p-adic Integration

A.Iovita (notes by Cameron Franc, Marc Masdeu)

Contents

Disclaimer

These notes are from a course on Fontaine's theory of p-adic integration, taken by the authors at Concordia University in the winter of 2009, given by Adrian Iovita. We have tried our best to present a faithful account of these lectures. Be warned that despite our efforts, many errors likely persist. Please do not take this as an indication of the quality of the lectures. Any errors are most likely due to carelessness while typesetting, or the authors' misunderstanding of the material.

Introduction

A motivating question for this course is the following:

> How can one "integrate" differential forms on a p-adic algebraic variety?

Before discussing the local picture, we will consider some global examples.

Block-Kato conjectures

Let $X/\operatorname{Spec}(\mathbf{Z})$ be a scheme. Attached to X is a complex L-function $L(X,s)$. The Block-Kato conjectures relate certain special values:

$$L(X,-n)$$

for $n \in \mathbf{Z}_{>0}$ to the geometry of X, for nice enough schemes X. We discuss several examples.

Example (Riemann ζ-function)**.** Let $\zeta(s)$ be the Riemann ζ-function, which for $\Re(s) > 1$ is given by the Euler product:

$$\zeta(s) = \prod_l (1 - l^{-s})^{-1}.$$

If B_{2k} is the $(2k)$-th Bernoulli number, then the following formula is well-known:

$$\zeta(1-2k) = -\frac{B_{2k}}{2k}.$$

It turns out that in this very classical case, one has the following geometric description of these special values:

$$\zeta(1-2k) = \pm \prod_l \left(\frac{\# H^1_{\mathrm{et}}(\operatorname{Spec}(\mathbf{Z}[1/l]), (\mathbf{Q}_l/\mathbf{Z}_l)(2k))}{\# H^0_{\mathrm{et}}(\operatorname{Spec}(\mathbf{Z}[1/l]), (\mathbf{Q}_l/\mathbf{Z}_l)(2k))} \right)$$

Here $(\mathbf{Q}_l/\mathbf{Z}_l)(2k)$ denotes the $(2k)$-th cyclotomic twist of $\mathbf{Q}_l/\mathbf{Z}_l$. We have been imprecise about the sign; note that each factor in the infinite product is a multiplicative euler characteristic.

Example (Smooth, proper algebraic varieties)**.** Let $X/\mathbf{Q}$ be a smooth, proper algebraic variety. In this case the L-function of X factors as:

$$L(X,s) = \prod_{i=0}^{2\dim X} L(H^i(X), s)^{(-1)^i}.$$

(Perhaps we should define $L(H^i(X),s)$?) Let $n > i/2 + 1$ be an integer, for a fixed index $0 \le i \le 2\dim X$. Deligne has predicted a geometrix description of the values

$$L(H^i(X), n),$$

up to rational factors.

In order to explain Deligne's conjecture, we must examine some comparison isomorphisms. To begin we introduce the notations:

$$\begin{aligned}\mathbf{Q}(n) &= (2\pi i n)\mathbf{Q},\\ M_B(X) &= H^i_B(X, \mathbf{Q}(n)),\\ M_{dR}(X) &= H^i_{\mathrm{dR}}(X, \mathbf{Q}(n)),\\ \langle\sigma\rangle &= \mathrm{Gal}(\mathbf{C}/\mathbf{R}).\end{aligned}$$

Here $H^i_B(X, \mathbf{Q}(n))$ denotes classical Betti-cohomology of the complex analytic variety associated to X, with coefficients in the twisted module $\mathbf{Q}(n)$. Note that σ acts on X and on the coefficients $\mathbf{Q}(n)$; this gives an action of $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ on $M_B(X)$. Put:

$$M_B(X)^+ = M_B(X)^{\sigma=1}.$$

We will first explain the existence of a natural "complex integration" comparison isomorphism:

$$M_B(X) \otimes_{\mathbf{Q}} \mathbf{C} \simeq M_{dR}(X) \otimes_{\mathbf{Q}} \mathbf{C}.$$

This isomorphism is even σ-equivariant, where σ acts on both factors of the left side, and only on the coeffients on the right. Thanks to this equivariance, one can take σ-invariants to obtain another canonical isomorphism:

$$(M_B(X) \otimes_{\mathbf{Q}} \mathbf{C})^{\sigma=1} \simeq M_{dR}(X) \otimes_{\mathbf{Q}} \mathbf{R}.$$

In order to define the complex integration map, first note that there are canonical isomorphisms:

$$M_B(X) \otimes_{\mathbf{Q}} \mathbf{C} \simeq H^i_B(X, \mathbf{C}) \simeq H^i(X^{an}, \underline{\mathbf{C}}),$$

where $\underline{\mathbf{C}}$ denotes the $\mathbf{C}$-valued constant sheaf on the complex analytic space X^{an}, and:

$$M_{dR}(X) \otimes_{\mathbf{Q}} \mathbf{C} \simeq H^i_{dR}(X, \mathbf{C}) \simeq H^i_{dR}(X^{an}).$$

The final isomorphism above follows by GAGA. We see that it suffices to prove that these two analytic cohomologies are isomorphic. To do this, we consider the de Rham complex of sheaves on X^{an}:

$$\Omega_{X^{an}} \ : \ \mathcal{O}_{X^{an}} \longrightarrow \Omega^1_{X^{an}} \longrightarrow \Omega^2_{X^{an}} \longrightarrow \cdots$$

The fundamental result concerning this complex was known to Poincaré:

Lemma (Poincaré)**.** *The de Rham complex is exact.*

In the case that $\dim X = 1$, so that X^{an} is a Riemann surface, the de Rham complex has a single differential:

$$\mathcal{O}_{X^{an}} \longrightarrow \Omega^1_{X^{an}}.$$

If $x \in X^{an}$ is a point and t a local parameter at x, then $\mathcal{O}_{X^{an},x}$ is isomorphic to $\mathbf{C}\{\{t\}\}$, the ring of convergent power series in t. Similarly, $\Omega^1_{X^{an},x}$ is isomorphic to $\mathbf{C}\{\{t\}\}dt$. Since each such differential can formally be integrated to give a local primitive that is also convergent in the same region, one sees that the differential is surjective. This is the Poincaré lemma for curves.

In order to apply the lemma to obtain our complex integration isomorphism, we first note that:

$$\underline{\mathbf{C}} \simeq \ker(d\colon \mathcal{O}_{X^{an}} \to \Omega^1_{X^{an}});$$

this simply says that the locally constant functions are precisely the kernel of d. This simple observation gives us a map α of complexes:

$$\begin{array}{cccccccc} C^\bullet : & \underline{\mathbf{C}} & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots \\ & \downarrow & & \downarrow & & \downarrow & & \\ \Omega^\bullet_{X^{an}} : & \mathcal{O}_{X^{an}} & \longrightarrow & \Omega^1_{X^{an}} & \longrightarrow & \Omega^2_{X^{an}} & \longrightarrow & \cdots \end{array}$$

The first vertical map is the inclusion of the locally constant functions into $\mathcal{O}_{X^{an}}$, and all other vertical maps are necessarily trivial. The Poincaré lemma implies that α is a quasi-isomorphism. Recall that this means that α induces an isomorphism between the cohomologies of these two complexes. Since the complex $C^\bullet$ is mostly trivial, hypercolohomology of $C^\bullet$ is just sheaf cohomology of $\underline{\mathbf{C}}$. We thus obtain an isomorphism:

$$H^i(X^{an}, \underline{\mathbf{C}}) \simeq \mathbb{H}^i(C^\bullet) \simeq \mathbb{H}^i(\Omega^\bullet_{X^{an}}) = H^i_{dR}(X^{an}).$$

In light of our initial remarks, this establishes the complex integration isomorphism. We leave checking the σ-equivariance to the reader. The canonicity of the isomorphism follows from the fact that each isomorphism in the definition is canonical.

The slick, modern proof given above does not give any indication of why this isomorphism:

$$M_B(X) \otimes_{\mathbf{Q}} \mathbf{C} \simeq M_{dR}(X) \otimes_{\mathbf{Q}} \mathbf{C}$$

deserves to be called "complex integration". One can show that it is induced by the Poincaré pairing. Recall that:

$$M_B(X) = H^i_B(X, \mathbf{Q}(n)) = H_i(X, \mathbf{Q}(n))^\vee.$$

The Poincaré pairing is a perfect bilinear map:

$$\langle , \rangle \colon H_i(X, \mathbf{C}) \times H^i_{dR}(X, \mathbf{C}) \to \mathbf{C},$$

defined by the formula:

$$\langle \gamma, \omega \rangle = \int_\gamma \omega.$$

The explains why we call this the complex integration isomorphism.

Example. Let $X = E$ be an elliptic curve defined over $\mathbf{Q}$. Then the closed points of $E(\mathbf{C})$ can be given the structure of a complex manifold, which we denote by E^{an}. There thus exists a lattice $\Lambda \subset \mathbf{C}$ such that:

$$\iota \colon E^{an} \simeq \mathbf{C}/\Lambda.$$

Recall that $\mathbf{C}$ is the universal covering space of E^{an}, where:

$$\begin{array}{c} \mathbf{C} \\ \pi \big\downarrow \\ E^{an} \end{array}$$

is the quotient map followed by ι^{-1}. Note that Λ acts by translation on $\mathbf{C}$, and this gives a natural isomorphism:

$$\pi_1(E^{an}, 0) \simeq \Lambda.$$

Since this is abelian we obtain:

$$H_1(E^{an}, \mathbf{Z}) \simeq \pi_1(E^{an}, 0) \simeq \Lambda.$$

On the other hand, GAGA gives:

$$H^1_{dR}(E) \otimes_{\mathbf{Q}} \mathbf{C} \simeq H^1_{dR}(E^{an}) \simeq \mathbf{C}\omega \oplus \mathbf{C}\eta,$$

where ω is a holomorphic form, and η is not. For instance, if E is given by a Weierstrass equation $y^2 = 4x^3 - ax - b$, one could take $\omega = dx/y$ and $\eta = xdx/y$.

We would like to describe the complex integration isomorphism:

$$H^1_B(E, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C} \simeq H^1_{dR}(E) \otimes_{\mathbf{Q}} \mathbf{C}$$

explicitely in this case. Let $\wp$ denote the Weierstrass $\wp$-function for the lattice Λ. Then the functions $x = \wp(z)$ and $y = \wp'(z)$ give coordinates for $E(\mathbf{C})$.

Given $\gamma \in \Lambda$ and $\alpha \in H^1_{dR}(E^{an})$, how does one integrate α over γ? First, consider the pullback $\pi^*(\alpha)$ to the simply connected space $\mathbf{C}$. It has the form $d(g(z))$ where $g(z)$ is a meromorphic function on $\mathbf{C}$. The cycle on E^{an} corresponding to γ is the image under π of any path from 0 to γ in $\mathbf{C}$. We thus have:

$$\int_\gamma \alpha = \int_0^\gamma d(g(z)) = g(\gamma) - g(0).$$

Let us compute this for ω and η. The holomorphic form ω is easy to treat since:

$$\pi^*(\omega) = d(\wp(z))/\wp'(z) = dz.$$

Hence, for $\gamma \in \Lambda$,

$$\int_\gamma \omega = \gamma.$$

The nonholomorphic form η is more interesting. For this we must introduce:

$$\xi(z) = -\sum_{\lambda\in\Lambda} \frac{1}{z-\lambda}.$$

For each $\lambda \in \Lambda$ this satsfies:

$$\xi(z+\lambda) = \xi(z) + c_\lambda$$

for all $z \in \mathbf{C}$, where $c_\lambda \in \mathbf{C}$ is a constant depending on λ. Note that:

$$d(\xi(z)) = \wp(z)dz,$$

and hence:

$$\int_\gamma \eta = \xi(\gamma) - \xi(0) = c_\gamma.$$

It is now possible to state Deligne's conjecture more precisely. Suppose again that $X/\mathbf{Q}$ is a smooth projective scheme. Taking σ-invariants under the complex integration isomorphism gives an isomorphism:

$$(M_B(X) \otimes_{\mathbf{Q}} \mathbf{R})^{\sigma=1} \simeq M_{dR}(X) \otimes_{\mathbf{Q}} \mathbf{R}.$$

Since $M_B(X)^+ = M_B(X)^{\sigma=1}$, we obtain an injection:

$$M_B(X)^+ \otimes_{\mathbf{Q}} \mathbf{R} \hookrightarrow M_{dR}(X) \otimes_{\mathbf{Q}} \mathbf{R}.$$

Let:

$$M_dR(X) \to M_dR(X)/F_0$$

be the projection onto the zero-th part of the Hodge filtration. Together these maps yield:

$$\xi_\infty \colon M_B(X)^+ \otimes_{\mathbf{Q}} \mathbf{R} \to (M_{dR}(X)/F_0) \otimes_{\mathbf{Q}} \mathbf{R}.$$

Deligne defines $X/\mathbf{Q}$ to be **critical** if for $n > i/2+1$, ξ_∞ is an isomorphism. For such critical schemes, Deligne conjectured that:

$$\frac{L(H^i(X), n)}{\det(\xi_\infty)} \in \mathbf{Q}.$$

If one could define similar maps ξ_p for finite primes, one might hope that the special values of p-adic L-functions $L_p(X,n)$ are related to the values $\det(\xi_p)$. Beilinson has conjectures of this flavor.

To recapitulate, we have studied a conjecture of Deligne that relates the special values of $L(X,s)$ to the geometry of X. At the heart of the story was the complex integration comparison isomorphism. In this course we will study various comparison isomorphisms at finite primes.

In order to be more precise about the types of statements that we will prove, let us fix some notations: let $p \in \mathbf{Q}$ be a finite prime, and let $K/\mathbf{Q}_p$ be a finite extension. Fix an algebraic closure $\overline{K}$ of K. Let $\mathbf{C}_p$ denote the completion of $\overline{K}$, and let $G_K = \mathrm{Gal}(\overline{K}/K$ denote the absolute Galois group of K. Recall that since G_K acts *continuously* on $\overline{K}$, the action extends to the completion $\mathbf{C}_p$.

Let A/K be an algebraic variety. One goal of the course will be to define the period rings B_{dR} and B_{dR}^+, and prove that:

$$H^i_{\mathrm{et}}(A_{\overline{K}}, \mathbf{Q}_p) \otimes_{\mathbf{Q}_p} B_{dR} \simeq H^i_{dR}(A, K) \otimes_K B_{dR}.$$

Moreover, this isomorphism will be compatible with "extra structure".

The left hand side of this isomorphism is well-understood in the case of abelian varieties; note, however, that it is quite mysterious for general schemes! Let:

$$T_p(A) = \varprojlim A[p^n]$$

denote the Tate-module of A. It is a free $\mathbf{Z}_p$-module of rank $2\dim(A)$, endowed with a continuous action of G_K. One has:

$$H^1_{\mathrm{et}}(A_{\overline{K}}, \mathbf{Z}_p) \simeq \mathrm{Hom}_{\mathbf{Z}_p}(T_pA, \mathbf{Z}_p) = (T_p(A))^\vee$$

as G_K-modules, and similarly:

$$H^n_{\mathrm{et}}(A_{\overline{K}}, \mathbf{Z}_p) \simeq \wedge^n_{\mathbf{Z}_p} H^1_{\mathrm{et}}(A_{\overline{K}}, \mathbf{Z}_p)$$

as G_K-modules for $n \geq 2$. One of the main theorems that we will see is the Hodge-Tate comparison isomorphism:

Theorem. *With notations as above,*

$$T_p(A) \otimes_{\mathbf{Z}_p} \mathbf{C}_p \simeq \left(H^0(A, \Omega^1_A)^\vee \otimes_K \mathbf{C}_p(1)\right) \oplus \left(H^1(A, \mathcal{O}_A)^\vee \otimes_K \mathbf{C}_p\right).$$

Here $\mathbf{C}_p(1)$ denotes $\mathbf{C}_p$ with the G_K action twisted by the cyclotomic character. Moreover, this is an isomorphism as G_K-modules.

This gives:

$$T_p(A) \otimes_{\mathbf{Z}_p} \mathbf{C}_p \simeq (\mathbf{C}_p(1))^{\dim(A)} \oplus (\mathbf{C}_p)^{\dim(A)}$$

as G_K-modules. In the language to be introduced later, this says that the representation $T_p(A)$ is Hodge-Tate. A second key theorem to be proved below is the following:

Theorem. *With notations as above,*

$$T_p(A) \otimes_{\mathbf{Z}_p} B^+_{dR} \simeq H^1_{dR}(A)^\vee \otimes B^+_{dR}$$

as G_K-modules. Moreover, this isomorphism respects the natural filtrations on these spaces.

