Higher Ramification Theory

Michael Fester

May 18, 2006

Contents

Introduction

In this essay, we present a theorem of Tate which relates p-adic representations with a "Hodge-Tate decomposition" to "locally algebraic" ones. The result appears in Serre's "Abelian ℓ-adic Representations" [**6**], as well as in the lecture notes of Coates [**3**] which, together with Serre's "Local Fields" [**7**], serve as our main references.

Several tools from ramification theory are needed, and we present these in Chapter I. Here we define the ramification groups and establish their basic properties (the theorems of Herbrand and Hasse-Arf). They notably give rise to formulas for the exponent of the different Galois extensions, which in turn are crucial for the definition of so-called "deeply ramified" extensions; for the sake of completeness, we give five equivalent definitions of these (Section 3.1). Then, ramified $\mathbb{Z}_p$-extensions, which are special cases of deeply ramified ones, are discussed (Section 3.2), and used in order to compute cohomology groups tracking the action of certain Galois groups on the completion $\mathbb{C}$ of the algebraic closure of $\mathbb{Q}_p$ (Section 3.2). A brief account on the cohomology of groups, and in particular of finite cyclic groups, is also given (Section 2).

In Chapter II, we prove Tate's theorem. An essential part of the proof is based on a certain character arising from the Lubin-Tate theory of formal groups (Section 1). As a by-product, we obtain almost for free a proof of the theorem of Hasse-Arf discussed in Chapter I. We then introduce p-adic representations, the analogues of the classical complex ones, and define a class of those with a "Hodge-Tate decomposition" (Section 2). Finally, we define "locally algebraic" representations and prove that they coincide with the Hodge-Tate ones (Section 3.1).

Notations and conventions. Throughout, K denotes a field with a normalized discrete valuation v_K for which it is *complete*. We denote by $\mathcal{O}_K$ the ring of integers of K, $\mathfrak{m}_K$ the maximal ideal in $\mathcal{O}_K$, and $k_K = \mathcal{O}_K/\mathfrak{m}_K$ the residue field of K. Unless otherwise stated, for a finite extension L of K, we will always assume that the extension k_L/k_K of residue fields is *separable*. In particular, $\mathcal{O}_L$ is a monogenous extension of $\mathcal{O}_K$.

Acknowledgement. I would like to thank Professor John Coates for proposing this essay topic, which has been a pleasure to work on from the beginning to the end.

CHAPTER 1

Higher ramification theory

The main objective of this chapter is to establish identities for the cohomology groups associated to certain Galois extensions, and which will reveal crucial for the proof of Tate's theorem. We start by giving the elementary properties of ramification groups, and consequently obtain formulas for the different of finite Galois extension L/K. Following Coates and Greenberg [**4**], we then define deeply ramified extensions, and end with examples of such extensions as well as important cohomological interpretations.

1. Ramification groups

1.1. Ramification groups in the upper numbering. Let L/K be a finite Galois extension, and let G be its Galois group. The group G acts on $\mathcal{O}_L$. For $i \geq -1$, we define the *i'th ramification group of* G (in the *lower numbering*) to be the subgroup of G operating trivially on the quotient $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$, that is, the kernel of the action,

$$G_i = \ker(G \to \mathrm{Aut}(\mathcal{O}_L/\mathfrak{m}_L^{i+1})).$$

The group G_{-1} is G itself, and G_0 is the inertia subgroup I of L/K. The G_i's form a decreasing filtration of normal subgroups $G \supset I \supset G_1 \supset G_2 \supset \ldots \supset \{1\}$, which eventually becomes stationary.

Fix a generator x of the $\mathcal{O}_K$-algebra $\mathcal{O}_L$, and define a function i_G on G by

$$i_G(s) = v_L(s(x) - x).$$

Then we have

$$G_i = \{s \in G \mid i_G(s) \geq i + 1\}.$$

Indeed, the image x_i of x in $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$ generates $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$ as an $\mathcal{O}_K$-algebra, and hence s operates trivially on $\mathcal{O}_L/\mathfrak{m}_L^{i+1}$ if and only if $s(x_i) = x_i$.

Let K' be an extension of K contained in L, and let $H = \mathrm{Gal}(L/K')$ be the corresponding Galois group. The ramification groups associated to the extension L/K' are determined by those associated with the extension L/K, as the following obvious Proposition shows:

Proposition 1.1. *We have* $H_i = G_i \cap H$.

In particular, we may take K' to be the maximal unramified extension K^{nr} of K contained in L (in which case L/K^{nr} is totally ramified), so that H is the inertia subgroup G_0 of G. Then, by virtue of the Proposition, the ramification groups G_i of G coincide with the ramification groups H_i of H for all $i \geq 0$. Hence, when investigating the ramification groups of index ≥ 0, it is sufficient to consider the totally ramified case only.

Suppose now, and for the rest of this section, that H is a *normal* subgroup of G, so that G/H can be identified with the Galois group of K'/K. The following result shows that the ramification groups of G/H are determined by those of G:

Proposition 1.2. *Let $\sigma \in G/H$. We have*

$$i_{G/H}(\sigma) = \frac{1}{e_{L/K'}} \sum_{s \to \sigma} i_G(s),$$

the sum being taken over the elements s of G whose image in G/H is σ.

PROOF. The equality holds for $\sigma = 1$, both sides being equal to $+\infty$. Hence, let us assume $\sigma \neq 1$. If x, resp. y, denotes a generator of the $\mathcal{O}_K$-algebra $\mathcal{O}_L$, resp. $\mathcal{O}_{K'}$, we have $i_G(s) = v_L(s(x) - x)$ and $i_{G/H}(\sigma) = v_L(\sigma(y) - y)/e_{L/K'}$, the latter equality following from the formula $v_L(x) = e_{L/K'} \cdot v_{K'}(x)$. □

1.2. Herbrand's Theorem. For a real number $u \geq -1$, set $G_u = G_i$, where i is the smallest integer $\geq u$. For $u \geq -1$, define

$$\varphi_{L/K}(u) = \int_0^u \frac{dt}{(G_0 : G_t)},$$

with the convention that $(G_0 : G_t) = 1$ for $-1 < t \leq 0$ so that $\varphi_{L/K}$ is the identity on $[-1, 0]$. [When there is no ambuiguity, we omit the reference to L/K and write φ instead.] Clearly, if $m \leq u \leq m + 1$ for some positive integer m, we have the formula

$$\varphi(u) = \frac{1}{g_0}(g_1 + \ldots + g_m + (u - m)g_{m+1}), \text{ where } g_i = \mathrm{Card}(G_i). \tag{1}$$

The following is immediate, and provides an alternative characterization of φ:

Proposition 1.3. *The function φ is the unique continuous, piecewise linear map from $[-1, \infty[$ to itself, satisfying $\varphi(0) = 0$ and $\varphi'(u) = g_u/g_0$ if $u \notin \mathbb{Z}$.*

In particular, since it is striclty increasing, it is a homeomorphism; denote by $\psi = \psi_{L/K}$ its inverse. The ramification groups in the *upper numbering* are defined by

$$G^v = G_{\psi(v)} \quad \text{or equivalently} \quad G^{\varphi(u)} = G_u.$$

By the remarks above, we have $G^{-1} = G$, $G^0 = G_0$, and $G^v = \{1\}$ for v sufficiently large. Furthermore, the upper numbering is adequate for quotients, by virtue of the following:

Theorem 1.4 (Herbrand)**.** *For all $v \geq -1$, we have $(G/H)^v = G^v H/H$.*

Before proving the Theorem, we will establish some facts about the functions φ and ψ.

Lemma 1.5. $\varphi_{L/K}(u) = \frac{1}{g_0} \sum_{s \in G} \mathrm{Inf}(i_G(s), u + 1) - 1$.

PROOF. Suppose $m < u \leq m + 1$ for some positive integer m. By comparing with formula (1), it clearly suffices to show that $\sum_{s \in G} \mathrm{Inf}(i_G(s), u + 1) = g_0 + \ldots + g_m + (u - m)g_{m+1}$. This follows by decomposing the sum into two sums running over $s \in G_u$, respectively $s \in G \backslash G_u$, as well as from the equivalence $s \in G_i \backslash G_{i+1} \iff i_G(s) = i + 1$. □

Lemma 1.6. *For $\sigma \in G/H$, let $j(\sigma)$ be the maximum of the integers $i_G(s)$, where s runs through the elements in G whose image in G/H is σ. Then*

$$i_{G/H}(\sigma) - 1 = \varphi_{L/K'}(j(\sigma) - 1).$$

PROOF. Let s be an element of G whose image in G/H is σ, and for which $i_G(s) = j(\sigma)$, and set $m = i_G(s)$. If $t \in H_{m-1}$, $i_G(t) \geq m$, so that $i_G(st) \geq m$; by maximality, $i_G(st) = m$. If $t \notin H_{m-1}$, $i_G(t) < m$ so that $i_G(st) = i_G(t)$. Hence, $i_G(st) = \mathrm{Inf}(i_G(t), m)$. Noting that the elements of G whose image in G/H is σ are of the form st, $t \in H$, it follows by Proposition 1.2 that

$$i_{G/H}(\sigma) = \frac{1}{e_{L/K'}} \sum_{t \in H} \mathrm{Inf}(i_G(t), m).$$

Noticing that $i_G(t) = i_H(t)$ and $e_{L/K'} = \mathrm{Card}(H_0)$, and applying the formula of Lemma 1.5 for $\varphi_{L/K'}$, we obtain the desired result. □

Lemma 1.7. $G_u H/H = (G/H)_{\varphi_{L/K'}(u)}$.

PROOF. We keep the notations of the previous lemma. We have the equivalences:

$$\begin{aligned} \sigma \in G_u H/H \quad &\iff \quad j(\sigma) \geq u+1 \iff \varphi_{L/K'}(j(\sigma)-1) \geq \varphi_{L/K'}(u) \\ &\iff \quad i_{G/H}(\sigma) - 1 \geq \varphi_{L/K'}(u) \iff \sigma(G/H)_{\varphi_{L/K'}(u)}. \end{aligned}$$

□

Lemma 1.8. *We have the transitivity relations*

$$\varphi_{L/K} = \varphi_{K'/K} \circ \varphi_{L/K'} \qquad \text{and} \qquad \psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}.$$

PROOF. Fix $u \notin \mathbb{Z}$, $u \geq -1$, and set $v = \varphi_{L/K'}(u)$. By the Chain Rule, the derivative of the composition $\varphi_{K'/K} \circ \varphi_{L/K'}$ is

$$\varphi'_{K'/K}(v) \cdot \varphi'_{L/K'}(u) = \frac{\mathrm{Card}((G/H)_v)}{e_{K'/K}} \cdot \frac{\mathrm{Card}(H_u)}{e_{L/K'}} = \frac{\mathrm{Card}(G_u)}{e_{L/K}},$$

the second equality following from Lemma 1.7 and the transitivity formula for the ramification index. The latter term is precisely the derivative of $\varphi_{L/K}(u)$, and the desired equality for φ follows. The equality for ψ is obtained from that for φ. □

PROOF OF THEOREM 1.4. By definition, $(G/H)^v = (G/H)_{\psi_{K'/K}(v)}$. By Lemma 1.7, this is equal to $G_w H/H$, where $w = \psi_{L/K'}(\psi_{K'/K}(v))$. By the transitivity formula for ψ, we have $w = \psi_{L/K}(v)$, and hence $G_w H/H = G_{\psi_{L/K}(v)} H/H = G^v H/H$. This completes the proof. □

1.3. The theorem of Hasse-Arf. If L/K is an *infinite* Galois extension, we can define, by virtue of Theorem 1.4, the ramification groups of G by setting $G^v_{L/K} = \varprojlim G^v_{L'/K}$, where L' runs through the finite Galois extensions of K contained in L. Again, we obtain an decreasing filtration, satisfying $G^v = \bigcap_{w<v} G^w$. We say that v is a *gap* in the filtration if $G^v \neq G^{v+\varepsilon}$ for all $\varepsilon > 0$. As the following example shows, gaps in $\{G^v\}$ may occur at non-integral values.

Example. Let $\mathbb{H}$ be the quaternionic group, and let $C = \{\pm 1\}$ be its centre. In [**8**], Serre shows that there exists a totally ramified extension L/K with Galois group G, and such that $G_4 = \{1\}$. We will show that a gap occurs in the filtration $\{G^v\}$ at the point $3/2$. A small computation shows that $\varphi_{L/K}$ is the identity on $[-1, 1]$, so that $G^v = G_v = G$ for $-1 \leq v \leq 1$. Furthermore, for $1 < u \leq 3$, $\varphi_{L/K}(u)$ takes its values in the interval $]1, 3/2]$. Hence, $G^v = G_2 = G_3 = C$ for $1 < v \leq 3/2$. Finally, $G^v = G_4 = \{1\}$ for $v > 3/2$.

In the case of abelian extensions, however, the gaps are more well-behaved, as the following theorem shows.

Theorem 1.9 (Hasse-Arf)**.** *Suppose G is abelian. Then the gaps in the filtration $\{G^v\}$ only occur at integral values of v.*

The proof is given Chapter II, §1, using Lubin-Tate formal groups. However, a direct (but longer) proof can also be obtained, see Serre [**7**], Chap. V, §7.

1.4. The group of units. Let $U = \mathcal{O}_K^*$ be the group of units of K. We define a filtration of U by setting

$$\begin{aligned} U^0 &= U \\ U^n &= 1 + \mathfrak{m}_K^n, \text{ for } n \geq 1. \end{aligned}$$

Notice that this forms a basis of neighbourhoods of 1.

Proposition 1.10. *For all $n \geq 1$, we have isomorphisms*

$$U/U^n \simeq (\mathcal{O}_K/\mathfrak{m}_K^n)^* \quad \text{and} \quad U^n/U^{n+1} \simeq \mathfrak{m}_K^n/\mathfrak{m}_K^{n+1} \simeq k_K^+.$$

Proof. The map $U \to (\mathcal{O}_K/\mathfrak{m}_K^n)^*$, obtained by sending $u \in U$ to $u \pmod{\mathfrak{m}_K^n}$, is surjective, with kernel U^n. This establishes the first isomorphism. The map $U^n \to \mathfrak{m}_K^n$, obtained by sending $x + 1 \in U^n$ to $x \in \mathfrak{m}_K^n$, clearly induces an isomorphism $U^n/U^{n+1} \simeq \mathfrak{m}_K^n/\mathfrak{m}_K^{n+1}$. Furthermore, k_K^n/k_K^{n+1} is a one-dimensional vector space over k_K, and hence is isomorphic to k_K^+, the additive group of k_K. This establishes the remaining isomorphisms. □

Proposition 1.11. *Let $e_K = e_{K/\mathbb{Q}_p}$ be the absolute ramification index of K.*

(i) *If $n \leq e_K/(p-1)$, then $U_n^p \subset U_{np}$.*
(ii) *If $n > e_K/(p-1)$, then $U_n \simeq U_{n+e_K}$, the isomorphism being given by $x \mapsto x^p$.*

Proof. (i) Obvious for $n = 0$. So suppose $n > 0$; let π be a uniformizer of $\mathcal{O}_K$, and let $x = 1 + a\pi^n$, $z \in \mathcal{O}_K$, be an element of U_n. We need to show that $x^p = 1 + pa\pi^n + \ldots + (a\pi^n)^p$ belongs to $U_n^p = 1 + \mathfrak{m}_K^p$, or equivalently, that all the terms in a belong to $\mathfrak{m}_K^p$. This is obviously true for the last term $(a\pi^n)^p$. On the other hand, each middle term $\binom{p}{i}(a\pi^n)^i$, $0 < i < p$, has order $\geq n + e_F$. Indeed, the binomial coefficient $\binom{p}{i}$ is divisible by p, so it is of the form pt for some t; thus, $v_K(pt) \geq v_K(p) = e_K v_{\mathbb{Q}_p}(p) = e_K$. But by assuption, $n + e_K \geq np$, and we are done.

(ii) We use the same notation as in (i). Let y be an element of U_{n+e_K}, say $y = 1 + b\pi^{n+e_K}$. We must show that there is a unique $x \in U_n$, say $x = 1 + z\pi^n$, such that $x^p = y$, i.e. that the equation

$$(1 + z\pi^n)^p = 1 + b\pi^{n+e_K} \tag{2}$$

has a unique solution in $z \in \mathcal{O}_K$. By the same argument as in (i), each term in z, in the expansion of x, belongs to $\mathfrak{m}_K^{n+e_K}$ (for the last term, the assumption $np > n + e_K$ is used). Hence, if we subtract 1 from both sides of equation (2) and divide by π^{n+e_K}, the equation becomes $f(z) = b$ for some polynomial $f \in \mathcal{O}_K[z]$ with coefficients all divisible by π. Moreover, the term of degree 1 is $zp\pi^n/\pi^{n+e_K} = p\pi^{-e_K}z$; let $a = p\pi^{-e_K}$ be its coefficient. Taking the valuation v_K of a, we obtain $v_K(a) = v_K(p) - e_K = e_K v(p) - e_K = 0$, where v is the valuation on $\mathbb{Q}_p$. Hence, $a \in \mathcal{O}_K^*$, so that $(*)$ becomes

$$az + F(z) = b,\ a \in \mathcal{O}_K^*,\ F \in \mathcal{O}_K[z]. \tag{3}$$

Reduction modulo $\mathfrak{m}_K$ yields the equation $\overline{a}\overline{z} = \overline{b}$, and since $b \in \mathcal{O}_K^*$, we have $\overline{b} \neq 0$ and hence this equation has a unique solution in $\overline{z}$. By applying Hensel's Lemma, we deduce that (3), and consequently (2), has a unique solution in z. □

1.5. The different. Let x denote a generator of $\mathcal{O}_L$ over $\mathcal{O}_K$, and let $f(X) = \prod_{s\in G}(X - s(x))$ be its minimal polynomial. The discriminant $\mathfrak{D}_{L/K}$ is generated by $f'(x)$ (Serre [**7**], Ch. III, Cor. 2 to Prop. 11).

Theorem 1.12. *Suppose L/K is a finite Galois extension. Then*

$$v_L(\mathfrak{D}_{L/K}) = \sum_{i=0}^{\infty}(g_i - 1) = \int_{-1}^{\infty}(g_w - 1)dw, \text{ where } g_i = \mathrm{Card}(G_i).$$

Notice that $g_i - 1 = 0$ for i sufficiently large; hence the sum is well-defined.

Proof. By the remarks above, we have $f'(x) = \prod_{s\neq 1}(x - s(x))$ and $v_L(\mathfrak{D}_{L/K}) = v_L(f'(x)) = \sum_{s\neq 1} i_G(s)$. We have $i_G(s) = i$ if $s \in G_{i-1}\backslash G_i$; hence, if $r_i = g_i - 1$, we get $\sum_{s\neq 1} i_G(s) = \sum_{i=0}^{\infty} i(r_{i-1} - r_i) = (r_0 - r_1) + 2(r_1 - r_2) + \ldots = \sum_{i=0}^{\infty} r_i$, and the first equality is established. The second equality is immediate. □

We prove the following generalization to the case where the extension L/K is not required to be Galois. For $u \in [1, \infty[$, let K^v denote the fixed field of $\mathrm{Gal}(L/K)^v$.

