, $K_n \cap F_\infty = F_\infty^{\Gamma_{K_n}} = F_\infty^{\Gamma_{F_n}} = F_n$ for $n \geq n_K$.

□

Remark 1.4.2. *We remind that $\Gamma_K = G_{K_\infty/K} = \varprojlim G_{K_n/K}$ where $G_{K_n/K} \leq G_{F_n/F}$ and since $G_{F_n/F} \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic ($p > 2$), then Γ_K is procyclic, i.e. there exists $\gamma \in \Gamma_K$ such that $\langle\gamma\rangle$ is dense in Γ_K. We will call γ the topological generator of Γ_K.*

Using the study of the Galois groups of the cyclotomic extensions of K and F we can now compare their upper ramification filtrations, keeping the same assumptions ($F = \mathbb{Q}_p$ and K/F finite).

Lemma 1.4.3. *1. For $n \geq n_K$ the extension K_{n+1}/K_n is totally ramified of degree p.*

2. The index $[K_n : F_n]$ is decreasing and if K/F is Galois, then $G_{K_n/F_n} = G_{K_\infty/F_\infty}$ for n big enough.

3. If K/F is a Galois extension, there exists u_K such that if $n \geq n_K$ and $u \geq u_K$ then $G^u_{K_n/F_{n_K}} \cong G^u_{F_n/F_{n_K}}$.

Proof. 1. For $n \geq n_K$, using Lemma 1.4.1, we have

$$\begin{aligned}
G_{K_{n+1}/K_n} &\cong G_{F_{n+1}/F_n} \\
&= I_{F_{n+1}/F_n} \\
&= \{g \in G_{F_{n+1}/F_n} : v(g(x) - x) > 0 \text{ for every } v(x) \geq 0\} \\
&= \{g \in G_{K_{n+1}/K_n} : v(g(x) - x) > 0 \text{ for every } v(x) \geq 0\} \\
&= I_{K_{n+1}/K_n}
\end{aligned}$$

where the second line follows since F_{n+1}/F_n is totally ramified of degree p and the fourth line follows because actually both defining conditions are equivalent to $v(g(\zeta_{n+1} - \zeta_{n+1}) > 0$. Thus the extension K_{n+1}/K_n is totally ramified of degree p.

2. We simply have $[K_n : F_n] = [KF_n : FF_n]$ bounded by $[K : F]$ and decreasing, so it must stabilise to $[K_\infty : F_\infty]$.

3. We can define u_K such that $G^{u_K}_{K_{n_K}/F_{n_K}} = \{1\}$ by proposition 1.2.2. By lemma 1.4.1 we have for $n \geq n_K$ that $K_n \cap F_\infty = F_n$ so $G_{K_n/F_{n_K}} \cong G_{K_n/K_{n_K}} \times G_{K_{n_K}/F_{n_K}} \cong G_{F_n/F_{n_K}} \times G_{K_{n_K}/F_{n_K}}$.

Using Herbrand's Theorem for $u \geq u_K$ we have that $G^u_{K_{n_K}/F_{n_K}} \cong G^u_{K_n/F_{n_K}}/(G^u_{K_n/F_{n_K}} \cap G^u_{K_n/K_{n_K}})$ and since $G^u_{K_{n_K}/F_{n_K}} = \{1\}$ then $G^u_{K_n/F_{n_K}} \hookrightarrow G_{K_n/K_{n_K}} \cong G_{F_n/F_{n_K}}$. Applying Herbrand's Theorem again, we get $G^u_{F_n/F_{n_K}} \cong G^u_{K_n/F_{n_K}}/(G^u_{K_n/F_{n_K}} \cap G_{F_n/F_n})$, so $G^u_{K_n/F_{n_K}} \twoheadrightarrow G^u_{F_n/F_{n_K}} \subset G_{F_n/F_{n_K}}$. We already have $G^u_{K_n/F_{n_K}} \hookrightarrow G_{F_n/F_{n_K}}$ that implies $G^u_{K_n/F_{n_K}} \hookrightarrow G^u_{F_n/F_{n_K}}$ by the same argument of part one. Combining the two arguments, we get $G^u_{K_n/F_{n_K}} \cong G^u_{F_n/F_{n_K}}$.

□

Before applying these lemmas to estimate the ramification of the cyclotomic extensions of K, we need to revise the case of the cyclotomic extensions of $F = \mathbb{Q}_p$. In the next proposition we will denote with $G(n)$ the Galois group of the totally ramified extension F_n/F so that $G(n) = (\mathbb{Z}/p^n\mathbb{Z})^\times$; moreover, we remind that $\zeta_n - 1$ is a uniformizer for F_n. To determine the ramification groups we define, for $0 \leq m \leq n$, the subgroup $G(n)^m$ consisting of the elements of $G(n)$ that are $\equiv 1 \pmod{p^m}$. In this way $G(n)^m = G_{F_n/F_m}$ since the automorphism corresponding to $a \in G(n)^m$ maps ζ_m to $\zeta_m^a = \zeta_m$ since $a \equiv 1 \pmod{p^m}$.

Proposition 1.4.4. *The lower ramification groups for F_n/F are:*

$$\begin{aligned}
&G_0 = G(n) && \\
&G_u = G(n)^1 && \textit{if } 1 \leq u \leq p-1 \\
&G_u = G(n)^2 && \textit{if } p \leq u \leq p^2-1 \\
&\dots && \dots \\
&G_u = G(n)^n = \{1\} && \textit{if } p^{n-1} \leq u
\end{aligned}$$

Thus, for every $n \in \mathbb{N}$ and $u \geq -1$ we have $G^u_{F_n/F} = G_{F_n/F_{\lfloor u \rfloor}}$.

Proof. Let a be an element of $G(n)$ and let σ the corresponding element in the Galois group. Let m be the largest integer such that $a \equiv 1 \pmod{p^m}$; this means that $a \in G(n)^m$ and $a \notin G(n)^{m+1}$. We have already mentioned that $\sigma \in G_u$ if and only if $v_{F_n}(\sigma(\zeta_n) - \zeta_n) \geq u+1$, so then:

$$v_{F_n}(\sigma(\zeta_n) - \zeta_n) = v_{F_n}(\zeta_n^a - \zeta_n) = v_{F_n}(\zeta_n^{a-1} - 1)$$

Using our assumption on a, we have that ζ_n^{a-1} is a primitive root of unity of order p^{n-m}, so $\zeta_n^{a-1} - 1$ is a uniformizer of F_{n-m} and we get

$$v_{F_n}(\zeta_n^{a-1} - 1) = [K_{p^n} : K_{p^{n-m}}] = \phi(p^n)/\phi(p^{n-m}) = p^m$$

that provides the characterization of the lower ramification groups as in the statement.

We know now that the jumps in the lower filtration happen when $u = p^m - 1$ with $0 \leq m \leq n-1$. Then if we prove that $\phi_{F_n/F}(p^m - 1) = m$, the upper ramification groups are as stated, since $G(n)^m$ is G_{F_n/F_m} as explained before the statement.

$$\phi_{F_n/F}(p^m - 1) = \int_0^{p^m-1} \frac{1}{[G_0 : G_t]} dt = \sum_{i=1}^{m} \frac{(p^i - p^{i-1})}{[G(n) : G(n)^i]} = \sum_{i=0}^{m} \frac{(p^i - p^{i-1})p^{n-i}}{\phi(p^n)} = m$$

□

Finally we can estimate the valuation of the relative different $\mathcal{D}_{K_n/F}$:

Lemma 1.4.5. *1. The sequence $\{p^n v_p(\mathcal{D}_{K_n/F_n})\}$ is bounded.*

2. *There exists a constant c and a bounded sequence a_n such that*
$$v_p(\mathcal{D}_{K_n/F}) = n + c + \frac{a_n}{p^n}$$

Proof. We first assume that K/F is a finite Galois extension and then we will derive the result for finite extension.

1. Assuming $n \geq n_K$ we have:
$$\begin{aligned} v_p(\mathcal{D}_{K_n/F_n}) &= v_p(\mathcal{D}_{K_n/F_{n_K}}) - v_p(\mathcal{D}_{F_n/F_{n_K}}) \\ &= \frac{1}{e_{F_{n_K}/F}} \int_{-1}^{\infty} \left(\frac{1}{\#G^u_{F_n/F_{n_K}}} - \frac{1}{\#G^u_{K_n/F_{n_K}}} \right) du \\ &= \frac{1}{e_{F_{n_K}/F}} \int_{-1}^{u_K} \left(\frac{1}{\#G^u_{F_n/F_{n_K}}} - \frac{1}{\#G^u_{K_n/F_{n_K}}} \right) du \\ &\leq \frac{1}{e_{F_{n_K}/F}} \int_{-1}^{u_K} \frac{1}{\#G^u_{F_n/F_{n_K}}} du \end{aligned}$$
where we used Theorem 1.2.7 and that, for $u \geq u_K$, $G^u_{K_n/F_{n_K}} \cong G^u_{F_n/F_{n_K}}$. Now using that $G_{F_n/F_{n_K},v} = G_{F_n/F,v} \cap G_{F_n/F_{n_K}}$ and that $G_{F_n/F,v} = G^{\phi_{F_n/F}(v)}_{F_n/F} = G_{F_n/F,v} = G_{F_n/F_{\lfloor \phi_{F_n/F}(v) \rfloor}}$ for proposition 1.4.4, we get
$$G^u_{F_n/F_{n_K}} = G_{F_n/F_{n_K}, \phi^{-1}_{F_n/F_{n_K}}(u)} = G_{F_n/F_{\lfloor \phi_{F_n/F} \circ \phi^{-1}_{F_n/F_{n_K}}(u) \rfloor}} \cap G_{F_n/F_{n_K}}$$
To conclude we use that $\phi_{F_n/F} = \phi_{F_{n_K}/F} \circ \phi_{F_n/F_{n_K}}$ by Herbrand's Theorem. Thus
$$G^u_{F_n/F_{n_K}} = G_{F_n/F_{\lfloor \phi_{F_{n_K}/F}(u) \rfloor}} \cap G_{F_n/F_{n_K}} = G_{F_n/F_{max(\lfloor \phi_{F_{n_K}/F}(u) \rfloor, n_K)}}$$
so $\#G^u_{F_n/F_{n_K}} = p^{n - max(\lfloor \phi_{F_{n_K}/F}(u) \rfloor, n_K)}$ and the integral becomes:
$$p^n v_p(\mathcal{D}_{K_n/F_n}) \leq \frac{1}{e_{F_{n_K}/F}} \int_{-1}^{u_K} p^{max(\lfloor \phi_{F_{n_K}/F}(u) \rfloor, n_K)} du$$
and the right hand side is independent of n so $p^n v_p(\mathcal{D}_{K_n/F_n})$ bounded.

2. The result follows from $v_p(\mathcal{D}_{K_n/F}) = v_p(\mathcal{D}_{K_n/F_n}) + v_p(\mathcal{D}_{F_n/F})$ and the explicit calculation of $v_p(\mathcal{D}_{F_n/F})$, using lemma 1.4.3 and that $\#G_{F_n/F_i} = p^{n-i}$ for $i > 0$:
$$\begin{aligned} v_p(\mathcal{D}_{F_n/F}) &= \int_{-1}^{\infty} \left(1 - \frac{1}{\#G_{F_n/F_{\lfloor u \rfloor}}} \right) du \\ &= \sum_{i=0}^{n} \left(1 - \frac{1}{\#G_{F_n/F_i}} \right) \\ &= 1 - \frac{1}{p^{n-1}(p-1)} + \sum_{i=1}^{n} (1 - p^{i-n}) \\ &= 1 - \frac{1}{p^{n-1}(p-1)} + n - \frac{p^n - 1}{p^{n-1}(p-1)} \\ &= n - \frac{1}{p-1} \end{aligned}$$
Indeed, now we can assign $c = -\frac{1}{p-1}$ and $a_n = p^n v_p(\mathcal{D}_{K_n/F_n})$ to satisfy $v_p(\mathcal{D}_{K_n/F}) = n + c + a_n p^{-n}$ with a_n bounded.

Finally the case K/F finite. We consider L the normal closure of K over F. Then the lemma applies to L so we get

$$v_p(\mathcal{D}_{L_n/F}) = n + c + \frac{a_n}{p^n}$$

Since $v_p(\mathcal{D}_{L_n/F}) = v_p(\mathcal{D}_{L_n/K_n}) + v_p(\mathcal{D}_{K_n/F})$ we just need to prove that $v_p(\mathcal{D}_{L_n/K_n})$ is definitely constant. If $\mathcal{O}_L = \mathcal{O}_K(x)$, then $\mathcal{O}_{L_n} = \mathcal{O}_{K_n}(x)$, so $\mathcal{O}_{L_\infty} = \mathcal{O}_{K_\infty}(x)$. This implies that, for n big enough, the minimal polynomial of x over K_n is also the minimal polynomial over K_∞. Then for n big enough we have $v_p(\mathcal{D}_{L_n/K_n}) = v_p(F'(x))$, where $F(X)$ is the minimal polynomial of x over K_∞.

□

1.5 Galois cohomology of $\widehat{K_\infty}$

In this section, we compute the first cohomology group of $\mathbb{C}_p$ with respect of $H_K = G_{K_\infty}$ and later this will result into an inflation-restriction sequence.

Theorem 1.5.1. *Let $L/K/\mathbb{Q}_p$ be finite extensions, then $\mathfrak{m}_{K_\infty} \subset \mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})$.*

Proof. For $n \geq \max(n_K, n_L)$ we know that $L_n = LF_n$ and $K_n = KF_n$, so $G_{L_n/K_n} = G_{L_\infty/K_\infty}$ for $n \geq c_{L,K}$ for some constant $c_{L,K} \geq \max(n_K, n_L)$. Thus for $n \geq c_{L,K}$,

$$\mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_n}) = \mathrm{Tr}_{L_n/K_n}(\mathfrak{m}_{L_n}) = \mathfrak{m}_{K_n}^{c_n}$$

where we can compute the exponent c_n thanks to Theorem 1.2.7:

$$c_n = \lfloor v_{K_n}(\mathfrak{m}_{L_n}\mathcal{D}_{L_n/K_n})\rfloor = \lfloor v_{K_n}(\mathfrak{m}_{L_n}) + e_{K_n/F}v_p(\mathcal{D}_{L_n/K_n})\rfloor =$$

$$= \lfloor e_{L_n/K_n} + e_{K_n/F_n}e_{F_n/F}(v_p(\mathcal{D}_{L_n/F}) - v_p(\mathcal{D}_{K_n/F}))\rfloor$$

Now for $n \geq c_{L,K}$ we have $e_{L_n/K_n} \leq [L_n : K_n] \leq [L : K]$ and $e_{K_n/F_n} \leq [K_n : F_n] \leq [K : F]$ and $e_{F_n/F} = p^{n-1}(p-1)$ since F_n/F is totally ramified of degree $\phi(p^n) = p^{n-1}(p-1)$. Using lemma 1.4.5, we have $v_p(\mathcal{D}_{L_n/F}) - v_p(\mathcal{D}_{K_n/F}) = c' + a_n p^{-n}$ with a_n bounded, so c_n is bounded by some constant c. Summing up, $\mathfrak{m}_{K_n}^c \subset \mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})$ for all n.