We remark that the first main theorem can be deduced from the second, since the isomorphism respects filtrations.

Chapter 1

Period rings and their Galois cohomology

1.1 Ramification in extensions of local fields

Fix a prime p. Consider the p-adic field $\mathbf{Q}_p$, and fix an algebraic closure $\overline{\mathbf{Q}}_p$. The non-archimedean valuation v on $\mathbf{Q}_p$, normalized so that $v(p) = 1$, extends in a unique way to a valuation on $\overline{\mathbf{Q}}_p$. Let $K \subseteq \overline{\mathbf{Q}}_p$ be a finite extension of $\mathbf{Q}_p$. Then K is complete and discretely valued for the restriction of v to K. Note that

$$v(K^\times) = \frac{1}{e_K}\mathbf{Z},$$

for some integer $e_K \geq 1$. The integer e_K is called the **ramification degree** of $K/\mathbf{Q}_p$. We will use the following standard notation:

$$\mathcal{O}_K \stackrel{\text{def}}{=} \{x \in K \mid v(x) \geq 0\} \supseteq \mathfrak{m}_K \stackrel{\text{def}}{=} \{x \in K \mid v(x) > 0\}.$$

Remark. The normalization for the valuation used here is different from the one in [Ser79]. We use this choice because we will consider towers of extensions.

A **uniformizer** for $K/\mathbf{Q}_p$ is an element $\pi_K \in K$ such that $v(\pi_K) = 1/e_K$. For such a uniformizer π_K we have

$$\mathfrak{m}_K = \pi_K \mathcal{O}_K,$$

so that the valuation ring $\mathcal{O}_K$ is a principal ideal domain.

With $K/\mathbf{Q}_p$ as above, let:

$$\kappa \stackrel{\text{def}}{=} \mathcal{O}_K/\mathfrak{m}_K.$$

This is a finite extension of $\mathbf{F}_p$ called the **residue field** of K. Given an extension of $\mathbf{Q}_p$ denoted by some roman numeral, the corresponding residue field will typically be denoted by the Greek equivalent. For instance, for $L/\mathbf{Q}_p$ an algebraic extension we will write $\lambda = \mathcal{O}_L/\mathfrak{m}_L$ for the residue field.

Consider another extension $K \subseteq L \subseteq \overline{K}$ with L/K finite. The valuation v on K extends again in a unique way to L, and it can be defined explicitly as

$$v(x) \stackrel{\text{def}}{=} \frac{1}{[L:K]} v(N_{L|K}(x)), \quad \text{for all } x \in L^\times.$$

Note that we have

$$\frac{1}{e_K}\mathbf{Z} = v(K^\times) \subseteq w(L^\times) = \frac{1}{e_L}\mathbf{Z} \subseteq \mathbf{Q},$$

so that we can define:

Definition 1.1.1. The **ramification index** of L over K is the integer

$$e_{L/K} \stackrel{\text{def}}{=} [w(L^\times) : v(K^\times)].$$

By definition it satisfies $e_L = e_{L/K} \cdot e_K$.

Note that $\mathfrak{m}_L \cap \mathcal{O}_K = \mathfrak{m}_K$, so that λ is a finite extension of κ.

Definition 1.1.2. The **residue degree** of L over K is the integer $f_{L/K} \stackrel{\text{def}}{=} [\lambda : \kappa]$.

The residue degree and ramification index are related by the following fundamental relation:

Proposition 1.1.3. *For $\mathbf{Q}_p \subset K \subset L \subset \overline{\mathbf{Q}}_p$ as above, with $L/\mathbf{Q}_p$ finite, the following equality holds:*

$$[L:K] = e_{L/K} \cdot f_{L/K}.$$

Proof. See [Ser79]. The idea is to construct an intelligent basis. Note that we will also prove this result below. □

Definition 1.1.4. We say that an extension L/K is **unramified** if $e_{L/K} = 1$. We say that it is **totally ramified** if $f_{L/K} = 1$.

Remark. The extension L/K being unramified is equivalent to $\mathcal{O}_L$ being étale over $\mathcal{O}_K$.

1.2 The discriminant and the different

Note that in [Ser79] the following is done for Dedekind domains (global case), whereas we will only treat the case of local fields. Note, however, that we will later apply these results to Dedekind domains.

Fix K as above, and let V be a finite dimensional K-vectorspace.

Definition 1.2.1. A subset $X \subseteq V$ is an $\mathcal{O}_K$**-lattice** if X is a finitely-generated $\mathcal{O}_K$-module which spans V over K.

Remark. As $\mathcal{O}_K$ is a PID, a lattice X is a free $\mathcal{O}_K$-module of rank equal to the K-dimension of V. Note that an $\mathcal{O}_K$-lattice is *not* a discrete subgroup of V. Multiplication by p on V is a contractive mapping, which implies that any nontrivial additive subgroup of V accumulates at 0.

Given two lattice $X_1 \subseteq X_2 \subseteq V$, the structure theory for modules over a PID gives:

$$X_2/X_1 \simeq \bigoplus_{i=1}^{t} \mathcal{O}_K/\mathfrak{m}^{n_i},$$

and we may hence define:

Definition 1.2.2. The **characteristic ideal** of X_2 with respect to X_1 is

$$\mathrm{char}_{\mathcal{O}_K}(X_2/X_1) \stackrel{\mathrm{def}}{=} \mathfrak{m}^{\sum n_i} \subseteq \mathcal{O}_K.$$

Note that given any two lattices $X_1, X_2 \subseteq V$, their intersection is also a lattice.

Definition 1.2.3. The **characteristic ideal** of two arbitrary lattices X_1 and X_2 is

$$\mathrm{char}_{\mathcal{O}_K}(X_1, X_2) \stackrel{\mathrm{def}}{=} \mathrm{char}_{\mathcal{O}_K}\left(X_1/(X_1 \cap X_2)\right) \cdot \mathrm{char}_{\mathcal{O}_K}\left(X_2/(X_1 \cap X_2)\right)^{-1} \subseteq L,$$

which is a fractional ideal of $\mathcal{O}_K$. Note that:

$$\mathrm{char}_{\mathcal{O}_K}(X_1, X_2) = \mathrm{char}_{\mathcal{O}_K}(X_2, X_1)^{-1}.$$

Let $T\colon V \times V \to K$ be a perfect bilinear pairing. The condition for T to be perfect is equivalent to requiring that the K-linear map

$$\alpha_T\colon V \to \mathrm{Hom}_K(V, K) \stackrel{\mathrm{def}}{=} V^\vee$$

which sends x to the linear form $y \mapsto T(x, y)$ is an isomorphism.

If $X \subseteq V$ is a lattice, define the **dual lattice** with respect to T:

$$X^* \stackrel{\mathrm{def}}{=} \{x \in V \mid T(x, y) \in \mathcal{O}_K \text{ for all } y \in X\}.$$

The dual lattice is an $\mathcal{O}_K$-submodule of V. In fact:

Lemma 1.2.4. *X^* is a lattice in V.*

Proof. Let $\{e_1, \ldots, e_n\}$ be an $\mathcal{O}_K$-basis for X, which is then also a K-basis for V. Let $\{e_1^\vee, \ldots, e_n^\vee\} \in V^\vee$ be the corresponding dual basis, so that $e_i^\vee(e_j) = \delta_{ij}$ is the Kronecker delta. Furthermore put $e_i^* = \alpha_T^{-1}(e_i^\vee) \in V$ and note that since α_T is an isomorphism, the e_i^*'s make up a K-basis for V.

Claim. *X^* is the free $\mathcal{O}_K$-submodule of V generated by $\{e_1^*, \ldots, e_n^*\}$.*

To prove the claim, take $y \in X$ and write:

$$y = \sum a_j e_j,$$

with $a_j \in \mathcal{O}_K$. Then:

$$T(e_i^*, y) = e_i^\vee(y) = a_i \in \mathcal{O}_K,$$

so that $e_i^* \in X^*$ for all i.

Now take $x \in X^*$ and write

$$x = \sum a_i e_i^*,$$

with $a_i \in K$. We want to conclude that $a_i \in \mathcal{O}_K$ for all i. But since $x \in X^*$, we have $T(x, e_i) \in \mathcal{O}_K$ for all i. Since $T(x, e_i) = a_i$, we obtain $a_i \in \mathcal{O}_K$ for all i. This proves the claim, and the lemma follows at once. □

Definition 1.2.5. Given a lattice $X \subseteq V$ and a perfect bilinear pairing T on V, the **discriminant** of X is

$$\delta_{X,T} \stackrel{\text{def}}{=} \operatorname{char}_{\mathcal{O}_K}(X^*, X).$$

We will apply the above theory to the case where $K \subset L \subset \overline{\mathbf{Q}}_p$ are finite extensions of $\mathbf{Q}_p$. Take $V = L$ and $X = \mathcal{O}_K$, which is a lattice. The pairing $T\colon L \times L \to K$ is defined via the trace:

$$T(x, y) \stackrel{\text{def}}{=} \operatorname{Tr}_{L|K}(x \cdot y) \in K.$$

This map is bilinear, and it is perfect because L is separable over K.

The **discriminant** of $\mathcal{O}_L$ is then

$$\delta_{L/K} \stackrel{\text{def}}{=} \operatorname{char}_{\mathcal{O}_K}(\mathcal{O}_L^*, \mathcal{O}_L).$$

It will be useful later to have an explicit description of $\mathcal{O}_L^*$:

$$\mathcal{O}_L^* = \{x \in L \mid \operatorname{Tr}_{L|K}(xy) \in \mathcal{O}_K \text{ for all } y \in \mathcal{O}_L\},$$

which is a fractional ideal of L. This description immediately shows that:

Lemma 1.2.6. *The fractional ideal $\mathcal{O}_L^*$ is the largest fractional ideal E of L such that*

$$\operatorname{Tr}_{L|K}(E) \subseteq \mathcal{O}_K.$$

Since $\mathcal{O}_L$ has the property from the lemma, it follows that $\mathcal{O}_L \subseteq \mathcal{O}_L^*$. Therefore,

$$\delta_{L/K} = \operatorname{char}_{\mathcal{O}_K}\left(\mathcal{O}_L^*/\mathcal{O}_L\right)$$

is an honest ideal of $\mathcal{O}_L$. The fact that $\mathcal{O}_L \subseteq \mathcal{O}_L^*$ also shows that our next definition is an ideal, and not simply a fractional ideal:

Definition 1.2.7. The **different** of L/K is the following ideal of $\mathcal{O}_L$:

$$\mathcal{D}_{L/K} \stackrel{\text{def}}{=} \left(\mathcal{O}_L^*\right)^{-1}.$$

Lemma 1.2.8. *In the setting above we have:*

1. $N_{L|K}(\mathcal{D}_{L/K}) = \delta_{L/K}$;
2. *If* $K \subseteq L \subseteq M$ *are all finite extensions of* $\mathbf{Q}_p$ *then*

$$\mathcal{D}_{M/K} = \mathcal{D}_{M/L} \cdot \mathcal{D}_{L/K},$$

   as ideals in $\mathcal{O}_M$;

3. *Let* $\mathfrak{a} \subseteq K$ *and* $\mathfrak{b} \subseteq L$ *be fractional ideals of* $\mathcal{O}_K$ *and* $\mathcal{O}_L$*, respectively. Then the following are equivalent:*
   (a) $\mathrm{Tr}_{L|K}(\mathfrak{b}) \subseteq \mathfrak{a}$,
   (b) $\mathfrak{b} \subseteq \mathcal{D}_{L/K}^{-1} \cdot \mathfrak{a}$.

Proof. The first two statements are left as exercise. For the third note that if $\mathfrak{a} = 0$ then the claim is trivial. So assume that $\mathfrak{a} \neq 0$. Then:

$$\begin{aligned} \mathrm{Tr}_{L|K}(\mathfrak{b}) \subseteq \mathfrak{a} \quad &\iff \quad \mathfrak{a}^{-1}\,\mathrm{Tr}_{L/K}(\mathfrak{b}) \subseteq \mathcal{O}_K \\ &\iff \quad \mathrm{Tr}_{L|K}(\mathfrak{a}^{-1}\mathfrak{b}) \subseteq \mathcal{O}_K \\ &\iff \quad \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{D}_{L/K}^{-1} \\ &\iff \quad \mathfrak{b} \subseteq \mathcal{D}_{L/K}^{-1}\mathfrak{a}. \end{aligned}$$

□

Remark. Write $\mathcal{D}_{L/K} = \mathfrak{m}_L^d$ for a positive integer d, and let $i \in \mathbf{Z}$. The third property above is equivalent to:

$$\mathrm{Tr}_{L|K}(\mathfrak{m}_L^i) = \mathfrak{m}_K^j,$$

where $j = \left\lfloor \frac{i+d}{e_{L/K}} \right\rfloor$. If we define $|\cdot| : \overline{\mathbf{Q}}_p \to \mathbf{R}$ by:

$$|x| \stackrel{\text{def}}{=} p^{-v(x)},$$

then this shows that for $x \in L$ and $e = e_{L/K}$:

$$\left|\mathrm{Tr}_{L|K}(x)\right| \leq p^{-de}\,|x|\,.$$

1.3 Computation of $\mathcal{D}_{L/K}$ for L/K finite

Consider again extensions $\mathbf{Q}_p \subseteq K \subseteq L \subseteq \overline{\mathbf{Q}}_p$ with $L/\mathbf{Q}_p$ finite. Then L/K is separable and there exists $\alpha \in L$ such that $L = K(\alpha)$. But what about $\mathcal{O}_K \subseteq \mathcal{O}_L$?

Proposition 1.3.1. *There exists* $a \in \mathcal{O}_L$ *such that* $\mathcal{O}_L = \mathcal{O}_K[a] \simeq \mathcal{O}_K[x]/(f(x))$.

Proof. We need two lemmas.

Lemma 1.3.2. *Let π be a uniformizer for $\mathcal{O}_L$, and let $x \in \mathcal{O}_L$ be such that $\lambda = \kappa(\overline{x})$, where $\overline{x}$ denotes the image of x in λ. Note that such an $\overline{x}$ exists since κ and λ are perfect. Write $e = e_{L/K}$ and $f = f_{L/K}$. Then:*

$$\{\pi^i x^j : 0 \leq i \leq e-1 \text{ and } 0 \leq j \leq f-1\}$$

is a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$. In particular, this proves that $[L : K] = ef$ as was claimed above.

Proof (of lemma). Clearly $\pi^i x^j \in \mathcal{O}_L$ for all i, j. First we show that they are linearly independent over $\mathcal{O}_K$. Suppose that

$$\sum_{i,j} a_{ij}\pi^i x^j = 0, \qquad \text{with } a_{ij} \in \mathcal{O}_K.$$

Without loss of generality suppose that at least one of the a_{ij} is a unit in $\mathcal{O}_K$. Write:

$$\sum_i \left(\sum_j a_{ij} x^j \right) \pi^i = 0.$$

Note that $v(x) = 0$ because its class in λ is nonzero, so that $v\left(\sum_j a_{ij}x^j\right) \in v(K)$ for all i. Then we have

$$v\left(\left(\sum a_{ij}x^j\right)\pi^i\right) = v(b_i) + iv(\pi), \qquad \text{where } b_i = \sum a_{ij}x^j.$$

Hence if $i_1 \neq i_2$,

$$v(b_{i_1}\pi^{i_1}) \neq v(b_{i_2}\pi^{i_2}),$$

for otherwise L would contain an element π' with $0 < v(\pi') < v(\pi)$, contradicting the choice of π as uniformizer. Thus $b_i = 0$ for all i.

But now,

$$\sum a_{ij}x^j \equiv 0 \pmod{\mathfrak{m}_L} \implies a_{ij} \in \mathfrak{m}_L$$

because $\{\overline{x}^j\}$ form a basis for λ over κ. This contradicts the fact that at least one of the a_{ij} is a unit. Thus, our candidate basis at least is linearly independent over $\mathcal{O}_K$.