Theorem 1.13. *Suppose L/K is a finite extension. Then*

$$v_L(\mathfrak{D}_{L/K}) = e_{L/K} \cdot \int_{-1}^{\infty}\left(1 - \frac{1}{[L : L \cap K^v]}\right)dv. \tag{4}$$

Proof. We reduce the theorem to the classical case of Galois extensions. To that purpose, let M be any finite Galois extension of K containing L. Let $H = \mathrm{Gal}(M/L)$ be the corresponding Galois group, and let h_u be the cardinality of the u'th ramification group H_u of H. By multiplicativity of the different, $\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L} \cdot \mathfrak{D}_{L/K}$, and thus $v_M(\mathfrak{D}_{L/K}) = v_M(\mathfrak{D}_{M/K}) - v_M(\mathfrak{D}_{M/L})$. This identity, combined with that of Theorem 1.12, yields

$$v_L(\mathfrak{D}_{L/K}) = \frac{1}{e_{M/L}}v_M(\mathfrak{D}_{L/K}) = \frac{1}{e_{M/L}} \cdot \int_{-1}^{\infty}(g_u - h_u)du. \tag{5}$$

On the other hand, $L \cap F^v$ is the fixed field of the smallest subgroup of G containing H and G^v, i.e. $G^v H = HG^v$ (since H is *normal* in G). Hence $\mathrm{Gal}(L/L \cap K^v) = HG^v/H$, and by the second isomorphism theorem, $[L : L \cap K^v] = \mathrm{Card}(G^v/(G^v \cap H))$. Passing to the lower numbering, we have $[L : L \cap K^v] = \mathrm{Card}(G_u/(G_u \cap H))$, where $u = \varphi_{M/K}(v)$. But by Proposition 1.1, $G_u \cap H = H_u$, so that $[L : L \cap K^v] =$

$\mathrm{Card}(G_u)/\mathrm{Card}(H_u)$. By Proposition 1.3, $\varphi'_{M/K}(u) = g_u/g_0$, so by making the variable change $u = \varphi_{M/K}(v)$, the right hand side of (4) is equal to

$$e_{L/K} \cdot \int_{-1}^{\infty} \left(1 - \frac{h_u}{g_u}\right) \frac{g_u}{g_0} du = \frac{e_{L/K}}{g_0} \cdot \int_{-1}^{\infty} (g_u - h_u) du$$

Recalling that G_0 is the inertia subgroup of G which has cardinality $e_{M/K}$, and that $e_{m/K} = e_{M/L} \cdot e_{L/K}$, we see that this formula coincides with (5), whence the result. □

If L/K is a finite extension, the *conductor* of L over K is the smallest integer v for which $L \subset K^{v-1}$; we denote it $f_{L/K}$.

Corollary 1.14. *Suppose L/K is a finite extension. Then*

$$e_{L/K} \cdot f_{L/K}/2 \leq v_L(\mathfrak{D}_{L/K}) \leq e_{L/K} \cdot f_{L/K}.$$

Proof. By definition, $L \cap K^v = L$ when $v > f_{L/K} - 1$. Thus, by Theorem 1.13,

$$v_L(\mathfrak{D}_{L/K}) = e_{L/K} \cdot \int_{-1}^{f_{L/K}-1} h(v) dv,$$

where $h(v) = 1 - 1/[L : L \cap K^v]$. Clearly, $1/2 \leq h(v) \leq 1$ for $-1 \leq v \leq f_{L/K} - 1$, and hence

$$f_{L/K}/2 \leq \int_{-1}^{f_{L/K}-1} h(v) dv \leq f_{L/K}.$$

The result follows immediately. □

Lemma 1.15. *Let M/L be a finite extension. Then $\mathrm{Tr}_{M/L}(\mathcal{O}_M) = \mathfrak{m}_L^N$, where N is the integral part of $v_L(\mathfrak{D}_{M/L})/e_{M/L}$.*

Proof. Let π be a uniformizer for L. The inequality $N \cdot e_{M/L} \leq v_L(\mathfrak{D}_{M/L})$ implies that $\pi^{-N}\mathcal{O}_M \subset \mathfrak{D}_{M/L}^{-1}$, and, taking the trace on both sides, we get that $\mathrm{Tr}_{M/L}(\mathcal{O}_M) \subset \pi^N \mathcal{O}_L (= \mathfrak{m}_L^N)$. On the other hand, the inequality $(N+1)e_{M/L} > v_L(\mathfrak{D}_{M/L})$ implies that $\mathrm{Tr}_{M/L}(\mathcal{O}_M)$ is not contained in $\mathfrak{m}_L^{N+1}$. Since $\mathrm{Tr}_{M/L}(\mathcal{O}_M)$ is an ideal of $\mathcal{O}_L$, it follows that the inclusion $\mathrm{Tr}_{M/L}(\mathcal{O}_M) \subset \mathfrak{m}_L^N$ is an equality. □

2. Cohomology of groups

In this section, we briefly recall the construction of the cohomology groups of G-modules, and establish some standard results: the inflation-retriction sequence and a "non-commutative" version of Hilbert's Theorem 90. Special emphasis is then put on the case where the group G is finite and cyclic, and it turns out that the cohomology groups are periodic of period 2. The definition of the Herbrand quotient arise from this observation.

2.1. Definitions and elementary properties. Let G be a group, and let A be a *G-module* (i.e. an abelian group on which the group algebra $\mathbb{Z}[G]$ acts). If B is another G-module, a *G-homomorphism* $f : A \to B$ is a homomorphism of $\mathbb{Z}[G]$-modules. If A^G, resp. B^G, denotes the largest subgroup of A, resp. B, of elements fixed by G, then f maps A^G into B^G; thus we may view A^G as a functor from the category of G-modules to the category of abelian groups. If we view $\mathbb{Z}$ as a G-module on which G acts trivially, we can identify A^G with the group $\mathrm{Hom}_G(\mathbb{Z}, A)$ of G-homomorphisms $\mathbb{Z} \to A$. By definition, the *cohomology groups*

of G, with coefficients in A, denoted $H^*(G, A)$, are the right derived functors of $A^G \simeq \mathrm{Hom}_G(\mathbb{Z}, A)$, that is,

$$H^q(G, A) = \mathrm{Ext}^q(\mathbb{Z}, A) \qquad (q \geq 0).$$

For their explicit computation, we choose a free resolution of $\mathbb{Z}$

$$\ldots \to L_1 \to L_0 \to \mathbb{Z} \to 0,$$

where L_n is the free $\mathbb{Z}$-module with basis $(x_0, \ldots, x_n)$, $x_i \in G$, on which G acts by translation. The differential $d : L_n \to L_{n-1}$ is given by the formula

$$d(x_0, \ldots, x_n) = \sum_{i=0}^{n} (-1)^i (x_0, \ldots, \widehat{x}_i, \ldots, x_n),$$

the notation $\widehat{x}_i$ meaning that the letter x_i is omitted, and the final map $L_0 \to \mathbb{Z}$ is simply chosen to send every $(x_0) \in L_0$ to $1 \in \mathbb{Z}$. As usual, denote by $C^n(G, A) = \mathrm{Hom}_G(L_n, A)$ the set of cochains on G. Its elements are thus functions $f : G^{n+1} \to A$ satisfying $f(s \cdot x_0, \ldots, s \cdot x_n) = s \cdot f(x_0, \ldots, x_n)$, $s \in G$. The coboundary map $d : C^n(G, A) \to C^{n+1}(G, A)$ is given by

$$\begin{aligned} df(x_1, \ldots, x_{n+1}) &= x_1 \cdot f(x_2, \ldots, xg_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(x_1, \ldots, x_i x_{i+1}, \ldots, x_{n+1}) \\ &\quad + (-1)^{n+1} f(x_1, \ldots, x_n), \end{aligned}$$

and we recover the definition

$$H^q(G, A) = \ker d / \mathrm{im}\ d.$$

Notice that a 1-cocycle is a map $f : G \to A$ satisfying $f(xx') = xf(x') + f(x)$, and that such a map is a 1-coboundary if there exists $a \in A$ such that $f(x) = x \cdot a - a$ for all $x \in G$. Two cocycles f, g on G are said to be *cohomologous* if there exists an element $a \in A$ such that $f(x) = a^{-1} g(x) x(a)$ for all $x \in G$.

Given an exact sequence of G-modules

$$0 \to A \to B \to C \to 0,$$

we obtain, in the usual manner (by choosing the above resolution of cochains and applying the Snake Lemma), a long exact sequence in cohomology,

$$(*) \qquad \ldots \to H^q(G, A) \to H^q(G, B) \to H^q(G, C) \to H^{q+1}(G, A) \to \ldots.$$

Hence, the functor $H^q(G, \ )$, besides being a derived functor (i.e. $H^0(G, A) = A^G$, and $H^q(G, A) = 0$ if $q \geq 1$ and if A is injective), is in fact a *cohomological functor*.

The following proposition shows that the cohomology groups behave well under passage to inductive limits. This is of particular interest when we deal with infinite Galois extensions, such as deeply ramified extensions, since the Galois groups in question are then the projective limit of the Galois groups corresponding to the finite Galois subextensions.

Proposition 2.1. *Let (G_i) be a projective system of groups, and let (A_i) be an inductive system of G_i-modules. Let $G = \varprojlim G_i$ and $A = \varinjlim A_i$. Then*

$$H^q(G, A) = \varinjlim H^q(G_i, A_i), \text{ for all } q \geq 0.$$

PROOF. It is clear that $\varinjlim C^*(G_i, A_i) \simeq C^*(G, A)$, and the result follows by taking homology. □

Let H be a subgroup of G. Then we have a natural restriction map

$$\mathrm{Res} : H^1(G, A) \to H^1(H, A).$$

If furthermore H is normal, we have the inflation map,

$$\mathrm{Inf} : H^1(G/H, A^H) \to H^1(G, A)$$

defined by sending the 1-cocyle $f : G/H \to A^H$ to the 1-cocycle $\mathrm{Inf}(f)$ defined by $\mathrm{Inf}(f)(x_0) = f(\overline{x}_0)$, where $\overline{x}_0$ denotes the image of x_0 in G/H.

Proposition 2.2. *The following sequence is exact:*

$$0 \to H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G, A) \xrightarrow{\mathrm{Res}} H^1(H, A).$$

PROOF. One immediately verifies that $\mathrm{Res} \circ \mathrm{Inf} = 0$. Hence it suffices to show exactness at $H^1(G/H, A^H)$ and $H^1(G, A)$.

If $f : G/H \to A^H$ is a cocycle on G/H whose inflation is a coboundary on G, then by definition there exists $a \in A$ such that $f(\overline{s}) = s \cdot a - a$ for all $s \in G$. In particular, if $s \in H$, we get $s \cdot a - a = f(\overline{s}) = f(0) = 0$ so that $a \in A^H$. Hence f is a coboundary on G/H, which proves exactness at $H^1(G/H, A^H)$.

Similarly, if $f \in \ker(\mathrm{Res})$, then there exists $a \in A$ such that $f(t) = t \cdot a - a$ for all $t \in H$. The cocycle $F(s) = f(s) - (s \cdot a - a)$ is cohomologous to f and zero on H. Suppose $s \in G$ and $t \in H$. The formula $F(st) = sF(t) + F(s) = F(s)$ shows that F defines a cocycle on G/H. Furthermore, since H is normal in G, we have $F(st) = F(t's) = t'F(s)$ for some $t' \in H$, showing that $F(s)$ is invariant under H, i.e. that F takes its values in A^H. This proves exactness at $H^1(G, A)$. □

We will need the following non-commutative version of Hilbert's Theorem 90:

Theorem 2.3 (Non-commutative Hilbert 90)**.** *Let L/K be a finite Galois extension with Galois group G. Then, for all $n \geq 1$, $H^1(G, GL_n(L))$ is trivial.*

PROOF. Let $f : G \to GL_n(L)$ be a 1-cocycle on G. For a matrix $\alpha \in M_n(L)$, form the sum $x = \sum_{s \in G} f(s)^{-1} s(\alpha)$. Then for any $\sigma \in G$, we have $\sigma(x) = \sum_{s \in G} \sigma(f(s)^{-1}) \sigma s(\alpha) = f(\sigma) \sum_{\sigma \in G} f(\sigma s)^{-1} \sigma s(\alpha) = f(\sigma)x$, the second equality following from the identity $f(\sigma s) = f(\sigma)\sigma f(s)$ on cocycles (in the multiplicative notation). Hence, f is a coboundary if we can choose α such that x is invertible (so that we can write $f(\sigma) = \sigma(x)/x$). But the linear form $\sum_{s \in G} X_s f(s)$ on L^G is non-zero since the elements $f(s)$ are invertible, and the result follows by linear independence of characters. □

We recover the standard version in the case $n = 1$:

Corollary 2.4 (Hilbert 90)**.** *Let L/K be a finite Galois extension with Galois group G. Then $H^1(G, L^*)$ is trivial.*

Remark. If the extension L/K is *infinite*, we also have $H^1(\mathrm{Gal}(L/K), L^*) = 0$ since we may pass to the projective limit and apply Proposition 2.1.

2.2. Cohomology of finite cyclic groups. Let G be a cyclic group of order n, and let s be a generator of G. Let

$$T = \sum_{t \in G} t \qquad \text{and} \qquad D = s - 1.$$

Since $\sum_{t\in G} ts = \sum_{t\in G} t$, these operators satisfy $ND = DN = 0$. Thus, for a G-module A, we have a cochain complex

$$\ldots \xrightarrow{D} A \xrightarrow{N} A \xrightarrow{D} A \xrightarrow{N} \ldots,$$

where the differentials are multiplication by D, resp. by N. Let $H^q(A)$ denote the q'th cohomology group of this complex. Explicitely, we have

$$H^q(A) = A^G/TA, \qquad \text{for } q \text{ even},$$
$$H^q(A) = A^0/DA, \qquad \text{for } q \text{ odd},$$

where A^0 denotes the kernel of the trace map $a \mapsto Ta$; of course, A^G is the kernel of D. It turns out that these groups are almost equal to the cohomology groups of G, as defined above. More precisely,

$$H^q(G, A) = H^q(A) \text{ for all } q > 0.$$

[This follows from the defining properties of the *Tate cohomology groups*, see Cassels-Fröhlich, Chap. IV, §6.] Now if $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules, the long sequence $(*)$ of cohomology becomes an exact hexagon:

$$\begin{array}{ccccc} & & H^2(A) & \longrightarrow & H^2(B) & & \\ & \nearrow & & & & \searrow & \\ H^1(C) & & & & & & H^2(C) \\ & \nwarrow & & & & \swarrow & \\ & & H^1(B) & \longrightarrow & H^1(A) & & \end{array}$$

Suppose that $H^1(A) = H^1(G, A)$ and $H^2(A) = H^2(G, A)$ are *finite*, and let $h_1(A)$ and $h_2(A)$ be their respective orders. Then the *Herbrand quotient* of A is

$$h(A) = h_2(A)/h_1(A).$$

Proposition 2.5. *Let $0 \to A \to B \to C \to 0$ be an exact sequence of G-modules. Then $h(B) = h(A)h(C)$ whenever these are defined.*

Proposition 2.6. *If A is a finite G-module, then $h(A) = 1$.*

Proof. We have an exact sequence of G-modules

$$0 \to A^G \to A \xrightarrow{D} A \to A_G \to 0.$$

In particular, if A is *finite*, then A^G and A_G have the same order. On the other hand, the exact sequence

$$0 \to H^1(A) \to A_G \xrightarrow{T} A^G \to H^0(A) \to 0,$$

shows that $H^0(A)$ and $H^1(A)$ have the same order. □

Corollary 2.7. *Let A and B be G-modules, and let $f : A \to B$ be a G-homomorphism with finite kernel and cokernel. Then A and B have the same Herbrand quotients, whenever these are defined.*

PROOF. Suppose that $h(A)$ is defined. We have the exact sequences

$$0 \to \ker f \to A \to f(A) \to 0$$
$$0 \to f(A) \to B \to \operatorname{coker} f \to 0.$$

By Proposition 2.5, we get $h(A) = h(\ker f)h(f(A))$ and $h(B) = h(f(A))h(\operatorname{coker} f)$, and by Proposition 2.6, we get $h(A) = h(f(A)) = h(B)$. □

3. Deeply ramified extensions

Throughout this section, K will be a finite extension of $\mathbb{Q}_p$.

3.1. Definitions. We introduce a class of infinite extensions of which all finite extensions are "almost unramified", and give equivalent definitions of these. For their definition, we first need a useful existence lemma:

Lemma 3.1. *Suppose L is the union of an increasing filtration of subfields $\{L_n\}_{n\in I}$, and let M be a finite extension of L of degree d. Then there exists an index $n_0 \in I$ and an extension M_{n_0} of L_{n_0} of degree d, such that $M_{n_0}L = M$ and M_{n_0} and L are linearly disjoint. If the extension M/L is Galois, then M_{i_0} can be chosen to be Galois over L_{n_0}.*

PROOF. Let $\{e_1, \dots, e_d\}$ be a basis of M over L. Define scalars c_{ij}^k by $e_i \cdot e_j = \sum c_{ij}^k e_k$. Choose n_0 large enough so that all the elements c_{ij}^k belong L_{n_0}, and define M_{n_0} to be the degree d extension $L_{n_0}(e_1, \dots, e_d)$ of L_{n_0}. If we extend the L_{n_0}-algebra M_{n_0} by L, we obtain M, i.e. $M_{n_0} \otimes_{L_{n_0}} L = M$. Since M is a field, M_{n_0} and L are linearly disjoint. Consequently, $M_{n_0}L = M_{n_0} \otimes_{L_{n_0}} L = M$, so M_{n_0} satisfies the desired conditions. Now if M/L is Galois, then linear disjointness implies that $s(M_{n_0})L = M$ for all $s \in \operatorname{Gal}(M/L)$. Hence, for $m \geq n_0$ sufficiently large, $s(M_{n_0})L_m = M_{n_0}L_m$. Hence, if we put $M_m = M_{n_0}L_m$, then M_m/M_{n_0} is Galois, as desired. □

Let $L_n \subset L_{n+1}$, $n \geq 0$, be successive finite extensions of K. Set $L = \bigcup L_n \subset \overline{\mathbb{Q}}_p$. For a finite extension M of L, and for a sufficiently large integer n_0, let M_{n_0} be the unique finite extension of L_{n_0} defined in Lemma 3.1. For all $n \geq n_0$, let $M_n = M_{n_0}L_n$.

Recall (§1.5) that the conductor $f_{L/K}$ of L over K is the smallest integer for which $L \subset K^{v-1}$. We say that L has *finite* conductor over K if this integer is bounded. Denote by v the valuation on $\overline{\mathbb{Q}}_p$, and by $\overline{\mathfrak{m}}$ the corresponding maximal ideal. The main result of this section is the following:

Theorem 3.2. *The following assertions are equivalent:*

(i) *L does not have finite conductor over K.*
(ii) $\lim_{n\to\infty} v_K(\mathfrak{D}_{L_n/\mathbb{Q}_p}) = +\infty$.
(iii) $H^1(L, \overline{\mathfrak{m}}) = 0$.
(iv) *For every finite extension M of L,* $\operatorname{Tr}_{M/L}(\mathfrak{m}_M) = \mathfrak{m}_L$.
(v) *For every finite extension M of L,* $\lim_{n\to\infty} v(\mathfrak{D}_{M_n/L_n}) = 0$.