Let $x \in \mathfrak{m}_{k_\infty}$ and let $x \in \mathfrak{m}_{K_m}$ for some m. Since e_{K_n/K_m} is unbounded for $n \gg m$, then we can choose n such that $e_{K_n/K_m} > c$ so $x \in \mathfrak{m}_{K_m} \subset \mathfrak{m}_{K_n}^c \subset \mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty})$. □

Corollary 1.5.2. *Let $K/\mathbb{Q}_p$ be a finite extension, then*

1. *Every finite extension of K_∞ is of the form $L_\infty = LK_\infty$ for a finite extension L/K.*

2. *If L/K is finite, then there exists $\alpha \in L_\infty$ such that $\mathrm{Tr}_{L_\infty/K_\infty}(\alpha) = 1$ and $v(\alpha) > -v(\pi_K)$ where π_K is the uniformizer for K.*

Proof.
1. Let L_∞ be a finite extension of K_∞, then it is a simple extension since it's finite and the characteristic of K is zero. Let $L_\infty = K_\infty(\beta)$ and $P(X)$ the minimal polynomial of β over K_∞. Since every coefficient of $P(X)$ is an element of K_n for some finite n, then β is algebraic over some K_n for n big enough. Thus β is algebraic over K, so $L = K(\beta)$ is a finite extension that gives $L_\infty = LK_\infty$.

2. Theorem 1.5.1 yields $\alpha' \in \mathfrak{m}_{L_\infty}$ such that $v(\alpha') > 0$ and $\mathrm{Tr}_{L_\infty/K_\infty}(\alpha') = \pi_K$. Then $\alpha = \alpha'/\pi_K$ satisfies our request since $\mathrm{Tr}_{L_\infty/K_\infty}(\alpha) = 1$ and $v(\alpha) > -v(\pi_K)$ by our choice of α'.

□

Lemma 1.5.3. *If $M \in H^1(H_K, p^n\mathcal{O}_{\mathbb{C}_p})$, then there exists $x \in p^{n-1}\mathcal{O}_{\mathbb{C}_p}$ such that the map $g \mapsto M(g) + g(x) - x \in H^1(H_K, p^{n+1}\mathcal{O}_{\mathbb{C}_p})$.*

Proof. Since $p^{n+2}\mathcal{O}_{\mathbb{C}_p}$ is open in $p^n\mathcal{O}_{\mathbb{C}_p}$, using continuity of $M : H_K \to p^n\mathcal{O}_{\mathbb{C}_p}$ we have $H' = M^{-1}(p^{n+2}\mathcal{O}_{\mathbb{C}_p})$ open subset of H_K. Now H' must contain $G_{L'}$ where L' is a finite extension of K_∞. By corollary 1.5.2, then $G_{L'} = H_L$, i.e. $L' = L_\infty = LK_\infty$, where L/K is a finite extension, and increasing L (so decreasing H_L) we can assume that L/K is a Galois extension and that $M(H_L) \subset p^{n+2}\mathcal{O}_{\mathbb{C}_p}$.
From corollary 1.5.2 let $\alpha \in L_\infty$ such that $\mathrm{Tr}_{L_\infty/K_\infty}(\alpha) = 1$ and $v(\alpha) > -v(\pi_K) > v(p)$. We fix a set $T = \{t_1, t_2, \dots, t_m\}$ of representatives of H_K/H_L in H_K, where T is finite since $\#T = \#G_{L_\infty/K_\infty}$. We define

$$x_T = \sum_i t_i(\alpha)M(t_i)$$

For $g \in H_K$ and $gT = \{gt_i : t_i \in T\}$ then we can compute $g(x_T)$ using the cocycle condition for M:

$$\begin{aligned} g(x_T) &= g\Big(\sum_i t_i(\alpha)M(t_i)\Big) \\ &= \sum_i (gt_i)(\alpha)g(M(t_i)) \\ &= \sum_{iT} (gt_i)(\alpha)(M(gt_i) - M(g)) \\ &= \sum_i (gt_i)(\alpha)M(gt_i) - \Big(\sum_i (gt_i)(\alpha)\Big)M(g) \\ &= x_{gT} - M(g) \end{aligned}$$

where at the end we used that $\sum_i (gt_i)(\alpha) = \mathrm{Tr}_{L_\infty/K_\infty}(\alpha) = 1$ since gT is another set of representatives of $H_K/H_L \cong G_{L_\infty/K_\infty}$. Moreover, we have $gt_i = h_i t_{j_i}$ where $h_i \in H_L$ and j_i is a permutation of $\{1, 2, \dots, m\}$. Thus

$$\begin{aligned} x_{gT} - x_T &= \sum_i (gt_i)(\alpha)M(gt_i) - x_T \\ &= \sum_i (h_i t_{j_i})(\alpha)M(h_i t_{j_i}) - x_T \\ &= \sum_i (t_{j_i} t_{j_i}^{-1} h_i t_{j_i})(\alpha)M(t_{j_i} t_{j_i}^{-1} h_i t_{j_i}) - x_T \\ &= \sum_i t_{j_i}(\alpha)[M(t_{j_i}) + t_{j_i}(M(t_{j_i}^{-1} h_i t_{j_i}))] - x_T \\ &= \sum_i t_{j_i}(\alpha)t_{j_i}(M(t_{j_i}^{-1} h_i t_{j_i})) \end{aligned}$$

where in the third line we use $t_{j_i}^{-1} h_i t_{j_i} \in H_L$ since H_L is normal in H_K, so it acts trivially on $\alpha \in L_\infty$ and in the fourth line we use that t_{t_j} is a permutation so x_T simplifies.

Finally, since $v(\alpha) > -v(p)$ and $M(t_{j_i}^{-1} h_i t_{j_i}) \in p^{n+2}\mathcal{O}_{\mathbb{C}_p}$ we get $x_{gT} - x_T \in p^{n+1}\mathcal{O}_{\mathbb{C}_p}$ for every $g \in H_K$, so $M(g) + g(x_T) - x_T = x_{gT} - x_T \in p^{n+1}\mathcal{O}_{\mathbb{C}_p}$ as wanted. □

Remark 1.5.4. *Note that $g \mapsto M(g)$ and $g \mapsto M(g) + g(x) - x$ are equivalent cocycles so they represent the same element in the first cohomology group $H^1(H_K, \mathbb{C}_p)$.*

Theorem 1.5.5. *We have $H^1(H_K, \mathbb{C}_p) = \{1\}$.*

Proof. Let $M \in H^1(H_K, \mathbb{C}_p)$. Since M is continuous and H_K compact, then $\mathrm{Im}(M) \subset p^{n_0}\mathcal{O}_{\mathbb{C}_p}$ for some $n_0 \in \mathbb{Z}$, i.e. $m \in H^1(H_K, p^{n_0}\mathcal{O}_{\mathbb{C}_p})$. Now, iterating lemma 1.5.3, we obtain for every $n \geq n_0$ elements $x_n \in p^{n-1}\mathcal{O}_{\mathbb{C}_p}$ such that

$$M(g) + \sum_{n=n_0}^{m} (g(x_n) - x_n) \in p^{m+1}\mathcal{O}_{\mathbb{C}_p}$$

Since $x_n \in p^{n-1}\mathcal{O}_{\mathbb{C}_p}$, then $x = \sum\limits_{n=n_0}^{m} x_n$ converges and $M(g) + g(x) - x \in p^m\mathcal{O}_{\mathbb{C}_p}$ for every m, so $M(g) = x - g(x)$ and this means that M is a coboundary, i.e. $H^1(H_K, \mathbb{C}_p) = \{1\}$. □

1.6 Normalized Traces and $\mathbb{C}_p(n)^{G_K}$

In this section we introduce a family of linear and continuous operators and their study will lead to $H^0(G_K, \mathbb{C}_p(n))$ together with the Ax–Sen–Tate Lemma.

Definition 1.6.1. *For $n \geq n_K$, we define $pr_n : K_\infty \to K_n$ defined in the following way: if $x \in K_{n+k}$ then $pr_n(x) = p^{-k}\mathrm{Tr}_{K_{n+k}/K_n}(x)$.*

We remark that pr_n is well defined, i.e. if $x \in K_{n+k}$ and we consider it as element of K_{n+k+1} we obtain

$$pr_n(x) = p^{-k-1}\mathrm{Tr}_{K_{n+k+1}/K_n}(x) = p^{-k-1}\mathrm{Tr}_{K_{n+k}/K_n}(\mathrm{Tr}_{K_{n+k+1}/K_{n+k}}(x)) =$$

$$= p^{-k-1}\mathrm{Tr}_{K_{n+k}/K_n}(px) = p^{-k}\mathrm{Tr}_{K_{n+k}/K_n}(x)$$

since K_{n+k+1}/K_{n+k} is cyclic of degree p.

Lemma 1.6.2. *Let $n \geq n_K$ and $x \in K_\infty$, then $v_p(pr_n(x)) \geq v_p(x) - \alpha_n p^{-n}$ where α_n is a bounded sequence.*

Proof. We assume $x \in K_{n+k}$. Then

$$v_p(pr_n(x)) = -k + v_p(\mathrm{Tr}_{K_{n+k}/K_n}(x)) = -k + v_p(\mathrm{Tr}_{K_{n+k}/K_n}(\mathfrak{m}_{K_{n+k}}^{v_{K_{n+k}}}(x)))$$

Now we are going to first use Theorem 1.2.7 and then estimating thanks to lemma 1.4.5

$$\begin{aligned}
v_p(pr_n(x)) &= -k + \frac{1}{e_{K_n/F}}\lfloor v_{K_n}(\mathfrak{m}_{K_{n+k}}^{v_{K_{n+k}}(x)})\mathcal{D}_{K_{n+k}/K_n})\rfloor \\
&> -k + \frac{1}{e_{K_n/F}}(v_{K_n}(\mathfrak{m}_{K_{n+k}}^{v_{K_{n+k}}(x)}) + v_{K_n}(\mathcal{D}_{K_{n+k}/K_n}) - 1) \\
&= -k + \frac{1}{e_{K_n/F}}(v_{K_n}(x) + e_{K_n/F}v_p(\mathcal{D}_{K_{n+k}/K_n}) - 1) \\
&= -k + v_p(x) + (v_p(\mathcal{D}_{K_{n+k}/F}) - v_p(\mathcal{D}_{K_n/F})) - \frac{1}{e_{K_n/F}} \\
&= v_p(x) - k + n + k + c + \frac{a_{n+k}}{p^{n+k}} - n - c - \frac{a_n}{p^n} - \frac{1}{e_{K_n/F_n}p^{n-1}(p-1)} \\
&= v_p(x) - \frac{\alpha_n}{p^n}
\end{aligned}$$

where

$$\alpha_n = a_n - \frac{a_{n+k}}{p^k} + \frac{p}{e_{K_n/F_n}(p-1)}$$

is bounded since since a_n is bounded and $e_{K_n/F_n} \leq [K_n : F_n] = [K_\infty : F_\infty]$ for n big enough. □

Corollary 1.6.3. *For $n \geq n_K$, the linear function pr_n is uniformly continuous on K_∞ and so it extends to a continuous function $pr_n : \widehat{K_\infty} \to K_n$*

Proof. It is just an application of the previous lemma:

$$|pr_n(x) - pr_n(y)| = |pr_n(x-y)| \leq |x-y|p^{\alpha_n p^{-n}}$$

and since α_n is bounded we have an upper-bound of $p^{\alpha_n p^{-n}}$. □

We define $K_n^\perp = \{x \in \widehat{K_\infty} : pr_n(x) = 0\}$. We can then write the following short exact sequence of $\mathbb{Q}_p-$vector spaces:

$$0 \to K_n^\perp \to \widehat{K_\infty} \to K_n \to 0$$

Since $pr_n|_{K_n} = id_{K_n}$, we have that the inclusion $K_n \hookrightarrow \widehat{K_\infty}$ is a right splitting, so for $n \geq n_K$ we get $\widehat{K_\infty} = K_n \oplus K_n^\perp$.

Finally, the next proposition will show the power of the family of continuous operators that enable to approximate equivariantly elements of $\widehat{K_\infty}$.

Proposition 1.6.4. *For $n \geq n_K$ and $x \in \widehat{K_\infty}$ we have*

1. *$v_p(pr_n(x)) \geq v_p(x) - \alpha_n p^{-n}$ where α_n is the bounded sequence of lemma 1.6.2;*
2. *$x = \lim_{n\to\infty} pr_n(x)$;*
3. *pr_n commutes with the action of $\Gamma_K = G_{K_\infty/K}$.*

Proof. 1. We know that pr_n is continuous on $\widehat{K_\infty}$ and v_p is continuous as well so the inequality is induced by lemma 1.6.2.

2. We fix n and we write $x = \lim_{m\to\infty} x_m$ with $x_m \in K_m$. For every $C > 0$, we can choose m such that for $x_{n+m} \in K_{n+m}$ we have $v_p(x - x_{n+m}) > C$. We remind that $pr_{n+m+j}(x_{n+m}) = x_{n+m}$ for every $j \geq 0$. So

$$\begin{aligned} v_p(x - pr_{n+m}(x)) &= v_p(x - x_{n+m} + pr_{n+m}(x_{n+m}) - pr_{n+m}(x)) \\ &\geq \min\{v_p(x - x_{n+m}), v_p(pr_{n+m}(x - x_{x+m}))\} \\ &\geq \min\{C, C - \alpha_{n+m}p^{-(n+m)}\} \\ &= C - \alpha_{n+m}p^{-(n+m)} \\ &> C - \alpha_{n+m}p^{-n} \end{aligned}$$

Since $\alpha_{n+m}p^{-n}$ is bounded as $m \to \infty$, then we obtain $x = \lim_{m\to\infty} pr_{n+m}(x) = \lim_{m\to\infty} pr_m(x)$ by making $C \to \infty$.

3. Let $\gamma \in \Gamma_K$ be a topological generator (see Remark 1.4.2). Then, for $n \geq n_K$ the group $G_{K_{n+k}/K_n} \cong G_{F_{n+k}/F_n}$ is cyclic and it is generated by a power γ^s, i.e. $\gamma^s|_{K_{n+k}}$ is a generator of G_{K_{n+k}/K_n} (we will write γ^s instead of $\gamma^s|_{K_{n+k}}$). Thus,

$$\gamma pr_n(x) = p^{-k}\gamma \sum_{i=1}^{p^n} (\gamma^s)^i(x) = p^{-k} \sum_{i=1}^{p^n} (\gamma^s)^i(\gamma(x)) = pr_n(\gamma(x))$$

□

Theorem 1.6.5. *Let $K/\mathbb{Q}_p$ be finite and $H_K = G_{K_\infty}$. Then,*

$$H^0(G_K, \mathbb{C}_p(n)) = \mathbb{C}_p(n)^{G_K} = \begin{cases} 0 & n \neq 0 \\ K & n = 0 \end{cases}$$

Proof. The case $n = 0$ is a direct application of Ax–Sen–Tate Theorem. So we assume $n \neq 0$. Assume that $\alpha e \in \mathbb{C}_p(n)^{G_K}$ with $\alpha \in \mathbb{C}_p^\times$. Then for every $g \in G_K$ we must have:

$$\alpha e = g(\alpha e) = g(\alpha)\chi_{\text{cycl}}^n(g)e$$

so $g(\alpha) = \alpha\chi_{\text{cycl}}(g)^{-n}$.