It remains to show that the candidate basis generates $\mathcal{O}_L$ over $\mathcal{O}_K$. By Nakayama's lemma, it is enough to show that the images of the elements generate $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ over κ. Note that $\mathfrak{m}_K\mathcal{O}_L = \mathfrak{m}_L^e$.

We will in fact show, by induction, that the images of $\{\pi^i x^j\}_{i,j}$ generate $\mathcal{O}_L/\mathfrak{m}_L^s$ as $\mathcal{O}_K/(\mathcal{O}_K \cap \mathfrak{m}_L^s)$-modules, for all integers $s \geq 1$. For the case $s = 1$ we have:

$$\{\overline{\pi^i x^j} \mid 0 \leq i \leq e-1, 0 \leq j \leq f-1\} = \{\overline{0}, \overline{1}, \overline{x}, \ldots, \overline{x}^{f-1}\}.$$

In this case note that $\mathcal{O}_K \cap \mathfrak{m}_L = \mathfrak{m}_K$, and this is a set of generators for $\mathcal{O}_L/\mathfrak{m}_L = \lambda$ over $\mathcal{O}_K/\mathfrak{m}_K = \kappa$ by choice of x.

Now suppose that the result is true for some $s > 1$, and consider the natural exact sequence:

$$0 \longrightarrow \mathfrak{m}_L^s/\mathfrak{m}_L^{s+1} \longrightarrow \mathcal{O}_L/\mathfrak{m}_L^{s+1} \longrightarrow \mathcal{O}_L/\mathfrak{m}_L^s \longrightarrow 0.$$

Since $\mathfrak{m}_L^s/\mathfrak{m}_L^{s+1} \simeq \lambda$, the images of $\{\pi^i x^j\}_{i,j}$ in the leftmost and rightmost terms generate by induction. It follows that the images also generate the middle term as well. This concludes the proof of the first lemma. □

Lemma 1.3.3. *In the preceding lemma, $x \in \mathcal{O}_L$ may be chosen such that there is a monic polynomial $R(X) \in \mathcal{O}_K[X]$ with the property that $R(x)$ is a uniformizer of $\mathcal{O}_L$.*

Proof. Choose any $x \in \mathcal{O}_L$ such that $\lambda = \kappa(\overline{x})$. Let $\overline{R}(X) \in \kappa[X]$ be the minimal polynomial for $\overline{x}$ over κ. Choose a monic polynomial $R(X) \in \mathcal{O}_K[X]$ which lifts $\overline{R}(X)$ in the obvious sense. Write $\alpha = R(x) \in \mathcal{O}_L$. Note that:

$$\overline{\alpha} = \overline{R}(\overline{x}) = 0,$$

so that $\overline{\alpha} \in \mathfrak{m}_L$. If $v(\alpha) = 1/e_L$ then we got lucky and $\alpha = R(x)$ is a uniformizer.

Suppose instead that $v(\alpha) > 1/e_L$, so that $\alpha \in \mathfrak{m}_L^2$. Let $\pi \in \mathcal{O}_L$ be any uniformizer and consider $y = x + \pi$. Since $\overline{y} = \overline{x}$, this y also satisfies the conditions of the preceding lemma. By considering formal Taylor expansions one obtains:

$$\beta = R(y) = R(x) + R'(x)\pi + M(x)\pi^2 = R'(x)\pi + \gamma\pi^2,$$

where $R'(X)$ is the formal derivative of $R(X)$ and $M(X) \in \mathcal{O}_L[X]$, $\gamma \in \mathcal{O}_L$. We have used the fact that $R(x) = \alpha$ is divisible by π^2 to reach the last step. Note that:

$$R'(x) \pmod{\mathfrak{m}_L} = \overline{R}'(\overline{x}) \neq 0,$$

since κ finite implies $\overline{R}$ is separable. The Taylor expansion above thus shows that $\beta = R(y)$ is a uniformizer, and concludes the proof of the lemma. □

We now return to the proof of the proposition. Choose $x \in \mathcal{O}_L$ and $R(X) \in \mathcal{O}_K[X]$ as in the second lemma above, and put $\pi = R(x)$. The first lemma shows that $\{x^j R(x)^i\}_{i,j}$ is a basis for $\mathcal{O}_L/\mathcal{O}_K$. The injection:

$$\mathcal{O}_K[x] \hookrightarrow \mathcal{O}_L$$

is thus an isomorphism. □

Remark. Suppose that $K \subset L$ is totally ramified. If π is a uniformizer of L then:

$$\mathcal{O}_L = \mathcal{O}_K[\pi].$$

If the residue degree is larger than 1, then one can use the proofs of the lemmas above to find an appropriate generator $x \in \mathcal{O}_L$.

Theorem 1.3.4. *Let $\mathbf{Q}_p \subset K \subset L \subset \overline{\mathbf{Q}}_p$ extensions with L finite over $\mathbf{Q}_p$. Let $x \in \mathcal{O}_L$ be such that $\mathcal{O}_L = \mathcal{O}_K[x]$, and let $f(X) \in K[X]$ be the characteristic polynomial of x over K. Then f is a monic polynomial in $\mathcal{O}_K[X]$ and:*

$$\mathcal{D}_{L/K} = f'(x)\mathcal{O}_L.$$

Proof. The proof of the first claim is rather elementary. Recall that the coefficients of $f(X)$ are symmetric functions in the conjugates of x. They are hence integral over $\mathcal{O}_K$. Since $\mathcal{O}_K$ is integrally closed in K, it follows that $f(X) \in \mathcal{O}_K[X]$. That $f(X)$ is monic is part of the definition of the irreducible polynomial.

We turn now to the proof of the second claim of the theorem. Note that the first claim at least proves that $f'(x) \in \mathcal{O}_L$. Recall that:

$$\mathcal{D}_{L/K}^{-1} = \mathcal{O}_L^* = \{a \in L \mid \mathrm{Tr}_{L/K}(ab) \in \mathcal{O}_K \text{ for all } b \in \mathcal{O}_L\}.$$

We begin with a lemma:

Lemma 1.3.5. *With $n = [L : K] = \deg f$, the elements:*

$$\left\{ \frac{x^i}{f'(x)} \mid 0 \leq i \leq n-1 \right\}$$

make up a basis for $\mathcal{D}_{L/K}^{-1}$ over $\mathcal{O}_K$.

Proof of lemma. By assumption $\{1, x, x^2, \ldots, x^{n-1}\}$ is a basis for $\mathcal{O}_L/\mathcal{O}_K$. This already shows that the elements in question are linearly independent over $\mathcal{O}_K$. We claim that to prove the lemma, it suffices to show that the $(n \times n)$-matrix:

$$T = \left(\mathrm{Tr}_{L/K}(x^i x^j / f'(x))\right)$$

is in $\mathrm{GL}_n(\mathcal{O}_K)$.

A priory T is just an $(n \times n)$-matrix with entries in K. If the coefficients of T are in $\mathcal{O}_K$, then it follows from the definition of $\mathcal{D}_{L/K}^{-1}$, and the fact that the powers x^i are an integral basis for $\mathcal{O}_L$, that each $x^j/f'(x)$ is contained in $\mathcal{D}_{L/K}^{-1}$. Now suppose that T is moreover invertible. It remains to show that the $x^j/f'(x)$ span $\mathcal{D}_{L/K}^{-1}$. Let $y \in \mathcal{D}_{L/K}^{-1}$, so that each trace $\mathrm{Tr}_{L/K}(x^i y)$ is an element of $\mathcal{O}_K$. It thus follows from the invertibility of T that we can define elements $\alpha_0, \ldots, \alpha_{n-1} \in \mathcal{O}_K$ by the formula:

$$\begin{pmatrix} \mathrm{Tr}_{L/K}(y) \\ \mathrm{Tr}_{L/K}(xy) \\ \vdots \\ \mathrm{Tr}_{L/K}(x^{n-1}y) \end{pmatrix} = T \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{pmatrix}.$$

This formula says precisely that y and

$$\sum_{j=0}^{n-1} \alpha_j x^j / f'(x)$$

take the same value upon pairing with each x^i. As the x^i are linearly independent over K, it follows from the nondegeneracy of the trace pairing that $y = \sum_j \alpha_j x^j / f'(x)$. Since the α_j's are contained in $\mathcal{O}_K$, this shows that the $x^j/f'(x)$ span $\mathcal{D}_{L/K}^{-1}$ if $T \in \mathrm{GL}_n(\mathcal{O}_K)$.

It thus remains to prove that $T \in \mathrm{GL}_n(\mathcal{O}_K)$. To begin we will show that:

$$\mathrm{Tr}_{L/K}(x^s/f'(x)) = 0$$

if $0 \leq s \leq n-2$, and

$$\mathrm{Tr}_{L/K}(x^{n-1}/f'(x)) = 1.$$

Let $x_1 = x, x_2, \ldots, x_n \in \overline{\mathbf{Q}}_p$ be the distinct conjugates of x over K. We want to compute:

$$\mathrm{Tr}_{L/K}(x^s/f'(x)) = \sum_{k=1}^{n} \frac{x_k^s}{f'(x_k)}.$$

Consider the partial fraction decomposition of $1/f(X)$:

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

for some $\alpha_k \in \overline{\mathbf{Q}}_p$. For each k this gives an equation:

$$1 = \alpha_k \prod_{i \neq k} (X - x_i) + (X - x_k)\left(\text{polynomial in } \overline{\mathbf{Q}}_p[X]\right).$$

Evaluating at x_k gives the expression:

$$1 = \alpha_k f'(x_k),$$

so that:

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

Consider the field of rational functions $K(X)$, which we regard as the function field of $\mathbf{P}^1_K$. The point $\infty \in \mathbf{P}^1_K$ corresponds to a valuation v_∞ of $K(X)$ with uniformizer $1/X$. There is an injection:

$$K(X) \hookrightarrow \mathrm{Frac}\left(\widehat{\mathcal{O}_{\mathbf{P}^1_{K,\infty}}}\right) = K((1/X)),$$

where $K((1/X)) = \mathrm{Frac}(K[[1/X]])$ is the field of formal Laurent series in $1/X$ over K. Write:

$$f(X) = x^n + a_1 x^{n-1} + \cdots + a_n.$$

Then:

$$\begin{aligned}\frac{1}{f(X)} &= \frac{1}{X^n(1+a_1(1/X)+\cdots+a_nX^{n-1})}\\ &= \frac{1}{X^n}\left(\frac{1}{1+(1/X)(a_1+a_2(1/X)+\cdots+a_n(1/X)^{n-1})}\right)\\ &= \frac{1}{X^n}\left(\sum_{u=0}(-1)^u(a_1/x+a_2/x^2+\cdots+a_nx^n)^u\right).\end{aligned}$$

We can expand $1/f(X)$ at infinity in a second way:

$$\begin{aligned}\frac{1}{f(X)} &= \sum_{k=1}^{n}\frac{1}{f'(x_k)(X-x_k)}\\ &= \frac{1}{X}\left(\sum_{k=1}^{n}\frac{1}{f'(x_k)(1-x_k/X)}\right)\\ &= \frac{1}{X}\left(\sum_{k=1}^{n}\sum_{t=0}^{\infty}x_k^t(1/X)^t\right)\\ &= \frac{1}{X}\left(\sum_{t=0}^{\infty}\left(\sum_{k=1}^{n}x_k^t\right)(1/X)^t\right).\end{aligned}$$

Now we compare coefficients in both expansions of $1/f(X)$ above. Both expansions have zero constant term. Comparing coefficients of the terms $(1/X)^r$ for $1 \le r \le n-1$ gives:

$$0 = \sum_{k=1}^{n}\frac{x_k^{r-1}}{f'(x_k)} = \mathrm{Tr}_{L/K}(x^{r-1}/f'(x)).$$

Similarly comparing the $(1/X)^n$ terms gives:

$$1 = \mathrm{Tr}_{L/K}(x^{n-1}/f'(x)).$$

Now to prove that:

$$T = (t_{i,j}) = \big(\mathrm{Tr}_{L/K}(x^ix^j/f'(x)\big)$$

lives in $\mathrm{GL}_n(\mathcal{O}_K)$, we first note that the calculation above shows that T is zero above the anti-diagonal, and the anti-diagonal entries all equal 1. This shows, at least, that T is invertible. To treat the entries below the anti-diagonal, note that:

$$x^n = -(a_1x^{n-1}+\cdots+a_n).$$

By induction and linearity of $\mathrm{Tr}_{L/K}$, we deduce that the remaining entries of T lie in $\mathcal{O}_K$. Thus $T \in \mathrm{GL}_n(\mathcal{O}_K)$, and this concludes the proof of the lemma. Here is how the matrix of T looks like:

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & \\ \vdots & \vdots & & & \\ 0 & 1 & & * & \\ 1 & & & & \end{pmatrix}$$

□

We now return to the proof of the second claim of the theorem. Since $\{x^i/f'(x)\}_i$ is a basis for $\mathcal{D}_{L/K}^{-1}$ we deduce that $\{x^i\}_i$ is a basis for $f'(x)\mathcal{D}_{L/K}^{-1}$. But since $\{x^i\}_i$ is a basis for $\mathcal{O}_L$ this gives:

$$\mathcal{O}_L = f'(x)\mathcal{D}_{L/K}^{-1}.$$

Hence also $\mathcal{D}_{L/K} = f'(x)\mathcal{O}_L$. This concludes the proof of the theorem. □

The preceding theorem has the following differential interpretation. If:

$$\mathcal{O}_L = \mathcal{O}_K[x] \simeq \mathcal{O}_K[X]/(f(X))$$

as above, then one can show that:

$$\Omega_{\mathcal{O}_L/\mathcal{O}_K} \simeq (\mathcal{O}_L/f'(X)\mathcal{O}_L)dX,$$

where $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ denotes the $\mathcal{O}_K$-module of Kähler differentials. We thus see that:

$$\mathrm{Ann}_{\mathcal{O}_L}(\Omega_{\mathcal{O}_L/\mathcal{O}_K}) = f'(x)\mathcal{O}_L = \mathcal{D}_{L/K}.$$

Example. Consider the case of $\overline{\mathbf{Q}}_p$ instead of finite extensions L, K. One can consider:

$$\mathcal{O} = \ker\left(\mathcal{O}_{\overline{\mathbf{Q}}_p} \longrightarrow \Omega_{\mathcal{O}_{\overline{\mathbf{Q}}_p}/\mathcal{O}_{\mathbf{Q}_p^{un}}}\right),$$

which is a subring of $\mathcal{O}_{\overline{\mathbf{Q}}_p}$. The p-adic completion of $\mathcal{O}$ maps into $\mathcal{O}_{\mathbf{C}_p}$:

$$\widehat{\mathcal{O}} \to \mathcal{O}_{\mathbf{C}_p}.$$

It turns out that this ring has the curious property that:

$$\widehat{\mathcal{O}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \simeq B_{dR}^+/I^2$$

is a quotient of the deRham period ring B_{dR}^+. We will discuss B_{dR}^+ and the connection with differentials of $\mathcal{O}_{\overline{\mathbf{Q}}_p}$ later in the course.

Consider now the case of a tower of finite extensions

$$\mathbf{Q}_p \subseteq K \subseteq L \subseteq M \subseteq \overline{\mathbf{Q}}_p, \quad [M : \mathbf{Q}_p] < \infty.$$

Proposition 1.3.6. *The canonical sequence of $\mathcal{O}_M$-modules*

$$0 \to \mathcal{O}_M \otimes_{\mathcal{O}_L} \Omega_{\mathcal{O}_L/\mathcal{O}_K} \to \Omega_{\mathcal{O}_M/\mathcal{O}_K} \to \Omega_{\mathcal{O}_M/\mathcal{O}_L} \to 0$$

is exact.

Proof. It is enough to show that the first map is injective (see [Har77], section II.8). That will say that $\mathcal{O}_M$ is smooth as an $\mathcal{O}_L$-module. This will be proved later; the reader can check that the eventual proof is independent of the intermediate material. □

Remark. The results of this section assume that K is a complete DVR with finite residue field, and that L/K is a finite extension. They are also true, and the same proof works, if K is replaced by a complete DVR with *perfect* residue field.