The extension L/K is said to be *deeply ramified* if it satisfies these equivalent conditions. We will successively establish the above equivalences. Let us start with the easiest one:

Proposition 3.3. *The following assertions are equivalent:*

(i) *The conductor of L over K is bounded.*
(ii) $v_K(\mathfrak{D}_{L_n/\mathbb{Q}_p})$ *is bounded.*

PROOF. By multiplicativity of the different, $\mathbb{Q}_p$ can be replaced by K in the Proposition. By Corollary 1.14, the conductor $f_{L_n/K}$ and $v_L(\mathfrak{D}_{L_n/K})$ mutually bound each other (up to multiplication by a scalar). The result follows by passing to the limit. □

Lemma 3.4. *Assume that L does not have finite conductor over K. Let H be a any finite extension of $\mathbb{Q}_p$. Then, for each $v \geq -1$, $\lim_{n\to\infty}[L_n : L_n \cap H^v] = +\infty$. In particular, $\lim_{n\to\infty} e_{L_n} = +\infty$.*

PROOF. The fact that L does not have finite conductor implies that L is an infinite extension of $L \cap H^v$. Indeed, if it was a finite extension, it would be the product of $L \cap H^v$ with a finite extension of $\mathbb{Q}_p$; these two factors have finite conductor, implying that L would have finite conductor, hence a contradiction. Now let $\{x_0, x_1, \ldots\}$ be a sequence of elements of L ordered such that, if d_i denotes the degree of x_i over $L \cap H^v$, then the corresponding sequence $\{d_0, d_1, \ldots\}$ is strictly increasing. Since $x_i \in L_{n_i}$ for n_i sufficiently large, we have that, for all $n \geq n_i$, $x_i \in L_n$ and x_i has degree $\geq d_i$ over $L_n \cap H^v$. Consequently, $[L_n : L_n \cap H^v] \geq d_i$ for all $n \geq n_i$, and the result follows. The statement $\lim_{n\to\infty} e_{L_n} = +\infty$ follows by taking $H = \mathbb{Q}_p$ and noting that $e_{L_n} = [L_n : L_n \cap (\mathbb{Q}_p)^0]$ (recall that $(\mathbb{Q}_p)^0$ is the fixed field of the inertia group of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, i.e. the maximal unramified extension of $\mathbb{Q}_p$). □

Proposition 3.5. *The following assertions are equivalent:*

(i) *L does not have finite conductor over K.*
(ii) *For every finite extension M of L, $\lim_{n\to\infty} v(\mathfrak{D}_{M_n/L_n}) = 0$.*
(iii) *For every finite extension M of L, $\mathrm{Tr}_{M/L}(\mathfrak{m}_M) = \mathfrak{m}_L$.*

PROOF. (i) $\Longrightarrow$ (ii): We may, without loss of generality, suppose that M is Galois over L. Indeed, if it is not, we can take its Galois closure and use multiplicatity of the different; this will obviously not affect the implication. In the same way, we can choose M_n to be Galois over L_n for all $n \geq n_0$ (by virtue of Lemma 3.1). For short we write

$$H = L_{n_0}, \quad J = M_{n_0}, \quad R_n^v = L_n \cap H^v, \quad S_n^v = M_n \cap H^v.$$

By multiplicativity of the different, $\mathfrak{D}_{M_n/L_n} = \mathfrak{D}_{M_n/H} \cdot \mathfrak{D}_{L_n/H}^{-1}$. Taking valuations on each side, we get $v(\mathfrak{D}_{M_n/L_n}) = v(\mathfrak{D}_{M_n/H}) - v(\mathfrak{D}_{L_n/H}) = 1/e_{M_n} v_{M_n}(\mathfrak{D}_{M_n/H}) - 1/e_{L_n} v_{e_{L_n}}(\mathfrak{D}_{L_n/H})$. By Theorem 1.13, and using multiplicativity of the ramification index, we get

$$v(\mathfrak{D}_{M_n/L_n}) = \frac{1}{e_H} \int_{-1}^{\infty} \left(\frac{1}{[L_n : R_n^v]} - \frac{1}{[M_n : S_n^v]} \right) dv.$$

Since J/H is finite, we have $J \subset H^v$ for v sufficiently large, say $v \geq v_0$. Furthermore, since F_n and H^v are Galois over H, it is easy to show that F_n and H^v are linearly disjoint over their intersection R_n^v (i.e. $F_n \otimes_{R_n^v} H^v$ is a *field*). Hence $[L_n : R_n^v] = [L_n S_n^v : R_n'(v)]$.

Claim. $L_n' = L_n S_n^v$.

PROOF. The inclusion $L_nS_n^v \subset L'_n$ is immediate. Furthermore, $J \subset H^v$ for all $v \geq v_0$ so that $L'_n = JL_n \subset S_n^v L_n$. □

It follows that $[L_n : R_n^v] = [M_n : S_n^v]$ for all $v \geq v_0$, and hence the above formula for $v(\mathfrak{D}_{M_n/L_n})$ reduces to

$$\begin{aligned} v(\mathfrak{D}_{M_n/L_n}) &= \frac{1}{e_H}\int_{-1}^{v_0}\left(\frac{1}{[L_n:R_n^v]} - \frac{1}{[M_n:S_n^v]}\right)dv \\ &\leq \frac{1}{e_H}\int_{-1}^{v_0}\frac{dv}{[L_n:R_n^v]} \\ &\leq \frac{v_0+1}{e_H\cdot[L_n:R_n^{v_0}]}, \end{aligned}$$

the last inequality following since $R_n^v \subseteq R_n^{v_0}$ for all $v \geq v_0$. Since K does not have finite conductor, it follows by Lemma 3.4 that this last term, and hence $v(\mathfrak{D}_{M_n/L_n})$, tends to 0 as $n \to \infty$.

(ii) $\Longrightarrow$ (iii): Suppose in the first instance that the absolute ramification index $e_{L_n} = e_{L_n/\mathbb{Q}_p}$ is bounded as n tends to ∞, i.e. there exists and integer $n_0 \geq 0$ such that $e_{L_n} = e_{L_{n_0}}$ for all $n \geq n_0$. By multiplicativity of the ramification index, $e_{L/L_n} = 1$ $(n \geq n_0)$. Hence L/L_n is unramified for all $n \geq n_0$. By multiplicativity of the different, it follows that $\mathfrak{D}_{M_{n+1}/L_{n+1}} = \mathfrak{D}_{M_n/L_n}$ for all $n \geq n_0$. By assumption, $v(\mathfrak{D}_{M_n/L_n})$ tends to 0, so that $\mathfrak{D}_{M_n/L_n}$ must be equal to $\mathcal{O}_{M_n}$ for all $n \geq n_0$, i.e. M_n/L_n is unramified. But by Lemma 1.15, we have $\mathrm{Tr}_{M_n/L_n}(\mathfrak{m}_{M_n}) = \mathfrak{m}_{L_n}$ and, passing to the limit, $\mathrm{Tr}_{M/L}(\mathfrak{m}_M) = \mathfrak{m}_L$. Suppose now that e_{L_n} is unbounded as $n \to \infty$. Let π_n be a uniformizer for L_n. Then $\lim_{n\to\infty} v(\pi_n) = \lim_{n\to\infty} 1/e_{L_n} = 0$. Let a_n be defined by $\mathrm{Tr}_{M_n/L_n}(\mathcal{O}_{M_n}) = \pi_n^{a_n}\mathcal{O}_{L_n}$. Using Lemma 1.15, we obtain an inequality

$$e_{L_n}\cdot v(\pi_n^{a_n}) = v_{L_n}(\pi_n^{a_n}) = a_n \leq \frac{v_{M_n}(\mathfrak{D}_{M_n/L_n})}{e_{M_n/L_n}} = e_{L_n}\cdot v(\mathfrak{D}_{M_n/L_n}),$$

from which we deduce $v(\pi_n^{a_n}) \leq v(\mathfrak{D}_{M_n/L_n})$. Hence $v(\pi_n^{a_n}) \to 0$ as $n \to \infty$, and consequently, $\lim_{n\to\infty} v(\pi_n^{a_n+1}) = \lim_{n\to\infty}(v(\pi_n^{a_n}) + v(\pi_n)) = 0$. Pick $x \in \mathfrak{m}_L$. Then, for n sufficiently large, $v(x) > v(\pi_n^{a_n+1})$. It follows that $x \in \pi_n^{a_n+1}\mathcal{O}_{L_n} = \pi_n^{a_n}(\pi_n\mathcal{O}_{L_n})$, which, by definition of a_n, implies that $x \in \mathrm{Tr}_{M_n/L_n}(\pi_n\mathcal{O}_{M_n})$. Passing to the limit, we get that $x \in \mathrm{Tr}_{M/K}(\mathfrak{m}_M)$, whence $\mathfrak{m}_L \subset \mathrm{Tr}_{M/L}(\mathfrak{m}_M)$.

(iii) $\Longrightarrow$ (i): For each $t \geq 0$, let Φ_t be the t'th layer of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$, i.e. the unique subfield of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}_p$ which is of degree p^t over $\mathbb{Q}_p$ (see Section 3.2, Example 3.12). Let $L'_n = L_n\Phi_t$. We will prove the implication by contradiction. Namely, we will prove that, if L has finite conductor over K, then, for all t large enough, we have

$$\mathrm{Tr}_{M_n/L_n}(\mathfrak{m}_{M_n}) \subset p\mathfrak{m}_{L_n}, \text{ for all } n \geq n_0, \tag{6}$$

where n_0 is to be defined. By passing to the limit, we obtain that $\mathrm{Tr}_{M/L}(\mathfrak{m}_M) \subset p\mathfrak{m}_L \nsubseteq \mathfrak{m}_L$ and hence the desired contradiction. So suppose that L has finite conductor over K. Define an increasing sequence $b_0 \leq b_1 \leq \ldots$ of integers by $\mathrm{Tr}_{L_n/\mathbb{Q}_p}(\mathcal{O}_{L_n}) = p^{b_n}\mathbb{Z}_p$. By Lemma 1.15, b_n is the integral part of $v(\mathfrak{D}_{L_n/\mathbb{Q}_p}) = v_{\mathbb{Q}_p}(\mathfrak{D}_{L_n/\mathbb{Q}_p})/e_{L_n}$. By Proposition 3.3, $v(\mathfrak{D}_{L_n/\mathbb{Q}_p})$ is bounded, and hence so is b_n; that is, there is an integer n_0 such that, for all $n \geq n_0$, b_n is equal to a fixed constant

b. Consequently, for $n \geq n_0$,

$$\mathrm{Tr}_{L_n/\mathbb{Q}_p}(\mathcal{O}_{L_n}) = p^b\mathbb{Z}_p. \tag{7}$$

Now suppose that (6) does not hold, i.e. that there exists an integer $n \geq n_0$ such that $\mathrm{Tr}_{M_n/L_n}(\mathfrak{m}_{M_n}) \supseteq p\mathfrak{m}_{L_n}$. Then, applying $\mathrm{Tr}_{L_n/\mathbb{Q}_p}$ on both sides yields $\mathrm{Tr}_{M_n/\mathbb{Q}_p}(\mathfrak{m}_{M_n}) \supseteq p\mathrm{Tr}_{L_n/\mathbb{Q}_p}(\mathfrak{m}_{L_n}) \supseteq p\mathrm{Tr}_{L_n/\mathbb{Q}_p}(p\mathcal{O}_{L_n}) = p^2\mathrm{Tr}_{L_n/\mathbb{Q}_p}(\mathcal{O}_{L_n}) = p^{b+2}\mathbb{Z}_p$, the last equality being that of formula (7). This inclusion clearly holds when replacing M_n by Φ_t, i.e.

$$\mathrm{Tr}_{\Phi_t/\mathbb{Q}_p}(\mathfrak{m}_{\Phi_t}) \supseteq p^{b+2}\mathbb{Z}_p. \tag{8}$$

Now let ζ_t be a root of unity of exact order p^{t+2} if $p = 2$, and of exact order p^{t+1} if $p \geq 2$. Let $\Omega_t = \mathbb{Q}_p(\zeta)$; this is an extension of $\mathbb{Q}_p$ of degree $\varphi(t+2) = p^{t+1}$ if $p = 2$, and of degree $\varphi(t+1) = (p-1)p^t$ if $p > 2$ (Serre [**7**], Chap. IV, §4). Hence, the degree $d = [\Omega_t : \Phi_t]$ is equal to p if $p = 2$, and $p-1$ if $p > 2$. We have $\mathcal{O}_{\Omega_t} = \mathbb{Z}_p[\zeta_t]$, and hence $\mathrm{Tr}_{\Omega_t/\mathbb{Q}_p}(\mathcal{O}_{\Omega_t}) \subseteq gp^t\mathbb{Z}_p$. By multiplicativity of the trace map, $\mathrm{Tr}_{\Phi_t/\mathbb{Q}_p}(\mathcal{O}_{\Omega_t}) = \mathrm{Tr}_{\Omega_t/\Phi_t}(\mathcal{O}_{\Omega_t})^{-1} \cdot \mathrm{Tr}_{\Omega_t/\mathbb{Q}_p}(\mathcal{O}_{\Omega_t}) = g^{-1} \cdot \mathrm{Tr}_{\Omega_t/\mathbb{Q}_p}(\mathcal{O}_{\Omega_t})$. By restricting the left hand side to $\mathfrak{m}_{\Phi_t}$, we get

$$\mathrm{Tr}_{\Phi_t/\mathbb{Q}_p}(\mathfrak{m}_{\Phi_t}) \subseteq g^{-1} \cdot \mathrm{Tr}_{\Omega_t/\mathbb{Q}_p}(\mathcal{O}_{\Omega_t}) \subseteq p^t\mathbb{Z}_p.$$

Comparing with (8), we must choose t smaller than $b+2$, contradicting the fact that t can be chosen arbitrarily large. □

The next proposition provides a "cohomological" description of deeply ramified extensions.

Proposition 3.6. *The following assertions are equivalent:*

(i) *L does not have finite conductor over K.*
(ii) $H^1(\mathrm{Gal}(\overline{\mathbb{Q}}_p/L), \overline{\mathfrak{m}}) = 0$.

In order to prove the Proposition, we need two little lemmas.

Recall that, in the proof of the previous proposition, we defined a sequence of positive integers a_n, for $n \geq n_0$, by $\mathrm{Tr}_{M_n/L_n}(\mathcal{O}_{M_n}) = \pi_n^{a_n}\mathcal{O}_{L_n}$, π_n being a uniformizer for L_n. Let $\mathcal{O}^0_{M_n}$ denote the kernel of the trace map from $\mathcal{O}_{M_n}$ to $\mathcal{O}_{L_n}$.

Lemma 3.7. *Suppose M is a cyclic extension of K, and let s denote a generator for its Galois group. Then, for all $n \geq n_0$,*

$$\pi_n^{a_n}\mathcal{O}^0_{M_n} \subset (s-1)\mathcal{O}_{M_n}.$$

Proof. Let $G = \mathrm{Gal}(M/L)$. The ring $\mathcal{O}_{M_n}$, viewed as a G-module, contains a free $\mathcal{O}_{L_n}[G]$-module X of rank 1 which is a finite index in $\mathcal{O}_{M_n}$. Hence, the inclusion $X \to \mathcal{O}_{M_n}$ has finite kernel and cokernel, so by Corollary 2.7, $\mathcal{O}_{M_n}$ and X have same Herbrand quotient. Consequently, this quotient is 1 (since $\mathcal{O}_{M_n}$ is a free $\mathcal{O}_{L_n}[G]$-module of rank 1?). Consequently, the groups $H^0(\mathcal{O}_{M_n})$ and $H^1(\mathcal{O}_{M_n})$ have same cardinality, i.e. $\mathrm{Card}(\mathcal{O}_{L_n}/\pi_n^{a_n}\mathcal{O}_{L_n}) = \mathrm{Card}(\mathcal{O}^0_{M_n}/(s-1)\mathcal{O}_{M_n})$. Since $\mathcal{O}^0_{M_n}/(s-1)\mathcal{O}_{M_n}$ is an $\mathcal{O}_{L_n}$-module, it follows by the structure theorem for modules over principal ideal domains that it decomposes into the direct sum $\oplus_{i=1}^r \mathcal{O}_{L_n}/\pi_n^{d_i}\mathcal{O}_{L_n}$. By comparing cardinalities, we must have that $a_n = \sum_{i=1}^r d_i$. Thus, $\pi_n^{a_n}$ annihilates $\oplus_{i=1}^r \mathcal{O}_{L_n}/\pi_n^{d_i}\mathcal{O}_{L_n}$, or equivalently, $\mathcal{O}^0_{M_n}/(s-1)\mathcal{O}_{M_n}$, and hence each element of $\pi_n^{a_n}\mathcal{O}^0_{M_n}$ is an element of $(s-1)\mathcal{O}_{M_n}$, which completes the proof. □

Let M be a finite extension of L of degree d. For each $n \geq n_0$, let N_n be an $\mathcal{O}_{L_n}$-submodule of $\mathcal{O}_{M_n}$ of rank d, and suppose that $\mathcal{O}_{M_m} N_n \subset N_m$ whenever $m \geq n$. Fix an $\mathcal{O}_{L_n}$-basis $\omega_1(n), \ldots, \omega_d(n)$ for N_n. Recall that the discriminant $\mathfrak{d}_{N_n} = \mathfrak{d}_{N_n/\mathcal{O}_{L_n}}$ is the ideal of $\mathcal{O}_{L_n}$ generated by $\det(\sigma_i(\omega_j(n)))^2$, where $\sigma_1, \ldots, \sigma_d$ are distinct embeddings $M_n \to \overline{\mathbb{Q}}_p$ which leave L_n fixed.

Lemma 3.8. *The limit* $\lim_{n\to\infty} v(\mathfrak{d}_{N_n})$ *exists in* $\mathbb{R}$.

Proof. Since the rank of N_n is independent of n, an $\mathcal{O}_{L_n}$-basis for N_n is also an $\mathcal{O}_{L_n}$-basis for N_m for $m \geq n$. Hence we define a $d \times d$ matrix $A = (a_{ih}) \in \mathrm{GL}(d, \mathcal{O}_{L_m})$, where a_{ih} is given by $\omega_i(n) = \sum_{h=1}^{d} a_{ih}\omega_h(m)$. It follows that $(\det(\sigma_j(\omega_i(n)))^2) = \det(\sum a_{ih}\sigma_j(\omega_h(m)))^2 = \det(A)^2 \det(\sigma_j(\omega_i(m)))^2$, and hence

$$\mathfrak{d}_{M_n} = (\det(A)^2 \det(\sigma_j(\omega_i(m)))^2).$$

Since each a_{ih} belongs to $\mathcal{O}_{L_n}$, so does $\det(A)^2$, and hence, taking valuations of both sides of the above formula yields $v(\mathfrak{d}_{M_n}) = v((\det(A)^2)) + v(\mathfrak{d}_{M_m}) \geq v(\mathfrak{d}_{M_m})$. The sequence $v(\mathfrak{d}_{N_n})$ is therefore decreasing, and since each term is ≥ 0, it is Cauchy, and the result follows. □

Recall that the *characteristic ideal* $c_n(R)$ R is the ideal of $\pi_m^D \mathcal{O}_{L_n}$, where $D = \sum_{i=1}^{r} d_i$, and where the d_i are the exponents appearing in the decomposition $R = \oplus_{i=1}^{r} \mathcal{O}_{L_m}/\pi_m^{d_i}\mathcal{O}_{L_m}$. Let A be as defined in the proof of Lemma 3.8. Then we have $\det(A)\mathcal{O}_{L_m} = c_m(N_m/\mathcal{O}_{L_m}M_n)$ and also $\mathfrak{d}_{N_n\mathcal{O}_{L_m}} = (\det A)^2\mathfrak{d}_{N_m}$. Taking valuations on both sides of both formulas, we obtain $v(c_m(N_m/\mathcal{O}_{L_m}M_n)) = v(\det(U))$, resp. $v(\mathfrak{d}_{M_n}) - v(\mathfrak{d}_{M_m}) = 2v(\det(U))$. By comparison, we get

$$v(c_m(N_m/\mathcal{O}_{L_m}M_n)) = \frac{1}{2}(v(\mathfrak{d}_{M_n}) - v(\mathfrak{d}_{M_m})),$$

which, by the above Proposition, implies that for each $\varepsilon > 0$, there exists an integer N_ε such that

$$v(c_m(N_m/\mathcal{O}_{L_m}M_n)) < \varepsilon \tag{9}$$

for all $m \geq n \geq N_\varepsilon$.

Proof of Proposition 3.6. (i) $\Longrightarrow$ (ii): We will first prove that if L does not have finite conductor over K, then for any cyclic extension M/L, we have

$$H^1(\mathrm{Gal}(M/L), \mathfrak{m}_M) = 0. \tag{10}$$

This amounts to show that, if s is a generator for the cyclic group $\mathrm{Gal}(M/L)$, and if $\mathfrak{m}_M^0$ denotes the kernel of the trace map $\mathrm{Tr} : \mathfrak{m}_M \to \mathfrak{m}_L$, then $\mathfrak{m}_M^0 = (s-1)\mathfrak{m}_M$ (cf. § 2.2). Clearly we have $(s-1)\mathfrak{m}_M \subseteq \mathfrak{m}_M^0$. Conversely, if $x \in \mathfrak{m}_M^0$, then, for $n \geq n_0$ sufficiently large, $x \in M_n$ and $v(x) > v(\pi_n^{a_n+1})$ (recall that when L does not have finite conductor over K, $v(\pi_n^{a_n+1})$ tends to 0 as n tends to ∞; see the proof of Proposition 3.5). Hence $x \in \pi_n^{a_n+1}\mathcal{O}_{M_n}^0$, and by Lemma 3.7, $x \in (s-1)\pi_n\mathcal{O}_{M_n} \subseteq (s-1)\mathfrak{m}_M$.