In the case $g = h \in H_K$, then $\chi_{\text{cycl}}(h) = 1$ so we have $h(\alpha) = \alpha$, i.e. $\alpha \in \mathbb{C}_p^{H_K} = \widehat{K_\infty}$ by Ax–Sen–Tate. This implies that $g(\alpha) = \alpha\chi_{\text{cycl}}(g)^{-n}$ must hold for every $g \in \Gamma_K = G_{K_\infty/K}$. Using proposition 1.6.4, we have $\alpha = \lim_{m\to\infty} pr_m(\alpha)$ and using that $g \in \Gamma_K$ commutes with pr_m we get

$$g(pr_m\alpha) = pr_m g(\alpha) = pr_m(\chi_{\text{cycl}}(g)^{-n}\alpha) = \chi_{\text{cycl}}(g)^{-n}pr_m(\alpha)$$

where we used that $\chi_{\text{cycl}}(g) \in \mathbb{Q}_p$. Comparing first and last term we obtain

$$\chi_{\text{cycl}}(g)^n = \frac{pr_m(\alpha)}{g(pr_m(\alpha))}$$

If we choose $g \in \Gamma_{K_m} = G_{K_\infty/K_n}$, which invaries $pr_m(\alpha) \in K_n$, then $\chi_{\text{cycl}}(\Gamma_{K_m})^n = 1$. This is a contradiction since for $m \geq n_K$ we have $\chi_{\text{cycl}}(\Gamma_{K_m}) \cong 1 + p^m\mathbb{Z}_p$ by lemma 1.4.1. This proves that $\mathbb{C}_p(n)^{G_K} = 0$ when $n \neq 0$. □

1.7 Topological generators

Let γ be a topological generator for Γ_K and γ_n a topological generator for Γ_{K_n}. Since Γ_{K_n} is subgroup of the procyclic group Γ_K we have $\gamma_n = \gamma^s$ for some integer s and for $n \geq n_K$ we can choose γ_n in order to have $\gamma_{n+k} = \gamma_n^{p^k}$ because K_{n+k}/K_n is a cyclic extension of degree p^k. We now need two lemmas in order to prove that the linear and continuous operator γ_n is a homeomorphism when restricted to $K_n^\perp$.

Lemma 1.7.1. *If $x \in K_\infty$ and $m \geq 1$, then $v_p((1-\gamma_n^m)) \geq v_p((1-\gamma_n)(x))$.*

Proof. We just use the factorization $1 - y^m = (1-y)(1+y+\cdots+y^{m-1})$:

$$\begin{aligned} v_p((1-\gamma_n^m)(x)) &= v_p\bigg(\sum_{i=0}^{m-1} \gamma_n^i(1-\gamma_n)(x)\bigg) \\ &\geq \min\{v_p(\gamma_n^i(1-\gamma_n)(x))\} \\ &= v_p((1-\gamma_n)(x)) \end{aligned}$$

□

Lemma 1.7.2. *If $x \in K_m$ with $m > n \geq n_K$ then*

$$v_p(x - pr_n(x)) \geq v_p((1-\gamma_n)(x)) - 1 - \sum_{k=n}^{m-1} \frac{\alpha_k}{p^k}$$

where α_K is the sequence defined in 1.6.2 or 1.6.4.

Proof. We prove by induction on $m-n$. The case $m = n+1$ is obtained using the previous lemma:

$$v_p(x - pr_n(x)) = v_p(px - \mathrm{Tr}_{K_{n+1}/K_n}(x)) - 1 =$$

$$= v_p\left(\sum_{i=1}^{p-1}(1-\gamma_n^i)(x)\right) - 1 \geq \min\{v_p((1-\gamma_n^i)(x))\} - 1 \geq v_p((1-\gamma_n)(x)) - 1$$

For the inductive case we assume the inequality for $m = n+k$ and we prove it for $m+1$. So we take $x \in K_{m+1}$, then we can use the inductive hypothesis on $\mathrm{Tr}_{K_{m+1}/K_m}(x) \in K_m$ to get

$$v_p(\mathrm{Tr}_{K_{m+1}/K_m}(x) - pr_n(\mathrm{Tr}_{K_{m+1}/K_m}(x))) \geq v_p((1-\gamma_n)(\mathrm{Tr}_{K_{m+1}/K_m}(x))) - 1 - \sum_{k=n}^{m-1} \frac{\alpha_k}{p^k}$$

On the other hand, by linearity of the trace we have

$$\begin{aligned} v_p((1-\gamma_n)(\mathrm{Tr}_{K_{m+1}/K_m}(x))) &= v_p(\mathrm{Tr}_{K_{m+1}/K_m}((1-\gamma_n)(x))) \\ &= v_p(pr_m((\gamma_n)(x))) + 1 \\ &\geq v_p((1-\gamma_n)(x)) + 1 - \frac{\alpha_m}{p^m} \end{aligned}$$

where we used proposition 1.6.4. Combining this with the inductive hypothesis we obtain

$$v_p(\mathrm{Tr}_{K_{m+1}/K_m}(x) - pr_n(\mathrm{Tr}_{K_{m+1}/K_m}(x))) \geq v_p((1-\gamma_n)(x)) - \sum_{k=n}^{m} \frac{\alpha_k}{p^k}$$

We conclude using again the inductive hypothesis for K_{m+1}/K_m:

$$\begin{aligned} v_p(x - \mathrm{pr}_n(x)) &= v_p\left(x - \frac{1}{p}\mathrm{Tr}_{K_{m+1}/K_m}(x) + \frac{1}{p}(\mathrm{Tr}_{K_{m+1}/K_m}(x) - p\ \mathrm{pr}_n(x))\right) \\ &\geq \min\{v_p(x - \mathrm{pr}_m(x)), v_p(\mathrm{Tr}_{K_{m+1}/K_m}(x) - p\ \mathrm{pr}_n(x)) - 1\} \\ &\geq \min\{v_p((1-\gamma_n)(x)) - 1, v_p((1-\gamma_n)(x)) - 1 - \sum_{k=n}^{m} \frac{\alpha_k}{p^k}\} \\ &= v_p((1-\gamma_n)(x)) - 1 - \sum_{k=n}^{m} \frac{\alpha_k}{p^k} \end{aligned}$$

where the fact that $p\ \mathrm{pr}_n(x) = \mathrm{pr}_n(px) = p^{n-m}\mathrm{Tr}_{K_{m+1}/K_n}(x) = \mathrm{pr}_n(\mathrm{Tr}_{K_{m+1}/K_m}(x))$ was used in the second line. □

We are now ready to discuss the invertibility of the operator $1 - \gamma_n$.

Proposition 1.7.3. *Let $n \geq n_K$. The operator $1-\gamma_n$ is bijective on $K_n^{\perp}$, its inverse $(1-\gamma_n)^{-1}$ is continuous and the operator norm $\|(1-\gamma_n)^{-1}\|$ is bounded independently of n.*

Proof. First, $1-\gamma_n(K_n^\perp) \subset K_n^\perp$ since γ_n commutes with pr_n by proposition 1.6.4. Moreover, γ_n is a generator of Γ_{K_n}, so the kernel of $1-\gamma_n$ on $\widehat{K_\infty}$ is $\widehat{K_\infty}^{\gamma_n} = \widehat{K_\infty}^{\Gamma_{K_n}} = K_n$ by Ax–Sen–Tate lemma. This implies that the operator $1-\gamma_n$ is injective on $K_n^\perp$ due to $K_n^\perp \cap K_n = \{0\}$. Thus, for $m \geq n$, the restriction of the linear map $1-\gamma_n$ to the finite dimensional $K-$vector space $K_m \cap K_n^\perp$ is bijective. Let $y \in K_m \cap K_n^\perp$; using surjectivity we have $y = (1-\gamma_n)(x)$ for some $x \in K_m \cap K_n^\perp$. We apply the previous lemma to x:

$$v_p(x - pr_n(x)) \geq v_p((1-\gamma_n)(x)) - 1 - \sum_{k=n}^{m-1} \frac{\alpha_k}{p^k}$$

Now $pr_n(x) = 0$ from $x \in K_n^\perp$ and $x = (1-\gamma_n)^{-1}(y)$, so

$$v_p((1-\gamma_n)^{-1}(y)) \geq v_p(y) - C$$

where $C = 1 + \sum\limits_{k=n}^{\infty} \frac{\alpha_k}{p^k}$ that converges since α_k are bounded. Thus on $K_m \cap K_n^\perp$ we deduce

$$\|(1-\gamma_n)^{-1}\| = \sup \frac{|(1-\gamma_n)^{-1}(y)|}{|y|} \leq |p|^C$$

so the operator $(1-\gamma_n)^{-1}$ is continuous on $K_m \cap K_n^\perp$ and its norm is bounded independent of n and m. Then, $(1-\gamma)^{-1}$ extends to a continuous operator on $K_n^\perp$ of norm bounded independent of n. □

Finally, we show how the previous proposition on $1-\gamma_n$ helps treating the general case $\widehat{K_\infty}(n)$.

Proposition 1.7.4. *Let $k \neq 0$. Let γ the topological generator of Γ_K, then $1-\gamma : \widehat{K_\infty}(k) \to \widehat{K_\infty}(k)$ is surjective.*

Proof. Let C be the uniform bound on $\|(1-\gamma_n)^{-1}\|$ on $K_n^\perp$ from the previous proposition. We know that χ^k_{cycl} is a continuous character and that Γ_{K_n} form a neighborhood around the identity in Γ_K, so we have $\lim\limits_{n\to\infty} \chi^k_{\text{cycl}}(\gamma_n) = 1$ in Γ_K that implies $|1-\chi^k_{\text{cycl}}(\gamma_n)| < C^{-1}$ for n big enough. For the rest of the proof, we will assume n such that the previous inequality holds. Then $\|(1-\chi^k_{\text{cycl}}(\gamma_n))(1-\gamma_n)^{-1}\| < 1$ and so working on $K_n^\perp$ we get:

$$\frac{1}{1-\gamma_n\chi^k_{\text{cycl}}(\gamma_n)} = \frac{1}{(1-\gamma_n)\Big(1+\Big(\frac{1-\chi^k_{\text{cycl}}(\gamma_n)}{1-\gamma_n}\Big)\gamma_n\Big)} = (1-\gamma_n)^{-1}\sum_{i=0}^{\infty}(\gamma_n(-1+\chi^k_{\text{cycl}}(\gamma_n))(1-\gamma_n)^{-1})^i$$

Remind that we have just implicitly used that $K_n^\perp$ is a Banach space (since pr_n is continuous), therefore the space of continuous operators on $K_n^\perp$ is a Banach space as well.

Since we were able to invert $1-\gamma_n\chi^k_{\text{cycl}}(\gamma_n) : K_n^\perp \to K_n^\perp$ it must be surjective. By definition of $K_n^\perp(m)$, this is equivalent to $1-\gamma_n : K_n^\perp(k) \to K_n^\perp(k)$ surjective. Note that we haven't used $k \neq 0$ so far.

Now we need surjectivity on $K_n(k)$. For $n \geq n_K$, we have that $\chi_{\text{cycl}}(\Gamma_{K_n}) \cong 1 + p^n\mathbb{Z}_p$ from lemma 1.4.1, so $\chi^k_{\text{cycl}}(\gamma_n) \neq 1$ because $k \neq 0$. Then, if $0 \neq x \in K_n(k)$, we have that $(1-\gamma_n)(x) = (1-\chi^k_{\text{cycl}}(\gamma_n))x \neq 0$, therefore $1-\gamma_n : K_n(k) \to K_n(k)$ is an injective $K-$linear map so it's also surjective by the finite dimension.

In this way, we get that $1-\gamma_n : \widehat{K_\infty(k)} \to \widehat{K_\infty(k)}$ is surjective. Finally, using that $\gamma_n = \gamma^s$ for some integer s, we have $1-\gamma_n = (1-\gamma)\left(\sum\limits_{i=0}^{s-1}\gamma^i\right)$ so $1-\gamma$ must be surjective as well. □

1.8 First cohomology group of $\mathbb{C}_p(n)$

Theorem 1.8.1.

$$H^1(G_K, \mathbb{C}_p(n)) = \begin{cases} 0 & \textit{if } n \neq 0 \\ V & \textit{if } n = 0 \end{cases}$$

where V is a 1-dimensional $K-$vector space.

Proof. We first write the inflation-restriction sequence for $H_K \subset G_K$ and $\Gamma_K \cong G_K/H_K$:

$$0 \to H^1(\Gamma_K, \mathbb{C}_p(n)^{H_K}) \to H^1(G_K, \mathbb{C}_p(n)) \to H^1(H_K, \mathbb{C}_p(n))$$

Now, since the action of the cyclotomic character is trivial on H_K, we have $\mathbb{C}_p(n)^{H_k} = (\mathbb{C}_p^{H_k})(n) = \widehat{K_\infty}(n)$ by Ax–Sen–Tate lemma and $H^1(H_K, \mathbb{C}_p(n)) = H^1(H_K, \mathbb{C}_p) = 0$ by Theorem 1.5.5. Then from the exact sequence and proposition 1.1.6 we obtain the following isomorphisms of $K-$vector spaces

$$H^1(G_K, \mathbb{C}_p(n)) \cong H^1(\Gamma_K, \widehat{K_\infty}(n)) \cong \widehat{K_\infty}(n)/(1-\gamma)\widehat{K_\infty}(n)$$

where γ is a topological generator of the procyclic group Γ_K.

If $n \neq 0$, the map $1-\gamma$ is surjective on $\widehat{K_\infty}(n)$ by proposition 1.7.4, thus the result $H^1(G_K, \mathbb{C}_p(n)) = 0$.

If $n = 0$, then $H^1(G_K, \mathbb{C}_p) \cong \widehat{K_\infty}/(1-\gamma)\widehat{K_\infty}$. Note that in the proposition 1.7.4 we have proved that $1-\gamma$ is surjective on $K_m^\perp(n)$ also for $n = 0$, so $\widehat{K_\infty}/(1-\gamma)\widehat{K_\infty} \cong K_n/(1-\gamma)K_n$.

To conclude, we prove that $K \cong K_n/(1-\gamma)K_n$ using the natural map from the inclusion $K \hookrightarrow K_n$.

The map is injective because if $x \in K$ satisfies $x = (1-\gamma_n)(y)$ for some $y \in K_n$, then recalling that $\gamma_n = \gamma^s$ for some s we have that

$$[K_n : K]x = \mathrm{Tr}_{K_n/K}(x) = (1 + \gamma + \cdots + \gamma^{s-1})(x) = (1-\gamma^s)(y) = 0$$

since γ_n fixes $y \in K_n$.

To prove surjectivity, we have to use the inflation-restriction sequence on $\Gamma_{K_n} \subset \Gamma_K$ acting on K_n; using that $\Gamma_K/\Gamma_{K_n} \cong G_{K_n/K}$ and that Γ_{K_n} fixes K_n we obtain:

$$0 \to H^1(G_{K_n/K}, K_n) \to H^1(\Gamma_K, K_n) \to H^1(\Gamma_{K_n}, K_n)^{G_{K_n/K}}$$

We know that $H^1(G_{K_n/K}, K_n)$ from Hilbert 90. So we get an injection

$$K_n/(1-\gamma)K_n \cong H^1(\Gamma_K, K_n) \hookrightarrow H^1(\Gamma_{K_n}, K_n)^{G_{K_n/K}} \cong (K_n/(1-\gamma_n)K_n)^{G_{K_n/K}} \cong K_n^{G_{K_n/K}} = K$$

This implies that the dimensione of the $K-$vector space $K_n/(1-\gamma)K_n$ is at most one and since we already proved that $K \hookrightarrow K_n/(1-\gamma)K_n$, we obtain an isomorphism. □

Chapter 2

Fontaine's theorem on Kähler differentials

In this chapter we keep the notation of the previous one. We consider a finite extension $K/\mathbb{Q}_p$, the Galois group $G = \mathrm{Gal}(\overline{K}/K)$ and $\mathbb{C}_p$ the p-adic closure of $\overline{K} = \overline{\mathbb{Q}_p}$. We denote with K_0 the maximal unramified $\mathbb{Q}_p-$extension contained in K, i.e. $K_0 = \mathrm{Frac}(W(k))$ where k is the (finite) residue field of K. When not specified, the valuation v is the $p-$adic valuation, i.e. $v(p) = 1$.
Before engaging with the work of Fontaine in [Fon82], we recall the general definitions and properties of formal groups and Kähler differentials. Further readings on formal groups are [LT65],[CF67], whereas regarding Kähler differentials we recommend [Har13].

2.1 Formal groups at one parameter

Let R be a ring (commutative with identity).