In the case that the residue field of K is non-perfect but has a finite p-basis (that means that $[\kappa : \kappa^p] < \infty$), then the previous proposition still holds, but the result about the annihilator will not be true in general. In that case one can show that $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ is of finite length and:

$$\text{length}_{\mathcal{O}_L}\left(\Omega_{\mathcal{O}_L/\mathcal{O}_K}\right) = \text{length}_{\mathcal{O}_L}\left(\mathcal{O}_L/\mathcal{D}_{L/K}\right).$$

1.4 Ramification in $\mathbf{Z}_p$-towers

Let $K/\mathbf{Q}_p$ be a finite extension contained in $\overline{\mathbf{Q}}_p$.

Definition 1.4.1. A **$\mathbf{Z}_p$-extension** of K is a sequence of fields $\{K_n\}_{n\geq 0}$ satisfying:

1. $K_0 = K$ and $K_n \subseteq K_{n+1}$ for all $n \geq 0$, and
2. K_n is Galois over K with $\text{Gal}(K_n/K) \simeq \mathbf{Z}/p^n\mathbf{Z}$.

Example. Fix a compatible sequence of primitive p^nth roots of unity $\{\zeta_{p^n}\}_{n\geq 0} \subset \overline{\mathbf{Q}}_p$. That is, choose primitive p^nth roots of unity ζ_{p^n} such that:

$$(\zeta_{p^{n+1}})^p = \zeta_{p^n}, \quad \text{for all } n \geq 0.$$

Let then $K = \mathbf{Q}_p(\zeta_p)$ and let $K_n = \mathbf{Q}_p(\zeta_{p^{n+1}})$. The sequence $\{K_n\}_{n\geq 0}$ is a $\mathbf{Z}_p$-extension.

In general, suppose that $\{K_n\}_{n\geq 0}$ is a $\mathbf{Z}_p$-extension. Let:

$$K_\infty \stackrel{\text{def}}{=} \bigcup_{n\geq 0} K_n,$$

which is a field since $K_n \subseteq K_{n+1}$ for all n. So we have $K \subseteq K_\infty \subseteq \overline{\mathbf{Q}}_p$, and moreover K_∞ is Galois over K with

$$\text{Gal}(K_\infty/K) = \varprojlim_n \mathbf{Z}/p^n\mathbf{Z} \simeq \mathbf{Z}_p.$$

In fact, this last condition characterizes $\mathbf{Z}_p$-extensions and explains the choice of terminology:

Proposition 1.4.2. *The following two sets of data are equivalent:*

1. *A $\mathbf{Z}_p$-extension over K, say $\{K_n\}_{n\geq 0}$.*
2. *A Galois extension K_∞ of K such that* $\mathrm{Gal}(K_\infty/K) \simeq \mathbf{Z}_p$.

Proof. □

Remark. We will typically work with $\mathbf{Z}_p$-extensions such that K_∞/K is totally ramified. In such cases the field K_∞ is "very strange". To explain we note that one has:

$$\mathfrak{m}_{K_n} \subset \mathfrak{m}_{K_\infty},$$

for all n. Thus if π_n is a uniformizer for K_n then we deduce that:

$$v(\pi_n) = \frac{1}{e_{K_n/\mathbf{Q}_p}} = \frac{1}{p^n e_{K/\mathbf{Q}_p}},$$

which tends to zero from above as n tends to infinity. Hence K_∞ contains elements of arbitrarily small positive valuation, and this fact implies the following three unfamiliar properties:

1. The maximal ideal $\mathfrak{m}_{K_\infty}$ is not finitely generated, since the valuation on K_∞ is not discrete.
2. The maximal ideal is idempotent: $\mathfrak{m}_{K_\infty}^2 = \mathfrak{m}_{K_\infty}$.
3. One has $\mathfrak{m}_{K_\infty}\mathcal{O}_{\overline{K}} = \mathfrak{m}_{\overline{K}}$.

Also, note that since K_∞/K is an infinite extension, K_∞ is not complete with respect to the natural valuation.

Example. We can obtain $\mathbf{Z}_p$ towers over any finite extension K of $\mathbf{Q}_p$ as follows. With the ζ_{p^n}'s as above, let

$$L \stackrel{\text{def}}{=} K(\zeta_p, \zeta_{p^2}, \ldots \zeta_{p^n}, \ldots).$$

Then L/K is a Galois extension, and we would like to understand $\mathrm{Gal}(L/K)$. Let:

$$F = \mathbf{Q}_p(\zeta_p, \zeta_{p^2}, \ldots \zeta_{p^n}, \ldots),$$

so that:

$$\mathrm{Gal}(F/\mathbf{Q}_p) \simeq \mathbf{Z}_p^\times \simeq (\mathbf{Z}/(p-1)\mathbf{Z}) \times \mathbf{Z}_p.$$

Restriction of automorphisms $\sigma \in \mathrm{Gal}(L/K)$ to $\sigma|_F \in \mathrm{Gal}(F/\mathbf{Q}_p)$ gives an injective continuous map:

$$\mathrm{Gal}(L/K) \hookrightarrow \mathbf{Z}_p^\times.$$

Since $\mathrm{Gal}(L/K)$ is compact and $\mathbf{Z}_p^\times$ is Hausdorff, the image is a closed subgroup of $\mathbf{Z}_p^\times$. From his one can show that there is a finite group Δ with:

$$\mathrm{Gal}(L/K) \simeq \Delta \times \mathbf{Z}_p.$$

Then $K_\infty = L^\Delta$, the fixed field of Δ, is a $\mathbf{Z}_p$-extension over K.

Theorem 1.4.3 (Tate, 1967). *Let K be a finite extension of $\mathbf{Q}_p$, or a finite extension of M^{ur}, where M is a finite extension of $\mathbf{Q}_p$. Let $\{K_n\}_{n\geq 0}$ be a $\mathbf{Z}_p$-tower such that K_n is totally ramified over K, for all n. Then the function $d_n \overset{def}{=} v(\mathcal{D}_{K_n/K})$ satisfies:*

$$d_n = c_0 + n + a_n p^{-n}, \qquad \textit{for all } n.$$

In particular, $d_n \to \infty$ when $n \to \infty$.

Remark. Such a tower is an example of a **deeply ramified** extension of K. We will see more on this later.

Proof. We only prove the theorem for the case that we will study later. The proof of the general statement uses higher ramification groups.

Let $K = \mathbf{Q}_p(\zeta_p)$, let $K_n = \mathbf{Q}_p(\zeta_{p^{n+1}})$ and set $d_n = v(\mathcal{D}_{K_n/K})$. Since $\mathcal{D}_{K_n/\mathbf{Q}_p} = \mathcal{D}_{K_n/K} \cdot \mathcal{D}_{K/\mathbf{Q}_p}$:

$$d_n = v(\mathcal{D}_{K_n/\mathbf{Q}_p}) - v(\mathcal{D}_{K/\mathbf{Q}_p}),$$

and so it will suffice to prove that $v(\mathcal{D}_{K_n/\mathbf{Q}_p})$ is of the form in the theorem.

The extension $K_n/\mathbf{Q}_p$ is totally ramified, so that $\mathcal{O}_{K_n} = \mathbf{Z}_p[\pi_n]$ with $\pi_n = \zeta_{p^{n+1}} - 1$. Let $f(X)$ be the irreducible polynomial of π_n over $\mathbf{Q}_p$:

$$f(X) = \frac{(X+1)^{p^{n+1}} - 1}{(X+1)^{p^n} - 1} = \phi_{p^{n+1}}(X+1)$$

.

Then by previous work, $v(\mathcal{D}_{K_n/\mathbf{Q}_p}) = v\left(f'(\pi_n)\right)$. Computing the formal derivative of $f(X)$ and evaluating at π_n gives:

$$f'(\pi_n) = p^{n+1}\zeta_p(\zeta_p - 1)^{-1},$$

so that $v(f'(\pi_n)) = 1 - \frac{1}{p-1} + n$, which proves the theorem in this case. □

Remark. In our example, the constant c_0 of the theorem is

$$c_0 = 1 - \frac{1}{p-1} - v(\mathcal{D}_{K/\mathbf{Q}_p}),$$

and the a_n are all 0. This is not what happens in general, of course. The fact that K contained a pth root of unity made this computation much easier.

Corollary 1.4.4. *Let K be a finite extension of $\mathbf{Q}_p$, and let $L = K_\infty$ be a totally ramified $\mathbf{Z}_p$-extension. Then there is a positive constant a such that for all n and $x \in K_{n+1}$,*

$$|\operatorname{Tr}_{K_{n+1}/K_n}(x)| \leq |p|^{1-ap^{-n}}|x|.$$

Proof. To be added later.[1] □

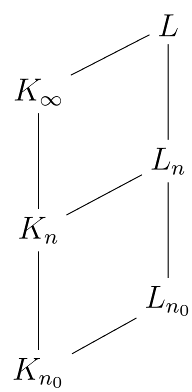
[1] **FIXME:** Add proof

Again, fix $K/\mathbf{Q}_p$ finite and let K_∞ be a totally ramified $\mathbf{Z}_p$-extension of K. Let L be a finite extension of K_∞. Later we will prove that L is unramified over K_∞, that is:

$$\Omega_{\mathcal{O}_L/\mathcal{O}_{K_\infty}} = 0.$$

For now we content ourselves with a weaker form of this fact. Use the primitive element theorem to write $L = K_\infty[x]$ for some $x \in L$. Let $f(X)$ be the irreducible polynomial of x over K_∞. Then there exists some n_0 such that $f(X) \in K_{n_0}[X]$, and $f(X)$ is obviously irreducible in $K_{n_0}[X]$.

Let $L_{n_0} = K_{n_0}[x]$ and let $L_n = L_{n_0} \cdot K_n$ be the composite field. We have a lattice:



Note that $L_n \subseteq L_{n+1}$ for all $n \geq 0$, that $L = \cup_{n \geq 1} L_n$, and that for $n \geq n_0$ one has $L_n \cap K_{n+1} = K_n$.

Remark. We will use the convention, found commonly in the literature, that if $M/\mathbf{Q}_p$ is a finite extension and $\alpha \in v(M^\times)$, we denote by p^α *any* element of $M^\times$ such that $v(p^\alpha) = \alpha$. Note that the element p^α is not well-defined, but the ideal $p^\alpha \mathcal{O}_M$ is.

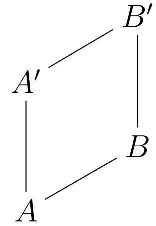
Theorem 1.4.5 (Tate)**.**

1. *Let* $\delta_n \overset{def}{=} v(\mathcal{D}_{L_n/K_n})$. *Then* $\delta_n \to 0$ *when* $n \to \infty$.
2. *The maximal ideal* $\mathfrak{m}_{K_\infty}$ *is contained in* $\mathrm{Tr}_{L/K_\infty}(\mathcal{O}_L)$.

Proof. We first need to study the modules of differentials. To lighten the notation, we set

$$A = \mathcal{O}_{K_n}, \quad A' = \mathcal{O}_{K_{n+1}}, \quad B = \mathcal{O}_{L_n}, \quad B' = \mathcal{O}_{L_{n+1}},$$

so that we have a diagram of ring extensions:



Consider the two exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Omega_{B/A} \otimes_B B' & \xrightarrow{\alpha} & \Omega_{B'/A} & \longrightarrow & \Omega_{B'/B} & \longrightarrow & 0\ , \\ & & & & \| & & & & \\ 0 & \longrightarrow & \Omega_{A'/A} \otimes_{A'} B' & \longrightarrow & \Omega_{B'/A} & \xrightarrow{\beta} & \Omega_{B'/A'} & \longrightarrow & 0 \end{array}$$

then we define a map

$$\gamma\colon \Omega_{B/A} \otimes_B B' \to \Omega_{B'/A'},$$

as $\gamma \stackrel{\text{def}}{=} \beta \circ \alpha$.

As $\Omega_{B/A} \simeq B/p^{\delta_n} B$ and B' is free over B (in particular, it is flat), we get

$$\Omega_{B/A} \otimes_B B' \simeq B'/p^{\delta_n} B'.$$

Similarly, we have

$$\Omega_{B'/A'} \simeq B'/p^{\delta_{n+1}} B'.$$

Let then

$$d_n \stackrel{\text{def}}{=} v(\mathcal{D}_{K_{n+1}/K_n}).$$

We want to compute the kernel of the map γ. The map α is injective, and by definition of β, we have

$$\ker \beta = \Omega_{A'/A} \otimes_{A'} B' \simeq A'/p^{d_n} A' \otimes_{A'} B' \simeq B'/p^{d_n} B',$$

so that

$$\ker \gamma = \alpha^{-1}(\ker \beta) \supseteq B'/p^{\min(d_n, \delta_n)} B'.$$

Similarly,

$$\operatorname{coker} \gamma \simeq$$

Similarly, we can prove that[2]

$$p^{\delta_n - \delta_{n+1}} \cdot \operatorname{coker}(\gamma) = 0.$$

Consider then the exact sequence

$$0 \to \ker \gamma \to B'/p^{\delta_n} B' \xrightarrow{\gamma} B'/p^{\delta_{n+1}} B' \to \operatorname{coker} \gamma \to 0,$$

which yields, by taking B'/pB'-ranks:

$$\delta_n - \delta_{n+1} \geq \min(d_n, \delta_n) - (\delta_n - \delta_{n+1}).$$

From the equality $\mathcal{D}_{K_{n+1}}/K = \mathcal{D}_{K_{n+1}/K_n} \cdot \mathcal{D}_{K_n/K}$, we get

$$d_n = v(\mathcal{D}_{K_{n+1}/K_n}) = v(\mathcal{D}_{K_{n+1}/K}) - v(\mathcal{D}_{K_n/K}) = n + 1 + c_0 + a_{n+1} p^{-n} - n - c_0 - a_n p^{-n},$$

[2] **FIXME:** Add the proof later!

so that $d_n = 1+b_n p^{-n}$ with $b_n = a_{n+1}/p - a_n$, which is a sequence bounded with respect to n. Hence we get:

$$0 \leq \delta_{n+1} \leq \delta_n - \frac{1}{2}\min(d_n, \delta_n),$$

and hence eventually $\delta_{n+1} \leq \delta_n/2$, yielding $\delta_n \to 0$ with n. This concludes the proof of the first claim.

We turn now to the second claim, namely proving that:

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

First one notes that for every $n \geq n_0$:

$$\mathrm{Tr}_{F_n/K_n}(\mathcal{O}_{F_n}) \subset \mathrm{Tr}_{L/K_\infty}(\mathcal{O}_L).$$

Next recall the following consequence of lemma 1.2.8: we have

$$\mathrm{Tr}_{F_n/K_n}(\mathcal{O}_{F_n}) = \mathfrak{m}_{K_n}^j$$

where:

$$j = \left[\frac{b_n}{e_{F_n/K_n}}\right],$$

and b_n is defined by the relation:

$$\mathcal{D}_{F_n/K_n} = \mathfrak{m}_{F_n}^{b_n}.$$

In other words,

$$b_n = \frac{v(\mathcal{D}_{F_n/K_n})}{v(\pi_{F_n})} = \frac{\delta_n e_{F_n/K_n}}{v(\pi_{K_n})}.$$

Thus, we have:

$$\pi_{K_n}^j \in \mathrm{Tr}_{F_n/K_n}(\mathcal{O}_{F_n}) \subset \mathrm{Tr}_{L/K_\infty}(\mathcal{O}_L),$$

and we can compute the valuation:

$$\begin{aligned} v(\pi_{K_n^j}) &= j v(\pi_{K_n}) \\ &= \left[\frac{b_n}{e_{F_n/K_n}}\right] v(\pi_{K_n}) \\ &\leq \left(\frac{\delta_n e_{F_n/K_n}}{v(\pi_{K_n}) e_{F_n/K_n}}\right) v(\pi_{K_n}) \\ &= \delta_n. \end{aligned}$$

Since the δ_n's go to zero as n tends to infinity, we see that $\mathrm{Tr}_{L/K_\infty}(\mathcal{O}_L)$ contains elements of arbitrarily small but positive valuation. Thus:

$$\mathfrak{m}_{K_\infty} \subset \mathrm{Tr}_{L/K_\infty}(\mathcal{O}_L)$$

as claimed. □

1.5 Calculus of algebraic integers

In this section we fix $\mathbf{Q}_p \subset M \subset \overline{\mathbf{Q}}_p$ with $[M\colon \mathbf{Q}_p] < \infty$. Let $K = M^{ur}$ be the maximal unramified extension of M in $\overline{\mathbf{Q}}_p$. Note that K is an infinite extension of $\mathbf{Q}_p$, since M is finite over $\mathbf{Q}_p$. We would like to describe $\mathcal{O}_K$, $\mathfrak{m}_K$ and κ. Since K is unramified over M, if π is a uniformiser for M then:

$$\mathfrak{m}_K = \pi \mathcal{O}_K.$$

Consider the residue field $\kappa = \mathcal{O}_K/\mathfrak{m}_K$ of K. It is an algebraic extension of $\mathbf{F}_p$, and it must in fact be an algebraic closure for $\mathbf{F}_p$. If not, one could construct an unramified algebraic extension of K inside $\overline{\mathbf{Q}}_p$, contradicting the fact that $K = M^{ur}$. In particular, κ is perfect.