We now pass to the general case. It suffices to show that $H^1(\mathrm{Gal}(L'/L), \mathfrak{m}_M) = 0$ for all *finite* Galois extensions L'/L, since we may then pass to the inductive limit and deduce (ii) (Proposition 2.1). But since $\mathrm{Gal}(L'/L)$ is a solvable group, it has a composition series of non-trivial cyclic subgroups, and hence there exists a non-trivial cyclic subextension K/L of L'/L. The corresponding inflation-restriction

sequence (Proposition 2.2) is

$$0 \to H^1(\mathrm{Gal}(M/L), \mathfrak{m}_M) \to H^1(\mathrm{Gal}(L'/L), \mathfrak{m}_{L'}) \to H^1(\mathrm{Gal}(L'/M), \mathfrak{m}_{L'}),$$

the left term $H^1(\mathrm{Gal}(M/L), \mathfrak{m}_M)$ being 0 by (10). Furthermore, by induction on the degree of L'/L, it immediately follows that $H^1(\mathrm{Gal}(L'/M), \mathfrak{m}_{L'}) = 0$. Hence $H^1(\mathrm{Gal}(L'/L), \mathfrak{m}_{L'}) = 0$, and this completes the proof of (i) $\Longrightarrow$ (ii).

(ii) $\Longrightarrow$ (i): Let $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$. We assume that $H^1(G, \overline{\mathfrak{m}}) = 0$. For all finite Galois extensions M/L, the inflation-restriction sequence becomes

$$0 \to H^1(\mathrm{Gal}(M/L), \mathfrak{m}_M) \to H^1(G, \overline{\mathfrak{m}}) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}_p/M), \overline{\mathfrak{m}}).$$

Hence, $H^1(\mathrm{Gal}(M/L), \mathfrak{m}_M)$ injects into $H^1(G, \overline{\mathfrak{m}})$, and is therefore 0. In particular, if the extension M/L is *cyclic* (as above), this implies that $\mathfrak{m}_M^0 = (s-1)\mathfrak{m}_M$, where again s is a generator of $\mathrm{Gal}(M/L)$ and $\mathfrak{m}_M^0$ denotes the kernel of the trace map $\mathrm{Tr} : \mathfrak{m}_M \to \mathfrak{m}_L$. Now let

$$N_n = \mathcal{O}_{Ln} \cdot (1 + \mathfrak{m}_{M_n}^0),$$

where $\mathfrak{m}_{M_n}^0$ denotes the kernel of the trace map $\mathrm{Tr} : \mathfrak{m}_{M_n} \to \mathfrak{m}_{L_n}$. This is an $\mathcal{O}_{L_n}$-module of rank $d = [M : L]$, and it satisfies $\mathcal{O}_{M_n} N_n \subset N_m$ whenever $m \geq n$ (in particular, formula (9) holds). By the equality $\mathfrak{m}_M^0 = (s-1)\mathfrak{m}_M$, we have an inclusion $\mathfrak{m}_{M_n}^0 \subset (s-1)\mathfrak{m}_{M_n}$, and hence

$$\mathcal{O}_{L_m} N_n \subset N_m = \mathcal{O}_{L_m} \cdot (1 + \mathfrak{m}_{M_m}^0) \subset \mathcal{O}_{L_m} \cdot (1 + (s-1)\mathfrak{m}_{M_m}.$$

Thus, there is a natural surjection

$$N_m/\mathcal{O}_{L_m} N_n \twoheadrightarrow \frac{\mathcal{O}_{L_m} + \mathfrak{m}_{M_m}^0}{\mathcal{O}_{L_m} + (s-1)\mathfrak{m}_{M_m}} \simeq \frac{\mathfrak{m}_{M_m}^0}{(s-1)\mathfrak{m}_{M_m}};$$

in particular, the characteristic ideal $c_m(\mathfrak{m}_{M_m}^0/(s-1)\mathfrak{m}_{M_m})$ contains the characteristic ideal $c_m(N_m/\mathcal{O}_{L_m} N_n)$. Now for a fixed $\varepsilon > 0$, the formula (9) implies

$$v(c_m(\mathfrak{m}_{M_m}^0(s-1)\mathfrak{m}_{M_m})) \leq c_m(N_m/\mathcal{O}_{L_m} N_n) < \varepsilon \tag{11}$$

whenever $n \geq N_\varepsilon$. The ideal $\mathfrak{m}_{M_m}$ is isomorphic as an $\mathcal{O}_{L_m}$-module to $\mathcal{O}_{M_m}$, and the Herbrand quotient of the latter is equal to 1 (see the comment in the proof of Lemma 3.6). Hence, the $\mathcal{O}_{L_m}$-modules $H^0(G, \mathfrak{m}_{M_m}) = \mathfrak{m}_{L_m}/\mathrm{Tr}(\mathfrak{m}_{M_m})$ and $H^1(\mathfrak{m}_{M_m}^0/(s-1)\mathfrak{m}_{M_m})$ have same order. Since this order uniquely determines the characteristic ideal of these modules (the sum of the exponents d_i in the direct sum decomposition above must be equal), we have

$$v(c_m(\mathfrak{m}_{L_m}/\mathrm{Tr}(\mathfrak{m}_{M_m}))) = v(c_m(\mathfrak{m}_{M_m}^0/(s-1)\mathfrak{m}_{M_m})).$$

If, for each n we define an integer a_n by $\mathrm{Tr}_{M_m/L_m}(\mathfrak{m}_{M_m}) = \pi_n^{a_m}\mathfrak{m}_{L_m}$, then we get $v(c_m(\mathfrak{m}_{L_m}/\mathrm{Tr}(\mathfrak{m}_{M_m}))) = v(c_m(\pi_m^{-a_m})) = v(\pi_m^{a_m})$, and by 11, we get $v(\pi_m^{a_m}) < \varepsilon$ for $m \geq n \geq N_\varepsilon$, or equivalently,

$$v(\pi_n^{a_n}) \to 0, \text{ as } n \to \infty.$$

Using exactly the same arguments as in the proof of Proposition 3.5, (ii) $\Longrightarrow$ (iii), we conclude that $\mathrm{Tr}_{M/L}(\mathfrak{m}_M) = \mathfrak{m}_K$. By Proposition 3.5, we deduce that L does not have finite conductor over K. $\square$

3.2. Ramified $\mathbb{Z}_p$-extensions. Let L/K be a $\mathbb{Z}_p$-*extension*, that is, a Galois extension whose Galois group G is isomorphic to $\mathbb{Z}_p$. Closed subgroups of $\mathbb{Z}_p$ are of the form $p^n\mathbb{Z}_p$, $n \geq 1$; denote these by $G(n)$. Thus we may form a tower

$$K = K_0 \subset K_1 \subset \ldots \subset K_\infty = \bigcup_{n \geq 0} K_n,$$

for which K_n/K is cyclic of order p^n (in fact, $\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$). Of particular interest will be the *cyclotomic $\mathbb{Z}_p$- extensions.*

Proposition 3.9. *Suppose that K is a local field, and suppose that L/K is a ramified $\mathbb{Z}_p$-extension. The L is deeply ramified.*

Proof. Let $G = \mathrm{Gal}(L/K)$, and let r be the local reciprocity map defined in Chap. II, Section 1.3. By Theorem 1.21 of Chapter II, we have $G^v = r(U_K^i)$, where i is the smallest integer $\geq v$. But since L/K is ramified, $r(U_K^0)$ must be infinite, and since U^i is of finite index in U^0 for all i, this implies that the conductor of L over K is not finite. Hence L is deeply ramified. □

Suppose again that L/K is a *ramified* $\mathbb{Z}_p$-extension. In this case the ramification groups of G (in the upper numbering) are easily identifiable. Let $-1 = v_{-1} < v_1 < v_2 < \ldots$ be the gaps in the filtration $\{G^v\}$ of G.

Proposition 3.10. *Suppose L/K is a ramified $\mathbb{Z}_p$-extension. Let $n_0 \geq 0$ be the integer such that K_{n_0}/K is the maximal unramified extension of K. Then, for all $i \geq -1$, we have*

$$G^v = G(n_0 + i + 1), \text{ for } v_i < v \leq v_{i+1}.$$

Proof. By induction on i, the case $i = -1$ being immediate. Assume it holds for i. By Proposition 1.11, $U^p_{v_{i+1}} \subset U_{v_{i+1}p}$ if $v_{i+1} \leq e_K/(p-1)$, and $U_{v_{i+1}} \simeq U_{v_{i+1}+e_K}$ if $v_{i+1} > e_K/(p-1)$, so that $U^p_{v_{i+1}} \subset U_{v_{i+1}+e_K}$ in this case. Hence there exists an integer r (namely $\min(v_{i+1}p, v_{i+1}+e_K)$) such that $U^p_{v_{i+1}} \subset U_r$, and therefore $G(n_0+i+2) = (G(n_0+i+1))^p = (G^{v_{i+1}})^p \subset G^r$, the first equality being true by definition of the subgroups groups $G(n)$, and the second equality being our induction hypothesis. Conversely, if $v > v_{i+1}$, G^v is strictly contained in $G^{v_{i+1}} = G(n_0+i+1)$ since v_{i+1} is a gap; hence it must be contained in a smaller subgroup, i.e. $G^v \subseteq G(n_0+i+2)$. We thus have the inclusions $G^v \subseteq G(n_0+i+2) \subseteq G^r$, $v_{i+1} < v \leq r$. Since $r \geq v$, $G^r \subseteq G^v$, and hence $G^v = G(n_0+i+2)$, and the induction is complete. □

Consequently, we have a nice description of the gaps in the filtration of G for large enough indices:

Proposition 3.11. *For all i such that $v_i > e_K/(p-1)$, we have $v_{i+1} = v_i + e_K$.*

Proof. By Proposition 1.11, we have an isomorphism $U_{v_i} \simeq U_{v_i+e_K}$ defined by $x \mapsto x^p$, so that $U^p_{v_i}$ can be identified to $U_{v_i+e_K}$. Now $G^{v_{i+1}} = G(n_0+i+1) = \rho_{k_\infty/K}(U^p_{v_i}) = \rho_{K_\infty/K}(U_{v_i+e_K}) = G^{v_i+e_K}$, the first equality following from Proposition 3.10. Hence we must show that $v_i + e_K$ is a gap, i.e. that for any $\varepsilon > 0$, $G^{v_i+e_K+\varepsilon}$ is strictly included in $G(n_0+i+1)$. But this is true since $G^{v_i+e_K+\varepsilon} = \rho_{K_\infty/K}(U_{v_i+e_K+n(\varepsilon)}) = \rho_{K_\infty/K}((U_{v_i+n(\varepsilon)})^p) \subseteq G(n_0+i+2)$ (here $n(\varepsilon)$ denotes the smallest integer $\geq \varepsilon$). □

Example 3.12. Let μ_{p^∞} be the group of all p-power roots of unity, and let $\mathbb{Q}_p(\mu_{p^\infty})$ be the extension of $\mathbb{Q}_p$ obtained by adjoining μ_{p^∞} to $\mathbb{Q}_p$. The action on μ_{p^∞} of the corresponding Galois group $G = \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$ is given by the *cyclotomic character* $\chi : G \to \mathrm{Aut}(\mu_{p^\infty}) = \mathbb{Z}_p^*$ define by $s(\zeta) = \zeta^{\chi(s)}$ for $\zeta \in \mu_{p^\infty}$ and $s \in G$. Since the cyclotomic equation is irreducible, this map is an isomorphism. Furthermore,

$$\mathbb{Z}_p^* = \begin{cases} \mu_p \times (1 + 2p\mathbb{Z}_p) & \text{if } p = 2, \\ \mu_{p-1} \times (1 + p\mathbb{Z}_p) & \text{if } p > 2. \end{cases}$$

The p-adic logarithm maps $(1 + n\mathbb{Z}_p)$ isomorphically to $n\mathbb{Z}_p \simeq \mathbb{Z}_p$ for any $n > 0$, and hence we see that the Galois group $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \simeq \mathbb{Z}_p^*$ is isomorphic to the product $\Delta \times \mathbb{Z}_p$, where $\Delta \simeq \mu_p$ for $p = 2$, and $\Delta \simeq \mu_{p-1}$ for $p > 2$. The *cyclotomic extenion* of $\mathbb{Q}_p$ is by definition the subfield of $\mathbb{Q}_p(\mu_{p^\infty})$ fixed by Δ.

Theorem 3.13. *Suppose K_∞/K is a ramified $\mathbb{Z}_p$-extension. Let $e = e_{K/\mathbb{Q}_p}$ be the absolute ramification index of K. Then there is a constant c and a bounded sequence $\{a_n\}$ such that*

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

Before proving the theorem, let us illustrate it with a simple example:

Example 3.14. Let $p > 2$. Set $K_p = \mathbb{Q}(\mu_p)$, $K_n = \mathbb{Q}_p(\mu_{p^{n+1}})$. We have $K_\infty = \mathbb{Q}_p(\mu_{p^\infty})$. Then K_n is totally ramified of degree $\varphi(p^n) = p^{n-1}(p-1)$ over $\mathbb{Q}_p$, where φ is the Euler φ-function (Serre [**7**], Chap. IV, §4, Prop. 17). Furthermore, using the formulas $\mathfrak{m}_K = \mathfrak{m}_{K_n}^{p^n}$ and $\mathfrak{D}_{K_n/\mathbb{Q}_p} = \mathfrak{m}_{K_n}^{np^n-(n+1)p^{n-1}}$, we obtain

$$\begin{aligned} \mathfrak{D}_{K_n/K} = \mathfrak{D}_{K_n/\mathbb{Q}_p} \cdot \mathfrak{D}_{K/\mathbb{Q}_p}^{-1} &= \mathfrak{m}_{K_n}^{(n+1)p^{n+1}-(n+2)p^n} \cdot \mathfrak{m}_K^{-(p-2)} \\ &= \mathfrak{m}_{K_n}^{(n+1)p^{n+1}-(n+2)p^n} \cdot \mathfrak{m}_{K_n}^{-p^{n+1}+2p^n} \\ &= m_{K_n}^{np^n(p-1)}. \end{aligned}$$

Thus, $v_K(\mathfrak{D}_{K_n/K}) = e_{K_n/K}^{-1} \cdot v_{K_n}(\mathfrak{D}_{K_n/K}) = p^{-n}np^n(p-1) = n(p-1) = en$.

Proof of theorem 3.13. By multiplicativity of the different, we may assume that K_∞/K is totally ramified. By Theorem 1.13, we get

$$v_K(\mathfrak{D}_{K_n/K}) = e_{K_n/K}^{-1} v_{K_n}(\mathfrak{D}_{K_n/K}) = \int_{-1}^{\infty} (1 - [K_n : K_n \cap K^v]^{-1}) dv. \tag{12}$$

We have $[K_n : K_n \cap K^v] = \mathrm{Gal}(K_n/K)^v = (G/G(n))^v = G^v G(n)/G(n)$, the last equality following from Herbrand's Theorem. By Proposition 3.10 (applied with $n_0 = 0$ since K_∞/K is totally ramified), we have $G^v = G(i+1)$ if $v_i < v \leq v_{i+1}$ $(i \geq -1)$. Hence $\mathrm{Card}(G^v(G(n)/G(n)) = p^{n-i-1}$ if $v_i < v \leq v_{i+1}$ and $i \leq n-1$, and $\mathrm{Card}(G^v(G(n)/G(n)) = 1$ otherwise, so that our integral expression becomes

$$v_K(\mathfrak{D}_{K_n/K}) = \sum_{i=-1}^{n-1} (v_{i+1} - v_i)(1 - p^{i+1-n}).$$

Now by Proposition 3.10, for i large enough, say $i \geq r$, $v_{i+1} - v_i = e$. If $n \geq r+1$, the sum decomposes into

$$\begin{aligned} v_K(\mathfrak{D}_{K_n/K}) &= \sum_{i=-1}^{r-1} (v_{i+1} - v_i)(1 - p^{i+1-n}) + \sum_{i=-1}^{r-1} e(1 - p^{i+1-n}) \\ &= en - \underbrace{er + \sum_{i=-1}^{r-1} (v_{i+1} - v_i)}_{c} + p^{-n} \underbrace{\sum_{i=-1}^{n-1} (v_i - v_{i+1}) p^{i+1}}_{a_n}. \end{aligned}$$

For $n < r+1$, we let i run up to $r+n-1$ in formula (12) and subtract the corresponding higher terms. Thus, by conveniently adding a constant term to a_n, we obtain the same formula. [I am not sure whether a_n is bounded]. □

Proposition 3.15. *Let $G = \mathrm{Gal}(K_\infty/K)$. Then $H^0(G, \widehat{K}_\infty) = K$.*

Proof. Let γ be a topological generator of G. By definition, $H^0(G, \widehat{K}_\infty)$ is the kernel of the the automorphism $\gamma - 1$. Hence it suffices to show that $\gamma - 1$ annihilates K, but this now follows from Tate [**9**], §3.1, Prop. 7. [I did not understand his argument.] □

3.3. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ on $\mathbb{C}$. We keep the notations of the previous section. Let $\mathbb{C}$ denote the completion of the algebraic closure of $\mathbb{Q}_p$. It is algebraically closed, by Krasner's lemma. The Galois group $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ operates on $\mathbb{C}$ by continuity.