Definition 2.1.1. *A one-parameter (commutative) formal group $\mathcal{F}$ over R is a power series $F(X,Y) \in R[\![X,Y]\!]$ such that:*

- *$F(X,Y) = X + Y + (\text{terms of degree } \geq 2)$;*
- *$F(X, F(Y,Z)) = F(F(X,Y), Z)$;*
- *$F(X,Y) = F(Y,X)$;*
- *there exists a unique power series $i(T) \in R[\![T]\!]$ such that $F(T, i(T)) = 0$;*
- *$F(X,0) = X$ and $F(0,Y) = Y$.*

We say that $F(X,Y)$ is the formal group law of $\mathcal{F}$.

Homomorphisms of formal groups are defined in the following way:

Definition 2.1.2. *Let $(\mathcal{F}, F)$ and $(\mathcal{G}, G)$ be formal groups over R. A homomorphism from $\mathcal{F}$ to $\mathcal{G}$ is a power series $f(T) \in R[\![T]\!]$ such that $f(0) = 0$ and*

$$f(F(X,Y)) = G(f(X), f(Y))$$

It's natural to define $\mathcal{F}$, $\mathcal{G}$ isomorphic if there exist homomorphisms $f : \mathcal{F} \to \mathcal{G}$ and $g : \mathcal{G} \to \mathcal{F}$ such that $f(g(T)) = g(f(T)) = T$ that is the trivial homomorphism.

It's possible also to define invariant differentials on a formal group.

Definition 2.1.3. *An invariant differential on a formal group $\mathcal{F}$ over R is a differential form $\omega(T) = P(T)dT$ with $P(T) \in R[\![T]\!]$ such that*

$$\omega \circ F(X, Y) = \omega(X) + \omega(Y)$$

or equivalently $P(F(X, Y))F_X(X, Y) = P(X)$ where $F_X(X, Y)$ is the partial derivative of F with respect to its first variable. An invariant differential form $\omega(T) = P(T)dT$ is said to be normalized if $P(0) = 1$.

Proposition 2.1.4. *Let $\mathcal{F}$ be a formal group over the ring R; there exists a unique normalized invariant differential form on $\mathcal{F}$ and it's given by*

$$\omega = F_X(0, T)^{-1}dT$$

Thus every invariant differential form on $\mathcal{F}$ is of the form $r\omega$ for some $r \in R$.

In this chapter we will be interested in the formal multiplicative group $\hat{\mathbb{G}}_m$ that is an example of the class of Lubin-Tate formal groups.

Let K a local field, q the cardinality of the residue field and π a uniformizer for $\mathcal{O}_K$. Let $\mathcal{F}_\pi$ the set of formal power series such that $f(T) \equiv \pi T \pmod{\deg \geq 2}$ and $f(T) \equiv x^q \pmod{\pi}$. The next proposition, proved by an inductive reasoning, leads to the definition of Lubin-Tate formal groups.

Proposition 2.1.5. *Let $f \in \mathcal{F}_\pi$, then there exists a unique formal group law F_f with coefficients in $\mathcal{O}_K$ such that f is an endomorphism of F_f. We say that F_f is the Lubin-Tate formal group associated with $f \in \mathcal{F}_\pi$.*

Proposition 2.1.6. *Let $f \in \mathcal{F}_\pi$ and F_f the corresponding group law, then for any $a \in \mathcal{O}_K$ there exists a unique $[a]_f \in \mathcal{O}_K[\![T]\!]$ such that*

- *$[a]_f$ commutes with f;*
- *$[a]_f(T) \equiv aT \pmod{deg \geq 2}$;*
- *$[a]_f$ is an endomorphism of F_f.*

Moreover, the map $a \mapsto [a]_f$ is an injective homomorphism of rings $\mathcal{O}_K \hookrightarrow End(F_f)$.

The Lubin-Tate formal groups or, more generally, formal groups over discrete valuation rings are interesting since their properties allow to define new operations on the maximal ideal (or on the principal units). Indeed, if R is a discrete valuation ring with maximal ideal $\mathfrak{M}$, then for every $m, n \in \mathfrak{M}$ the map $(m, n) \mapsto F(m, n) \in \mathfrak{M}$ is a well-defined abelian operation, since the converge of the series is given by the positive valuation of m and n. The inverse of m is of course $i(m)$. Lubin-Tate formal groups are even more powerful since they give rise to a module structure; this will be discussed in detail in section 2.3.

2.2 Kähler differentials

Let A a ring, B an $A-$algebra and M a $B-$module.

Definition 2.2.1. *A $A-$derivation of B into M is an additive map $d : B \to M$ such that $d(bb') = bd(b') + b'd(b)$ for every $b, b' \in B$ and $d(a) = 0$ for every $a \in A$.*

Definition 2.2.2. *The module of Kähler differentials of B over A is a $B-$module $\Omega_A(B)$ endowed with an $A-$derivation $d : B \to \Omega_A(B)$ satisfying the following universal property: for every $B-$module M and for every $A-$derivation $d' : B \to M$ there exists a unique $B-$module homomorphism $f : \Omega_A(B) \to M$ such that $d' = f \circ d$.*

Lemma 2.2.3. *The module of Kähler differentials commutes with direct limits, i.e. if $\{B_i, \phi_{i,j}\}_{i,j\in I}$ is a direct system of rings over A (for a direct set I), then*

$$\Omega_A(B) \cong \varinjlim \Omega_A(B_i)$$

where $B = \varinjlim B_i$.

Proof. We sketch the proof. From the definition we have a functorial isomorphism

$$\mathrm{Hom}_B(\Omega_A(B_i), N) \cong \mathrm{Der}_A(B_i, N)$$

for every B_i-module N. Then if M is a $B-$module, we have

$$\mathrm{Der}_A(B, M) = \mathrm{Der}_A(\varinjlim B_i, M) \cong \varprojlim \mathrm{Der}_A(B_i, M) \cong$$

$$\cong \varprojlim \mathrm{Hom}_{B_i}(\Omega_A(B_i), M) \cong \mathrm{Hom}_B(\varinjlim \Omega_A(B_i), M)$$

so $\varinjlim \Omega_A(B_i)$ satisfies the universal property of $\Omega_A(B)$. □

Proposition 2.2.4. *Let B an $A-$algebra, let I be an ideal of B and let $C = B/I$. Then there is a natural exact sequence of $C-$modules:*

$$I/I^2 \xrightarrow{\gamma} \Omega_A(B) \otimes_B C \to \Omega_A(C) \to 0$$

where for every $b \in I$, if $\bar{b}$ is its image in I/I^2, then $\gamma\bar{b} = db \otimes 1$.

Construction
There is a constructive proof of the existence of the module of Kähler differentials. Indeed, we consider the free $B-$module generated by the symbols $\{db \mid b \in B\}$ and we divide by the relations $d(b + b') = db + db'$; $d(bb') = bdb' + b'db$ and $da = 0$ for all $b, b' \in B$ and $a \in A$; this $B-$module Ω, endowed with the map $d : B \to \Omega$ that maps $b \mapsto db$, satisfies the required universal property.
Examples
An important example is the case $B = A[X]$. The Kähler differentials module $\Omega_{B/A}$ is a free B-module generated by dX, since the relations imply $dF(X) = F'(X)dX$.
Therefore, the case $B = A[X]/(F(X))$, with $F(X)$ an irreducible polynomial over A derives by the previous one using proposition 2.2.4. Indeed, $\Omega_A(B)$ is again generated by dX, but it is not a free $B-$module, since $F'(X)dX = dF(X) = 0$. Using that $\mathrm{Im}(\gamma)$ is generated by $dF(X) \otimes 1$, we get the annihilator of dX is generated by $F'(X)$.

2.3 Main Theorem

As previously mentioned, we now focus our attention to the formal multiplicative group $\hat{\mathbb{G}}_m(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$. This is a Lubin-Tate formal group defined over $\mathbb{Q}_p$ and associated with $f(T) = (1+T)^p - 1$. Moreover, for every $a \in \mathbb{Z}_p$ the series $[a]_f$ becomes the series

$$[a]_f(T) = (1+T)^a - 1 = \sum_{n=1}^{\infty} \binom{a}{n} T^n$$

Notice that the binomial coefficient $\binom{a}{n}$ is defined in $\mathbb{Z}_p$ since the binomial is a continuous function in a and so we use the fact that a is a limit of integer numbers, whose binomials are of course integers.
We use the formal multiplicative group to redefine the sum operation on $\mathfrak{m}_{\overline{\mathbb{Q}}_p}$, i.e. $x \oplus y = x + y + xy$ for every $x, y \in \mathfrak{m}_{\overline{\mathbb{Q}}_p}$. Moreover, we can define also a multiplication of $a \in \mathbb{Z}_p$ and $x \in \mathfrak{m}_{\overline{\mathbb{Q}}_p}$ as follows:

$$a * x = [a]_f(x) = \sum_{n=1}^{\infty} \binom{a}{n} x^n$$

well-defined since $v(x) > 0$. Proposition 2.1.4 yields that the sum $\oplus$ and the scalar product $*$ are compatible, so they defined a new $\mathbb{Z}_p-$module structure on $\mathfrak{m}_{\overline{\mathbb{Q}}_p}$, that will be denoted with Γ.

Therefore, we consider the Tate module $T_p\Gamma = \varprojlim \Gamma[p^n]$. We can study it easily since if $x_n \in \Gamma[p^n]$ then

$$0 = p^n * x_n = (1+x_n)^{p^n} - 1$$

that is equivalent to $x_n = \epsilon_n - 1$ where ϵ_n is a p^n-adic root of unity in $\overline{\mathbb{Q}}_p$. This means that a family of ($*$ -) compatible $x_n = \epsilon_n - 1$ corresponds to a family of compatible p^n-adic roots. Thus, $T_p\Gamma$ is a $\mathbb{Z}_p$-free module of rank 1 and we consider a generator $u = (u_n)_n$, corresponding to a compatible family of primitive p^n-adic roots ϵ_n. The correspondence between x_n and ϵ_n shows that the action of G on $T_p\Gamma$ is given by the cyclotomic character (cf section 1.1).

We consider ω_Γ the $\mathbb{Z}_p-$module of invariant differentials of Γ. It is a $\mathbb{Z}_p$-free module of rank 1 as well, and it can be easily checked that it is generated by $\omega_0 = \frac{1}{1+X}dX$. We can define a trivial action of G on ω_Γ.
Let $\Omega = \Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{\mathbb{Q}}_p})$ be the module of Kähler differentials. The action of G on Ω is the natural action deriving from $\sigma(d\alpha) = d\sigma(\alpha)$.

We know define an *integration* of invariant differentials along elements of $T_p\Gamma$. Given an element $\alpha \in \Gamma$ and $\omega = a\omega_0 \in \omega_\Gamma$ we can combine them naturally in $a\frac{1}{1+\alpha}d\alpha \in \Omega$.

Proposition 2.3.1. *The application $\langle -, - \rangle : \Gamma \times \omega_\Gamma \to \Omega$ that maps*

$$(\alpha, a\omega_0) \longmapsto \langle \alpha, \omega \rangle = a\frac{1}{1+\alpha}d\alpha \in \Omega$$

is a $\mathbb{Z}_p-$bilinear map and it verifies $\langle g(\alpha), \omega \rangle = g(\langle \alpha, \omega \rangle)$ for every $g \in G, \alpha \in \Gamma, \omega \in \omega_\Gamma$.

Proof. The linearity in the second variable and the compatibility with the $G-$action derive from the definitions. We now discuss the linearity with respect to the first entry. Indeed,

$$\begin{aligned}\langle \alpha+\beta,\omega_0\rangle &= \frac{1}{1+\alpha\oplus\beta}d(\alpha\oplus\beta) = \\ &= \frac{1}{1+\alpha+\beta+\alpha\beta}d(\alpha+\beta+\alpha\beta) = \\ &= \frac{1}{(1+\alpha)(1+\beta)}d((1+\alpha)(1+\beta)) = \\ &= \frac{1}{1+\alpha}d(1+\alpha)+\frac{1}{1+\beta}d(1+\beta) = \\ &= \langle\alpha,\omega_0\rangle+\langle\beta,\omega_0\rangle\end{aligned}$$

where we used that $d(1)=0$ and the product relation. Similarly, if $a\in\mathbb{Z}_p$, then

$$\begin{aligned}\langle a\alpha,\omega_0\rangle &= \frac{1}{(1+\alpha)^a}d((1+\alpha)^a-1) = \\ &= \frac{1}{(1+\alpha)^a}d((1+\alpha)^a) = \\ &= \frac{a(1+\alpha)^{a-1}}{(1+\alpha)^a}d(1+\alpha) = a\langle\alpha,\omega_0\rangle\end{aligned}$$

where we used again that a is a limit of integers and that the map $\alpha\mapsto d\alpha\in\Omega$ is continuous with respect to the $\mathfrak{m}_{\overline{\mathbb{Q}}_p}$-adic topology on Ω. □

Assuming a trivial action of G on ω_Γ, then $\overline{\mathbb{Q}}_p\otimes_{\mathbb{Z}_p}T_p(\Gamma)\otimes_{\mathbb{Z}_p}\omega_\Gamma$ is a $\overline{\mathbb{Q}}_p-$vector space of dimension 1 endowed with a semi-linear continuous action of G.
Every element of $\overline{\mathbb{Q}}_p\otimes_{\mathbb{Z}_p}T_p(\Gamma)\otimes_{\mathbb{Z}_p}\omega_\Gamma$ can be written (not uniquely) in the form $p^{-r}a\otimes u\otimes\omega_0$ where u and ω_0 are the generators of the respective $\mathbb{Z}_p$-module and $a\in\mathcal{O}_{\overline{\mathbb{Q}}_p}$. Proposition 2.3.1 allows us to show that the element $a\langle u_r,\omega_0\rangle$ does not depend on how we write the element of $\overline{\mathbb{Q}}_p\otimes_{\mathbb{Z}_p}T_p(\Gamma)\otimes_{\mathbb{Z}_p}\omega_\Gamma$; indeed, using $p^{-r}a\otimes u\otimes\omega_0=p^{-r-1}(pa)\otimes u\otimes\omega_0$ we have

$$pa\langle u_{r+1},\omega_0\rangle = a\langle p*u_{r+1},\omega_0\rangle = a\langle u_r,\omega_0\rangle$$

where we used that $p*u_{r+1}=u_r$ and the linearity given by the previous proposition.

Therefore we can define a map

$$\xi_{K,\Gamma}=\xi:\overline{\mathbb{Q}}_p\otimes_{\mathbb{Z}_p}T_p(\Gamma)\otimes_{\mathbb{Z}_p}\omega_\Gamma\to\Omega$$

that maps $p^{-r}a\otimes u\otimes\omega_0$ to $a\langle u_r,\omega_0\rangle$. It is a well-defined $\mathcal{O}_{\overline{\mathbb{Q}}_p}-$linear map that commutes with the action of G.

Theorem 2.3.2. *The map ξ is surjective and if*

$$\mathfrak{a}_{K,\Gamma}=\mathfrak{a}=\{a\in\overline{\mathbb{Q}}_p\mid v_p(a)\geq -v(\mathcal{D}_{K/K_0})-1/(p-1)\}$$

then the kernel of ξ is the $\mathcal{O}_{\overline{\mathbb{Q}}_p}-$submodule $\mathfrak{a}_{K,\Gamma}\otimes T_p(\Gamma)\otimes\omega_\Gamma$ of $\overline{\mathbb{Q}}_p\otimes_{\mathbb{Z}_p}T_p(\Gamma)\otimes_{\mathbb{Z}_p}\omega_\Gamma$.

The proof of the theorem is explained in detail in section 4; we now focus on this important corollary.