Since $K/\mathbf{Q}_p$ is an infinite extension, it is not hard to show that it is not complete for the natural valuation induced from $\mathbf{Q}_p$. Hence nor is $\mathcal{O}_K$ a complete local ring. It is, however, **henselian**: if $f(X) \in \mathcal{O}_K[X]$ is a monic polynomial such that:

$$f(X) \equiv \overline{g}(X)\overline{h}(X) \pmod{\mathfrak{m}_K[X]},$$

for monic polynomials $\overline{g}(X), \overline{h}(X) \in \kappa[X]$ such that $(\overline{g}, \overline{h}) = 1$, then there exist monic polynomials $g, h \in \mathcal{O}_K[X]$ such that:

1. $f(X) = g(X)h(X)$,
2. $g(X) \equiv \overline{g}(X) \pmod{\mathfrak{m}_K[X]}$, and $h(X) \equiv \overline{h}(X) \pmod{\mathfrak{m}_K[X]}$.

The reader can check that the theory of differents and discriminants for finite extensions of K is the same as for finite extensions of $\mathbf{Q}_p$. The advantage of working with $K = M^{ur}$ is that all algebraic extensions of K are totally ramified.

Basic object of study

Retain the notation as above. We would like to understand:

$$\Omega = \Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K},$$

and the differential:

$$d\colon \mathcal{O}_{\overline{K}} \to \Omega.$$

Note that since $\mathcal{O}_{\overline{K}}$ is the union of the $\mathcal{O}_L$ for L/K finite, one has:

$$\mathcal{O}_{\overline{K}} = \varinjlim_{L/K \text{ finite}} \mathcal{O}_L.$$

Similarly, if

$$\mathcal{O}_K \subset \mathcal{O}_{L_1} \subset \mathcal{O}_{L_2} \subset \mathcal{O}_{L_3} \subset \overline{K},$$

for finite extensions L_i of K, $L_i \subset L_{i+1}$ for each i, then composition of the differentials with inclusion maps gives a natural commutative diagram:

$$\begin{array}{ccc} \Omega_{\mathcal{O}_{L_1}/\mathcal{O}_K} & \longrightarrow & \Omega_{\mathcal{O}_{L_2}/\mathcal{O}_K} \\ & \searrow \quad \swarrow & \\ & \Omega_{\mathcal{O}_{L_3}/\mathcal{O}_K} & \end{array}$$

This gives a directed system, and one can show that the natural maps:

$$\Omega_{\mathcal{O}_L/\mathcal{O}_K} \to \Omega$$

give a natural isomorphism:

$$\Omega \simeq \varinjlim_{L/K \text{ finite}} \Omega_{\mathcal{O}_L/\mathcal{O}_K}.$$

Since the standard construction of Ω is as a quotient, it is not always easy to recognize if a given differential, say $df \in \Omega$, is zero. Viewing Ω as a direct limit in this way, one sees that $\omega \in \Omega$ is identically zero if and only if there exists a finite extension L/K with $\omega \in \Omega_{\mathcal{O}_L/\mathcal{O}_K}$ already vanishing in this module. In fact, we will show that $\omega = 0$ if it vanishes in $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ for *every* finite extension L/K. This will follow from the next lemma, since it proves that the transition maps:

$$\Omega_{\mathcal{O}_{L_1}/K} \to \Omega_{\mathcal{O}_{L_2/K}}$$

for the direct system above are injective. Thus, one may think of Ω as the union of the submodules $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ for L/K finite.

Lemma 1.5.1. *Let $K \subset L_1 \subset L_2$ be extensions with $[L_2 : K] < \infty$, then:*

$$\alpha \ : \ \mathcal{O}_{L_2} \otimes_{\mathcal{O}_{L_1}} \Omega_{\mathcal{O}_{L_1}/\mathcal{O}_K} \to \Omega_{\mathcal{O}_{L_2/\mathcal{O}_K}}$$

is injective. In particular,

$$\Omega_{\mathcal{O}_{L_1/\mathcal{O}_K}} \to \Omega_{\mathcal{O}_{L_2/\mathcal{O}_K}}$$

is injective.

Proof. In our proof we will refrain from being very pedantic by omitting subscripts for the various differential maps appearing. All will be denoted d.

Fix uniformizers π_1, π_2 for L_1 and L_2, respectively. We first claim that every element:

$$\omega \in \mathcal{O}_{L_2} \otimes_{\mathcal{O}_{L_1}} \Omega_{\mathcal{O}_{L_1}/\mathcal{O}_K}$$

can be written in the form:

$$\omega = a \otimes d\pi_1$$

with $a \in \mathcal{O}_{L_2}$. This follows since $d\pi_1$ generates $\Omega_{\mathcal{O}_{L_1}/\mathcal{O}_{K_1}}$ as an $\mathcal{O}_{L_1}$-module.

Suppose that $\omega = a \otimes d\pi_1 \in \ker \alpha$, so that:

$$\alpha(\omega) = a d\pi_1 = 0$$

in $\Omega_{\mathcal{O}_{L_2}/\mathcal{O}_K}$. Since L_2/K is totally ramified, we have $\mathcal{O}_{L_2} = \mathcal{O}_K[\pi_2]$. Let $f(X) \in \mathcal{O}_K[X]$ be such that $\pi_1 = f(\pi_2)$. Then:

$$0 = a d\pi_1 = a d(f(\pi_2)) = a f'(\pi_2) d\pi_2.$$

Since $\mathcal{D}_{L_2/K}$ is the annihilator of $\mathcal{O}_{L_2/K}$, this is true if and only if:

$$v(a) + v(f'(\pi_2)) = v(a f'(\pi_2)) \geq v(\mathcal{D}_{L_2/K}) = v(\mathcal{D}_{L_2/L_1}) + v(\mathcal{D}_{L_1/K}).$$

We will now show that $v(f'(\pi_2)) = v(\mathcal{D}_{L_2/L_1})$. Let $F(X) \in \mathcal{O}_{L_1}[X]$ be the (monic) minimal polynomial of π_2 over L_1. Since L_2/L_1 is totally ramified, one has $F(0) = u\pi_1$, where $u \in \mathcal{O}_{L_1}^{\times}$. This follows since the constant coefficient a_0 of $F(X)$ is the product of the conjugates of π_2 over L_1. Since L_2/L_1 is totally ramified, we have $[L_2 : L_1] = e_{L_2/L_1}$ and hence:

$$v(a_0) = v(\pi_2^{e_{L_2/L_1}}) = v(\pi_1).$$

In fact, $F(X)$ is an Eisenstein polynomial. All coefficients must be divisible by π_1 since the roots all reduce to zero mod $\mathfrak{m}_{L_1}$, and we have just shown that the constant term has the same valuation as π_1.

Since $f(\pi_2) - \pi_1 = 0$ and $f(X) - \pi_1 \in \mathcal{O}_{L_1}[X]$, we deduce that:

$$f(X) - \pi_1 = F(X)G(X),$$

for some monic polynomial $G(X) \in \mathcal{O}_{L_1}[X]$. By comparing coefficients above, one can show that $v(G(\pi_2)) = 0$. Thus:

$$f'(\pi_2) = F'(\pi_2)G(\pi_2),$$

and taking valuations gives:

$$v(f'(\pi_2)) = v(F'(\pi_2)) = v(\mathcal{D}_{L_2/L_1}).$$

Combining this with the inequality above shows that:

$$v(a) \geq v(\mathcal{D}_{L_1/K}).$$

Write $\mathcal{D}_{L_1/K} = \pi_1^b \mathcal{O}_{L_1}$ where $b \geq 0$ is an integer. Then by what we have just seen, $a/\pi_1^b \in \mathcal{O}_{L_1}$ and hence:

$$\begin{aligned}
\omega &= a \otimes d\pi_1 \\
&= \left(\frac{a}{\pi_1^b}\right) \pi_1^b \otimes d\pi_1 \\
&= \left(\frac{a}{\pi_1^b}\right) \otimes (\pi_1^b d\pi_1) \\
&= 0
\end{aligned}$$

in $\mathcal{O}_{L_2} \otimes_{\mathcal{O}_{L_1}} \Omega_{\mathcal{O}_{L_1}/\mathcal{O}_K}$, since π_1^b annihilates $\Omega_{\mathcal{O}_{L_1}/\mathcal{O}_K}$. This concludes the proof of the first claim.

The second claim follows from the first, since the natural map factors as:

$$\Omega_{\mathcal{O}_{L_1}/\mathcal{O}_K} \to \mathcal{O}_{L_2} \otimes_{\mathcal{O}_{L_1}} \Omega_{\mathcal{O}_{L_1}/\mathcal{O}_K} \to \Omega_{\mathcal{O}_{L_2}/\mathcal{O}_K}.$$

We have just seen that the second factor is injective. The first is injective since $\mathcal{O}_{L_2}$ is a free $\mathcal{O}_{L_1}$-module of rank $[L_2 : L_1]$. □

The map δ

Let $a \in \mathcal{O}_{\overline{K}}$, so that $a \in \mathcal{O}_F$ for some F/K finite. Let π be a uniformizer for F and let $f(X) \in \mathcal{O}_K[X]$ be such that $f(\pi) = a$. We again remind the reader that such f exists since F/K is totally ramified.

Define a map $\delta = \delta_K \colon \mathcal{O}_{\overline{K}} \to (-\infty, 0]$ by putting:

$$\delta(a) = \min\left\{ v\left(\frac{f'(\pi)}{\mathcal{D}_{F/K}}\right), 0 \right\}.$$

Lemma 1.5.2. *For δ defined as above:*

1. *δ is independent of $f(X)$, π and F. Hence δ is well-defined.*
2. *If $a, b \in \mathcal{O}_{\overline{K}}$ then:*
$$\delta(a+b) \geq \min(\delta(a), \delta(b)),$$
and if $\delta(a) \neq \delta(b)$, there is equality. For products one has:
$$\delta(ab) \geq \min\{\delta(a) + v(b), v(a) + \delta(b)\}.$$
3. *If $f(X) \in \mathcal{O}_K[X]$ and $a \in \mathcal{O}_{\overline{K}}$ then:*
$$\delta(f(a)) = \min\{v(f'(a)) + \delta(a), 0\}.$$
4. *If $x, y \in \mathcal{O}_{\overline{K}}$ then $xdy = 0$ if and only if $v(x) + \delta(y) \geq 0$. In particular, $dy = 0$ if and only if $\delta(y) = 0$.*
5. *For $x, y \in \mathcal{O}_{\overline{K}}$, the formula:*
$$\delta(xdy) = \min\{v(x) + \delta(y), 0\}$$
gives a well-defined map:
$$\delta \colon \Omega \to (-\infty, 0]$$
which is compatible with $\delta \colon \mathcal{O}_{\overline{K}} \to (-\infty, 0]$.

Proof. 1. First, suppose that F remains fixed, and consider two (possibly distinct) uniformizers of F, say π and $u\pi$, for some $u \in \mathcal{O}_F^\times$. Let $f(x), g(x) \in \mathcal{O}_K[x]$ be such that

$$f(\pi) = a, \quad g(u\pi) = a.$$

Taking $d = d_F$, we get $f'(\pi)d\pi = ug'(u\pi)d\pi$, where $()'$ denotes the (formal) derivative with respect to x. So we get that

$$v(f'(\pi) - ug'(u\pi)) \geq v(\mathcal{D}_{F/K}).$$

Suppose that $v(f'(\pi)) \neq v(g'(u\pi))$, say without loss of generality that $v(f'(\pi)) < v(g'(u\pi))$. Then

$$v(f'(\pi) - ug'(u\pi)) = v(f'(\pi)),$$

so the previous inequality implies that $v(f'(\pi)) \geq v(\mathcal{D}_{F/K})$, and so δ will be 0, no matter what the valuations are.

Now, given F_1, F_2 two fields such that $a \in F_1 \cap F_2$, as $F_1 \cap F_2$ is also a field we can assume without loss of generality that $a \in F_1 \subseteq F_2$. Compute then $\delta(a)$ thinking of a as belonging to F_2, and we will show that the result is as we took a as belonging to F_1. To do this, we choose a uniformizer π for F_2, and let $\mathbf{N}(\pi)$ be a uniformizer for F_1. Let $f \in \mathcal{O}_K[x]$ be a polynomial such that $f(\mathbf{N}(\pi)) = a$. Let also $\phi(x)$ be the minimal polynomial of π over F_1, and note that $\pi(x) = \mathbf{N}(\pi) - h(x)$, for some polynomial $h(x)$ divisible by x. Then the polynomial $g \stackrel{\text{def}}{=} f \circ h$ has coefficients in $\mathcal{O}_K$ as well, and is such that $g(\pi) = f(h(\pi)) = f(\mathbf{N}(\pi)) = a$. Then we have:

$$\begin{aligned} v(g'(\pi)) - v(\mathcal{D}_{F_2/K}) &= v(h'(\pi)f'(\mathbf{N}(\pi))) - v(\mathcal{D}_{F_2/K}) \\ &= v(h'(\pi)) + v(f'(\mathbf{N}(\pi)) - v(\mathcal{D}_{F_2/F_1}) - v(\mathcal{D}_{F_1/K}), \end{aligned}$$

and just note that $v(\mathcal{D}_{F_2/F_1}) = v(\phi'(\pi)) = v(-h'(\pi)) = v(h'(\pi))$.

2. First, let F be a finite extension of K such that $a, b \in F$. Let π be a uniformizer for F. Then, if $f(x), g(x) \in \mathcal{O}_K[x]$ are such that $f(\pi) = a$ and $g(\pi) = b$, we have:

$$v(f'(\pi) + g'(pi)) \geq \min\{v(f'(\pi)), v(g'(\pi))\},$$

so that the first inequality follows. If $\delta(a) \neq \delta(b)$, it means that $v(f'(\pi)) \neq v(g'(\pi))$, so that the previous inequality is an equality, and hence we get equality for the δ's.

To compute $\delta(ab)$ use the polynomial $fg \in \mathcal{O}_K[x]$. Then $(fg)'(\pi) = f'(\pi)g(\pi) + f(\pi)g'(\pi)$ and the valuations satisfy:

$$v((fg)'(\pi)) \geq \min\{v(f'(\pi)) + v(b), v(a) + v(g'(\pi))\}.$$

3. If $g(x) \in \mathcal{O}_K[x]$ is such that $g(\pi) = a$, then $f(a) = f(g(\pi))$, so we need to consider the polynomial $f \circ g$. Then we have

$$(f \circ g)'(\pi) = f'(g(\pi)) \cdot g'(\pi),$$

so that in valuations we get:

$$\delta(f(a)) = \min \{v(f'(a)) + v(g'(\pi)), 0\} = \min \{v(f'(a)) + \delta(a), 0\}.$$

4. Let F be a finite extension of K such that $x, y \in F$. Let π be a uniformizer in F. Write $y = f(\pi)$ for some $f(x) \in \mathcal{O}_K[x]$. Then, as $\mathcal{D}_{F/K}$ is the exact annihilator of $\Omega_{\mathcal{O}_F/\mathcal{O}_K} \simeq (\mathcal{O}_F/\mathcal{D}_{F/K}) \cdot d\pi$, we get

$$xdy = xd(f(\pi)) = xf'(\pi)d\pi,$$

so that

$$\begin{aligned} xdy = 0 &\iff xf'(\pi) \in \mathcal{D}_{F/K} \\ &\iff v(x) + v(f'(\pi)) \geq v(\mathcal{D}_{F/K}) \\ &\iff v(x) + \delta(y) = 0. \end{aligned}$$

5. We know that $\Omega \supseteq \Omega_{\mathcal{O}_F/\mathcal{O}_K} = (\mathcal{O}_F/\mathcal{D}_{F/K}) \cdot d\pi$, so that to show that δ is well-defined it is enough to show that if $x \in \mathcal{D}_{F/K}$, then $\min\{v(x) + \delta(\pi), 0\} = 0$. But $\delta(\pi) = -\mathcal{D}_{F/K}$, so that $v(x) - \mathcal{D}_{F/K} \geq 0$, and then the minimum is 0, as we wanted.