Theorem 3.16. *Suppose that K_∞ is deeply ramified, and let $H = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K_\infty)$. Then $H^0(H, \mathbb{C}) = \widehat{K}_\infty$ and $H^i(H, \mathbb{C}) = 0$, for $i > 0$.*

Lemma 3.17. *Suppose that K_∞ is deeply ramified and let L_∞ be a finite extension of K_∞, with Galois group $G_\infty = \mathrm{Gal}(L_\infty/K_\infty)$. Let c be a fixed constant > 1. For each $y \in L_\infty$, there exists $z \in L_\infty$ such that*

$$|y - \mathrm{Tr}_{L_\infty/K_\infty}(z)| \leq c \max_{s \in G_\infty} |s(y) - y| \quad \textit{and} \quad |z| < c|y|.$$

Proof. Since $e_{K_n/\mathbb{Q}_p}$ tends to ∞ as $n \to \infty$, it is clear that, for every $\varepsilon > 0$, there exists an element $x \in \mathfrak{m}_{K_\infty}$ with $|x| \geq 1 + \varepsilon$. Since K_∞ is deeply ramified, $\mathrm{Tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty}) = \mathfrak{m}_{K_\infty}$ (cf. Theorem 3.2), and hence there exists an element $w \in \mathfrak{m}_{L_\infty}$ such that $\mathrm{Tr}_{L_\infty/K_\infty}(w) \geq c^{-1}$. Let $z = y \cdot w \cdot \mathrm{Tr}_{L_\infty/K_\infty}(w)^{-1}$; then $|z| \leq c|y||w| \leq c|y|$ and $\mathrm{Tr}_{L_\infty/K_\infty}(z) = \mathrm{Tr}_{L_\infty/K_\infty}(w)^{-1} \sum_{s \in G_\infty} s(y)s(w)$. Writing y as $y \cdot \mathrm{Tr}_{L_\infty/K_\infty}(w)^{-1} \cdot \sum_{s \in G_\infty} s(w)$, we get

$$\mathrm{Tr}_{L_\infty/K_\infty}(z) - y = \frac{1}{\mathrm{Tr}_{L_\infty/K_\infty}(w)} \cdot \sum_{s \in G_\infty} s(w)(s(y) - y).$$

Taking absolute values, and using the fact that $|s(w)| < 1$, we obtain the desired inequality. □

Proof of Theorem 3.16. We first prove that $H^0(H, \mathbb{C}) = \mathbb{C}^H = \widehat{K}_\infty$. This is an easy consequence of the previous lemma. First note that, for all $n \geq 1$, any element of $\mathbb{C}$ can be written as a sum $x + \pi^n y$, where $x \in \overline{\mathbb{Q}}_p$, $y \in \mathcal{O}_\mathbb{C}$, and π is a uniformizer of some finite extension of $\mathbb{Q}_p$ contained in K_∞. Fix an element $\alpha \in \mathbb{C}^H$ and define, for each $n \geq 1$, elements x_n and y_n by $x_n + \pi^n y_n = \alpha$. By Lemma 3.17,

for each element in the sequence $\{x_n\}$, there is an element $z_n \in K_\infty$ such that $|x_n - z_n| \leq c \cdot \max_{s\in H} |s(x_n) - x_n|$. Since H acts on $\mathcal{O}_\mathbb{C}$, $s(x_n) - x_n \in \pi^n \mathcal{O}_\mathbb{C}$ for all $s \in H$ and all $n \geq 1$, and hence $|x_n - z_n|$ tends to 0 as n tends to infinity ($\pi^n y_n$ becomes arbitrarily small). Likewise, x_n tends tends to α as n tends to infinity and hence so does z_n. Since $\widehat{K}_\infty$ is complete and $z_n \in K_\infty$ for all n, we get $\alpha \in \widehat{K}_\infty$. □

Theorem 3.18. *Suppose K is a finite extension of $\mathbb{Q}_p$, and let G be its absolute Galois group. Then $H^0(G, \mathbb{C}) = K$ and $H^1(G, \mathbb{C})$ is a one-dimensional vector space over K.*

Proof. Let K_∞ be the cyclotomic $\mathbb{Z}_p$-extension of K defined in Example 3.12. Since it is ramified, it is deeply ramified by Proposition 3.9.Let G/H be its Galois group over K, where $H = \mathrm{Gal}(\overline{\mathbb{Q}}_p, K_\infty)$. By Theorem 3.16, $H^0(G, \mathbb{C}) = \mathbb{C}^G = (\mathbb{C}^H)^{G/H} = (\widehat{K}_\infty)^{G/H}$. By Proposition 3.15, this is equal to K, so the first assertion is clear. For the second assertion, we have the inflation-restriction sequence (Proposition 2.2)

$$0 \to H^1(G/H, \widehat{K}_\infty) \to H^1(G, \mathbb{C}) \to H^1(H, \mathbb{C}).$$

The group $H^1(H, \mathbb{C})$ is trivial by Prop. 3.16, and $H^1(G/H, \widehat{K}_\infty)$ has dimension 1 over K, hence the result. □

Given a continuous homomorphism $\psi : G \to K^*$, we denote by $\mathbb{C}(\psi)$ the field $\mathbb{C}$ endowed with the "twisted action"

$$\tilde{s}(x) = \psi(s)s(x), \quad s \in G,\ x \in \mathbb{C}.$$

Using similar arguments to the previous, we obtain the following:

Theorem 3.19. *Let K and G be as in Theorem 3.18. Furthermore, let I_K denote the inertia subgroup of G, and let $\psi : G \to K^*$ be a continuous homomorphism such that $\psi(I_K)$ is infinite. Then $H^0(G, \mathbb{C}(\psi)) = H^1(G, \mathbb{C}(\psi)) = 0$.*

Proof. Notice first that since G is compact, ψ takes its values in the group $\mathbb{Z}_p$ of units of $\mathbb{Q}_p^*$. If $\psi(I_K)$ is infinite, then it contains a subgroup $p^n\mathbb{Z}_p$, for some $n \geq 0$. Consequently, L_∞ contains a ramified $\mathbb{Z}_p$-extension K_∞ of K, and the result follows by Proposition 3.16. □

CHAPTER 2

p-adic Hodge-Tate theory

In this chapter, we introduce p-adic representations, which are finite-dimensional vector spaces over $\mathbb{Q}_p$ together with a continuous action of the absolute Galois group of some local field. We establish Tate's theorem, relating those with a "Hodge-Tate decomposition" to those which are "locally algebraic". Before doing so, we construct in Section 1 an important example of a p-adic representations arising from Lubin-Tate formal groups and which will play a central role in the proof of the theorem. We also use this opportunity to prove the theorem of Hasse-Arf (Chapter I, Theorem 1.9).

1. Lubin-Tate formal groups

1.1. Formal group laws. Let R be a ring. A *formal group law over* R is a power series $F \in R[[X, Y]]$ satisfying

(i) $F(X, Y) \equiv X + Y (\text{mod deg } 2)$;
(ii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$;
(iii) $F(X, Y) = F(Y, X)$;
(iv) There is a unique $i(X) \in R[[X]]$ such that $F(X, i(X)) = 0$;
(v) $F(X, 0) = X$ and $F(0, Y) = Y$.

Two power series are congruent (mod deg n) if they agree on terms of degree strictly less that n. Note that (ii) makes sense because (i) ensures that $F(X, Y)$ has no constant term. Note also that conditions (ii), (iii) and (iv) together imply conditions (i) and (iv).

Examples 1.1. (a) Let K be a local field. If $R = \mathcal{O}_K$, then the maximal ideal $\mathfrak{m}_K$ of $\mathcal{O}_K$ can be given the structure of an abelian group by defining $x +_F y = F(x, y)$ (convergence is guaranteed since K is complete). We will denote this group by $F(\mathfrak{m}_K)$.
(b) By letting $F(X, Y) = X + Y + XY$ in the previous example, we recover the usual multiplicative group $(1 + \mathfrak{m}_K, \times)$. This law is called the *formal multiplicative group law*.
(c) Let E/K be an elliptic curve over K, given by the Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with $a_1, \ldots, a_6 \in K$. Let π be a uniformizer for $\mathcal{O}_K$. Then the kernel of the reduction of E modulo π contained in $E(K)$ is isomorphic to $F(\mathfrak{m}_K)$, where F is given by

$$\begin{aligned} F(X, Y) &= X + Y - a_1XY - a_2(X^2Y + XY^2) \\ &\quad -(2a_3X^3Y - (a_1a_2 - 3a_3)X^2Y^2 + 2a_3XY^3) + \ldots \end{aligned}$$

Let F, G be two formal groups over R. A *morphism* $f : F \to G$ of formal groups is a power series $f \in R[[T]]$ with no constant term, satisfying

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

The notion of endomorphism and isomorphism of a formal group are defined accordingly. Furthermore, the set $\mathrm{End}(F)$ of endomorphisms of F may be given the structure of a ring, when equipped with the following addition and multiplication:

$$\begin{aligned}(f +_F g)(X) &= F(f(X), g(X)),\\ (f \circ_F g)(X) &= f(g(X)).\end{aligned}$$

1.2. Lubin-Tate formal groups. Suppose now, and for the rest of this section, that K is a *local field of characteristic 0*. In particular, K is a finite extension of $\mathbb{Q}_p$, and its separable and algebraic closures coincide. Let $q = \mathrm{Card}(k) > 0$ be the cardinality of its residue field k, and let $\pi \in \mathcal{O}_K$ be a uniformizer. Let $\mathfrak{F}_\pi$ be the set of formal power series in $\mathcal{O}_K[[X]]$ satisfying

$$(\dagger) \qquad \begin{aligned} f(X) &\equiv \pi X \pmod{\deg 2};\\ f(X) &\equiv X^q \pmod{\pi}.\end{aligned}$$

The second condition means that $\overline{f}(X) = X^q$, where $\overline{f} \in k[[X]]$ denotes the reduction of f modulo π.

Theorem 1.2. *For each $f \in \mathfrak{F}_\pi$, there is a unique formal group law F_f for which f is an endomorphism. This formal group law is called the* Lubin-Tate formal group over $\mathcal{O}_K$ for π.

For the proof, we will need the following fundamental lemma:

Lemma 1.3. *Let n be a positive integer, and let $\phi(X_1, \ldots, X_n)$ be a linear form in $X_1, \ldots, X_n$ with coefficients in $\mathcal{O}_K$. Let $f, g \in \mathfrak{F}_\pi$. Then there exists a unique power series $F \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ such that*

$$\begin{aligned} F &\equiv \phi \ \textit{(mod deg 2)}\\ f \circ F &= F \circ (g \times \ldots \times g).\end{aligned}$$

Proof. To ease notation, write $X = (X_1, \ldots, X_n)$, and $g = g \times \ldots \times g$. By the first condition, F must not contain any constant term, and hence it must be of the form $F = \sum_{i=1}^{\infty} H_i(X)$, where H_i is a homogeneous polynomial of degree i. Let $F_r = \sum_{i=1}^{n} H_i(X)$. Then the conditions of the lemma can be restated as

$$\begin{aligned} F_1 &= \phi\\ f \circ F_r &\equiv F_r \circ g \pmod{\deg (r+1)} \text{ for all } r \geq 1.\end{aligned}$$

So let us determine H_i by induction. For $i = 1$, we must have $H_1 = \phi$. Suppose that for each $i \leq r$, H_i is uniquely determined. We then construct H_{r+1} in the following way. Notice first that $f \circ F_r$ and $F_r \circ g$ agree on terms of degree $\leq r$, by hypothesis. Going one degree up, there might be an "error" term E_{r+1}, i.e. we have $f \circ F_r \equiv F_r \circ g + E_{r+1}$ (mod deg (r+2)), with $E_{r+1} \equiv 0$ mod deg (r+1). Recalling that $f(X) = \pi X + X^2(\sum \ldots)$, we have

$$f \circ F_{r+1} = f \circ (F_r + H_{r+1}) = f \circ F_r + \pi H_{r+1} + H_{r+1}^2 \left(\sum \ldots\right) + 2F_r H_{r+1} \left(\sum \ldots\right),$$

and hence

$$f \circ F_{r+1} \equiv f \circ F_r + \pi H_{r+1} \pmod{\deg (r+2)}. \tag{13}$$

On the other hand, we have

$$H_{r+1}\circ g = \sum_i c_i \prod_{j=1}^n g(X_j)^{\alpha_j} = \sum_i c_i \pi^{r+1} \left(\prod_{j=1}^n X_j^{\alpha_j} + (\text{terms of degree} \geq r+2) \right).$$

Hence, $H_{r+1} \circ g = \pi^{r+1} H_{r+1}$ (mod deg (r+2)), and together with the identity $F_{r+1} \circ g = F_r \circ g + H_{r+1} \circ g$, we deduce

$$F_{r+1} \circ g \equiv F_r \circ g + \pi^{r+1} H_{r+1} \text{ (mod deg (r+2))}. \tag{14}$$

Combining the identities (13) and (14), we have that

$$H_{r+1} = \frac{-E_{r+1}}{\pi - \pi^{r+1}},$$

is the unique choice of H_{r+1} which works. Thus it remains to prove that H_{r+1} indeed is a polynomial with coeffiecients in $\mathcal{O}_K$, i.e. that $E_{r+1} \equiv 0 \pmod{\pi}$. But f and g are congruent to X^q mod π, so $E_{r+1} = f \circ F_r(X) - F_r \circ g(X) \equiv F_r(X)^q - F_r(X^q) \equiv 0 \pmod{\pi}$. Thus we have an explicit construction of F, which is unique; this completes the proof. □

Proof of Theorem 1.2. By Lemma 1.3, applied with $n = 2$, $\phi(X,Y) = X+Y$ and $f = g$, it suffices to show that the unique power series F_f that we obtain is indeed a formal group law. We first show associativity: by definition, we have

$$\begin{aligned} F_f(F_f(X,Y),Z) &\equiv X+Y+Z \text{ (mod deg 2)} \\ F_f(F_f(f(X),f(Y)),f(Z)) &= f(F_f(F_f(X,Y),Z)). \end{aligned}$$

The same holds for $F_f(X, F_f(Y,Z))$, and hence the unicity part of the lemma shows that $F_f(F_f(X,Y),Z) = F_f(X,F_f(Y,Z))$. The same argument applies for $F_f(X,0)$ and X, showing the existence of the neutral element. Commutativity and congruence mod 2 is obvious, and, as noted above, the existence of inverse is automatic. Hence F_f is the desired unique formal group law for which f is an endomorphism. □

We have a dual result:

Proposition 1.4. *Let $f \in \mathfrak{F}_\pi$, and let F_f be the corresponding formal group law. Then for all $a \in \mathcal{O}_K$, there is a unique endomorphism $[a]_f \in \mathrm{End}(F_f)$ satisfying*

$$\begin{aligned} [a]_f(X) &\equiv aX \text{ (mod deg 2)} \\ [a]_f \circ f &= f \circ [a]_f. \end{aligned}$$

[Of course, when $a = \pi$, this endomorphism is f itself.]

Proof. By Lemma 1.3 with $n = 1$, $\phi(X) = aX$ and $f = g$, we immediately get existence and uniqueness of $[a]_f$. Since $F_f([a]_f(X), [a]_f(Y))$ and $[a]_f(F_f(X,Y))$ are congruent to $aX + aY$ (mod deg 2) and commute with f, they must be equal, again by the uniqueness part of Lemma 1.3. Thus $[a]_f$ is an endomorphism of F_f. □

Example 1.5. If $K = \mathbb{Q}_p$, $\pi = p$, then the formal power series

$$f(X) = (1+X)^p - 1 = pX + \binom{p}{2} X^2 + \ldots + X^p$$

verifies conditions (†) above. It is an endomorphism of the formal multiplicative group law $F(X,Y) = X + Y + XY$ since $F(f(X), f(Y)) = (1+X)^p(1+Y)^p - 1 = f(F(X,Y))$. On the other hand, for any $a \in \mathbb{Z}_p$, the formal power series

$$[a]_f(X) = \sum_{i=1}^{\infty} \binom{a}{i} X^i = (1+X)^a - 1.$$

is the unique endomorphism of F commuting with f, and whose derivative at the origin is a.

Proposition 1.6. *The map $\varphi : \mathcal{O}_K \to \mathrm{End}(F_f)$, $a \mapsto [a]_f$ is an injective ring homomorphism.*

Proof. We use the same technique as above to show that φ is a homomorphism. Namely, one readily verifies that $[a+b]_f$ and $F_f \circ ([a]_f \times [b]_f)$ are congruent to $(a+b)T$ (mod deg 2), and commute with f, and hence must be equal by Lemma 1.3. In the same way one obtains $[a \cdot b]_f = [a]_f \circ [b]_f$. Injectivity of φ is clear since $[a]_f = aX$ (mod deg 2). □

A Lubin-Tate formal group F_f together with the homomorphism φ of Proposition 1.6 is called a *formal $\mathcal{O}_K$-module for π*. If we pick group elements in $\overline{\mathfrak{m}}$, the maximal ideal of the ring of integers of $\overline{\mathbb{Q}}_p$, we obtain an $\mathcal{O}_K$-module, in the usual sense, by setting $x + y = x +_F y = F_f(x,y)$ and $a \cdot x = [a]_f(x)$, $x, y \in \overline{\mathfrak{m}}$, $a \in \mathcal{O}_K$. Actually, this module depends solely on π:

Proposition 1.7. *Let f, g be elements of $\mathfrak{F}_\pi$. Then the corresponding formal groups F_f and F_g are isomorphic.*

Proof. Let $[a]_{f,g}$ be the unique solution of $[a]_{f,g}(X) \equiv aX$ (mod deg 2) and $f([a]_{f,g}(X)) = [a]_{f,g}(g(X))$. Applying the arguments of the proof of Proposition 1.6, one sees that $[a]_{f,g}$ is a homomorphism of F_f into F_g. If a is a unit in $\mathcal{O}_K$, then $[a]_{f,g}$ is invertible (with inverse $[a^{-1}]_{f,g}$), and thus $[a]_{f,g}$ gives an isomorphism between F_f and F_g. □

1.3. The abelian representation associated to a Lubin-Tate formal group. Fix a uniformizer $\pi \in \mathcal{O}_K$ and a formal power series $f \in \mathfrak{F}_\pi$, and let $F_f \in \mathcal{O}_K[[X,Y]]$ be the correponding formal group law, viewed as a formal $\mathcal{O}_K$-module. Let $\overline{\mathfrak{m}}$ be the maximal ideal of the ring of integers of $\overline{\mathbb{Q}}_p$, and let q be the cardinality of the corresponding residue field. Let E_f^n be the kernel of $[\pi^n]_f$, i.e. the set $\{x \in \overline{\mathfrak{m}} \mid \pi^n \cdot x = 0\}$; since all its elements are killed by $\pi^n\mathcal{O}_K$, E_f^n is also an $\mathcal{O}_K/\pi^n\mathcal{O}_K$-module. We first have a general fact:

Lemma 1.8. *Let R be a ring, and M an R-module. Let $\psi : M \to M$ be a homomorphism, and let M_n be the kernel of the composition $\psi \circ \ldots \circ \psi$, n times. If ψ is surjective, and if M_1 has cardinality q, then M_n has cardinality q^n.*

Proof. By induction on n, the case $n = 1$ being clear. Since ψ is surjective, we have an exact sequence $0 \to M_1 \to M_n \xrightarrow{\psi} M_{n-1} \to 0$. By hypothesis, M_1 and M_{n-1} have cardinality q, resp. q^{n-1}, so M_n has cardinality q^n. □

Proposition 1.9. *For each $n \geq 0$, the $\mathcal{O}_K/\pi^n\mathcal{O}_K$-module E_f^n is free of rank 1.*

PROOF. Let $F = F_f$. By Proposition 1.7, we may without loss of generality choose $f(X) = \pi X + X^q = [\pi]_f(X)$. This polynomial is separable, and hence has q solutions, which belong to $\overline{\mathfrak{m}}$. Indeed, if α is a root, then either $\alpha = 0$, in which case $v(\alpha) = +\infty$ (here, v denotes the valuation on $\overline{\mathbb{Q}}_p$), or $v(x) = 1/(q-1) > 0$. Hence $E_f^1 = \ker f$ has cardinality q.

Now let $f^{(n)} = f \circ \ldots \circ f$ be the composition n times, and notice that $E_f^n = \ker f^{(n)}$. We want to show that $[\pi]_f : F(\overline{\mathfrak{m}}) \to F(\overline{\mathfrak{m}})$ is surjective. So let $a \in F(\overline{\mathfrak{m}})$, and let α be a solution to the equation $\pi X + X^q - a$. Clearly, $[\pi]_f$ is surjective if and only if α belongs to $F(\overline{\mathfrak{m}})$. But we have $0 < v(y) = \inf(v(\alpha) + 1, qv(\alpha)) \leq qv(\alpha)$, i.e. $\alpha \in F(\overline{\mathfrak{m}})$. Applying Lemma 1.8 with $R = \mathcal{O}_K$, $M = F(\overline{\mathfrak{m}})$ and $f = [\pi]_f$, we conclude that E_f^n has cardinality q^n. Let $\alpha \in E_f^n \backslash E_f^{n-1}$. Multiplication by α defines an $\mathcal{O}_K$-module homomorphism $\mathcal{O}_K \to E_f^n$ with kernel $\pi^n \mathcal{O}_K$. The result follows by comparing cardinalities. □

The *Tate module* E_f of F is the torsion submodule of $F(\overline{\mathfrak{m}})$, that is,

$$E_f = \varinjlim E_f^n = \bigcup_{n=1}^{\infty} E_f^n.$$

Applying Proposition 1.9, and passing to the limit, we obtain the following characterization of E_f:

Corollary 1.10. *The Tate module E_f is isomorphic, as an $\mathcal{O}_K$-module, to $K/\mathcal{O}_K$.*

Let U_K denote the group of units of $\mathcal{O}_K$. Recall (Chapter I, Prop. 1.10) that we have isomorphisms $U_K/U_K^n \simeq (\mathcal{O}_K/\mathfrak{m}_K)^*$ for all $n \geq 1$. Hence, by Proposition 1.9, we get:

Corollary 1.11. *For each $n \geq 1$, the map $\varphi : a \mapsto [a]_f$ induces isomorphisms*

$$\mathcal{O}_K/\pi^n\mathcal{O}_K \simeq \mathrm{End}(E_f^n) \qquad \textit{and} \qquad U_K/U_K^n \simeq \mathrm{Aut}_{\mathcal{O}_K}(E_f^n).$$

Let $K_\pi^n = K(E_f^n)$, and let $K_\pi = \bigcup K_\pi^n$. This is an extension of K with Galois group $\mathrm{Gal}(K_\pi/K) = \varprojlim \mathrm{Gal}(K_\pi^n/K)$.