Corollary 2.3.3. *Let $\hat{\mathfrak{a}}$ be the closure of $\mathfrak{a}_{K,\Gamma}$ in $\mathbb{C}_p$. Then,* *1.* $\Omega \cong (\overline{\mathbb{Q}}_p/\mathfrak{a}) \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma$

2. $T_p(\Omega) := \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Omega) \cong \hat{\mathfrak{a}} \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma$

3. $V_p(\Omega) := \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega) \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma$

are isomorphisms of $\mathcal{O}_{\overline{\mathbb{Q}}_p}-$modules (resp. $\mathcal{O}_{\mathbb{C}_p}-$modules, $\mathbb{C}_p-$vector spaces) that commute with the action of G.

Proof. 1. The first isomorphism derives from the fact that

$$\Omega \cong \overline{\mathbb{Q}}_p \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma / \mathfrak{a} \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma$$

that is isomorphic as $\mathcal{O}_{\overline{\mathbb{Q}}_p}-$module to $(\overline{\mathbb{Q}}_p/\mathfrak{a}) \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma$.

2. We have that

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \Omega) &\cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, (\overline{\mathbb{Q}}_p/\mathfrak{a})) \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma \\ &\cong \mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim 1/p^n\mathbb{Z}_p/\mathbb{Z}_p, (\overline{\mathbb{Q}}_p/\mathfrak{a})) \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma \\ &\cong \varprojlim \mathrm{Hom}_{\mathbb{Z}_p}(1/p^n\mathbb{Z}_p/\mathbb{Z}_p, (\overline{\mathbb{Q}}_p/\mathfrak{a})) \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma \\ &\cong \varprojlim \frac{1}{p^n}\mathfrak{a}/\mathfrak{a} \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma \\ &\cong \hat{\mathfrak{a}} \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma \end{aligned}$$

where at the last line we used that every compatible sequence $\frac{1}{p^n}a_n$ (with $a_n \in \mathfrak{a}$) gives rise to a Cauchy sequence. This correspondence is compatible with the equivalence relations, i.e. the quotient by $\mathfrak{a}$ corresponds to converging to the same limit in $\overline{\mathbb{Q}}_p$.

3. Similarly:

$$\begin{aligned} \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega) &\cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, (\overline{\mathbb{Q}}_p/\mathfrak{a})) \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma \\ &\cong \mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim 1/p^n\mathbb{Z}_p, (\overline{\mathbb{Q}}_p/\mathfrak{a})) \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma \\ &\cong \varprojlim \mathrm{Hom}_{\mathbb{Z}_p}(1/p^n\mathbb{Z}_p, (\overline{\mathbb{Q}}_p/\mathfrak{a})) \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma \\ &\cong \varprojlim \overline{\mathbb{Q}}_p/p^n\mathfrak{a} \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma \\ &\cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} T_p(\Gamma) \otimes_{\mathbb{Z}_p} \omega_\Gamma \end{aligned}$$

since $\mathbb{C}_p$ is the closure of $\overline{\mathbb{Q}}_p$.

□

A choice of generator of $T_p(\Gamma)$ and for ω_Γ provides the following $G-$equivariant isomorphisms:

$$\Omega \cong (\overline{\mathbb{Q}}_p/\mathfrak{a})(1) \qquad T_p(\Omega) \cong \hat{\mathfrak{a}}(1) \qquad V_p(\Omega) \cong \mathbb{C}_p(1)$$

since the action on ω_Γ is trivial and the action on $T_p(\Gamma)$ is exactly the one of the cyclotomic character.

2.4 Proof of Theorem 2.3.2

This section is totally devoted to the proof of Theorem 2.3.2. As in the previous sections, if $K' \subset L$ are two finite extension of K_0 we denote with $d_{L/K'} : \mathcal{O}_L \to \Omega_{\mathcal{O}_{K'}}(\mathcal{O}_L)$ the canonical map from $\mathcal{O}_L$ and the $\mathcal{O}_L$-module of $\mathcal{O}_{K'}-$differentials of $\mathcal{O}_L$. We also denote with $d : \mathcal{O}_{\overline{K}} \to \Omega$ the canonical map. We will subdivide the proof in many lemmas.

We have already mentioned in the first chapter that there exists an element $x \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_{K'}[x]$ and that the different $\mathcal{D}_{L/K'}$ is generated by $P'(x)$ where $P(X)$ is the minimal polynomial of x over K'.

Lemma 2.4.1. 1. *The $\mathcal{O}_L-$module $\Omega_{\mathcal{O}_{K'}}(\mathcal{O}_L)$ is generated by $d_{L/K'}x$ and its annihilator is $\mathcal{D}_{L/K'}$.*

2. *The extension L/K' is unramified if and only if $\mathcal{D}_{L/K'} = \mathcal{O}_L$, equivalently if and only if $\Omega_{\mathcal{O}_{K'}}(\mathcal{O}_L) = 0$.*

Proof. 1. Since $\mathcal{O}_L \cong \mathcal{O}_{K'}[X]/(P(X))$, we have already seen in section 2.2 that $\Omega_{\mathcal{O}_{K'}}(\mathcal{O}_L)$ is generated by $d_{L/K'}x$, where x has minimal polynomial $P(X)$. Moreover, since $P(X)$ is the minimal polynomial we have that $P'(x)dx = dP((x)) = 0$, hence the annihilator of dx is $\mathcal{D}_{L/K'} = (P'(x))$.

2. The second equivalence is a direct consequence of part 1. The first equivalence derives from the following property of the inverse different: since $\mathrm{Tr}(\mathfrak{m}_L) \subset \mathfrak{m}_{K'}$ then $\mathfrak{m}_L \subset \mathfrak{m}_{K'} \cdot \mathcal{D}^{-1}_{L/K'}$ that is equivalent to $\mathfrak{m}_L \cdot \mathcal{D}_{L/K'} \subset \mathfrak{m}_{K'} \cdot \mathcal{O}_L$.
Indeed, if $\mathcal{D}_{L/K'} = \mathcal{O}_L$, then we get $\mathfrak{m}_L \subset \mathfrak{m}_{K'} \cdot \mathcal{O}_L$, i.e. L/K' is unramified. If L/K' is unramified, then $\mathfrak{m}_L = \mathfrak{m}_{K'} \cdot \mathcal{O}_L$, hence $\mathcal{D}_{L/K'}$ must be $\mathcal{O}_L$.

□

If If $K' \subset K" \subset L$ then we can define a canonical map $r : \Omega_{\mathcal{O}_{K'}}(\mathcal{O}_L) \to \Omega_{\mathcal{O}_{K''}}(\mathcal{O}_L)$ that maps $d_{L/K'}a$ to $d_{L/K''}a$ for $a \in \mathcal{O}_L$.

Lemma 2.4.2. *Let $K' \subset K" \subset L$ be finite extensions of K_0 and π the canonical map just defined, then π is surjective and for every $\omega \in \Omega_{\mathcal{O}_{K'}}(\mathcal{O}_L)$*

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

. So in particular r is an isomorphism if K''/K is unramified.

Proof. Let b be a generator of $\mathcal{O}_L$ as $\mathcal{O}_{K'}-$algebra, i.e. $\mathcal{O}_L = \mathcal{O}_{K'}[b]$. Then of course $\mathcal{O}_L = \mathcal{O}_{K''}[b]$ as well so by lemma 2.4.1 we have that $d_{L/K'}b$ (resp. $d_{L/K''}b$) generates the $\mathcal{O}_L-$module $\Omega_{\mathcal{O}_{K'}}(\mathcal{O}_L)$ (resp. $\Omega_{\mathcal{O}_{K''}}(\mathcal{O}_L)$) which implies r surjective.
If $\omega = a \cdot d_{L/K'}b$ is a nontrivial element of $\Omega_{\mathcal{O}_{K'}}(\mathcal{O}_L)$, by lemma 2.4.1 we have $v(\mathrm{Ann}(\omega)) = v(\mathcal{D}_{L/K'}) - v(a)$; similarly, for $r(\omega) = a \cdot d_{L/K''}b$ we have two cases: if $v(\mathcal{D}_{L/K''}) \leq v(a)$ then $r(\omega) = 0$, otherwise we have $v(\mathrm{Ann}(r(\omega))) = v(\mathcal{D}_{L/K''}) - v(a)$, so in general

$$v(\mathrm{Ann}(r(\omega))) = \max\{0, v(\mathcal{D}_{L/K''}) - v(a)\}$$

. To conclude, we know that $v(\mathcal{D}_{L/K''}) = v(\mathcal{D}_{L/K'}) - v(\mathcal{D}_{K''/K'})$, so we substitute $v(\mathcal{D}_{L/K''}) - v(a) = v(\mathrm{Ann}(\omega)) - v(\mathcal{D}_{K''/K})$. □

Lemma 2.4.3. *Let L be a finite extension of K and π_L a uniformizer for L. Then the $\mathcal{O}_L-$module $\Omega_{\mathcal{O}_K}(\mathcal{O}_L)$ is generated by $d_{L/K}\pi_L$.*

Proof. Let K' be the maximal unramified extension of K contained in L. Then $\mathcal{O}_L$ is generated by π_L as $\mathcal{O}_{K'}$ algebra and by lemma 2.4.1 we have that $\Omega_{\mathcal{O}_{K'}}(\mathcal{O}_L)$ is generated by $d_{L/K'}\pi_L$; by lemma 2.4.2 we have that the canonical map $\Omega_{\mathcal{O}_K}(\mathcal{O}_L) \to \Omega_{\mathcal{O}_{K'}}(\mathcal{O}_L)$ is an isomorphism, so $\Omega_{\mathcal{O}_K}(\mathcal{O}_L)$ is generated by $d_{L/K}\pi_L$ since it's mapped to $d_{L/K'}\pi_L$. □

If $L \subset L'$ are extensions of K then we can define a canonical map $i : \Omega_{\mathcal{O}_K}(\mathcal{O}_L) \to \Omega_{\mathcal{O}_K}(\mathcal{O}_{L'})$ mapping $d_{L/K}a$ to $d_{L'/K}a$ for every $a \in O_L$.

Lemma 2.4.4. *Let $L \subset L'$ be finite extensions of K. Then the canonical map $i : \Omega_{\mathcal{O}_K}(\mathcal{O}_L) \to \Omega_{\mathcal{O}_K}(\mathcal{O}_{L'})$, induced by the inclusion $\mathcal{O}_L \subset \mathcal{O}_{L'}$, is injective. Moreover, for every $\omega \in \Omega_{\mathcal{O}_K}(\mathcal{O}_L)$*

$$\mathrm{Ann}(i(\omega)) = \mathrm{Ann}(\omega) \cdot \mathcal{O}_{L'}$$

Proof. We can separately solve the cases L'/L unramified and totally ramified, since we can always decompose a finite extension as the composition of an unramified and a totally ramified extension.
If L'/L is unramified, we choose a uniformizer π_L of L. Lemma 2.4.3 implies that if ω is a nontrivial element of $\Omega_{\mathcal{O}_K}(\mathcal{O}_L)$, then $\omega = a \cdot d_{L/K}\pi_L$ with $a \in \mathcal{O}_L$ and by lemma 2.4.1 $v(\mathrm{Ann}(\omega)) = v(\mathcal{D}_{L/K}) - v(a)$. We consider $i(\omega) = a \cdot d_{L'/K}\pi_L$; since π_L is also a uniformizer for L', then $v(\mathrm{Ann}(i(\omega))) = v(\mathcal{D}_{L'/K}) - v(a)$. Finally, $v(\mathcal{D}_{L'/K}) = v(\mathcal{D}_{L/K})$, since we have $\mathcal{D}_{L'/L} = \mathcal{O}_{L'}$, thus $\mathrm{Ann}(i(\omega)) = \mathrm{Ann}(\omega) \cdot \mathcal{O}_{L'}$.
If L'/L is totally ramified, we choose $\pi_{L'}$ a uniformizer for L'. Let $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ the minimal polynomial of $\pi_{L'}$ over L; it is an Eisenstein polynomial and so $\pi_L = -a_0$ is a uniformizer for L. We write a nontrivial element of $\Omega_{\mathcal{O}_K}(\mathcal{O}_L)$ as $\omega = a \cdot d_{L/K}\pi_L$ with $a \in \mathcal{O}_L$ and by lemma 2.4.1 $v(\mathrm{Ann}(\omega)) = v(\mathcal{D}_{L/K}) - v(a)$. The image is $i(\omega) = a \cdot d_{L'/K}\pi_L$ and since $\pi_L = a_1\pi_{L'} + a_2\pi_{L'}^2 + \cdots + \pi_{L'}^n$ then

$$d_{L'/K}\pi_L = (a_1 + 2a_2\pi_{L'} + \cdots + n\pi_{L'}^{n-1}) \cdot d_{L'/K}\pi_{L'} = P'(\pi_{L'}) \cdot d_{L'/K}\pi_{L'}$$

Thus, $i(\omega) = P'(\pi_{L'}) \cdot a \cdot d_{L'/K}\pi_{L'}$ so we have $v(\mathrm{Ann}(i(\omega))) = v(\mathcal{D}_{L'/K}) - v(P'(\pi_{L'})) - v(a)$; reminding that $v(P'(\pi_{L'})) = v(\mathcal{D}_{L'/L})$, we get

$$v(\mathrm{Ann}(i(\omega))) = v(\mathcal{D}_{L'/K}) - v(\mathcal{D}_{L'/L}) - v(a) = v(\mathcal{D}_{L/K}) - v(a) = v(\mathrm{Ann}(\omega))$$

so we obtain $\mathrm{Ann}(i(\omega)) = \mathrm{Ann}(\omega) \cdot \mathcal{O}_{L'}$. □

Lemma 2.2.3 implies that $\Omega = \Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{\mathbb{Q}}_p}) = \varinjlim \Omega_{\mathcal{O}_K}(\mathcal{O}_L)$ where the limit is over all L/K finite extensions. The previous lemma implies that the canonical maps $\Omega_{\mathcal{O}_K}(\mathcal{O}_L) \to \Omega$ are injective, thus we can identify $\Omega_{\mathcal{O}_K}(\mathcal{O}_L)$ with a $\mathcal{O}_L-$submodule of Ω.
Moreover, the previous lemma shows that if $\omega \in \Omega$ and L/K finite extension such that $\omega \in \Omega_{\mathcal{O}_K}(\mathcal{O}_L)$ and denoting with $\mathfrak{a}$ the annihilator of ω considered as element of $\Omega_{\mathcal{O}_K}(\mathcal{O}_L)$, then, passing to the limit, $\mathrm{Ann}(\omega)$ as element of Ω is $\mathfrak{a} \cdot \mathcal{O}_{\overline{\mathbb{Q}}_p}$. In particular, $\mathrm{Ann}(\omega)$ is a principal ideal of $\mathcal{O}_{\overline{\mathbb{Q}}_p}$ with same $p-$adic valuation of $\mathfrak{a}$.