   The compatibility with the previously defined δ is then clear.

□

Lemma 1.5.3. *Let M be a finite extension of $\mathbf{Q}_p$, and let $K = M^{ur}$. Then the natural map*

$$\Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_M} \to \Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$$

is an isomorphism.

Proof. From the fundamental exact sequence, this is equivalent to showing that

$$\mathcal{O}_{\overline{K}} \otimes_{\mathcal{O}_K} \Omega_{\mathcal{O}_K/\mathcal{O}_M} = 0.$$

But recall that

$$\Omega_{\mathcal{O}_K/\mathcal{O}_M} = \varinjlim \Omega_{\mathcal{O}_L/\mathcal{O}_M},$$

where L runs through all finite extensions $M \subseteq L \subseteq K$. Such an L/M is finite and unramified, which implies that $\mathcal{O}_L/\mathcal{O}_M$ is étale. Hence

$$\Omega_{\mathcal{O}_L/\mathcal{O}_M} = 0.$$

□

Define a map $\delta_M \colon \mathcal{O}_{\overline{K}} \to (-\infty, 0]$ via the formula:

$$\delta_M(a) \stackrel{\text{def}}{=} -v\left(\mathrm{Ann}_{\mathcal{O}_{\overline{K}}}(d_M(a))\right), \quad a \in \mathcal{O}_{\overline{K}},$$

where we think of $d_M(a) \in \Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_M}$.

Lemma 1.5.4. *We have*

$$\delta_M = \delta_K.$$

Proof. From Lemma 1.5.2 we know that

$$\delta_K(a) = -v\left(\mathrm{Ann}_{\mathcal{O}_{\overline{K}}}(d_K(a))\right).$$

This proves $d_K(a) \in \Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$, and the result follows from the previous lemma. □

Definition 1.5.5. An extension L of K is said to be **deeply ramified** if there is some sequence $\{F_n\}$ of finite extensions of K such that $L = \bigcup_n F_n$, and such that

$$v(\mathcal{D}_{F_n/K}) \to \infty \text{ when } n \to \infty.$$

Remark. It follows, although we won't prove it here, that if this happens for a sequence $\{F_n\}$ then it is also true for any other sequence $\{F_n'\}$ such that $L = \cup_n F_n'$.

Example. Let K be a finite extension of $\mathbf{Q}_p$, or $K = M^{\mathrm{ur}}$, where M is a finite extension of $\mathbf{Q}_p$. Then the extension $L = K(\mu_{p^\infty}) = \cup_n K(\mu_{p^n})$ is deeply ramified. Also, Theorem 1.4.3 shows that any $\mathbf{Z}_p$ extension of K is deeply ramified.

Recall that our object of interest is the module

$$\Omega = \Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K} \simeq \Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_M}.$$

Note that Ω is a torsion module: for any $\omega \in \Omega$, there exists $N \geq 1$ such that $p^N\omega = 0$. In fact, one can take any $N > -\delta(\omega)$.

Lemma 1.5.6. *Let $a, b \in \mathcal{O}_{\overline{K}}$ be such that $\delta(a) \leq \delta(b)$. Then there exists $c \in \mathcal{O}_{K[a,b]}$ such that $cda = db$ as elements of Ω.*

Proof. If $\delta(b) = 0$ then $db = 0$, so that we may take $c = 0$. Hence we assume that $\delta(b) < 0$.

Let π be a uniformizer of $K[a, b]$. Let $h_1(X), h_2(X) \in \mathcal{O}_K[X]$ be such that $h_1(\pi) = a$, and $h_2(\pi) = b$. Then:

$$v(h_1'(\pi)) - v(\mathcal{D}_{K[a,b]/K}) = \delta(a) \leq \delta(b) = v(h_2'(\pi)) - v(\mathcal{D}_{K[a,b]/K}),$$

so that $v(h_1'(\pi)) \leq v(h_2'(\pi))$. If

$$c = \frac{h_2'(\pi)}{h_1'(\pi)} \in \mathcal{O}_{K[a,b]},$$

then $cda = db$ in $\Omega_{\mathcal{O}_{K[a,b]}/\mathcal{O}_K}$, which concludes the proof since $\Omega_{\mathcal{O}_{K[a,b]}/\mathcal{O}_K} \hookrightarrow \Omega$. □

Lemma 1.5.7. *Let L/K be an algebraic extension of K. Then the following are equivalent:*

1. *$\delta(\mathcal{O}_L)$ is unbounded.*

2. *If F/L is an algebraic extension of L then:*

$$\Omega_{\mathcal{O}_F/\mathcal{O}_K} = \mathcal{O}_F \cdot \Omega_{\mathcal{O}_L/\mathcal{O}_K}.$$

as subgroups of Ω. In particular, taking $F = \overline{K}$ gives:

$$\Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K} = \mathcal{O}_{\overline{K}} \cdot \Omega_{\mathcal{O}_L/\mathcal{O}_K}.$$

Proof. We first claim that in any case, $\Omega_{\mathcal{O}_L/\mathcal{O}_K} \subseteq \Omega_{\mathcal{O}_F/\mathcal{O}_K}$. This has been proved for finite extensions, and since direct limits are exact, one obtains the inclusion for infinite extensions by passing to the limit. It follows that:

$$\mathcal{O}_F \cdot \Omega_{\mathcal{O}_L/\mathcal{O}_K} \subseteq \Omega_{\mathcal{O}_F/\mathcal{O}_K},$$

where we regard the left side as a subgroup, say.

Assume first that $\delta(\mathcal{O}_L)$ is unbounded, and let $udv \in \Omega_{\mathcal{O}_F/\mathcal{O}_K}$. Let $x \in \mathcal{O}_L$ be such that

$$\delta(x) \leq \delta(v).$$

Then, by the previous lemma, there exists $y \in \mathcal{O}_{K[x,v]} \subseteq \mathcal{O}_F$ such that $ydx = dv$. So $uydx = udv$ and we obtain the reverse inclusion.

Conversely, if $\delta(\mathcal{O}_L)$ is bounded by $-N$ for some $N \in \mathbf{N}$, then note that p^N annihilates $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ by the basic properties of δ. On the other hand, Ω is not annihilated by any fixed power of p, so that $\Omega \neq \mathcal{O}_{\overline{K}} \cdot \Omega_{\mathcal{O}_L/\mathcal{O}_K}$. This finishes the proof of the lemma. □

Theorem 1.5.8. *Let L be an algebraic extension of K. Then the following statements are equivalent:*

1. *L is deeply ramified over K.*

2. *$\delta(\mathcal{O}_L)$ is unbounded.*

3. *$\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ is a nonzero p-divisible group.*

4. *For every algebraic extension F/L we have $\omega_{\mathcal{O}_F/\mathcal{O}_L} = 0$.*

5. *For every algebraic extension F/L we have $\omega_{\mathcal{O}_F/\mathcal{O}_K} = \mathcal{O}_F \cdot \Omega_{\mathcal{O}_L/\mathcal{O}_K}$.*

Proof. $2 \iff 5$: This was done in the previous lemma.

$1 \iff 2$: For this it is enough to show that if $K \subseteq N \subseteq L$, N/K finite and π is a uniformizer for N, then $\delta(\pi) = -v(\mathcal{D}_{N/K})$. Since this is in fact true, this establishes the equivalence.

$4 \iff 5$: This follows formally from the fundamental exact sequence corresponding to:

$$\mathcal{O}_K \subseteq \mathcal{O}_L \subseteq \mathcal{O}_F.$$

$2 \implies 3$: Let $\omega \in \Omega_{\mathcal{O}_L/\mathcal{O}_K}$. We want to find $\eta \in \Omega_{\mathcal{O}_L/\mathcal{O}_K}$ such that $\omega = p\eta$. Write $\omega = udv$ and find $x \in \mathcal{O}_L$ such that $\delta(x) \leq \delta(v) - 1$. Then there exists $y \in \mathcal{O}_L$ such that $pydx = dv$, and we are done.

$3 \implies 2$: The proof will be by contradiction; suppose that $\delta(\mathcal{O}_L)$ is bounded. Let $\varepsilon = \inf_{a \in \mathcal{O}_L}\{\delta(a)\}$, which is strictly less than 0. Let $x \in \mathcal{O}_L$ be such that $0 \leq \delta(x) - \varepsilon \leq 1/2$. As $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ is p-divisible, one can find $a, b \in \mathcal{O}_L$ such that $dx = padb$. But then

$$\delta(x) = 1 + v(a) + \delta(b) \implies \delta(b) \leq \delta(x) - 1 \leq \varepsilon - 1/2 < \varepsilon,$$

which contradicts the definition of ε. □

Remark. Using Lemma 1.5.3, we can replace K by M in the previous theorem.

Let $L = \overline{K}$, where still $K = M^{ur}$. Then L is a deeply ramified extension of K, and the previous theorem implies that $\Omega = \Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_M}$ is a p-divisible group. Every p-divisible group has an associated **Tate module**, which we construct below for Ω.

For every $n \geq 1$, consider the submodule of Ω:

$$\Omega[p^n] \stackrel{\text{def}}{=} \{\omega \in \Omega \mid p^n\omega = 0\}.$$

Multiplication by p gives a natural map $\Omega[p^{n+1}] \to \Omega[p^n]$, so that the submodules $\Omega[p^n]$ define a projective system. Let:

$$T_p\Omega \stackrel{\text{def}}{=} \varprojlim_n \Omega[p^n].$$

Let $G_M = \mathrm{Gal}(\overline{K}/M)$. For $\omega = adb \in \Omega$, if $\sigma \in G_M$ we can define

$$\sigma(\omega) \stackrel{\text{def}}{=} \sigma(a)d(\sigma(b)).$$

It is an easy exercise to show that this is well-defined, and that it gives a continuous action of G_M on Ω. Also, G_M acts on each of the discrete modules $\Omega[p^n]$, so that it acts continuously on $T_p\Omega$ when this is given the p-adic topology.

Definition 1.5.9. The **Tate module** of Ω is the G_M-module $T_p\Omega$.

1.6 Cyclotomic twists

In this section K will denote a finite extension of $\mathbf{Q}_p$.

Fix a compatible sequence of primitive p^nth roots of unity $\varepsilon = (\varepsilon^{(n)})_{n\geq 0} \subseteq \overline{K}$. Compatible means that $(\varepsilon^{(n+1)})^p = \varepsilon^{(n)}$.

Definition 1.6.1. The **cyclotomic character** is the continuous homomorphism:

$$\chi\colon G_K \to \mathbf{Z}_p^\times$$

defined by the formula:

$$\sigma(\varepsilon^{(n)}) = \left(\varepsilon^{(n)}\right)^{\chi(\sigma)}.$$

If $\boldsymbol{\mu}_{p^n}$ denotes the group of p^nth roots of unity, which we write additively as $\varepsilon^{(n)} \cdot \mathbf{Z}/p^n\mathbf{Z}$, then there is a map:

$$\boldsymbol{\mu}_{p^n} \to \boldsymbol{\mu}_{p^{n-1}}, \quad \varepsilon^{(n)} \mapsto \varepsilon^{(n-1)} = \left(\varepsilon^{(n)}\right)^p.$$

Set:

$$\mathbf{Z}_p(1) \stackrel{\text{def}}{=} T_p\mathbb{G}_m \stackrel{\text{def}}{=} \varprojlim_n \boldsymbol{\mu}_{p^n} \simeq \varepsilon \cdot \mathbf{Z}_p,$$

with the G_K action given by

$$\sigma(a\varepsilon) = a\sigma(\varepsilon) = a\chi(\sigma)\varepsilon = \chi(\sigma)(a\varepsilon).$$

For every $n \geq 1$, define also:

$$\mathbf{Z}_p(n) \stackrel{\text{def}}{=} \underbrace{\mathbf{Z}_p(1) \otimes_{\mathbf{Z}_p} \cdots \otimes_{\mathbf{Z}_p} \mathbf{Z}_p(1)}_{n \text{ times}},$$

and if $n \leq -1$ we let $\mathbf{Z}_p(n) \stackrel{\text{def}}{=} \operatorname{Hom}(\mathbf{Z}_p(-n), 1)$.

The Galois action of these twists $\mathbf{Z}_p(1)$ is actually quite simple: $x \in \mathbf{Z}_p(n)$ and $\sigma \in G_K$, then we have

$$\sigma(x) = \chi(\sigma)^n x.$$

We also set $\overline{K}(1) \stackrel{\text{def}}{=} \overline{K} \otimes_{\mathbf{Z}_p} \mathbf{Z}_p(1) = \overline{K} \otimes \varepsilon$, where G_K acts diagonally: if $x \in \overline{K}$ and $\sigma \in G_K$,

$$\sigma(x \otimes \varepsilon) = \sigma(x) \otimes \chi(\sigma)\varepsilon = \chi(\sigma)\sigma(x) \otimes \varepsilon.$$

Following the work of Fontaine, define a function $f\colon \overline{K}(1) \to \Omega = \Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$ by the formula:

$$f(x \otimes \varepsilon) \stackrel{\text{def}}{=} a\frac{d\varepsilon^{(n)}}{\varepsilon^{(n)}} \in \Omega,$$

if $x = a/p^n$ with $a \in \mathcal{O}_{\overline{K}}$.

Remark. This is well defined: if $x = \frac{a}{p^n} = \frac{b}{p^m}$, with $a, b \in \mathcal{O}_{\overline{K}}$, then it is easy to check that $a \operatorname{dlog} \varepsilon^{(n)} = b \operatorname{dlog} \varepsilon^{(m)}$.

Theorem 1.6.2 (Fontaine)**.** *The following properties for f hold:*

1. *f is an $\mathcal{O}_K$-liner map which is G_K-equivariant.*
2. *f is surjective.*
3. $\ker f = D(1) = D \otimes \varepsilon$, *where*

$$D = \left\{ x \in \overline{K} \mid v(x) \geq -v(\mathcal{D}_{K/\mathbf{Q}_p}) - \frac{1}{p-1} \right\}.$$

Proof. For the first property, take $x \otimes \varepsilon \in \overline{K}(1)$ and write $x = a/p^n$ where $a \in \mathcal{O}_{\overline{K}}$, $n \geq 0$. Hence for any $\sigma \in G_K$, one has $\sigma(a) \in \mathcal{O}_{\overline{K}}$ as well. It follows that:

$$f(\sigma(x \otimes \varepsilon)) = f((\sigma(a)\chi(\sigma)/p^n) \otimes \varepsilon) = \frac{\sigma(a)\chi(\sigma)}{p^n} \frac{d(\varepsilon^{(n)})}{\varepsilon^{(n)}}.$$

On the other hand:

$$\sigma(f(x \otimes \varepsilon)) = \sigma\left(a \frac{d(\varepsilon^{(n)})}{\varepsilon^{(n)}} \right) = \sigma(a) \frac{d(\sigma(\varepsilon^{(n)}))}{\sigma(\varepsilon^{(n)})}.$$

Recall that σ acts on ε via the cyclotomic character. If $\chi(\sigma) = m + p^n \alpha$ for $m \in \mathbf{Z}$ and $\alpha \in \mathbf{Z}_p$, then:

$$\sigma(\varepsilon^{(n)}) = (\varepsilon^{(n)})^{\chi(\sigma)} = (\varepsilon^{(n)})^m,$$

and hence:

$$d(\sigma(\varepsilon^{(n)})) = m(\varepsilon^{(n)})^{m-1} d(\varepsilon^{(n)}) = \chi(\sigma)(\varepsilon^{(n)})^{m-1} d(\varepsilon^{(n)}),$$

where the last equality above follows since p^n annihilates $d(\varepsilon^{(n)})$. Splicing these two computations together gives:

$$\sigma(f(x \otimes \varepsilon)) = \sigma(a) \frac{d(\sigma(\varepsilon^{(n)}))}{\sigma(\varepsilon^{(n)})} = f(\sigma(x \otimes \varepsilon)).$$

For the second property we begin by showing that:

$$\delta_{\mathbf{Q}_p}(\varepsilon^{(n)}) = -n + \frac{1}{p-1},$$

for all $n \geq 1$. This is quite simple at this point, as in theorem 1.4.3 we showed that:

$$v(\mathcal{D}_{\mathbf{Q}_p(\varepsilon^{(n)})/\mathbf{Q}_p}) = n - \frac{1}{p-1}.$$

Note that $\pi_n = \varepsilon^{(n)} - 1$ is a uniformizer for $\mathbf{Q}_p(\varepsilon^{(n)})$, and $f(X) = X + 1$ obviously satisfies $f(\pi_n) = \varepsilon^{(n)}$. Since $f'(X) = 1$, we see that in this case:

$$\delta_{\mathbf{Q}_p}(\varepsilon^{(n)}) = v(f'(\pi_n)) - v(\mathcal{D}_{\mathbf{Q}_p(\varepsilon^{(n)})/\mathbf{Q}_p}) = -n + \frac{1}{p-1}.$$

Note also that multiplicativity of the different in finite towers gives:

$$\delta_K(\varepsilon^{(n)}) = \delta_{\mathbf{Q}_p}(\varepsilon^{(n)}) + v(\mathcal{D}_{K/\mathbf{Q}_p}).$$

Let $\omega \in \Omega$ and write $\omega = udv$ for u, v in some finite extension of K. The preceding computation shows that there exists an integer $n \geq 1$ such that:

$$\delta_K(\varepsilon^{(n)}) \leq \delta_K(v).$$

Hence lemma 1.5.6 shows that there exists $a \in \mathcal{O}_{\overline{K}}$ such that:

$$ad(\varepsilon^{(n)}) = dv.$$

For this a write $x = (au/p^n)\varepsilon^{(n)}$, which is an element of $\overline{K}$. Now one simply computes:

$$f(x \otimes \varepsilon) \quad = \quad au\varepsilon^{(n)}\frac{d(\varepsilon^{(n)})}{\varepsilon^{(n)}} = udv = \omega,$$

which shows that f is surjective.