Proposition 1.12. *For each $n \geq 0$, the extension K_π^n/K is abelian, totally ramified, of degree $q^{n-1}(q-1)$, and its Galois group is isomorphic to U_K/U_K^n. Furthermore, if $\alpha \in E_\pi^n \backslash E_\pi^{n-1}$, then $K_\pi^n = K[\alpha]$, and α is a uniformizer.*

PROOF. As in the proof of Proposition 1.9, choose $f(X) = \pi X + X^q$. Let $\alpha \in E_f^n \backslash E_f^{n-1}$, and define $\phi_n(X) = f^{(n)}(X)/f^{(n-1)}(X)$. One readily verifies that ϕ_n is an Eisenstein polynomial of degree $q^{n-1}(q-1)$, and that $\phi_n(\alpha) = 0$. Hence $K(\alpha)/K$ is totally ramified of degree $q^{n-1}(q-1)$, and α is a uniformizer (Serre [**7**], Chap. I, §6, Prop. 17).

We have a map $\varphi : \mathrm{Gal}(K_\pi^n/K/K) \to \mathrm{Aut}(E_\pi^n)$, which maps $s \in \mathrm{Gal}(K_\pi^n/K/K)$ to its restriction $s|_{E_\pi^n}$ to E_π^n. Since K_π^n is generated by E_π^n, this map is injective. But $\mathrm{Card}(\mathrm{Gal}(K_\pi^n/K/K)) \geq [K(\alpha) : K] = \mathrm{Card}(U_K/U_K^n) = \mathrm{Card}(\mathrm{Aut}(E_\pi^n))$, the last equality following from Lemma 1.11. Thus φ is bijective and the extension K_π^n/K is abelian. Finally, $K(\alpha) \subset K(E_\pi^n)$, and $[K_\pi^n : K] = [K(\alpha) : K]$, so that $K_\pi^n = K(\alpha)$. □

Hence $\mathrm{Gal}(K_\pi/K) = \varprojlim \mathrm{Gal}(K_\pi^n/K) \simeq \varprojlim U_K/U_K^n \simeq U_K$, and consequently:

Corollary 1.13. *The extension K_π/K is abelian, totally ramified, and its Galois group is isomorphic to U_K.*

Now let $L_\pi = K^{nr}K_\pi$, where K^{nr} is the maximal unramified extension of K; since K^{nr} and K_π are linearly disjoint, we have $\mathrm{Gal}(L_\pi/K) = \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K^{nr}/K)$. Let π and ω be uniformizers of K with $\omega = u\pi$ for some unit $u \in \mathcal{O}_K^*$. Let $f \in \mathfrak{F}_\pi$ and $g \in \mathfrak{F}_\omega$, and let φ be the Frobenius automorphism of $\mathrm{Gal}(K^{nr}/K)$. Let A be the ring of integers of $\widehat{K}^{ur}$. We will need the following:

Proposition 1.14. *There exists a power series $\varphi \in A[[X]]$ with $\varphi(X) \equiv \varepsilon X$ (mod deg 2), for some $\varepsilon \in A^*$, such that*

(a) $\sigma\varphi = \varphi \circ [u]_f$;
(b) $\varphi \circ F_f = F_g \circ (\varphi \times \varphi)$;
(c) $\varphi \circ [a]_f = [a]_g \circ \varphi$ *for all* $a \in A$.

[Hence φ is an A-module isomorphism of F_f into F_g.]

Lemma 1.15. *Let A be the ring of integers of $\widehat{K}^{ur}$. The sequences*

$$0 \longrightarrow \mathcal{O}_K \longrightarrow A \xrightarrow{\sigma-1} A \longrightarrow 0$$

$$1 \longrightarrow \mathcal{O}_K^* \longrightarrow A^* \xrightarrow{\sigma/\mathrm{id}} A^* \longrightarrow 1$$

are exact.

Proof. Let B be the ring of integers of K^{nr}, and let $\mathfrak{m}_B$ be its maximal ideal. The residue field $B/\mathfrak{m}_B$ is an algebraic closure $\overline{k}$ of k. By passage to the limit, it suffices to show that the sequence

$$(*) \qquad 0 \to \mathcal{O}_K/\mathfrak{m}_K^n \to B/\mathfrak{m}_B^n \xrightarrow{\sigma-1} B/\mathfrak{m}_B^n \to 0$$

is exact. We prove it by induction. For $n = 1$, the sequence is

$$0 \to k \to \overline{k} \xrightarrow{\sigma-1} \overline{k} \to 0,$$

which is clearly exact. Now suppose that $(*)$ is exact. We may apply the snake lemma to the following diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B/\mathfrak{m}_B^n & \longrightarrow & B/\mathfrak{m}_B^{n+1} & \longrightarrow & B/\mathfrak{m}_B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \sigma-1} & & \downarrow{\scriptstyle \psi=\sigma-1} & & \downarrow{\scriptstyle \sigma-1} & & \\ 0 & \longrightarrow & B/\mathfrak{m}_B^n & \longrightarrow & B/\mathfrak{m}_B^{n+1} & \longrightarrow & B/\mathfrak{m}_B & \longrightarrow & 0. \end{array}$$

Together with the hypothesis that $(*)$ is exact, this proves that $\mathrm{Card}(\ker\psi) = q^{n+1}$. However, $\ker\psi$ contains $\mathcal{O}_K/\mathfrak{m}_K^{n+1}$, and by comparing cardinalities, this implies that $0 \to \mathcal{O}_K/\mathfrak{m}_K^{n+1} \to B/\mathfrak{m}_B^{n+1} \xrightarrow{\sigma-1} B/\mathfrak{m}_B^{n+1} \to 0$ is exact, completing the induction argument. Exactness of the second sequence follows immediately. □

Lemma 1.16. *There exists a power series $\varphi \in A[[X]]$ with $\varphi(X) \equiv \varepsilon X$ (mod deg 2), for some $\varepsilon \in A^*$, verifying condition (a) of Propositon 1.14.*

Proof. We construct φ by successive approximation. That is, we construct a sequence (a_i) of elements of A such that the polynomial $\varphi_n(X) = a_1X + a_2X^2 + \ldots + b_nX^n$ verifies condition (a), that is,

$$(*) \qquad \sigma\varphi_n = \varphi_n \circ [u]_f.$$

By Lemma 1.15, there exists $\varepsilon \in A^*$ verifying $\sigma\varepsilon = u\varepsilon$. So for $n = 1$, we choose $a_1 = \varepsilon$, and $(*)$ clearly holds. Suppose now that φ_n has been constructed. Let $b \in A$ be such that $\varphi_n \circ [u]_f - \sigma\varphi_n \equiv bX^{n+1} \pmod{\deg r+2}$, and let $c \in A$ be such that $\sigma c - c = b/(\varepsilon u)^{n+1}$. If we choose $a_{n+1} = c\varepsilon^{n+1}$, a small computation shows that φ_{n+1} verifies $(*)$. By induction, the map $\varphi(X) = \varepsilon X + a_2X^2 + \ldots + a_nX^n + \ldots$ verifies condition (a). □

Lemma 1.17. *In Lemma 1.16, we may choose φ such that $g = \sigma\varphi \circ f \circ \varphi^{-1}$.*

Proof. Let $h = \sigma\varphi \circ f \circ \varphi^{-1}$. Then $h = \varphi \circ [u]_f \circ f \circ \varphi^{-1} = \varphi \circ f \circ [u]_f \circ \varphi^{-1}$. Since f and $[u]_f$ have coefficients in $\mathcal{O}_K$, it follows that $\sigma h = \sigma\varphi \circ f \circ [u]_f \circ \sigma\varphi^{-1} = \sigma\varphi \circ f \circ \varphi^{-1} = h$. Hence $h \in \mathcal{O}_K[[X]]$. Moreover, $h \in \mathfrak{F}_\rho$, where $\rho = (\sigma\varepsilon/\varepsilon)\pi$. Recall that $[a]_{g,h}$ denotes the unique solution of $[a]_{g,h}(X) \equiv aX \pmod{\deg 2}$ and $g([a]_{g,h}(X)) = [a]_{g,h}(h(X))$. Now let $\tilde{\varphi} = [1]_{g,h}$. Then $\sigma\tilde{\varphi} \circ f \circ \sigma\tilde{\varphi} = g$, and $\tilde{\varphi}$ also verifies the conditions of Lemma 1.16. □

Proof of Proposition 1.14. Let φ be as in Lemma 1.17. Using the uniqueness part of Lemma (recall the technique used in the proof of Theorem 1.2), we have

$$\varphi \circ F_f(\varphi^{-1} \times \varphi^{-1}) = F_g \qquad \text{and} \qquad \varphi \circ [a]_f = [a]_g \circ \varphi, \ \forall\ a \in A.$$

Hence, φ verifies condions (a)-(c). □

Now let $r_\pi : K^* \to \mathrm{Gal}(L_\pi/K)$ be the homomorphism satisfying:

(i) $r_\pi(\pi)$ is the identity on K_π and the Frobenius automorphism on K^{nr}, and
(ii) If $u \in U_K$, then $r_\pi(u)$ is equal to $[u^{-1}]_f$ on K_π and the identity on K^{nr}.

Proposition 1.18. *The homomorphism r_π is independent on the choice of uniformizer π.*

Proof. Let $\omega = u\pi$ be another uniformizer (u a unit), and let $f \in \mathfrak{F}_\pi$, $g \in \mathfrak{F}_\omega$. Notice that it suffices to prove that r_π and r_ω coincide on uniformizers only, since these generate the multiplicative group K^*; i.e. we must show that $r_\pi(\omega) = r_\omega(\omega)$. Clearly $r_\pi(\omega)$ and $r_\omega(\omega)$ both induce the Frobenius automorphism on K^{nr}. Hence it suffices to prove that $r_\pi(\omega)$ is the identity on K_ω. Let $\alpha \in E_g$, and $\beta = \varphi^{-1}(\alpha)$, where φ is the map of Proposition 1.14. Set $s = r_\pi(\omega) = r_\pi(u) \cdot r_\pi(\pi)$. Since the coefficiens of φ are contained in $\widehat{K}^{nr}$, it follows by Proposition 1.14 that $s\varphi = \sigma\varphi = \varphi \circ [u]_f$. Then $s(\alpha) = s(\varphi(\beta)) = s\varphi(s(\beta)) = (\varphi \circ [c]_f \circ [u^{-1}]_f)(\mu)$ (using the defining properties of r_π on units and on π). This is readily seen to be equal to α, which completes the proof. □

The map $r_\pi : K^* \to \mathrm{Gal}(L_\pi/K)$ is called the *local reciprocity map.*

Proposition 1.19. *L_π is the maximal abelian extension K^{ab} of K.*

Proof. Let $I = \mathrm{Gal}(K^{ab}/K^{nr})$ and $I' = \mathrm{Gal}(L_\pi/K^{ur})$ be the inertia subgroups of the extensions K^{ab}/K, resp. L_π/K. Since K_π and K^{nr} are abelian and linearly disjoint, it follows by the identity $\mathrm{Gal}(L_\pi/K) = \mathrm{Gal}(K_\pi/K) \times \mathrm{Gal}(K^{nr}/K)$ that L_π is contained in K^{ab}. Consequently, we have a surjection $I \twoheadrightarrow I'$ induced by the quotient map $\mathrm{Gal}(K^{ab}/K^{nr}) \twoheadrightarrow \mathrm{Gal}(L_\pi/K^{nr})$ (Serre [**7**], Chap. I, §7, Prop. 22 applied to the tower $K^{ab}/L_\pi/K$). Since $r_\pi(U_K)$ fixes K^{nr}, we have a surjection $r_\pi : U_K \twoheadrightarrow I$. Hence we obtain a sequence of surjective maps

$$U_K \twoheadrightarrow I \twoheadrightarrow I'$$

Furthermore, U_K and I' are isomorphic by the map $u \mapsto u^{-1}$, so that the above groups are all isomorphic. In particular, $\mathrm{Gal}(K^{ab}/K^{nr}) = I \simeq I' = \mathrm{Gal}(L_\pi/K^{nr})$, and since K^{ab} and L_π both contain K^{nr}, we get $K^{ab} = L_\pi$. □

Example 1.20. Let $K = \mathbb{Q}_p$, $\pi = p$, and let $f = (1+X)^p - 1$ of Example 1.5. Then $E_f = \mu_{p^\infty}$, the group of all p^n'th roots of unity $n \geq 0$, and $K_\pi = \mathbb{Q}_p(\mu_{p^\infty})$. The maximal unramified extension of $\mathbb{Q}_p$ is the field $K^{nr} = \mathbb{Q}_p^{nr}$ generated over $\mathbb{Q}_p$ by the roots of unity of order prime to p (Serre [**7**], Chap. IV, §4). Then the compositum $L_\pi = \mathbb{Q}_p^{cycl} = \mathbb{Q}_p(\mu_{p^\infty}) \cdot \mathbb{Q}_p^{nr}$, consisting of the adjunction to $\mathbb{Q}_p$ of *all* roots of unity, is the maximal abelian extension of $\mathbb{Q}_p$.

1.4. Application: the theorem of Hasse-Arf. In Chapter I, Section 1.2, we defined, for a Galois extension L/K, a filtration $(\mathrm{Gal}(L/K)^v)$ of the Galois group $\mathrm{Gal}(L/K)$. We now consider the case when such an extension is abelian. More precisely, we prove that the gaps in the filtration only occur at integral points.

Let $L_\pi = K^{nr}K_\pi$ be the maximal abelian extension of K constructed in the previous paragraph, and let $G_\pi = \mathrm{Gal}(L_\pi/K)$ be its Galois group. Furthermore, let $r = r_\pi : K^* \to G_\pi$ be the local reciprocity map constructed in the previous paragraph.

Theorem 1.21. *For any real number $v \geq -1$, $r^{-1}((G_\pi)^v) = U_K^i$, where i is the smallest integer $\geq v$.*

Proof. We prove the theorem for the extensions K_π^n only, i.e. for $\mathrm{Gal}(K_\pi^n/K)$. Indeed, by passing to the projective limit, the theorem will be true for $\mathrm{Gal}(K_\pi/K)$, and since $G_\pi = \mathrm{Gal}(K^{nr}/K) \times \mathrm{Gal}(K_\pi/K)$, the general case will follow.

Let $G = \mathrm{Gal}(K_\pi^n/K)$, and let $r_n : K^* \to G$ be given by $u \mapsto [u^{-1}]_f$ (with f an element of $\mathfrak{F}_\pi$). Fix an integer $i \leq n$. Let $u \in U_K^i \backslash U_K^{i+1}$, and let $s = r_n(u)$. If $\alpha \in E_f^n \backslash E_f^{n-1}$, that is, if $[\pi^n]_f(\alpha) = 0$ and $[\pi^{n-1}]_f(\alpha) \neq 0$, then $s(\alpha) = [u^{-1}]_f(\alpha)$. Let $u' \in U_K$ such that $u^{-1} = 1 + \pi^i u'$. Then $s(\alpha) = [1 + \pi^i u'](\alpha) = [1]_f(\alpha) +_F [\pi^i u'](\alpha) = F_f(\alpha, \beta)$, where $\beta = [\pi^i u']_f(\alpha)$, and where F_f is the formal group law associated to f. Hence

$$s(\alpha) - \alpha = \beta + \sum_{i,j>1} a_{i,j}\alpha^i\beta^j,\ a_{i,j} \in \mathcal{O}_K.$$

Let $i(s) = v_{K_\pi^n}(s\alpha - \alpha)$. By Proposition 1.12, α and β are uniformizers for K_π^n, resp. K_π^{n-i}, and K_π^n/K_π^{n-i} is totally ramified. Furthermore, $v_{K_\pi^n}(\beta) \leq v_{K_\pi^n}(a_{i,j}\alpha^i\beta^j)$ for all i, j. Hence

$$i(s) = v_{K_\pi^n}(\beta) = [K_\pi^n : K_\pi^{n-i}] = q^i.$$

Thus, if $u \in U_K^i \backslash U_K^{i-1}$, then $i(r_n(u)) = q^i$. Equivalently (cf. Chapter I, Section 1), if $q^{i-1} - 1 \leq w \leq q^i - 1$, then $r_n^{-1}(G_w) = U_K^i$, G_w denoting the ramification group in the lower number defined in Chapter I. Let ψ be the function defined in Chapter I, Section 1.2. If $i - 1 < v \leq i$, then $q^{i-1} - 1 < \psi(v) \leq q^i - 1$, and thus $r_n^{-1}(G^v) = r_n^{-1}(G_{\psi(v)}) = U_K^i$, which completes the proof in the case of K_π^n, and thus also in the general case of L_π. □

Remark. If we drop the assumption that the residue extension k_L/k_K is separable, a weaker version can be obtained, namely that the image of U_K^i in G_π^n is *dense*; see Serre [**7**], Chap. XV, §2, Th. 2.

By Proposition 1.19, L_π is the maximal abelian extension of K, and thus we may pick any subextension of K contained in L_π and obtain:

Corollary 1.22 (Hasse-Arf)**.** *Let L/K be a finite abelian Galois extension with Galois group G. Then the gaps in the filtration (G^v) only occur for integral values of v.*

2. p-adic Hodge-Tate representations

We suppose now, and for the rest of this chapter, that K is a *local field of characteristic* 0 with residue field k of order $q > 0$. Let $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ be its absolute Galois group, equipped with the Krull topology. Let V be a finite dimensional vector space over $\mathbb{Q}_p$, and denote by $\mathrm{Aut}(V)$ the group of $\mathbb{Q}_p$-automorphisms of V. A *p-adic representation of G* is a continuous homomorphism

$$\rho : G \to \mathrm{Aut}(V).$$

Example 2.1. 1) Let μ_{p^n} denote the group of p^n'th roots of unity, and let $T_p = \varprojlim(\mu_{p^n})$ denote the group of all p-power roots of unity. Let $V_p = T_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$; it is a one-dimensional vector space over $\mathbb{Q}_p$. The group G acts on μ_{p^n}, and hence also on T_p and on V_p. This action defines a one-dimensional p-adic representation of G,

$$\chi : G \to \mathbb{Z}_p^* \subset \mathbb{Q}_p^* = \mathrm{Aut}(V_p),$$

the *cyclotomic character* of G (Chapter I, §3.2, ex. 3.12). Recall that this is the map tracking the action of G on p-power roots of unity:

$$s(x) = x^{\chi(s)}, \qquad s \in G,\ x \in \mu_{p^n},\ \text{some } n > 0.$$

2) Let E be an elliptic curve over K (or more generally, an *abelian variety*). Similarly to the case of formal groups, we let E^n denote the group of p^n-torsion points of E, and define the Tate module $T_p(E)$ as the projective limit $\varprojlim E^n$. It is a free $\mathbb{Z}_p$-module on which G acts. This action extends to $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, and the corresponding homomorphism $\rho : G \to \mathrm{Aut}(V_p)$ is a p-adic representation of G.

Let $\mathbb{C} = \widehat{\overline{\mathbb{Q}}}_p$ denote the completion of the algebraic closure of $\mathbb{Q}_p$, and let X be a finite dimensional vector space over $\mathbb{C}$ on which G acts continuously and semi-linearly (i.e. $s(cx) = s(c)s(x)$ whenever $s \in G$, $c \in \mathbb{C}$, $x \in X$). For each integer i, we define the quantities

$$\begin{aligned} X_i &= \{x \in X \mid s(x) = \chi(s)^i x \text{ for all } s \in G\}; \\ X(i) &= \mathbb{C} \otimes_K X_i. \end{aligned}$$

The action of G on $X(i)$ is given by $s(c \otimes x) = s(c) \otimes s(x)$. Let $\alpha_i : X(i) \to X$ be the $\mathbb{C}$-linear map obtained by extending the natural inclusion $X_i \hookrightarrow X$.