Lemma 2.4.5. *Let $\omega, \omega' \in \Omega$. Then there exists $c \in \mathcal{O}_{\overline{K}}$ such that $\omega' = c\omega$ if and only if $\mathrm{Ann}(\omega) \subset \mathrm{Ann}(\omega')$.*

Proof. It's clear that if $\omega' = c\omega$ then $\mathrm{Ann}(\omega) \subset \mathrm{Ann}(\omega')$.
We assume $\mathrm{Ann}(\omega) \subset \mathrm{Ann}(\omega')$. We can also assume $\omega' \neq 0$, that implies $\omega \neq 0$. From the limit description of Ω, we have that $\omega, \omega' \in \Omega_{\mathcal{O}_K}(\mathcal{O}_L)$ for a finite extension L/K. Let π_L be a uniformizer for L; we have $\omega = a \cdot d_{L/K}\pi_L$ and $\omega' = a' \cdot d_{L/K}\pi_L$ for some $a, a' \in \mathcal{O}_L$. The assumption of $\omega, \omega' \neq 0$ implies that $v(\mathcal{D}_{L/K}) > v(a)$ and $v(\mathcal{D}_{L/K}) > v(a')$, so

$v(\mathrm{Ann}(\omega)) = v(\mathcal{D}_{L/K}) - v(a)$ and $v(\mathrm{Ann}(\omega')) = v(\mathcal{D}_{L/K}) - v(a')$. The assumption $\mathrm{Ann}(\omega) \subset \mathrm{Ann}(\omega')$ implies that $v(a') \geq v(a)$ hence there exists $c \in \mathcal{O}_L$ such that $a' = ca$, thus $\omega' = c\omega$. □

Lemma 2.4.6. *Let $\Omega_0 = \Omega_{\mathcal{O}_{K_0}}(\mathcal{O}_{\overline{K}})$. Then the canonical map $pr : \Omega_0 \to \Omega$ is surjective and its kernel are the differentials that are annihilated by $\mathcal{D}_{K/K_0}$. More precisely, if $\omega \in \Omega_0$ we have*

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

.

Proof. The proof derives by the limit on L of lemma 2.4.2 for $K' = K_0$ and $K'' = K$, since we know that $\omega \in \Omega_0$ is also an element of $\Omega_{\mathcal{O}_{K_0}}(\mathcal{O}_L)$ for some L/K_0 finite. □

Lemma 2.4.7. *Let ω_0 be a generator of ω_Γ and let $u = (u_n)_{n\in\mathbb{N}}$ a generator of $T_p(\Gamma)$. For every integer $r \geq 0$ we have*

$$v(\mathrm{Ann}(\langle u_r, \omega_0\rangle)) = \max\left(0, r - \frac{1}{p-1} - v(\mathcal{D}_{K/K_0})\right).$$

Proof. Lemma 2.4.6 allows to assume that $K = K_0$, i.e. that $K/\mathbb{Q}_p$ is unramified. We can also assume $r \geq 1$. We have already seen that $u_r = \epsilon_r - 1$ where ϵ_r is a p^r-adic root of unity and that $\omega_0 = \frac{1}{1+x}dx$. We have discussed in section 1.4 that $F_r = \mathbb{Q}_p(u_r)$ is a totally ramified extension of $F = \mathbb{Q}_p$ with uniformizer u_r. We have also computed in lemma 1.4.5 $v(\mathcal{D}_{F_r/F}) = r - \frac{1}{p-1}$. Since K/F is unramified, then u_r is also a uniformizer for $K_r = K(u_r)$, so we get $[K_r : K] = [F_r : F] = \phi(p^r)$. Therefore the minimal polinomial of π_r over K is the minimal polinomial of π_r over $F = \mathbb{Q}_p$, so

$$v(\mathrm{Ann}(d\pi_r)) = v(\mathcal{D}_{F_r/F}) = r - \frac{1}{p-1}.$$

Moreover, $\frac{1}{1+\pi_r}$ is a unit in $\mathcal{O}_{F_r}$ so we have $v(\mathrm{Ann}(\langle u_r, \omega_0\rangle)) = r - 1/(p-1)$. □

Conclusion of proof of Theorem 2.3.2.
Assuming again the choice of generators u and ω_0, we fix $\omega \in \Omega$. We can choose r big enough in order to have $v(\mathrm{Ann}(\omega)) \leq r - 1/(p-1) - v(\mathcal{D}_{K/K_0})$. Thus by lemma 2.4.7 we have that $\mathrm{Ann}(\langle u_r, \omega_0\rangle) \subset \mathrm{Ann}(\omega)$ and by lemma 2.4.5 there exists $c \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$ such that $\omega = c\langle u_r, \omega_0\rangle$. Therefore,

$$\omega = \xi(p^{-r}c \otimes u \otimes \omega_0)$$

and this prove that ξ is surjective.
Every element $\alpha \in \overline{\mathbb{Q}}_p \otimes T_p(\Gamma) \otimes \omega_\Gamma$ can be written uniquely as $a \otimes u \otimes \omega_0$ with $a \in \overline{\mathbb{Q}}_p$. We choose r big enough such that $r \geq 1/(p-1) + v(\mathcal{D}_{K/K_0})$ and such that $a_r = p^r a \in \mathcal{O}_{\overline{\mathbb{Q}}_p}$. Then by lemma 2.4.7, $\xi(\alpha) = a_r\langle u_r, \omega_0\rangle$ is zero if and only if $v(a_r) \geq r - 1/(p-1) - v(\mathcal{D}_{K/K_0})$ that is equivalent to $v(a) \geq -1/(p-1) - v(\mathcal{D}_{K/K_0})$. Thus the kernel of ξ is $\mathfrak{a}_{K,\Gamma} \otimes T_p(\Gamma) \otimes \omega_\Gamma$.

Chapter 3

Hodge–Tate decomposition of the Tate module of an abelian variety

In this final chapter we will prove the Hodge–Tate decomposition for the Tate module of an abelian variety over K with *good reduction* (following [Fon82]). This last assumption is not necessary as shown in Fontaine's paper, but it will ease the dissertation from a geometric point of view. We will assume the results on abelian varieties stated in chapter 0, whose main references are [Mil86] and [MRM74]; all the results are generalizations of results on elliptic curve presented in [Sil09].

3.1 Tate-Raynaud theorem

Let X be an abelian variety over K of dimension d and let $\Omega_X = \Omega^1_{X/K}$ the sheaf of differential forms.

Theorem 3.1.1 (Tate, Raynaud). *There exists an injective K-linear and functorial (in X) map*

$$\rho_X : \Omega_X(X) \to \mathrm{Hom}_{\mathbb{Z}_p[G]}(T_p(X), \mathbb{C}_p(1)).$$

Definition of ρ_X
As mentioned, we assume X to have *good reduction*, i.e. there exists an abelian scheme $\mathfrak{X}$ defined over $\mathcal{O}_K$ such that $X = \mathfrak{X} \times_{Spec(\mathcal{O}_K)} \mathrm{Spec}K$.

$$\begin{tikzcd}
X \arrow[r] \arrow[d] & \mathfrak{X} \arrow[d] \\
\text{Spec } K \arrow[r] & \text{Spec } \mathcal{O}_K
\end{tikzcd}$$

This reduction needs also to be compatible with the two operations, i.e.

$$\begin{tikzcd}
X \times X \arrow[r, "m_X"] \arrow[d] & X \arrow[d] \\
\mathfrak{X} \times \mathfrak{X} \arrow[r, "m_{\mathfrak{X}}"] & \mathfrak{X}
\end{tikzcd}$$

is a commutative diagram of schemes over $\mathrm{Spec}\mathcal{O}_K$ and similarly for the identity and the inverse morphism.
If $u : \text{Spec } \mathcal{O}_{\overline{\mathbb{Q}}_p} \to \mathfrak{X}$ is a point of $\mathfrak{X}(\mathcal{O}_{\overline{\mathbb{Q}}_p})$ and ω is a global section of the sheaf $\Omega_{\mathfrak{X}}$, then

$u^*(\omega)$ is an element of $\Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{\mathbb{Q}}_p}) = \Omega$. Indeed, $u^*(\omega)$ is the image of ω under the map $u^* : \Omega_{\mathfrak{X}/\mathrm{Spec}\mathcal{O}_K} \to \Omega_{\mathrm{Spec}\mathcal{O}_{\overline{\mathbb{Q}}_p}/\mathrm{Spec}\mathcal{O}_K} = \Omega$.
Thus, we can define a map

$$\langle , \rangle : \Omega_{\mathfrak{X}}(\mathfrak{X}) \times \mathfrak{X}(\mathcal{O}_{\overline{\mathbb{Q}}_p}) \to \Omega$$

mapping (ω, u) to $\langle \omega, u\rangle = u^*(\omega)$. This map is of course $\mathcal{O}_K$-linear in the first variable; since the action of $g \in G$ on u is given by the composition with an isomorphism of $\mathrm{Spec}\mathcal{O}_{\overline{\mathbb{Q}}_p}$, the map verifies $\langle \omega, gu\rangle = g(\langle \omega, u\rangle)$ for every $g \in G$, $u \in \mathfrak{X}(\mathcal{O}_{\overline{\mathbb{Q}}_p})$ and $\omega \in \Omega_{\mathfrak{X}}(\mathfrak{X})$.

Lemma 3.1.2. *We have an isomorphism of K-vector spaces $\Omega_X(X) = K \otimes_{\mathcal{O}_K} \Omega_{\mathfrak{X}}(\mathfrak{X})$ and an isomorphism of groups $\mathfrak{X}(\mathcal{O}_{\overline{\mathbb{Q}}_p}) = X(\overline{\mathbb{Q}}_p)$.*

Proof. Using proposition 8.10 of [Har13], we have that $\Omega_X(X) \cong g^*\Omega_{\mathfrak{X}}(\mathfrak{X})$ where $g : X \to \mathfrak{X}$ is the projection map given by the base extension. For every affine open $U = \mathrm{Spec}A$ of $\mathfrak{X}$, we have $V = U \times_{\mathrm{Spec}\mathcal{O}_K} \mathrm{Spec}\ K = \mathrm{Spec}(A \otimes_{\mathcal{O}_K} K)$ is an affine open of X. So $\Omega_X(V) = \Omega_{V/K}(V) = \Omega_K(A \otimes_{\mathcal{O}_K} K) = \Omega_{\mathcal{O}_K}(A) \otimes_{\mathcal{O}_K} K = \Omega_{\mathfrak{X}}(U) \otimes_{\mathcal{O}_K} K$, where we used the compatibility of tensor product and Kähler differentials. Since it holds for every affine open U and the gluing is unique, we get $\Omega_X(X) = \Omega_{\mathfrak{X}}(\mathfrak{X}) \otimes_{\mathcal{O}_K} K$.

Regarding the second part, we can identify $X(\overline{\mathbb{Q}}_p)$ with $\mathfrak{X}(\overline{\mathbb{Q}}_p)$ just using the universal property of base extension. Then, we apply the Valuative Criterion of properness to the proper morphism $\mathfrak{X} \to \mathrm{Spec}\ \mathcal{O}_K$:

$$\begin{tikzcd}
\mathfrak{X} \arrow[r] & \mathrm{Spec}\ \mathcal{O}_K \\
\mathrm{Spec}\ \overline{\mathbb{Q}}_p \arrow[u] \arrow[r] & \mathrm{Spec}\ \mathcal{O}_{\overline{\mathbb{Q}}_p} \arrow[u] \arrow[ul, dotted]
\end{tikzcd}$$

Indeed, for every $u : \mathrm{Spec}\ \overline{\mathbb{Q}}_p \to \mathfrak{X}$, u is extended uniquely to $\mathrm{Spec}\mathcal{O}_K$ since we are working with schemes over $\mathcal{O}_K$; hence the valuation criterion implies a unique factorization through Spec $\mathcal{O}_{\overline{\mathbb{Q}}_p}$. Finally, these identifications commute with operations $m_X, m_{\mathfrak{X}}$ since the operations commute with the projection morphism $X \to \mathfrak{X}$. □

Proposition 3.1.3. *We have that*

- *the map $\omega \mapsto 1 \otimes \omega$ from $\Omega_{\mathfrak{X}}(\mathfrak{X})$ to $\Omega_X(X)$ is injective;*
- *if $\omega \in \cdot\Omega_{\mathfrak{X}}(\mathfrak{X})$ and $u_1, u_2 \in \mathfrak{X}(\mathcal{O}_{\overline{\mathbb{Q}}_p}) = X(\overline{\mathbb{Q}}_p)$ then*

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

Proof. It is sufficient to prove each part independently.

- Since $\mathrm{Spec}\mathcal{O}_K$ is Noetherian, then $\Omega_{\mathfrak{X}}$ is a coherent sheaf, so $\Omega_{\mathfrak{X}}(\mathfrak{X})$ is finitely generated as $\mathcal{O}_K-$module since it's a coherent sheaf on a finite type scheme over $\mathcal{O}_K$. Since $\mathfrak{X} \to \mathrm{Spec}\mathcal{O}_K$ is smooth, then $\Omega_{\mathfrak{X}}$ is also a locally free $\mathcal{O}_{\mathfrak{X}}$-module of finite rank. Hence, the global sections $\Omega_{\mathfrak{X}}(\mathfrak{X})$ is torsion free and the kernel of the map $\omega \mapsto 1 \otimes \omega$ is the torsion of $\Omega_{\mathfrak{X}}(\mathfrak{X})$.

- Using the fundamental property of the product and the one of the fiber product, we have $X \times X = (\mathfrak{X} \times \mathfrak{X}) \times_{\text{Spec } \mathcal{O}_K} \text{Spec } K$. We know that the differential forms of $\Omega_X(X)$ are invariant, i.e. that $pr_{1,X}^*(\omega) + pr_{2,X}^*(\omega) = m_X^*(\omega)$ for every $\omega \in \Omega_X(X)$. Moreover, by the functoriality of the differentials, we have the following commutative diagrams:

$$\begin{tikzcd}
\Omega_{\mathfrak{X}}(\mathfrak{X}) \arrow[r, "-\otimes K"] \arrow[d] & \Omega_X(X) \arrow[d] \\
\Omega_{\mathfrak{X}\times\mathfrak{X}}(\mathfrak{X} \times \mathfrak{X}) \arrow[r, "-\otimes K"'] & \Omega_{X\times X}(X \times X)
\end{tikzcd}$$

  where the vertical arrows are $pr_{1,\mathfrak{X}}^*$ and $pr_{1,X}^*$ (for pr_2 and m as well). Thus if $\omega \in \Omega_{\mathfrak{X}}(\mathfrak{X})$, then $pr_{1,\mathfrak{X}}^*(\omega) + pr_{2,\mathfrak{X}}^*(\omega) - m_{\mathfrak{X}}^*(\omega)$ is in the kernel of $\Omega_{\mathfrak{X}\times\mathfrak{X}}(\mathfrak{X} \times \mathfrak{X}) \to \Omega_{X\times X}(X \times X)$ that is $\Omega_{\mathfrak{X}\times\mathfrak{X}}(\mathfrak{X} \times \mathfrak{X})_{tor}$. The same reasoning for the previous point implies that the torsion is trivial, so $\Omega_{\mathfrak{X}\times\mathfrak{X}}(\mathfrak{X} \times \mathfrak{X})$ is torsion free, hence $pr_{1,\mathfrak{X}}^*(\omega) + pr_{2,\mathfrak{X}}^*(\omega) = m_{\mathfrak{X}}^*(\omega)$ for every $\omega \in \Omega_{\mathfrak{X}}(\mathfrak{X})$. Let u_1, u_2 two points of $\mathfrak{X}(\mathcal{O}_{\overline{\mathbb{Q}}_p})$ and let v be the point (u_1, u_2) of $\mathfrak{X} \times \mathfrak{X}$; then $u_1 = pr_{1,\mathfrak{X}} \circ v$, $u_2 = pr_{2,\mathfrak{X}} \circ v$ and $u_1 + u_2 = m_{\mathfrak{X}} \circ v$ and also $u_1^*(\omega) = v^*(pr_{1,\mathfrak{X}}^*(\omega))$, $u_2^*(\omega) = v^*(pr_{2,\mathfrak{X}}^*(\omega))$. Finally,

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

  for all $\omega \in \Omega_{\mathfrak{X}}(\mathfrak{X})$.

□

Using the previous proposition, we can define a pairing

$$\Omega_{\mathfrak{X}}(\mathfrak{X}) \times X(\overline{\mathbb{Q}}_p) \to \Omega$$

that is $\mathcal{O}_K-$linear in the first variable and $\mathbb{Z}[G]-$linear in the second; this pairing defines an $\mathcal{O}_K-$linear map $\Omega_{\mathfrak{X}}(\mathfrak{X}) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{X}(\overline{\mathbb{Q}}_\mathrm{p}), \Omega)$. Moreover, defining $V_p(X) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\mathrm{p}^{-1}], \mathrm{X}(\overline{\mathbb{Q}}_\mathrm{p}))$ we need a lemma.