For the final claim note that for $x = a/p^n$ with $a \in \mathcal{O}_{\overline{K}}$ and $n \geq 1$:

$$\begin{aligned} f(x \otimes \varepsilon) = 0 \quad &\Longleftrightarrow \quad ad(\varepsilon^{(n)}) = 0 \\ &\Longleftrightarrow \quad v(a) + \delta_K(\varepsilon^{(n)}) \geq 0 \\ &\Longleftrightarrow \quad v(a) + n + \frac{1}{p-1} + v(\mathcal{D}_{K/\mathbf{Q}_p}) \geq 0 \\ &\Longleftrightarrow \quad v(x) = v(a/p^n) \geq -v(\mathcal{D}_{K/\mathbf{Q}_p}) - \frac{1}{p-1}. \end{aligned}$$

This concludes the proof of the theorem. □

Corollary 1.6.3. *Let* $\xi_K \in \overline{K}$ *be such that* $v(\xi_K) = -v(\mathcal{D}_{K/\mathbf{Q}_p}) - \frac{1}{p-1}$. *Then:*

$$D(1) \simeq \xi_K \mathcal{O}_{\overline{K}}(1),$$

and there is an exact sequence of G_K*-modules:*

$$0 \longrightarrow D(1) \longrightarrow \overline{K}(1) \longrightarrow \Omega \longrightarrow 0.$$

Since multiplication by p^n commutes with the G_K-action, one deduces commutative diagrams of G_K-modules with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D(1) & \longrightarrow & \overline{K}(1) & \longrightarrow & \Omega & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \\ 0 & \longrightarrow & D(1) & \longrightarrow & \overline{K}(1) & \longrightarrow & \Omega & \longrightarrow & 0 \end{array}$$

for every $n \geq 0$. The middle map is obviously an isomorphism. Note that $D(1)$ is torsion free, which implies that the leftmost vertical map is injective. Analogously, the p-divisibility of Ω shows that the rightmost vertical map is surjective. The snake lemma thus gives an isomorphism of G_K-modules:

$$\delta_n \;:\; \Omega[p^n] \simeq (D/p^nD)(1).$$

These all fit together to give an isomorphism:

$$T_p\Omega \simeq \varprojlim (D/p^nD)(1) \simeq \widehat{D}(1) \simeq \xi_K \mathcal{O}_{\mathbf{C}_p}(1),$$

where ξ_K is as in the preceding corollary. Hence:

$$V_p(\Omega) = T_p\Omega \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \simeq \mathbf{C}_p(1)$$

as G_K-modules. This gives a deep geometric interpretation of the G_K-module $\mathbf{C}_p(1)$.

1.7 Continuous representations

In this section we again fix a finite extension $K/\mathbf{Q}_p$ contained in our fixed algebraic closure $\overline{K}$.

Let U be a topological abelian group along with a map:

$$f\colon G_K \times U \to U$$

which we will denote as $(\sigma, x) \mapsto \sigma x$. If f is continuous for the product topology on $G_K \times U$, and moreover gives a linear action of G_K on U, then we say that U is a **continuous G_K-representation**.

Example. If U is a discrete abelian group and G_K acts on U algebraically, then the action is continuous if and only if the stabilizer subgroup $\mathrm{stab}_{G_K}(x)$ is open in G_K for all $x \in U$. If E/K is an elliptic curve, then $U = E[p^n](\overline{K})$ is a naturally occurring example of such a group. Similarly for the étale cohomology groups of varieties over K with finite coefficients. We will refer to such examples as **discrete G_K-representations**.

Example (p-adic representations of G_K)**.** If V is a finite dimensional $\mathbf{Q}_p$ vector space, then it has a unique canonical p-adic topology which makes V into a topological vector space. It can be defined by choosing a basis for V and thereby identifying $V \simeq \mathbf{Q}_p^n$ for some $n \geq 0$. Suppose that G_K acts continuously on the additive group of V, such that if $a \in \mathbf{Q}_p$ then:

$$\sigma(av) = a\sigma(v)$$

for all $v \in V$ and $\sigma \in G_K$. Then V is said to be a **p-adic representation**.

Fix a $\mathbf{Q}_p$-basis for V, say $e = \{e_1, \ldots, e_n\}$. For each $\sigma \in G_K$ write:

$$\sigma(e_j) = \sum_{i=1}^{n} a_{ij}(\sigma) e_i$$

for $a_{ij}(\sigma) \in \mathbf{Q}_p$. This gives a matrix $A(\sigma) = (a_{ij}(\sigma)) \in \mathrm{GL}_n(\mathbf{Q}_p)$. One obtains a map:

$$\rho_{V,e} \ : \ G_K \longrightarrow \mathrm{GL}_n(\mathbf{Q}_p),$$

which is in fact a continuous group homomorphism.

Since G_K is a compact group, the image of $\rho_{V,e}$ lies in one of the maximal compact subgroups of $\mathrm{GL}_n(\mathbf{Q}_p)$. Changing the basis e amounts to conjugating $\rho_{V,e}$, and all maximal compact subgroups of $\mathrm{GL}_n(\mathbf{Q}_p)$ are conjugate. It follows that there is a choice of basis e for V such that:

$$\mathrm{im}\, \rho_{V,e} \subset \mathrm{GL}_n(\mathbf{Z}_p).$$

For this choice of basis define:

$$T = \mathbf{Z}_p e_1 \oplus \cdots \oplus \mathbf{Z}_p e_n.$$

This gives a $\mathbf{Z}_p$-lattice $T \subset V$ that is preserved by G_K. For each $n \geq 1$ one thus obtains an induced continuous action of G_K on the finite discrete groups T/p^nT. One thus obtains:

$$V \simeq T \otimes_{\mathbf{Z}} \mathbf{Q}_p \simeq \left(\varprojlim T/p^nT\right) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p.$$

This realizes V as a limit of finite discrete G_K-representations, with p inverted. One can hence deduce information about V by studying finite discrete G_K-representations.

We introduce at this point the following two categories:

$$\mathbf{Rep}^{\mathrm{cont}}(G_K) = \{\text{ continuous } G_K\text{-representations on topological abelian groups}\},$$

and:

$$\mathbf{Rep}_{\mathbf{Q}_p}(G_K) = \{p\text{-adic representations of } G_K\}.$$

Note that forgetting the linear structure of objects in $\mathbf{Rep}_{\mathbf{Q}_p}(G_K)$ gives a functor

$$\mathbf{Rep}_{\mathbf{Q}_p}(G_K) \to \mathbf{Rep}^{\mathrm{cont}}(G_K),$$

which is a fully faithful embedding. To see that the embedding is full, one notes that an additive morphism f of $\mathbf{Q}_p$-vectorspaces satisfies

$$f(rv) = rf(v), \quad \text{for all } r \in \mathbf{Q}.$$

Thus continuity of f and the density of $\mathbf{Q}$ in $\mathbf{Q}_p$ ensure the $\mathbf{Q}_p$-linearity of f. In this way $\mathbf{Rep}_{\mathbf{Q}_p}(G_K)$ is a *full* subcategory of $\mathbf{Rep}^{\mathrm{cont}}(G_K)$.

Example. Let $V \in \mathbf{Rep}_{\mathbf{Q}_p}(G_K)$ and put $W = V \otimes_{\mathbf{Q}_p} \mathbf{C}_p$. If $\sigma \in G_K$ then define an action of G_K on W by:

$$\sigma(v \otimes x) = \sigma(v) \otimes \sigma(x).$$

Then one can show that the action on W is continuous for the natural p-adic topology. As a $\mathbf{Q}_p$-vector space, W is infinite dimensional. It is also naturally a finite dimensional $\mathbf{C}_p$-vector space via the second factor of W. However, the G_K action of $\mathbf{C}_p$ does not commute with scalar multiplication by elements in $\mathbf{C}_p$. Rather, the action is **semi-linear**: for $a \in \mathbf{C}_p$ one has

$$\sigma(a(v \otimes x)) = \sigma(v \otimes (ax)) = \sigma(v) \otimes (\sigma(a)\sigma(x)) = \sigma(a)\sigma(v \otimes x).$$

One can attempt to copy what was done above, and fix a $\mathbf{C}_p$ basis for W to obtain a map:

$$\rho \ : \ G_K \longrightarrow \mathrm{GL}_n(\mathbf{C}_p).$$

Since the G_K action is only semi-linear, one obtains a cocycle, or crossed homomorphism, rather than a group homomorphism. Thus:

$$\rho \in H^1\left(G_K, \mathrm{GL}_n(\mathbf{C}_p)\right),$$

which is a pointed set.

Let $T \subset V$ be a G_K-invariant $\mathbf{Z}_p$-lattice as above. Then put:

$$W_0 = T \otimes_{\mathbf{Z}_p} \mathcal{O}_{\mathbf{C}_p}.$$

Note that using the basis for T, we can identify W_0 inside W. Under this identification one has $\sigma(W_0) \subset W$ for all $\sigma \in G_K$. Also:

$$W_0 \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \simeq W.$$

Once again we see that W can be regarded as a limit of discrete (although not finite) G_K-representations:

$$W_0 \simeq \varprojlim \left(T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p / p^n (T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)\right),$$

followed by inverting p.

Example. Take $V \in \mathbf{Rep}_{\mathbf{Q}_p}(G_K)$ and put $W_{\text{cris}} = V \otimes_{\mathbf{Q}_p} B^+_{\text{cris}}$, where B^+_{cris} is a field to be defined below. It is again the case that B^+_{cris} contains a p-adically complete lattice. Thus, we will see that W_{cris} is also a limit of discrete modules with p inverted.

Example. We will also define the deRham period ring B^+_{dR}. The above phenomena will not hold for:

$$W_{dR} = V \otimes_{\mathbf{Q}_p} B^+_{dR}.$$

One thus requires different methods to study these representations.

1.8 Continuous group cohomology

1.8.1 Cohomology of finite groups

Let G be a finite group. Denote by $\mathbf{Rep}\, G$ the category of G-modules (or representations of G). Its objects are abelian groups M endowed with a G-action which respects the additive structure. That is, there is a map

$$G \times M \to M, \quad (\sigma, m) \mapsto \sigma m,$$

satisfying, for all $\sigma, \tau \in G$, and for all $a, b \in M$:

$$\sigma(\tau a) = (\sigma\tau)a$$
$$\sigma(a+b) = \sigma a + \sigma b$$
$$1_G a = a.$$

For two objects M_1 and M_2 in $\mathbf{Rep}\, G$, a morphism $f\colon M_1 \to M_2$ is a group homomorphism such that, for all $\sigma \in G$ and for all $a \in M$, satisfies

$$f(\sigma a) = \sigma f(a).$$

The category $\mathbf{Rep}\, G$ just defined is abelian. Indeed, one easily proves that it is isomorphic to the category of $\mathbf{Z}[G]$-modules, and thus it is a module category. This already implies that it has enough injectives and projectives, for example.

More generally, suppose that R is a commutative ring. Denote by $\mathbf{Rep}_R\, G$ the category of R-modules with a linear G-action. Again, $\mathbf{Rep}_R\, G \simeq \mathbf{Mod}(R[G])$, so it is also abelian and has enough injectives and projectives. The forgetful functor $\mathbf{Rep}_R\, G \to \mathbf{Rep}\, G$ is faithful.

If S in a R-algebra and G is a subgroup of the group of R-algebra isomorphisms of S, then one defines the category $\mathbf{Rep}_{(R,S)}\, G$ to have as objects the S-modules M with a semilinear action by G. That is, for $s \in S, a \in M$ and $\sigma \in G$, one requires

$$\sigma(sa) = (\sigma s)(\sigma a).$$

Note that if $\alpha \in R$, then $\sigma(\alpha a) = \alpha(\sigma a)$, so that there is again a forgetful functor $\mathbf{Rep}_{(R,S)}\, G \to \mathbf{Rep}_R\, G$, which again is faithful. The category $\mathbf{Rep}_{(R,S)}\, G$ is abelian as well, although it cannot be directly seen as a module category.[3]

We define the functor of G-invariants $F\colon \mathbf{Rep}\, G \to \mathbf{Ab}$. On objects M of $\mathbf{Rep}\, G$, it is:

$$F(M) \overset{\text{def}}{=} M^G \overset{\text{def}}{=} \{m \in M \mid \sigma m = m \text{ for all } \sigma \in G\}.$$

If $f\colon M \to N$ is a morphism, then it maps an element $m \in M$ fixed by G to an element $f(m)$ which will also be fixed by G, and thus its restriction induces a group homomorphism

$$F(f)\colon F(M) \to F(N).$$

It is an easy exercise to show that F is a functor. It is also easy to show that F is left exact. This means that if

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

is an exact sequence in $\mathbf{Rep}\, G$, then the induced sequence

$$0 \to F(M_1) \xrightarrow{F(f)} F(M_2) \xrightarrow{F(g)} F(M_3)$$

is exact in $\mathbf{Ab}$.

[3] **FIXME:** Shouldn't be an abelian categories ALWAYS a module category?

We define the functors $H^n(G,-)$ from $\mathbf{Rep}\,G$ to $\mathbf{Ab}$, for all non-negative integers n, as the nth right derived functors of F. The family

$$\{H^n(G,-)\}_{n\geq 0}$$

is a cohomological δ-functor. This means that given a short exact sequence of G-modules

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

there exists a sequence of group homomorphisms $\delta_n\colon H^n(G,M_3) \to H^n(G,M_1)$ which yields a long exact sequence in $\mathbf{Ab}$:

$$\cdots \to H^n(G,M_1) \to H^n(G,M_2) \to H^n(G,M_3) \overset{\delta_n}{\to} H^{n+1}(G,M_1) \to \cdots$$

1.8.2 Construction using injective resolutions

Let M be a G-module. Consider an injective resolution for M in $\mathbf{Rep}\,G$

$$0 \to M \to I^0 \to I^1 \to \cdots$$

This means that the sequence is exact, and each of the I^j is an injective object in $\mathbf{Rep}\,G$.

Define then

$$H^n(G,M) \overset{\text{def}}{=} H^n\left(0 \to F(M) \to F(I^0) \to F(I^1) \to \cdots\right)$$

One checks that the definition is independent of the chosen resolution.

Remark. If M is in $\mathbf{Rep}_R\,G$, to compute $H^n(G,M)$ one may take an injective resolution in $\mathbf{Rep}_R\,G$, and it follows that $H^n(G,M)$ has in fact a structure of an R-module. Similarly, if M is in $\mathbf{Rep}_{(R,S)}\,G$, one may compute $H^n(G,M)$ by using an injective resolution in $\mathbf{Rep}_{(R,S)}\,G$, which will endow the cohomology groups with an S^G-module structure.