Proposition 2.2. *The direct sum $\alpha = \oplus_i \alpha_i : \bigoplus_i X(i) \to X$ is injective.*

Proof. For each i, let $\{e_{ij}\}_{j=0,\dots,n_i}$ be an F-basis of X_i. Suppose that α is not injective. Then there exists at least one family (c_{ij}) of elements in $\mathbb{C}$, not all zero, such that

$$\sum_i \sum_{j=0}^{n_i} c_{ij} e_{ij} = 0.$$

Among these families, choose one with fewest non-zero element, and denote the corresponding sum S. Without loss of generality, we may assume that $c_{i_0 j_0} = 1$ for some pair (i_0, j_0). If $s \in G$, then we have

$$(\chi(s)^{i_0} - s)S = \sum_i \sum_{j=0}^{n_i} (c_{ij}\chi(s)^{i_0} - s(c_{ij})\chi(s)^i)e_{ij} = 0.$$

This sum has strictly less terms that S, since the i_0'th term cancels out. By our minimality assumption, this relation must then be trivial, that is, $c_{ij}\chi(s)^{i_0} - s(c_{ij})\chi(s)^i = 0$, or equivalently, $c_{ij} = \chi(s)^{i-i_0}s(c_{ij})$. Hence, $c_{ij} \in \mathbb{C}(\chi^{i-i_0})^G$, $\mathbb{C}(\chi^{i-i_0})$ denoting $\mathbb{C}$ with the "twisted action" defined in Chapter I, §3.3. But by Theorems 3.18 and 3.19 of Chapter I, $\mathbb{C}(\chi^{i-i_0})^G = H^0(G, \mathbb{C}(\chi^{i-i_0}))$ is K when $i = i_0$, and is trivial when $i \neq i_0$, and thus S is reduced to the non-trivial relation

$$\sum_{j=1}^{n_{i_0}} c_{i_0 j} e_{i_0 j} = 0,$$

contradicting the linear independence of the basis elements $\{e_{i_0 j}\}$ of X_{i_0}. □

Proposition 2.2 allows us to identify $\bigoplus_i X(i)$ with a subspace of X. If this subspace is the whole of X, that is, if $\alpha : \oplus_i X(i) \to X$ is an isomorphism, then X is said to be of *Hodge-Tate type*. Given a p-adic representation $\rho : G \to \mathrm{Aut}(V)$, we may take

$$X = \mathbb{C} \otimes_{\mathbb{Q}_p} V$$

and let G act on X by the formula $s(c \otimes x) = s(c) \otimes \rho(s)(x)$, $s \in G, c \in \mathbb{C}, x \in X$. We then say that ρ is of *Hodge-Tate type* is X is of Hodge-Tate type.

3. Local algebraicity; Tate's Theorem

We keep the notations of Section 2, and will now be interested in the case where $\rho : G \to \mathrm{Aut}(V)$ is a p-adic *abelian* representation.

3.1. Locally algebraic representations. Let $G^{ab} = \mathrm{Gal}(K^{ab}/K)$, and suppose that $\rho : G^{ab} \to \mathrm{Aut}(V)$ is an *abelian* p-adic representation with V simple. Let I_K be the inertia subgroup of $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$; it acts on V through ρ, so that V may be viewed as an I_K-module.

Lemma 3.1. *Suppose that V is a simple I_K-module and that $\rho(I_K)$ is abelian. Then there exists a finite extension L of $\mathbb{Q}_p$, with the action of I_K given by a continuous character $\varphi : I_K \to L^*$, such that we have an isomorphism of I_K-modules*

$$V \simeq L.$$

Proof. This is a simple application of Wedderburn's Theorem. Indeed, let $R = \mathbb{Q}_p[\rho(I_K)]$, and view V as an R-module. By Schur's Lemma, since V is a simple R-module, $D = \mathrm{End}_R(V)$ is a division ring. Furthermore, V is a faithful R-module, and hence by Wedderburn's Theorem, $R \simeq M_n(D)$, for some $n \geq 1$. By assumption, R is commutative, so $n = 1$, and consequently $R \simeq D$ so $V \simeq D$ as I_K-modules. Put $L = D$. Now L is a finite extension of $\mathbb{Q}_p$, and the action of I_K on L is given by $\varphi : I_K \to \mathrm{End}_R(L) \simeq L^*$, which completes the proof. □

Let $r : K^* \to G^{ab}$ be the local reciprocity map defined in Section 1.3. As described in the proof of Proposition 1.19, r maps the units U_K of K isomorphically into the inertia subgroup I_K^{ab} of G^{ab}. Composing this map with the character $\varphi : I_K^{ab} \to L^*$ of Lemma 3.1 gives rise to a homomorphism

$$\tilde{\varphi} : U_K \xrightarrow{r|_{U_K}} I_K^{ab} \xrightarrow{\varphi} L^*.$$

Suppose that the extension L is large enough to contain all conjugates of K, and denote by Σ_K the set of embeddings $K \hookrightarrow L$. The representation ρ is said to be *locally algebraic* if there exist integers n_σ, $\sigma \in \Sigma_K$, such that

$$\tilde{\varphi}(x) = \prod_{\sigma \in \Sigma_K} \sigma(x)^{n_\sigma}$$

whenever x is sufficiently close to 1.

If V is *semi-simple*, say $V = \bigoplus_{i=1}^n V_i$, then ρ is said to be *locally algebraic* if each representation V_i is locally algebraic.

Theorem 3.2 (Tate)**.** *Let $\rho : G \to \mathrm{Aut}(V)$ be an abelian p-adic representation, such that its restriction to the inertial subgroup I_K of G is semi-simple. Then the following are equivalent:*

(i) *ρ is of Hodge-Tate type.*
(ii) *ρ is locally algebraic.*

The remaining part of this section will be devoted to the proof of this theorem.

Remark. We make the requirement that the representation be semi-simple on the inertia subgroup because Serre does. In fact, in his original definition via algebraic tori, this property is intrinsic (Serre [**6**], Chap. III, §1, Prop. 1).

3.2. Extension of the ground field. Let K' be a finte extension of an unramified extension of K, and suppose K' is contained in $\overline{\mathbb{Q}}_p$. Let $\widehat{K}'$ be the completion of K' in $\mathbb{C}$. The group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K')$ acts continuously and semi-linearly on $\mathbb{C}$. Define

$$\begin{aligned} X_i' &= \{x \in X \mid s(x) = \chi(s)^i x \text{ for all } s \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/K')\}; \\ X(i)' &= \mathbb{C} \otimes_{\widehat{K}'} X_i'. \end{aligned}$$

Theorem 3.3. *For all i, the map*

$$\widehat{K}' \otimes_K X_i \to X_i',$$

is an isomorphism of $\widehat{K}'$-modules

Proof. It suffices to prove the theorem for $i = 0$. Indeed, we recover the general case by letting G act on X by $(s, x) \mapsto \chi(s)^{-1} sx$. Now X_0, resp. X_0', is the set of elements of X invariant under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$, resp. $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K')$. Clearly the $\widehat{K}' \otimes_K X_0 \to X_0'$ is injective since, by Proposition 2.2, the map $\mathbb{C} \otimes_K X_0$ is injective. It remains to prove surjectivity. But since K' is a finite extension of an unramified extension of K, it suffices to prove it for K'/K finte, respectively unramified.

So suppose that K'/K is *finite Galois*, and let G' be its Galois group. The group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K')$ acts trivially on X_0', and hence $\mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ acts on X_0' through the finite quotient G' which acts semi-linearly on X_0'. Let $e_1, \ldots, e_n$ be a basis for X_0', viewed as a K'-vector space, and let $f : G' \to \mathrm{GL}_n(K')$ be the continuous

1-cocycle which to each $s \in G'$ associates the matrix $f(s) \in \mathrm{GL}_n(K')$ of s in this basis. Explicitely,

$$s(e_j) = \sum_{i=1}^{n} a_{ij}(s)e_i, \quad a_{ij} \in K',$$

and we set $f(s) = (a_{ij}(s))$. Notice that if we change basis, say by a base-change matrix M, the corresponding matrix of s is $\tilde{f}(s) = M^{-1}f(s)s(M)$, so that f and $\tilde{f}$ are cohomologous in $H^1(G', \mathrm{GL}_n(K'))$. Now by the non-commutative version of Hilbert's Theorem 90 (Chapter I, Th. 2.3), f is cohomologically trivial, i.e. there exists $g = (g_{ij}) \in \mathrm{GL}_n(K')$ such that $g = f(s)s(g)$ for all $s \in G'$. Now the elements $e'_j = \sum_{i=1}^{n} b_{ij}e_j$, $j = 1, \ldots, n$, form a new basis for X'_0 and are clearly invariant under G'. Hence they belong to X_0, and consequently the map $\widehat{K}' \otimes_K X_0 \to X'_0$ is surjective, completing the proof in the finite Galois case.

Suppose now that K'/K is *unramified Galois*, and again let G' be its Galois group. Let A be the ring of integers of $\widehat{K}'$, and let Λ ben an A-lattice of X'_0. The group G' acts continuously on X'_0, and hence the stabilizer in G' of Λ is open (for the Krull topology) and therefore of finite index. We may therefore form a finite sum $\Lambda^0 = \sum_s s(\Lambda)$ running over the elements of the stabilizer of Λ. This sum is then invariant under the action of G'. We now use the same argument as in the finite case. Namely, by picking a basis $e_1, \ldots, e_m$ of Λ^0, we obtain a continuous 1-cocycle $f : G \to \mathrm{GL}_m(A)$ obtained by assigning to each $s \in G$ the matrix $f(s) \in \mathrm{GL}_m(A)$ of σ in this basis. Now if we can prove that $H^1(G, \mathrm{GL}_m(A))$ is trivial, we may complete the proof in the same way as in the finite case.

Claim. $H^1(G, \mathrm{GL}_m(A)) = \{1\}$.

Proof. The idea is to pass to the quotient in order to reduce to a finite case, where Hilbert's Theorem 90 can be applied. So let π be a uniformizer for A, and define a filtation $\{R_n\}$ on the ring $R = \mathrm{GL}_m(A)$ by setting $R_n = \{x \in R \mid a \equiv 1 \pmod{\pi^n}\}$. Notice that $R/R_1 \simeq \mathrm{GL}_m(k')$, where $k' = A/(\pi)$ is the residue field of A, and that for $n \geq 1$, $R_n/R_{n+1} \simeq (M_n(k'), +)$ (the determinant can now vanish). Now G acts on A/A_1 and A_n/A_{n+1} through a finite quotient, and hence by Hilbert's Theorem 90 (Chapter I, Th. 2.3), $H^1(G, A/A_1) = H^1(G, A_n/A_{n+1}) = \{1\}$. By successive approximations, the result follows. □

This completes the proof in the finite Galois, resp. unramified Galois cases. The general case is obtained by the up-down argument. □

Now $X(i)' = \mathbb{C} \otimes_{\widehat{K}'} X'_i \simeq \mathbb{C} \otimes_{\widehat{K}'} \widehat{K}' \otimes_K X_i = \mathbb{C} \otimes_K X_i = X(i)$, and consequently:

Corollary 3.4. *The Galois modules $X(i)$ and $X'(i)$ are isomorphic. In particular, extending K to K' does not alter the Hodge-Tate property of X.*

3.3. Admissible characters. We keep the notations of the previous sections. A character $\varphi : G \to K^*$ is said to be *admissible* if there exists a non-zero element $x \in \mathbb{C}$ such that

$$\varphi(s) = s(x)/x, \quad \text{for all } s \in G.$$

If this is the case, we write $\varphi \sim 1$. We obtain an equivalence relation by writing $\varphi \sim \varphi'$ if φ/φ' is admissible. Let $\mathbb{C}(\varphi)$ denote $\mathbb{C}$ together with the "twisted" action of G given by

$$(s, x) \mapsto \varphi(s)s(x), \quad s \in G,\ x \in \mathbb{C}.$$

We denote this twisted action by s_φ. It is easy to see that

$$\varphi \sim \varphi' \iff \mathbb{C}(\varphi) \simeq \mathbb{C}(\varphi'),$$

the isomorphism being understood as an isomorphism of G-modules. Indeed, if $\lambda : \mathbb{C}(\varphi) \to \mathbb{C}(\varphi')$ is such an isomorphism, then $\varphi(s)\lambda(1) = \lambda(\varphi(s)\cdot 1) = \lambda(s_\varphi(1)) = s_{\varphi'}\lambda(1) = \varphi'(s)s(\lambda(1))$ so that $\varphi/\varphi'(s) = s(\lambda(1))/\lambda(1)$. Conversely, if $\varphi/\varphi'(s) = s(x)/x$ for all $x \in G$, then the map $\lambda : \mathbb{C}(\varphi) \to \mathbb{C}(\varphi')$ defined by $\lambda(y) = yx$ is readily seen to be an isomorphism if G-modules.

The following proposition shows that admissibility is a local property. It is a direct consequence of Theorem 3.3.

Proposition 3.5. *Suppose there exists an element $x \in \mathbb{C}^*$ such that $\varphi(s) = s(x)/x$ for all s in some open subgroup $N \subset I_K$. Then φ is admissible.*

Proof. Let K'/K be the subextension of $\overline{\mathbb{Q}}_p/K$ corresponding to $N \subset I_K = \mathrm{Gal}(K^{nr}/K)$; it is a finite extension of the maximal unramified extension of K. Let $X = \mathbb{C}(\varphi)$. As previously, let X_0, resp. X_0', be the set of elements of X fixed by G, resp. N. We have $X_0' \neq 0$ by hypothesis, so by Theorem 3.3, $X_0 \neq 0$; hence φ is admissible. □

We now define a second equivalence relation on characters $\varphi, \varphi' : G \to K^*$ by

$$\varphi \equiv \varphi' \iff \varphi|_N = \varphi'|_N \text{ for some open subset } N \text{ of } I_K.$$

Then, by picking $x = 1$ in Proposition 3.5, we obtain:

Corollary 3.6. *If $\varphi \equiv 1$, then $\varphi \sim 1$.*

3.4. The logarithm map. Let v be the valuation on $\mathbb{C}$, and let $\mathfrak{m}$, resp. U, denote the corresponding maximal ideal and unit group. The group of Teichmüller representatives can be identified with the units $\overline{k}^*$ of the residue field of $\mathbb{C}$ (cf. Serre [**7**], Chap. II, §4, Prop. 8), and we have the decomposition:

$$U = U^1 \times \overline{k}^*.$$

The logarithm map $\log : U \to \mathbb{C}$ is defined by

$$\log(x) = \begin{cases} 0 & \text{if } x \in \mu_{q-1} \\ \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(x-1)^n}{n} & \text{if } x \in U^1 \end{cases}$$

Lemma 3.7. *Let F be a finite extension of $\mathbb{Q}_p$. Let U_F, resp. $\mathfrak{m}_F$, denote the group of units of F, resp. the maximal ideal in the ring of integers of F. For n sufficiently large, we have an isomorphism*

$$\log : U_F^n \xrightarrow{\sim} \mathfrak{m}_F^n$$

with inverse exp.

Proof. Let v_p, resp. v_F, be the normalized valuation on $\mathbb{Q}_p$, resp. F, and let e_F be the ramification index of $F/\mathbb{Q}_p$. Every integer $n > 1$ has the form $n = p^a u$, where $(p, u) = 1$ and $a > 0$. Then

$$\frac{v_p(n)}{n-1} = \frac{a}{p^a u - 1} \leq \frac{a}{p^a - 1} \leq \frac{1}{p-1}.$$

Furthermore, if $x \in U_F$ and $v_F(x-1) > e_F/(p-1)$, then $v_p(x-1) > 1/(p-1)$ and hence

$$v_p\left(\frac{(x-1)^n}{x}\right) - v_p(x-1) > (n-1)\left(\frac{1}{p-1} - \frac{v_p(n)}{n-1}\right) \geq 0.$$

Hence $v_F(\log(x)) = v_F(x-1)$, and for $n > e/(p-1)$, $\log(U_F^n) \subset \mathfrak{m}_F^n$. In the same manner, one shows that $v_p((x-1)^n/n!) \geq 0$, so that $v_F(\exp(x-1)-1) = v_F(x)$, and hence that for $n > e_F/(p-1)$, $\exp(\mathfrak{m}_F^n) \subset U_F^n$. Furthermore, the standard identities of formal power series show immediately that $\log(\exp(x-1)) = x-1$ and that $\exp(\log(x)) = x$. This completes the proof. □

The map $\log : U \to \mathbb{C}$ is surjective, with kernel the group μ_∞ of all roots of unity, so we have an exact sequence

$$0 \to \mu_\infty \to U \xrightarrow{\log} \mathbb{C} \to 0,$$

which in turn gives rise to the exact sequence in cohomology,

$$H^1(G, \mu_\infty) \xrightarrow{i} H^1(G, U) \xrightarrow{\lambda} H^1(G, \mathbb{C}).$$

On the other hand, since the valuation ring of $\mathbb{C}$ is $\mathbb{Q}$, and since U by definition is the kernel of the corresponding valuation map, we get an exact sequence

$$(*) \qquad 1 \to U \to \mathbb{C}^* \to \mathbb{Q} \to 1.$$

By Theorem 3.18 of Chapter I, we have $H^0(G, \mathbb{C}^*) = K^*$. Furthermore, $\mathbb{Q} \subset \mathbb{Q}_p$, and hence G acts trivially on $\mathbb{Q}$ so that $H^0(G, \mathbb{Q}) = \mathbb{Q}$. In particular, all cocycles $f : G \to \mathbb{Q}$ are zero, and hence $H^1(G, \mathbb{Q})$ are trivial. Therefore, the long exact sequence in cohomology corresponding to $(*)$ reduces to $K^* \to \mathbb{Q} \to H^1(G, U) \to H^1(G, \mathbb{C}^*) \to 0$, or equivalently, since $v_K(K^*) = \mathbb{Z}$,

$$0 \to \mathbb{Q}/\mathbb{Z} \xrightarrow{\delta} H^1(G, U) \xrightarrow{j} H^1(G, \mathbb{C}^*) \to 0.$$

Proposition 3.8. *There is a unique injective map $L : H^1(G, \mathbb{C}^*) \to H^1(G, \mathbb{C})$ such that $L \circ j = \lambda$.*

Proof. Existence and uniqueness follows from the fact that the composition $\mathbb{Q}/\mathbb{Z} \xrightarrow{\delta} H^1(G, U) \xrightarrow{\lambda} H^1(G, \mathbb{C})$ is be zero (since $H^1(G, \mathbb{C})$ is a vector space over $\mathbb{C}$, so that the only homomorphism of $\mathbb{Q}/\mathbb{Z}$ into $H^1(G, \mathbb{C})$ must be 0). So it remains to prove injecvity of L. By combining the above sequences in cohomology, we obtain a commutative diagram

$$\begin{array}{ccccc} & & & & H^1(G, \mathbb{C}) \\ & & & \overset{\lambda}{\nearrow} & \uparrow L \\ H^1(G, \mu_\infty) & \xrightarrow{i} & H^1(G, U) & & \\ & & & \underset{j}{\searrow} & \\ & & & & H^1(G, \mathbb{C}^*). \end{array}$$

We have $0 = \lambda \circ i = L \circ j \circ i$, and hence L is injective if and only if the composition $j \circ i$ is 0. However, $\mu_\infty \subset \overline{\mathbb{Q}}_p^*$, so $j \circ i$ factors through $H^1(G, \overline{\mathbb{Q}}_p^*)$, which is zero by Hilbert's Theorem 90 (Chapter I, Cor. 2.4), and hence $j \circ i = 0$. □

Let us apply this result to characters. A continuous character $\varphi : G \to K^* \subset \mathbb{C}^*$ defines a 1-cocycle on G with values in $\mathbb{C}^*$. Let $[\varphi] \in H^1(G, \mathbb{C}^*)$ denote its cohomology class. Suppose ϕ is a cohomologically trivial cocycle in $H^1(G, \mathbb{C}^*)$,

say the constant map equal to 1 on G. Then if φ is admissible, we have $\varphi(s) = s(x)x^{-1} = s(x)\phi(x)x^{-1}$, i.e. φ and ϕ are cohomologous:

$$\varphi \sim 1 \iff [\varphi] = 0.$$

Using the fact that L is injective, we can say more:

Corollary 3.9. *The character φ is admissible if and only if $L[\varphi] = [\log \varphi]$ is trivial in $H^1(G, \mathbb{C})$.*

And since $L[\varphi^n] = nL[\varphi]$, we get:

Corollary 3.10. *If $\varphi^n \sim 1$ for some integer $n > 0$, then $\varphi \sim 1$.*

3.5. Locally trivial characters. Let F be a finite extension of $\mathbb{Q}_p$, such that K contains all conjugates of F. Let $G_F = \mathrm{Gal}(\overline{\mathbb{Q}}_p/F)$ be its absolute Galois group, and let Σ_F be the set of embeddings of F into K. Let $\varphi : G \to F^*$ be continuous character. Composition with an embedding $\sigma \in \Sigma_K$ gives rise to a new character $\sigma \circ \varphi$ of G into K^*.