Lemma 3.1.4. *We have the following $\mathcal{O}_K-$module isomorphism:*

$$V_p(\Omega) = \mathrm{Hom}_{\mathbb{Z}_\mathrm{p}}(\mathbb{Q}_\mathrm{p}, \Omega) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\mathrm{p}^{-1}], \Omega)$$

and the following $\mathcal{O}_K$-inclusion:

$$\mathrm{Hom}_{\mathbb{Z}[\mathrm{G}]}(\mathrm{X}(\overline{\mathbb{Q}}_\mathrm{p}), \Omega) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}[\mathrm{G}]}(\mathrm{V_p(X)}, \mathrm{V_p}(\Omega)).$$

Proof. For the first isomorphism, we consider $\mathbb{Z}[p^{-1}] \subset \mathbb{Q}_p$, so the restriction is an injective map $\mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p, \Omega) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], \Omega)$. On the other hand, given a map $\phi \in Hom_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], \Omega)$, we consider the map $\phi'(a) = ap^{-v(a)}\phi(p^{v(a)})$ for $a \in \mathbb{Q}_p$. This map is the inverse of the restriction.
Regarding the inclusion, the map is given by post-composition. Let $\phi : X(\overline{\mathbb{Q}}_p) \to \Omega$ and assume $\phi \circ f = 0$ for every $f \in V_p(X)$. Let $f_x \in V_p(X)$ such that $f(1) = x$; this is always possible since $X(\overline{\mathbb{Q}}_p)$ is p-divisible. Then $\phi(f_x(1)) = \phi(x) = 0$ and varying $x \in X(\overline{\mathbb{Q}}_p)$ we get that the post composition map $\mathrm{Hom}_{\mathbb{Z}[G]}(X(\overline{\mathbb{Q}}_p), \Omega) \to \mathrm{Hom}_{\mathbb{Z}[G]}(V_p(X), V_p(\Omega))$ is injective. □

By lemma 3.1.4, the map $\Omega_{\mathfrak{X}}(\mathfrak{X}) \to \mathrm{Hom}_{\mathbb{Z}[G]}(X(\overline{\mathbb{Q}}_p), \Omega)$ induces an $\mathcal{O}_K-$linear map $\Omega_{\mathfrak{X}}(\mathfrak{X}) \to \mathrm{Hom}_{\mathbb{Z}[G]}(V_p(X), V_p(\Omega))$ and by extension of scalars we obtain a $K-$linear map

$$\hat{\rho}_X = \hat{\rho}_{X,r} : \Omega_X(X) = K \otimes_{\mathcal{O}_K} \Omega_{\mathfrak{X}}(\mathfrak{X}) \to \mathrm{Hom}_{\mathbb{Z}[G]}(V_p(X), V_p(\Omega))$$

since $V_p(\Omega)$ is already a $K-$vector space. Finally, for every $\omega \in \Omega_X(X)$ the restriction of $\rho_X(\omega)$ to $T_p(X)$ is $\mathbb{Z}_p-$linear, so this gives the $K-$linear map

$$\rho_X = \rho_{X,r} : \Omega_X(X) \to \mathrm{Hom}_{\mathbb{Z}[G]}(T_p(X), V_p(\Omega))$$

We remind that Theorem 2.3.2 gives $V_p(\Omega) \cong \mathbb{C}_p(1)$, so ρ_X is the candidate solution for Tate-Raynaud theorem.

Lemma 3.1.5. *The maps $\hat{\rho}_X$ and ρ_X depend functorially on X.*

Proof. It is sufficient to prove this for $\hat{\rho}$. The commutativity of the following diagram

$$\begin{tikzcd}
\Omega_X(X) \arrow[r] \arrow[d] & \mathrm{Hom}_{\mathbb{Z}[G]}(V_p(X), V_p(\Omega)) \arrow[d] \\
\Omega_{X'}(X') \arrow[r] & \mathrm{Hom}_{\mathbb{Z}[G]}(V_p(X'), V_p(\Omega))
\end{tikzcd}$$

is given by the compatibility of the reductions $\mathfrak{X}$ and $\mathfrak{X}'$ (that we have to assume). In this sense $\hat{\rho}_X$ and ρ_X are functorial in X. □

3.2 Proof of Tate-Raynaud theorem

We are left to prove that ρ_X is injective. We will subdivide this task in two propositions:

Proposition 3.2.1. *The map $\hat{\rho}_X$, defined in section 3.1, is injective.*

Proposition 3.2.2. *The map $\mathrm{Hom}_{\mathbb{Z}_p[G]}(V_p(X), \mathbb{C}_p(1)) \to \mathrm{Hom}_{\mathbb{Z}_p[G]}(T_p(X), \mathbb{C}_p(1))$ induced by the inclusion of $T_p(X)$ in $V_p(X)$ is injective.*

We begin with a lemma:

Lemma 3.2.3. *For every K-rational point u of X we have that the completion of the local ring at u is $\hat{\mathcal{O}}_{X,u} = K[\![\xi_1, \xi_2, \dots, \xi_d]\!]$; analogously for $\mathfrak{X}$ and $\bar{u}$ the corresponding closed point of $\mathfrak{X}$ we have $\hat{\mathcal{O}}_{\mathfrak{X},\bar{u}} = \mathcal{O}_K[\![\xi_1, \xi_2, \dots, \xi_d]\!]$.*

Proof. We remind that by smoothness $\mathcal{O}_{X,u}$ is a regular local ring of dimension d. This means that $\mathfrak{m}_u/\mathfrak{m}_u^2$ is a $\mathcal{O}_{X,u}/\mathfrak{m}_u = K$-vector space of dimension d and we consider $m_1, m_2, \dots, m_d \in \mathfrak{m}_u$ a K-basis. By completion, we have a morphism $\phi : K[\![\xi_1, \xi_2, \dots, \xi_d]\!] \to \hat{\mathcal{O}}_{X,u}$ mapping ξ_i to the image of m_i in $\hat{\mathcal{O}}_{X,u}$ and mapping K to the image of the global regular maps; by Nakayama's lemma the homomorphism ϕ is surjective. Since $\hat{\mathfrak{m}}_u = \mathfrak{m}_u\hat{\mathcal{O}}_{X,u}$, then the residue field of $\hat{\mathcal{O}}_{X,u}$ is again K. The ring $\hat{\mathcal{O}}_{X,u}$ is a regular local ring, a fortiori an integral domain. Hence ϕ is a surjective ring homomorphism between two integral domains of the same dimension and thus is an isomorphism.
The case for $\mathfrak{X}$ is analogous, with the accuracy that $\mathcal{O}_{\mathfrak{X},\bar{u}}$ is a regular local ring of dimension $d+1$. □

Proof of proposition 3.2.1 Let e the identity point of X. We define $\Omega^{\text{cont}}_{\mathcal{O}_K}(\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}})$ as the $\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}}$ module of $\mathcal{O}_K$ continuous differentials of $\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}}$. It is defined as the solution of the universal problem for *continuous* $\mathcal{O}_K$-derivations. It can be proved that in this case it is a $\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}}$ free module generated by $d\xi_1, d\xi_2, \ldots, d\xi_d$ and that it is isomorphic to the completion of $\Omega_{\mathcal{O}_K}(\mathcal{O}_{\mathfrak{X},\bar{e}})$ (see [Gro64] 0.20.4.5 and 0.20.7.14.2). We also have the compatibility $(\Omega_{\mathfrak{X}/\mathcal{O}_K})_{\bar{e}} \cong \Omega_{\mathcal{O}_K}(\mathcal{O}_{\mathfrak{X},\bar{e}})$, so we have an injective $\mathcal{O}_K$-linear map

$$\Omega_{\mathcal{O}_K}(\mathcal{O}_{\mathfrak{X},\bar{e}}) \hookrightarrow \Omega^{\text{cont}}_{\mathcal{O}_K}(\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}}).$$

We want to compose this map with the localization $\Omega_{\mathfrak{X}}(\mathfrak{X}) \to \Omega_{\mathcal{O}_K}(\mathcal{O}_{\mathfrak{X},\bar{e}})$. This localization is injective because if a global section $\omega \in \Omega_{\mathfrak{X}}(\mathfrak{X}) \subset \Omega_X(X)$ becomes zero in the stalk $\Omega_{\mathcal{O}_K}(\mathcal{O}_{\mathfrak{X},\bar{e}})$ then it becomes zero in every stalk (global differentials are translation invariant) and by sheaf property $\omega = 0$. Summing up, we have a canonical and injective map

$$\Omega_{\mathfrak{X}}(\mathfrak{X}) \to \Omega^{\text{cont}}_{\mathcal{O}_K}(\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}}).$$

Every continuous $\mathcal{O}_K$-homomorphism of $\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}}$ to $\mathcal{O}_{\overline{\mathbb{Q}}_p}$ corresponds to some $\alpha_1, \alpha_2, \ldots, \alpha_d$ elements of $\mathfrak{m}_{\overline{\mathbb{Q}}_p}$. Then to every $\omega \in \Omega^{\text{cont}}_{\mathcal{O}_K}(\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}})$ and continuous $\mathcal{O}_K$-homomorphism of $\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}}$ to $\mathcal{O}_{\overline{\mathbb{Q}}_p}$ can be associated an element of $\Omega = \Omega_{\mathcal{O}_K}(\mathcal{O}_{\overline{\mathbb{Q}}_p})$ that is ω *computed* in $\alpha_1, \alpha_2, \ldots, \alpha_d$ (the substitution is well-defined since $\alpha_i \in \mathfrak{m}_{\overline{\mathbb{Q}}_p}$). Now, every continuous $\mathcal{O}_K$-homomorphism of $\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}}$ to $\mathcal{O}_{\overline{\mathbb{Q}}_p}$ induces a local homomorphism $\mathcal{O}_{\mathfrak{X},\bar{e}} \to \mathcal{O}_{\overline{\mathbb{Q}}_p}$ which can be identified with a point $\mathfrak{X}(\mathcal{O}_{\overline{\mathbb{Q}}_p}) = X(\overline{\mathbb{Q}}_p)$ by Proposition 2.6.3 in [Mum99]; thus the set of continuous $\mathcal{O}_K$-homomorphisms of $\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}}$ to $\mathcal{O}_{\overline{\mathbb{Q}}_p}$ can be identified with a subset of $\mathfrak{X}(\mathcal{O}_{\overline{\mathbb{Q}}_p}) = X(\overline{\mathbb{Q}}_p)$. When operating on this subset, the pairing $\langle , \rangle$ described in section 3.1 coincides with the pairing on $\Omega_{\mathfrak{X}}(\mathfrak{X})$ considered as element of $\Omega^{\text{cont}}_{\mathcal{O}_K}(\hat{\mathcal{O}}_{\mathfrak{X},\bar{e}})$.
Hence, in order to prove 3.2.1, is sufficient to prove the next lemma:

Lemma 3.2.4. *For every nonzero continuous differential form*

$$\omega = \sum_{i=1}^{d} \alpha_i(\xi_1, \xi_2, \ldots, \xi_d) \cdot d\xi_i \in \Omega^{\text{cont}}_{\mathcal{O}_K}(\mathcal{O}_K[\![\xi_1, \xi_2, \ldots, \xi_d]\!])$$

there exist $x_1, x_2, \ldots, x_d \in \mathfrak{m}_{\overline{\mathbb{Q}}_p}$ *such that* $\sum_{i=1}^{d} \alpha_i(x_1, x_2, \ldots, x_d) \cdot dx_i$ *is a nonzero element of* Ω.

Proof. We first prove this lemma in the case $d = 1$. So we assume $\omega = \alpha(\xi) \cdot d\xi$ with $\alpha(\xi) = \sum_{i=0}^{\infty} a_i \xi^i$ is a formal nonzero power series in ξ with coefficients in $\mathcal{O}_K$. Let v_K the valuation on $\overline{\mathbb{Q}}_p$ normalized for K, i.e. $v(K^\times) = \mathbb{Z}$ and let

$$s = \inf_{i \in \mathbb{N}} v(a_i) \qquad i_0 = \text{smallest integer such that } v(a_{i_0}) = s.$$

For every $x \in \overline{\mathbb{Q}}_\mathfrak{p}$ with $v(x) < 1/i_0$ then $v(a_{i_0} x^{i_0}) < s + 1 \leq v(a_j x^j)$ for every $i \neq i_0$ and this implies $v(\alpha(x)) < s + 1$. Now it's always possible to find a finite extension L/K such that $v(\mathcal{D}_{L/K}) \geq s + 1$ and such $v(\pi_L) < 1/i_0$; an example is a cyclotomic extension K_n for n big enough. Then, under these assumptions, the annihilator of $d\pi_L$ is $\mathcal{O}_{\overline{\mathbb{Q}}_p} \cdot \mathcal{D}_{L/K}$ (see section 2.4), so $\alpha(x) \cdot dx \neq 0$.
The general case is implied by the case $d = 1$ and the next lemma. □

Lemma 3.2.5. *Let $\alpha_1(\xi_1, \xi_2, \dots, \xi_d), \dots, \alpha_d(\xi_1, \xi_2, \dots, \xi_d)$ be formal power series in the variables $\xi_1, \xi_2, \dots, \xi_d$ with coefficients in $\mathcal{O}_K$. Assuming that not all α_i are zero, then there exist formal power series $\phi_1, \phi_2, \dots, \phi_d$ in one variable ξ and coefficients in $\mathcal{O}_K$ such that $\sum_{i=1}^{d} \alpha_i(\phi_1, \phi_2, \dots, \phi_d)\phi_i'$ is a nonzero element of $\mathcal{O}_K[\![\xi]\!]$.*

Proof. First we will assume that a power series $f(\xi_1, \xi_2, \dots, \xi_d) \in \mathcal{O}_K[\![\xi_1, \dots, \xi_d]\!]$ is identically zero if and only every it is evaluated to zero for every choice of $x_1, x_2, \dots, x_d \in \mathfrak{m}_K$. Indeed, this can be proved considering the smallest (by degree) nonzero term among the one involving the minimum number of variables; giving those variables a valuation equal to 1 and then giving all the other variables a big enough valuation.

We choose ϕ_i of the form $\phi_i = a_i\xi + bi\xi^2$ with $a_i, b_i \in \mathcal{O}_K$. Writing $\lambda = \sum_{i=1}^{d} \alpha_i(\phi_1, \phi_2, \dots, \phi_d)\phi_i'$ we have

$$\lambda = \sum_{i=1}^{d} \alpha_i(a_1\xi + b_1\xi^2, \dots, a_d\xi + b_d\xi^2) \cdot (a_i + 2b_i\xi).$$

If $\alpha_i = \sum_{m=0}^{\infty} \alpha_{i,m}$ with $\alpha_{i,m}$ a homogeneous polynomial of degree m and if r is the smallest integer such that there exists j with $\alpha_{j,r} \neq 0$ then

$$\lambda = (\sum_i a_i \cdot \alpha_{i,r}(a_1, \dots, a_d)) \cdot \xi^r + \Bigg(\sum_i a_i \cdot \alpha_{i,r+1}(a_1, \dots, a_d) +$$
$$+ \sum_j 2b_j \cdot \alpha_{j,r}(a_1, \dots, a_d) + \sum_{i,j} a_i b_j \cdot \frac{\partial \alpha_{i,r}}{\partial \xi_j}(a_1, \dots, a_d) \Bigg) \cdot \xi^{r+1} + \dots$$

where we have written explicitly only the terms of degree $\leq r+1$. We have 3 cases now.