Proposition 3.11. *The following statements are equivalent:*

(i) $\varphi \equiv 1$;
(ii) $\sigma \circ \varphi \sim 1$ *for all* $\sigma \in \Sigma_K$.

Proof. Let N be an open subgroup of the inertia group I_K of G. If $\varphi \mid_N = 1$, then $\sigma \circ \varphi \mid_N = 1$ for all $\sigma \in \Sigma_K$, and the implication (i) $\implies$ (ii) follows from Corollary 3.6. For the converse, notice first that φ is a continuous map on a compact group, and hence takes its values in U_K. Hence, the composition $\log \circ \varphi : G \to F$ is well-defined. Moreover I_K is closed in G since it is the preimage of $0 \in \mathrm{Gal}(\overline{k}/k)$ via the natural map $G \to \mathrm{Gal}(\overline{k}/k)$ ($\overline{k}$ and k denoting the residue fields of $\overline{\mathbb{Q}}_p$, resp. K). Since G is compact, so is I_K. Hence, $\log \circ \varphi(I_K)$ is a compact subgroup of the additive group of F (the multiplicative structure of U_F being brought to the additive one in F), and so it is isomorphic to $\mathbb{Z}_p^n$ for some $n \geq 0$. Let W be the n-dimensional $\mathbb{Q}_p$-vector subspace of L generated by $\log \circ \varphi(I_K)$; since F is quasi-compact, $\log \circ \varphi(I_K)$ is a lattice in W. Furthermore, since log is a local isomorphism by Lemma 3.7, condition (i) is equivalent to saying that $\log \circ \varphi$ is 0 on I_K. We suppose that this is not the case, i.e. that $n \geq 1$. Let

$$f : F \to K$$

be a $\mathbb{Q}_p$-linear map with $\dim f(W) = 1$. For instance, if we pick a basis of W and extend it to a basis of F, we obtain such a map by sending the first basis element to a non-zero element of K, and all remaining basis elements to 0. By linear independence of characters, (Bourbaki [**1**], Chapt. V, §10, Th. 2), Σ_F generates $\mathrm{Hom}_{\mathbb{Q}_p}(F, K)$, and hence f can be written as the sum

$$f = \sum_{\sigma \in \Sigma_K} k_\sigma \sigma, \quad k_\sigma \in K,$$

and hence $f \circ \log \circ \varphi = (\Sigma\, k_\sigma \sigma) \circ \log \circ \varphi = \Sigma\, k_\sigma \log(\sigma \circ \varphi)$. By assumption, $[\sigma \circ \varphi] = 0$ and so by Corollary 3.9, $[\log(\sigma \circ \varphi)] = 0$. Consequently, $[f \circ \log \circ \varphi] = 0$. By Lemma 3.7, we have, for n large enough and for $x \in \mathfrak{m}_K^n$,

$$\exp(\log(1 + x)) = 1 + x \quad \text{and} \quad \log(\exp(x)) = x.$$

By replacing f by $p^N f$, with N large enough, we may assume that $p^N f \circ \log(U_E) \subset \mathfrak{m}_K^n$, and hence obtain a well-defined map $g : U_E \to U_K$,

$$g(z) = \exp(f(\log(z)),$$

which satisfies $\log \circ g = f \circ \log$. Set $\psi = g \circ \varphi$. Then $f \circ \log \circ \varphi = \log(\psi)$, and by Proposition 3.9, ψ is admissible. But now $\psi(I_K)$ is the product of $\mathbb{Z}_p$ with a finite group, hence infinite, and by Proposition 3.19, $\mathbb{C}(\psi)^G = 0$. However, ψ is admissible, so $\mathbb{C}(\psi) \simeq \mathbb{C}$. Then by Theorem 3.18, $\mathbb{C}(\psi)^G = \mathbb{C}^G = K \neq 0$, hence a contradiction, as desired. □

3.6. Hodge-Tate decompositions. Let V be a one-dimensional vector space over F, and let $\rho : G \to U_F$ be a continuous homomorphism of $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ into the unit group of F. We give V the structure of a G-module by means of the action $(s, v) \mapsto \rho(s)v$, $s \in G, v \in V$. As previously, put

$$X = \mathbb{C} \otimes_{\mathbb{Q}_p} V.$$

Let $d = [F : \mathbb{Q}_p]$ denote the dimension of X over $\mathbb{C}$, and endow $\mathbb{C}$ with the semi-linear action of G. Define a representation $F \to \mathrm{End}_{\mathbb{C}}(X)$ by $z \mapsto a_z$, where a_z is the $\mathbb{C}$-endomorphism of X given by

$$a_z\left(\sum c_i \otimes v_i\right) = \sum c_i \otimes z v_i, \quad c_i \in \mathbb{C}, v_i \in V.$$

If $s \in G_L$ and $x = \sum c_i \otimes v_i \in X$, then $a_z(s(x)) = \sum s(c_i) \otimes \rho(s) z v_i = s(a_z(x))$, so the action of a_z commutes with that of G. For $\sigma \in \Sigma_F$, let

$$X_\sigma = \{x \in X \mid a_z(x) = \sigma(z)x, \text{ for all } z \in F\}.$$

This is a 1-dimensional $\mathbb{C}$-vector space, stable under the action of G; indeed, for all $s \in G$, we have $a_z(s(x)) = s(a_z(x)) = s(\sigma(z)x) = \sigma(z)s(x)$.

Lemma 3.12. *There is a natural isomorphism of G-modules*

$$X \xrightarrow{\sim} \bigoplus_{\sigma \in \Sigma_K} \mathbb{C}(\sigma \circ \rho).$$

This isomorphism maps X_σ onto $\mathbb{C}(\sigma \circ \rho)$.

Proof. Since V is a one-dimensional vector space over F, it follows that X is isomorphic to $\mathbb{C} \otimes_{\mathbb{Q}_p} F$, which in turn is isomorphic to a product $\mathbb{C} \times \ldots \times \mathbb{C}$ of d copies of $\mathbb{C}$, the projections $\mathbb{C} \otimes_{\mathbb{Q}_p} F \to \mathbb{C}$ being given by the d elements of Σ_F. Since X_σ is a one-dimensional vector space over $\mathbb{C}$, this extablishes the direct sum decomposition $X = \bigoplus_{\sigma \in \Sigma_F} X_\sigma$.

Moreover, we have an isomorphism $\mathbb{C} \otimes_{\mathbb{Q}_p} F \xrightarrow{\sim} \prod_{\sigma \in \Sigma_F} \mathbb{C}(\sigma \circ \rho)$ which sends $c \otimes v$ to $(c \cdot \sigma(v))_{\sigma \in \Sigma_F}$. This map commutes with the action of G since $s(c \otimes v) = s(c) \otimes \rho(s)v \mapsto (s(c) \cdot (\sigma \circ \rho)(s)\sigma(v))_\sigma = (\tilde{s}(c \cdot \sigma(x))_\sigma$. This completes the proof. □

3.7. The character associated to a Lubin-Tate formal group. Let π be a uniformizer of F, and for an element $f \in \mathfrak{F}_\pi$, let $F_f \in \mathcal{O}_F[[X, Y]]$, resp. E_f, be the corresponding formal group law, resp. Tate module, constructed in Section 1.3. Set $F_\pi = F(E_f)$. Denote by F^{ab}, resp. F^{nr}, the maximal abelian, resp. maximal unramified, extension of F. The residue field of F^{nr} is an algebraic closure of the residue field of F and hence $\mathrm{Gal}(F^{nr}/F)$ is isomorphic to the completion $\widehat{\mathbb{Z}}$ of $\mathbb{Z}$ (that is, the inverse limit of all finite cyclic groups), via the map $n \mapsto F^n$ (here $n \in \widehat{\mathbb{Z}}$ and F is the Frobenius element in $\mathrm{Gal}(F^{ur}/F)$). Moreover, recall (Section 1.3) that

$\mathrm{Gal}(F^{ab}/F^{nr}) \simeq U_K$. Combining with Corollary 1.13 and the remark following it, we get

$$\mathrm{Gal}(F^{ab}/F) = \mathrm{Gal}(F_\pi/F) \times \mathrm{Gal}(F^{ur}/F) \simeq U_K \times \widehat{\mathbb{Z}}.$$

Let $\mathrm{pr}_\pi : \mathrm{Gal}(F^{ab}/F) \to U_F$ be the projection onto the first factor. Also, let $\nu : G \to \mathrm{Gal}(F^{ab}/F)$ be the homomorphism on Galois groups induced by the inclusion $F \hookrightarrow K$. Finally, let $i : U_F \to U_F$ be given by $i(u) = u^{-1}$. We define the character $\chi_F : G \to U_F$ as the composition

$$(\dagger) \qquad G \xrightarrow{\nu} \mathrm{Gal}(F^{ab}/F) \xrightarrow{\mathrm{pr}_\pi} U_F \xrightarrow{i} U_F.$$

Since ν maps the inertia group I_F of G into that of $\mathrm{Gal}(F^{ab}/F)$, which in turn is isomorphic to U_F via the local reciprocity map, we get that the restriction of χ_F to I_F is given by $x \mapsto \nu(x^{-1})$.

Lemma 3.13. *We have the following:*

(a) $\chi_F \sim \chi$;
(b) *If $\sigma \in \Sigma_F$ is not the natural inclusion, then $\sigma \circ \chi_F \sim 1$.*

Proof. We only sketch the proof (see also Serre [**6**], Chap. III, §A5). Let $V = E_f \otimes_{\mathcal{O}_F} \mathbb{Q}_p$. Recall that G acts on E_f, and hence of V, through the character $\chi_F : G \to U_K$ (Section 1.3). Let $X = \mathbb{C} \otimes_{\mathbb{Q}_p} V$. Now before we proceed, we introduce a few notions. The tangent space t of F_f at the origin is, by definition, the set of $\mathcal{O}_F$-linear maps $\tau : \mathcal{O}_F[[X]] \to K$ satisfying $\tau(fg) = f(0)\tau(g) + g(0)\tau(f)$ for all $f, g \in \mathcal{O}_F[[X]]$, or, in the standard way, the set of $\mathcal{O}_F$-linear maps $I/I^2 \to F$, where $I = (X)$ denotes the augmentation ideal in $\mathcal{O}_F[[X]]$. Thus, t is a one-dimensional vector space over K. Let t' be $(d-1)$-dimensional tangent space of the dual of F_f, where again $d = [F : \mathbb{Q}_p]$. Let V_p be the one-dimensional $\mathbb{Q}_p$-vector space of Example 2.1. By a theorem of Tate ([**9**], §4, Cor. 2 to Th. 3), there is a canonical isomorphism of G-modules

$$X = X(0) \oplus X(1),$$

where, $X(0) = \mathbb{C} \otimes_K \mathrm{Hom}_F(t', K)$ and $X(1) = (\mathbb{C} \otimes_{\mathbb{Q}_p} V_p) \otimes_K t$. By construction, $\mathbb{C} \otimes \mathbb{Q}_p V_p \simeq \mathbb{C}(\chi)$, so that $X(1) \simeq \mathbb{C}(\chi) \otimes_K t$. Since t is a vector space over K, $F \subset K$ acts on t via the inclusion $\sigma_1 : F \hookrightarrow K$, and so X_{σ_1} cannot be contained in $X(0)$, hence must be equal to $X(1)$. Thus, by Lemma 3.12, $\mathbb{C}(\sigma_1 \circ \rho) \simeq \mathbb{C}(\chi) \otimes_K t$, and this can be shown to imply $\mathbb{C}(\chi_F) \simeq \mathbb{C}(\chi)$, that is, $\chi_F \sim \chi$. Using the same argument, we have, for $\sigma \neq \sigma_1$, that X_σ must be contained in $X(0)$, implying $\mathbb{C}(\sigma \circ \chi_F) \simeq \mathbb{C}(1)$ and thus $\sigma \circ \chi_F \sim 1$. □

We may now prove the following crucial theorem. For $\sigma \in \Sigma_K$, let $\chi_{\sigma F}$ be the character attached to the subfield σF of K.

Theorem 3.14. *The following statements are equivalent:*

(i) *V is of Hodge-Tate type;*
(ii) *For each $\sigma \in \Sigma_F$, there exists an integer n_σ such that*

$$\rho \equiv \prod_{\sigma \in \Sigma_F} \sigma^{-1} \circ \chi_{\sigma F}^{n_\sigma}.$$

Proof. Statement (i) is equivalent to the statement $\sigma \circ \rho \sim \chi^{n_\sigma}$ for all $\sigma \in \Sigma_F$. We will prove that the latter is equivalent to (ii). To this purpose, define a character

$\theta : G_F \to K^*$ by

$$\theta = \prod_{\sigma \in \Sigma_F} \sigma^{-1} \circ \chi_{\sigma F}^{n_\sigma}.$$

If F is replaced by σF in Lemma 3.13, we have that, if $\tau \in \Sigma_F$ is different from σ (so that $\tau \circ \sigma^{-1}$ is not the identity on σF), then $\tau \circ \sigma^{-1} \circ \chi_{\sigma F}$ is admissible. If $\tau = \sigma$, then $\tau \circ \sigma^{-1} \circ \chi_{\sigma F} \sim \chi$. These observations can be applied to the composition $\tau \circ \theta = \prod_{\sigma \in \Sigma_F} \tau \circ \sigma^{-1} \circ \chi_{\sigma F}^{n_\sigma}$, to get that $\tau \circ \theta \sim \chi^{n_\tau}$, and hence that statement (i) is equivalent to $\tau \circ \theta \sim \tau \circ \rho$ for all $\tau \in \Sigma_F$. By Proposition 3.11, this is equivalent to $\rho \equiv \theta$. □

Corollary 3.15. *The following statements are equivalent:*

(i) *V is of Hodge-Tate type;*
(ii) *V is locally algebraic.*

PROOF. Let $N_{L/K} : L^* \to K^*$ be the norm map for a finite abelian extension L/K. It is well-known (Cassels-Fröhlich [**2**], Chap. VI, §2.2, Th. 2) that $K^*/N_{L/K}L^* \simeq \mathrm{Gal}(L/K)$. Taking the projective limit over all such extensions (with respect to the norm maps), we get $\widehat{K}^* \simeq \mathrm{Gal}(K^{ab}/K)$. Similarly, $\widehat{F}^* \simeq \mathrm{Gal}(F^{ab}/F)$. Hence, the composition (†) becomes

$$\chi_F : \widehat{K}^* \xrightarrow{N_{K/F}} \widehat{F}^* \xrightarrow{\mathrm{pr}_\pi} U_F \xrightarrow{i} U_F.$$

The norm maps the inertia subgroup I_K^{ab} of $\mathrm{Gal}(K^{ab}/K)$, to that of $\mathrm{Gal}(F^{ab}/F)$, which is isomorphic to U_F via the local reciprocity map. Hence, χ_F restricted to I_K^{ab} is $x \mapsto N_{K/F}(x^{-1})$. Consider now the composition $\sigma^{-1} \circ N_{K/\sigma F} : I_K \to U_{\sigma F} \to U_F$ restricted to the inertia subgroup if $\mathrm{Gal}(K^{ab}/K)$. Since admissibility can be seen on an open subgroup of the inertia group, we then get by Theorem 3.14 that V is of Hodge-Tate type if and only if

$$\rho \equiv \prod_{\sigma \in \Sigma_F} \sigma^{-1} \circ N_{K/\sigma F}^{-n_\sigma} = \prod_{\sigma \in \Sigma_F} (\sigma^{-1}(N_{K/\sigma F}))^{-n_\sigma},$$

and this coincide with the definition of local algebraicity. □

3.8. Proof of Tate's theorem. We now go back to the case where V is a finite dimensional vector space over $\mathbb{Q}_p$ and prove Tate's theorem.

Theorem 3.16 (Tate)**.** *Let $\rho : G \to \mathrm{Aut}(V)$ be an abelian p-adic representation, such that its restriction to the inertial subgroup I_K of G is semi-simple. Then the following are equivalent:*

(i) *ρ is of Hodge-Tate type.*
(ii) *ρ is locally algebraic.*

PROOF. Replacing ρ by $\rho' = \rho \circ \mathrm{pr}_\pi$ does not affect the Hodge-Tate property (Corollary 3.4), nor the local algebraicity. Recall that pr_π maps G into the inertia subgroup, and since ρ by assumption is semi-simple on the inertia subgroup, we may assume that ρ' is semisimple. Furthermore, by the definitions of Hodge-Tate and locally algebraic representations (in terms of their direct sum decompositions), we may furthermore assume that ρ' is simple.

Now let $F \subset K$ be the commutant of the algebra $\mathrm{End}(V)$; since ρ' is simple and abelian, it follows by Shur's Lemma that V is a one-dimensional vector space over F. Let L be a finite extension of K, large enough to contain all conjugates

of F. By Corollary 3.4, passing to this extension again does not affect the Hodge-Tate property, nor does it affect local algebraicity. Hence, it suffices to prove the equivalence for the representation $\rho_L : \mathrm{Gal}(L^{ab}/L) \to \mathrm{Aut}(V)$. But this is precisely the setting of the previous section, and by Corollary 3.15, the result follows. □

3.9. Application: Imai's Theorem. It is the following:

Theorem 3.17 (Imai)**.** *Let K be a local field, and let L be the smallest field containing K and μ_{p^∞}. Let A be an abelian variety with good reduction. Then the torsion subgroup of $A(L)$ is finite.*

The proof appears in Imai [**5**]. Roughly, the idea in such a proof is to consider the Tate modules $T_p(A(L))$ and $V_p(A(L))$ and the associated p-adic representation $\rho : \mathrm{Gal}(L/K) \to \mathrm{Aut}V_p(A(L))$, as in Example 2.1 above, and obtain a Hodge-Tate decomposition of $X = \mathbb{C} \otimes_{\mathbb{Q}_p} V_p(A(L))$. Hopefully, one is able to "rule out" some of the summands, for instance by considering the Lie algebra of $\rho(\mathrm{Gal}(L/K))$ (which in this case has dimension less than that of X, and hence the Lie algebras of some of the summands are 0, and the Lie algebras of the remaining summands have a nice form). Thereby, one obtains a more and more precise structure on X, and hence on the Tate modules.

Bibliography

[1] N. Bourbaki. *Algèbre*. Ch. IV–VII, Masson, 1981.

[2] J. Cassels and A. Fröhlich. *Algebraic Number Theory*. Academic Press, 1967.

[3] J. Coates. *p-adic Hodge-Tate Theory*, Part III Lecture Notes, Michaelmas 1999.

[4] J. Coates and R. Greenberg. *Kummer Theory for Abelian Varieties over Local Fields*, pp. 129–174. Invent. Math., **124**, 1996.

[5] H. Imai. *A remark on the rational points of abelian varieties with values in cyclotomic Z_p-extensions*, pp. 12–16, Proc. Japan Acad., **51** (1975).

[6] J.-P. Serre. *Abelian ℓ-Adic Representations and Elliptic Curves*. Benjamin, 1968.

[7] J.-P. Serre. *Corps Locaux*. Hermann, 1968.

[8] J.-P. Serre. *Sur la Rationalité des Représentations d'Artin*, pp. 406–420. Ann. of Math., **72**, 1960.

[9] J. Tate. *p-Divisible Groups*. In: "Proceedings of a Conference on Local Fields (Driebergen, 1966)", pp. 158–183. Springer, 1967.