- If $\sum_i \xi_i \cdot \alpha_{i,r}(\xi_1, \dots, \xi_d) \neq 0$ then there exists $a_1, a_2, \dots, a_d$ such that $\sum_i a_i \cdot \alpha_{i,r}(a_1, \dots, a_d) \neq 0$ so $\lambda \neq 0$ for every choice of the b_i.
- If $\sum_i \xi_i \cdot \alpha_{i,r}(\xi_1, \dots, \xi_d) = 0$, but $\sum_i \xi_i \cdot \alpha_{i,r+1}(\xi_1, \xi_2, \dots, \xi_d) \neq 0$ then there exists $a_1, a_2, \dots, a_d$ such that $\sum_i a_i \cdot \alpha_{i,r+1}(a_1, a_2, \dots, a_d) \neq 0$, so choosing $b_i = 0$ we get $\lambda \neq 0$.
- If $\sum_i \xi_i \cdot \alpha_{i,r}(\xi_1, \dots, \xi_d) = 0$ and $\sum_i \xi_i \cdot \alpha_{i,r+1}(\xi_1, \xi_2, \dots, \xi_d) = 0$, then for every j the derivation of the first identity with respect to ξ_j yields:

  $$\alpha_{j,r}(\xi_1, \xi_2, \dots, \xi_d) + \sum_i \xi_i \cdot \frac{\partial \alpha_{i,r}}{\partial \xi_j}(\xi_1, \xi_2, \dots, \xi_d) = 0$$

  Then

  $$\lambda = \left[\sum_j b_j \Bigg(2\alpha_{j,r}(a_1, \dots, a_d) + \sum_{i,j} a_i \cdot \frac{\partial \alpha_{i,r}}{\partial \xi_j}(a_1, \dots, a_d) \Bigg) \right] \cdot \xi^{r+1} + \dots$$
  $$= (\sum_j b_j \cdot \alpha_{j,r}(a_1, \dots, a_d)) \cdot \xi^{r+1} + \dots.$$

  Since we have chosen j and r such that $\alpha_{j,r}(\xi_1, \dots, \xi_d) \neq 0$ then we can find $a_1, a_2, \dots, a_d$ such that $\alpha_{j,r}(a_1, \dots, a_d) \neq 0$. We conclude choosing $b_j = 1$ and the other $b_i = 0$ in order to get $\lambda \neq 0$.

□

Proof proposition 3.2.2. For every abelian group H, we define $V_p(H) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], H)$. The subgroup $X_{p^\infty}(\overline{\mathbb{Q}}_p)$ is the normal subgroup of $X(\overline{\mathbb{Q}}_p)$ given by the points of order a power of p. Since $X(\overline{\mathbb{Q}}_p)$ is p-divisible, then $J = X(\overline{\mathbb{Q}}_p)/X_{p^\infty}(\overline{\mathbb{Q}}_p)$ is uniquely p-divisible, i.e. for every $j \in J$ there exists a unique j' such that $pj' = j$. So we have an exact sequence of abelian groups

$$0 \to X_{p^\infty}(\overline{\mathbb{Q}}_p) \to X(\overline{\mathbb{Q}}_p) \to J \to 0.$$

Applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], -)$ the following sequence is exact:

$$0 \to V_p(X_{p^\infty}(\overline{\mathbb{Q}}_p)) \to V_p(X(\overline{\mathbb{Q}}_p)) \to J.$$

Indeed, we used the left exactness of Hom and that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], J) = J$ since J is uniquely p-divisible. Moreover, we want to prove also and that $V_p(X(\overline{\mathbb{Q}}_p)) \to J$ is surjective.

Indeed, if $j \in J$, then we can define a map $\mathbb{Z}[p^{-1}] \to X(\overline{\mathbb{Q}}_p)$ mapping 1 to j, mapping p^{-1} to a p-th root of j and so on. This is always possible since $X(\overline{\mathbb{Q}}_p)$ is $p-$divisible and all the possible choices will be mapped to the same j as element of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[p^{-1}], J)$. So we have the following exact sequence:

$$0 \to V_p(X_{p^\infty}(\overline{\mathbb{Q}}_p)) \to V_p(X(\overline{\mathbb{Q}}_p)) \to J.$$

We apply the contravariant $\mathrm{Hom}_{\mathbb{Z}[G]}(-, \mathbb{C}_p(1))$ recalling that $V_p(X_{p^\infty}(\overline{\mathbb{Q}}_p)) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(X)$, hence the exact sequence

$$0 \to \mathrm{Hom}_{\mathbb{Z}[G]}(J, \mathbb{C}_p(1)) \to \mathrm{Hom}_{\mathbb{Z}[G]}(V_p(X), \mathbb{C}_p(1)) \to \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(X), \mathbb{C}_p(1)).$$

Thus the kernel of the restriction $\mathrm{Hom}_{\mathbb{Z}[G]}(V_p(X), \mathbb{C}_p(1)) \to \mathrm{Hom}_{\mathbb{Z}[G]}(T_p(X), \mathbb{C}_p(1))$ can be identified with $\mathrm{Hom}_{\mathbb{Z}[G]}(J, \mathbb{C}_p(1))$.

Since $X(\overline{\mathbb{Q}}_p)$ is the union of $X(L)$ for every finite Galois extension L/K, then $J = \cup J^H$ for all H normal open subgroup of G. If $f : J \to \mathbb{C}_p(1)$ is a $\mathbb{Z}[G]$ homomorphism, then, for every normal open subgroup H, we have $f(J^H) \subset \mathbb{C}_p(1) = 0$ since we apply Theorem 1.6.5 to $H = \mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$ for some L/K finite Galois extension. Hence, since $f(J) = \cup f(J^H) = 0$ we proved that the restriction map $\mathrm{Hom}_{\mathbb{Z}[G]}(V_p(X), \mathbb{C}_p(1)) \to \mathrm{Hom}_{\mathbb{Z}[G]}(T_p(X), \mathbb{C}_p(1))$ is injective and this implies that the map $\mathrm{Hom}_{\mathbb{Z}_p[G]}(V_p(X), \mathbb{C}_p(1)) \to \mathrm{Hom}_{\mathbb{Z}_p[G]}(T_p(X), \mathbb{C}_p(1))$ is injective. □

3.3 Hodge-Tate decomposition

We are now able to prove the Hodge-Tate decomposition for the Tate module of an abelian variety X with good reduction. We need to work with the dual abelian variety $X^\vee$; it can be proved that $X^\vee$ has good reduction as well. We define the K-vector spaces $\mathrm{Lie}X = \mathrm{Hom}_K(\Omega_X(X), K)$ and $\mathrm{Lie}X^\vee = \mathrm{Hom}_K(\Omega_{X^\vee}(X^\vee), K)$; they both are vector spaces of dimension d equal to the dimension of X and $X^\vee$ and they are both endowed with a trivial G-action.

Theorem 3.3.1. *There exists a G-equivariant $\mathbb{C}_p$-linear isomorphism*

$$T_p(X) \otimes_{\mathbb{Z}_p} \mathbb{C}_p \cong ((\mathrm{Lie}X^\vee)^* \otimes_K \mathbb{C}_p) \oplus (\mathrm{Lie}X \otimes_K \mathbb{C}_p(1)).$$

Proof of Theorem 3.3.1
The Tate-Reynaud theorem yields an injective K-linear map

$$\Omega_X(X) \to \mathrm{Hom}_{\mathbb{Z}_p[G]}(T_p(X), \mathbb{C}_p(1)) = \mathrm{Hom}_{\mathbb{C}_p[G]}(T_p(X) \otimes_{\mathbb{Z}_p} \mathbb{C}_p, \mathbb{C}_p(1))$$

that implies a surjective K-linear map and G-equivariant map

$$T_p(X) \otimes_{\mathbb{Z}_p} \mathbb{C}_p(-1) \to \mathrm{Hom}_K(\Omega_X(X), K)$$

hence a surjective $\mathbb{C}_p$-linear map and G-equivariant map

$$T_p(X) \otimes_{\mathbb{Z}_p} \mathbb{C}_p \to \mathrm{Lie}X \otimes \mathbb{C}_p(1).$$

Applying the Tate-Raynaud theorem to $X^\vee$ leads to the G-equivariant injection

$$(\mathrm{Lie}X^\vee)^* \otimes \mathbb{C}_p \to (T_p(X^\vee) \otimes \mathbb{C}_p)^*(1).$$

Now we consider the Weil pairing $T_p(X) \times T_p(X^\vee) \to \mathbb{Z}_p(1)$; it is a nondegenerate pairing so it induces a perfect pairing $(T_p(X) \otimes \mathbb{C}_p) \times (T_p(X^\vee) \otimes \mathbb{C}_p) \to \mathbb{C}_p(1)$, i.e.

$$(T_p(X^\vee) \otimes \mathbb{C}_p)^*(1) \cong T_p(X) \otimes \mathbb{C}_p.$$

We can then assemble a sequence

$$0 \to (\mathrm{Lie}X^\vee)^* \otimes \mathbb{C}_p \xrightarrow{\alpha} T_p(X) \otimes \mathbb{C}_p \xrightarrow{\beta} \mathrm{Lie}X \otimes \mathbb{C}_p(1) \to 0 \qquad (*)$$

where α (resp. β) is an injective (resp. surjective) G-equivariant $\mathbb{C}_p$-linear map.

Proposition 3.3.2. *The sequence* $(*)$ *is exact.*

Proof. We have that $\dim_{\mathbb{C}_p}\mathrm{Im}\alpha = \dim_{\mathbb{C}_p}(\mathrm{Lie}X^\vee)^* \otimes \mathbb{C}_p = d$; moreover $\dim_{\mathbb{C}_p}\ker\beta = 2d - d = d$ since $T_p(X)$ is a free $\mathbb{Z}_p-$module of rank $2d$. Hence to prove that $(*)$ is exact, it is sufficient to prove $\beta \circ \alpha = 0$.
Let $e_1, e_2, \ldots, e_d$ basis of $(\mathrm{Lie}X^\vee)^*$, then $e_1 \otimes 1, e_2 \otimes 1, \ldots, e_d \otimes 1$ is a $\mathbb{C}_p$-basis of $(\mathrm{Lie}X^\vee)^* \otimes \mathbb{C}_p$. Since $e_i \otimes 1$ is G-invariant then the $(\beta \circ \alpha)(e_i \otimes 1) \in (\mathrm{Lie}X \otimes \mathbb{C}_p(1))^G = 0$ since Theorem 1.6.5. This holds for every e_i, so $\beta \circ \alpha = 0$. □

Proposition 3.3.3. *The sequence* $(*)$ *is G-equivariant split.*

Proof. The sequence is exact and therefore it splits as sequence of $\mathbb{C}_p$-vector spaces (finite dimensional vector spaces are projective). We need then to prove that there exists a G_K-equivariant splitting.
We start by twisting by $\mathbb{C}_p(-1)$ the sequence:

$$0 \to (\mathrm{Lie}X^\vee)^* \otimes \mathbb{C}_p(-1) \xrightarrow{\alpha} T_p(X) \otimes \mathbb{C}_p(-1) \xrightarrow{\beta} \mathrm{Lie}X \otimes \mathbb{C}_p \to 0.$$

Let $v_1, v_2, \ldots, v_d$ basis of $\mathrm{Lie}X$. Since the sequence splits there exists $w \in W = T_p(X) \otimes \mathbb{C}_p(-1)$ such that $\beta(w) = e_1 \otimes 1$. For every $\sigma \in G$, we have

$$\beta(\sigma w - w) = \sigma\beta(w) - \beta(w) = e_1 \otimes 1 - e_1 \otimes 1 = 0$$

so $\sigma w - w \in \alpha((\mathrm{Lie}X^\vee)^* \otimes \mathbb{C}_p(-1))$. Thus for every $\sigma \in G$ there exists $\gamma_\sigma \in (\mathrm{Lie}X^\vee)^* \otimes \mathbb{C}_p(-1)$ such that $\alpha(\gamma_\sigma) = \sigma w - w$. The map

$$\begin{aligned} \gamma : G &\to (\mathrm{Lie}X^\vee)^* \otimes \mathbb{C}_p(-1) \\ \sigma &\mapsto \gamma_\sigma \end{aligned}$$

is a continuous 1-cocycle. To prove $\gamma_{\sigma\tau} = \sigma\gamma_\tau + \gamma_\sigma$ it is sufficient to prove that the two terms have same through the injective G-equivariant map α. Indeed, $\alpha(\gamma_{\sigma\tau}) = \sigma\tau w - w$ and

$$\alpha(\sigma\gamma_\tau - \gamma_\sigma) = \sigma(\tau w - w) + \sigma w - w = \sigma\tau w - w.$$

The cocycle $[\gamma] \in H^1(G, (\mathrm{Lie}X^\vee)^* \otimes \mathbb{C}_p(-1)) = 0$ by Theorem 1.8.1, hence γ is a coboundary, so there exists $y \in U^* \otimes \mathbb{C}_p(-1)$ such that for every $\sigma \in G$, it holds $\gamma_\sigma = \sigma y - y$. Then

$$\sigma w - w = \alpha(\gamma_\sigma) = \alpha(\sigma y - y) = \sigma\alpha(y) - \alpha(y)$$

i.e. $\sigma(w - \alpha(y)) = w - \alpha(y)$ for every $\sigma \in G$. We define $w' = w - \alpha(y)$; w is G-invariant and $\beta(w') = \beta(w - \alpha(y)) = \beta(w) - \beta(\alpha(y)) = e_1 \otimes 1$. Analogously for every e_i, we can find G-invariant elements $w'_i \in W$ such that $\beta(w'_i) = e_i \otimes 1$. The map

$$\begin{aligned} s : \mathrm{Lie}X \otimes \mathbb{C}_p &\to W \\ e_i \otimes 1 &\mapsto w'_i \end{aligned}$$

is a G-equivariant section of β.

□

Bibliography

[Gro64] Alexander Grothendieck. “Éléments de géométrie algébrique: IV. Étude locale des schémas et des morphismes de schémas”. In: *Publications Mathématiques de l'IHÉS* 20 (1964).

[LT65] Jonathan Lubin and John Tate. “Formal complex multiplication in local fields”. In: *Annals of Mathematics* (1965), pp. 380–387.

[CF67] John William Scott Cassels and Albrecht Fröhlich. *Algebraic number theory: proceedings of an instructional conference*. Academic press, 1967.

[Tat67] John T Tate. “p-Divisible groups”. In: *Proceedings of a conference on Local Fields*. Springer. 1967, pp. 158–183.

[MRM74] David Mumford, Chidambaran Padmanabhan Ramanujam, and Jurij Ivanovič Manin. *Abelian varieties*. Vol. 5. Oxford university press Oxford, 1974.

[Spr81] T. Springer. *Linear Algebraic Groups*. Birkhäuser, 1981.

[Fon82] Jean-Marc Fontaine. “Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux”. In: *Inventiones mathematicae* 65.3 (1982), pp. 379–409.

[Mil86] James S Milne. “Abelian varieties”. In: *Arithmetic geometry* (1986), pp. 103–150.

[Mum99] David Mumford. *The red book of varieties and schemes: includes the Michigan lectures (1974) on curves and their Jacobians*. Vol. 1358. Springer Science & Business Media, 1999.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*. Vol. 106. Springer, 2009.

[Jor12] Andrei Jorza. *p-adic Galois Representations*. Math 162b Winter 2012 Lecture Notes California Institute of Technology. 2012. URL: `https://www3.nd.edu/~ajorza/courses/m162b-w2012/notes/lectures.pdf`.

[Har13] Robin Hartshorne. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013.

[Neu13] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Springer Science & Business Media, 2013.

[Ser13] Jean-Pierre Serre. *Local fields*. Vol. 67. Springer Science & Business Media, 2013.