1.8.3 The Hochschild-Serre spectral sequence

Suppose that $H \subseteq G$ is a *normal* subgroup of G, and let M be a G-module. By restriction of the action, M is also an H-module and $H^i(H,M)$ has the structure of a G/H-module.

Theorem 1.8.1 (Hochschild-Serre spectral sequence)**.** *There is a spectral sequence*

$$H^p\left(G/H, H^q(H,M)\right) \implies H^{p+q}(G,M).$$

In particular, there is an exact sequence (inflation-restriction exact sequence):

$$0 \to H^1(G/H, M^H) \overset{\mathit{Inf}}{\to} H^1(G,M) \overset{\mathit{Res}}{\to} H^1(H,M)^{G/H} \to \cdots$$

1.8.4 Computation using the chain complex

Let M be a G-module, and consider the chain complex:

$$C^\bullet(G,M)\colon\quad C^0(G,M)\xrightarrow{d_0}C^1(G,M)\xrightarrow{d_1}C^2(G,M)\to\cdots,$$

where

$$C^i(G,M)\overset{\text{def}}{=}\{\text{ functions } f\colon G^i\to M\},$$

made into an abelian group using the additive structure of M. The maps d_i are defined as

$$d_i\colon C^i(G,M)\to C^{i+1}(G,M),\quad f\mapsto d_i f,$$

where

$$\begin{aligned}(d_i f)(\sigma_1,\ldots,\sigma_{i+1}) &= \sigma_1\cdot f(\sigma_2,\sigma_3,\ldots,\sigma_{i+1})+\sum_{j=1}^{i}(-1)^j f(\sigma_1,\ldots,\sigma_j\sigma_{j+1},\ldots\sigma_{i+1})+\\ &\quad +(-1)^{i+1}f(\sigma_1,\ldots,\sigma_i).\end{aligned}$$

A tedious but simple calculation shows that $d_{i+1}\circ d_i=0$, so that $C^\bullet(G,M)$ is a complex.

Theorem 1.8.2. *For each non-negative integer n, there are canonical isomorphisms*

$$H^n(G,M)\simeq H^n\left(C^\bullet(G,M)\right).$$

In particular, one can compute using this definitions:

$$H^0(G,M)=M^G,$$
$$H^1(G,M)=\frac{\{f\colon G\to M\mid f(\sigma\tau)=\sigma\cdot f(\tau)+f(\sigma),\ \text{for all } \sigma,\tau\in G\}}{\{g\colon G\to M\mid\ \text{there exists } m\in M \text{ s.t. } g(\sigma)=\sigma m-m,\ \text{for all } \sigma\}}.$$

1.8.5 Continuous cohomology

Let G be a profinite group. For example, if K is an algebraic extension of $\mathbf{Q}_p$, one may take $G=G_K=\operatorname{Gal}(\overline{K}/K)$. But note that there are some groups in which we may be interested, like $\mathrm{GL}_2(\mathbf{Q}_p)$, which are *not* profinite.

Consider the category $\mathbf{Rep}^{\text{cont}}\,G$. An object M is a topological abelian group, together with a continuous action. This means that the map $G\times M\to M$ giving the action is continuous, where $G\times M$ is given the product topology. A map $f\colon M\to N$ is a morphism in $\mathbf{Rep}^{\text{cont}}\,G$ if f is a continuous group homomorphism commuting with the action of G.

Remark. Although there is a forgetful functor $\mathbf{Rep}^{\text{cont}}\,G\to\mathbf{Rep}\,G$, it is rarely used.

We will be primarily interested in simpler subcategories of $\mathbf{Rep}^{\mathrm{cont}}\, G$. In these cases there are simpler definitions of continuous cohomology. At the present level of generality one defines continuous cohomology using continuous cochains. Let M be a continuous G-module and consider the chain complex:

$$C^\bullet_{\mathrm{cont}}(G,M)\colon \quad C^0_{\mathrm{cont}}(G,M) \xrightarrow{d_0} C^1_{\mathrm{cont}}(G,M) \xrightarrow{d_1} C^2_{\mathrm{cont}}(G,M) \to \cdots ,$$

where

$$C^i_{\mathrm{cont}}(G,M) \stackrel{\mathrm{def}}{=} \{\text{ continuous functions } f\colon G^i \to M\},$$

made into an abelian group using the additive structure of M. The maps d_i are defined as before:

$$d_i\colon C^i_{\mathrm{cont}}(G,M) \to C^{i+1}_{\mathrm{cont}}(G,M), \quad f \mapsto d_i f,$$

where

$$\begin{aligned}(d_i f)(\sigma_1,\ldots,\sigma_{i+1}) \;&=\; \sigma_1 \cdot f(\sigma_2,\sigma_3,\ldots,\sigma_{i+1}) + \sum_{j=1}^{i}(-1)^j f(\sigma_1,\ldots,\sigma_j\sigma_{j+1},\ldots \sigma_{i+1}) \\ &\quad +(-1)^{i+1} f(\sigma_1,\ldots,\sigma_i).\end{aligned}$$

The **continuous cohomology groups** are defined as

$$H^n_{\mathrm{cont}}(G,M) \stackrel{\mathrm{def}}{=} H^n\left(C^\bullet_{\mathrm{cont}}(G,M)\right).$$

It is easy to check that $H^0_{\mathrm{cont}}(G,M) = M^G$. However, the family $\{H^n_{\mathrm{cont}}(G,-)\}_{n\geq 0}$ is *not* a cohomological δ-functor. It satisfies a weaker property:[4]

Theorem 1.8.3. *Let*

$$0 \to M_1 \to M_2 \xrightarrow{g} M_3 \to 0$$

be an exact sequence in $\mathbf{Rep}^{\mathit{cont}}\, G$. *Assume that there is a continuous group homomorphism* $s\colon M_3 \to M_2$, not necessarily commuting with the G-action, *such that* s *is a section to* g. *That means that* $g \circ s = \mathit{Id}_{M_3}$. *Then there is a long exact sequence of abelian groups*

$$\cdots \to H^n_{\mathit{cont}}(G,M_1) \to H^n_{\mathit{cont}}(G,M_2) \to H^n_{\mathit{cont}}(G,M_3) \xrightarrow{\delta_n} H^{n+1}_{\mathit{cont}}(G,M_1) \to \cdots .$$

We will apply this theorem later in the course to what will be called the fundamental exact sequence for period rings. Also, suppose that $H \subseteq G$ is a *closed, normal* subgroup. Then one can find sections to the restriction map and one obtains again the inflation-restriction exact sequence.

[4] **FIXME:** Explain better the problem here.

1.8.6 Distinguished subcategories of $\mathbf{Rep}^{\mathrm{cont}}\, G$

In this subsection we discuss subcategories of $\mathbf{Rep}^{\mathrm{cont}}\, G$ that allow us to work with limits of cohomology of finite groups. First consider the category $\mathbf{Rep}^{\mathrm{disc}}\, G$ of **discrete topological abelian groups** M, together with a continuous G-action. It is a full subcategory of $\mathbf{Rep}^{\mathrm{cont}}\, G$.

Remark. Given a discrete abelian group M with a G-action, the continuity of the action is equivalent to the fact that, for all $m \in M$, the stabilizer of m in G is an open subgroup of G.

Let M be an object in $\mathbf{Rep}^{\mathrm{disc}}\, G$, and let $H \subseteq G$ be an *open, normal* subgroup. Then M^H has a natural structure of G/H-module and

$$M = \bigcup_{\substack{H \subseteq G \\ H \text{ open, normal}}} M^H.$$

Moreover, if $H' \subseteq H \subseteq G$ are both open, normal subgroups of G, then there is a surjection $G/H' \twoheadrightarrow G/H$, and $M^H \subseteq M^U$. This gives maps for all $n \geq 0$,

$$H^n(G/H, M^H) \to H^n(G/H', M^{H'}),$$

which yield an inductive system.

The following theorem reduces the computation of continuous group cohomology to that of finite group cohomology:

Theorem 1.8.4. *Let M be a discrete G-module. Then there are canonical isomorphisms*

$$H^n_{cont}(G, M) \simeq \varinjlim_{H \subseteq G} H^n(G/H, M^H), \quad \textit{for all } n \geq 0,$$

where the injective limit is taken over all open, normal subgroups $H \subseteq G$.

We can generalize the previous construction by enlarging the category we consider. Let $(\mathbf{Rep}^{\mathrm{disc}}\, G)^{\mathbf{N}}$ denote the category having as objects projective systems of discrete modules

$$(M_0 \longleftarrow M_1 \longleftarrow M_2 \longleftarrow \cdots)$$

and as morphisms families $\{h_i\}_{i \geq 0}$ of morphisms of discrete representations of G, such that the resulting diagrams commute:

$$\begin{array}{ccccccc} M_0 & \longleftarrow & M_1 & \longleftarrow & M_2 & \longleftarrow & \cdots \\ \downarrow{\scriptstyle h_0} & & \downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \\ N_0 & \longleftarrow & N_1 & \longleftarrow & N_2 & \longleftarrow & \cdots \end{array}$$

There is a functor from $(\mathbf{Rep}^{\mathrm{disc}}\, G)^{\mathbf{N}}$ to $\mathbf{Rep}^{\mathrm{cont}}\, G$, which takes a projective system to the corresponding projective limit. There is also a functor $F^{\mathbf{N}}$ mapping $(\mathbf{Rep}^{\mathrm{disc}}\, G)^{\mathbf{N}}$ to $\mathbf{Ab}$, which on objects is

$$F^{\mathbf{N}}(M_0 \leftarrow M_1 \leftarrow M_2 \leftarrow \cdots) = \left(\varprojlim_i M_i\right)^G .$$

For the sake of brevity we begin denoting projective systems as sets $\{M_n\}_{n\geq 0}$, or even just $\{M_n\}$. The projective limit functor is left exact in general. We write $\varprojlim^{(n)}$ for $n \in \mathbf{N}$ to denote the nth right derived functor of $\varprojlim$. The following is a sufficient condition for $\varprojlim$ to preserve an exact sequence:

Definition 1.8.5. Let $\{A_n\}$ be a projective system of abelian groups with transition homomorphisms $u_n \colon M_{n+1} \to M_n$. We say that $\{A_n\}$ satisfies the **ML condition**, for Mittag-Leffler, if for every $n \geq 0$ the decreasing sequence of subgroups:

$$\left\{U_n^{(m)} = (u_n \circ u_{n+1} \circ \cdots \circ u_m)(M_{m+1}) \mid m > n\right\}$$

is stationary.

For instance, if the transition morphisms u_n above are surjective, then $U_n^{(m)} = A_n$ for all $m > n$. In this case the ML condition is trivially satisfied. Another simple case is when the groups A_n are all finite or, more generally, when they all satisfy the decreasing chain condition. The ML condition is immediate in this case.

Below we will sometimes discuss the ML condition for modules over rings; in this context one forgets any extra structure and regards the objects as abelian groups.

Lemma 1.8.6. *Let $\{A_n\}$ be a projective system of abelian groups which satisfies ML. Then $\varprojlim^{(1)} A_n = 0$.*

In particular, if $\{B_n\}$ and $\{C_n\}$ are projective systems of abelian groups and the sequence:

$$0 \to \{A_n\} \to \{B_n\} \to \{C_n\} \to 0$$

is exact, then the resulting sequence of abelian groups:

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$$

is exact.

Theorem 1.8.7. *1. Let $\{M_n\} \in (\mathbf{Rep}^{disc}\, G)^{\mathbf{N}}$ satisfy the ML condition. Put $M = \varprojlim M_n$. Then there are canonical isomorphisms*

$$H^n_{cont}(G, M) \simeq R^n F^{\mathbf{N}}\left(\{M_n\}\right)$$

for all $n \geq 0$.

2. *Moreover, suppose that:*

$$0 \to \{R_n\} \to \{S_n\} \to \{M_n\} \to 0$$

is exact in $(\mathbf{Rep}^{disc} G)^{\mathbf{N}}$*, and that the three projective systems satisfy the ML condition. Then if we put* $R = \varprojlim R_n$*,* $S = \varprojlim S_n$ *and* $M = \varprojlim M_n$*, the induced sequence:*

$$0 \to R \to S \to M \to 0$$

is exact in $\mathbf{Rep}^{cont} G$*, and the topology on* M *is the induced quotient topology of* S/R*. In particular, theorem 1.8.3 applies, and one obtains a long exact sequence in continuous cohomology.*

3. *The isomorphisms of cohomology in (1) are compatible with long exact sequences in the sense that:*

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & H^i_{cont}(G,R) & \longrightarrow & H^i_{cont}(G,S) & \longrightarrow & H^i_{cont}(G,M) & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & (R^i F^{\mathbf{N}})(\{R_n\}) & \longrightarrow & (R^i F^{\mathbf{N}})(\{S_n\}) & \longrightarrow & (R^i F^{\mathbf{N}})(\{M_n\}) & \longrightarrow & \cdots \end{array}$$

commutes.

Since $F^{\mathbf{N}}$ is a composition of left exact functors, one can use the Leray spectral sequence, and the fact that the higher derived functors of $\varprojlim$ vanish (see [Wei94]) to prove:

Theorem 1.8.8. *Given* $\{M_n\} \in (\mathbf{Rep}^{disc} G)^{\mathbf{N}}$*, there are exact sequences for all* $i \geq 1$*:*

$$0 \to \varprojlim{}^{(1)} H^{i-1}_{cont}(G, M_n) \to (R^i F^{\mathbf{N}})(\{M_n\}) \to \varprojlim H^i_{cont}(G, M_n) \to 0.$$

The proofs of these claims can be found in [Jan88].

Remark. Note in particular that if $\{M_n\}$ satisfies ML, and for some $i \geq 1$ the projective system of abelian groups $\{H^{i-1}_{\mathrm{cont}}(G, M_n)\}$ satisfies ML, then:

$$\varprojlim{}^{(1)} H^{i-1}_{\mathrm{cont}}(G, M_n) = 0$$

and the preceding two theorems give:

$$H^i_{\mathrm{cont}}(G, \varprojlim M_n) \simeq \varprojlim H^i_{\mathrm{cont}}(G, M_n).$$

We end this section by discussing a technical condition that will be useful in subsequent computations. Our terminology is presently nonstandard.

Definition 1.8.9. Let $\{A_n, d_n\}$ be a projective system in $(\mathbf{Mod}_{\mathcal{O}_L})^{\mathbf{N}}$. We say that $\{A_n, d_n\}$ is **almost ML** if for every $a \in \mathfrak{m}_L$, one has $a \operatorname{coker} d_n = 0$.

[5]

Note that if the cokernels vanish, then $\{A_n, d_n\}$ is a projective system with surjective transition maps, and hence ML. This explains the choice of terminology.

The importance of the almost ML condition is encapsulated in the following:

Lemma 1.8.10. *If $\{A_n\}$ is almost ML, then $\varprojlim^{(1)} A_n$ is annihilated by every $a \in \mathfrak{m}_L$.*

Proof. $\square$

One can regard this lemma as saying that if $\{A_n\}$ is almost ML, then $\varprojlim^{(1)} A_n$ is almost zero.

1.9 Cohomology of $\mathbf{C}_p$

One can prove that there is a bijection

$$\{\text{subfields } \mathbf{Q}_p \subseteq K \subseteq \overline{\mathbf{Q}}_p\} \longleftrightarrow \{\text{complete subfields } \mathbf{Q}_p \subseteq L \subseteq \mathbf{C}_p\}$$

where to a subfield $K \subseteq \mathbf{Q}_p$ one assigns its completion $\widehat{K}$, and to a complete subfield L one assigns $K = L \cap \overline{\mathbf{Q}}_p$. Moreover, if K is a subfield of $\overline{\mathbf{Q}}_p$ and $G_K = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$, then:

$$\mathbf{C}_p^{G_K} = \widehat{K}.$$

This provides us with a Galois theory for $\mathbf{C}_p$ which relates complete subfields of $\mathbf{C}_p$ and closed subgroups of $G_{\mathbf{Q}_p}$. All of this follows quite easily from a theorem of Ax. This result can be stated equivalently as:

$$H^0_{\mathrm{cont}}(K, \mathbf{C}_p) = \mathbf{C}_p^{G_K} = \widehat{K}.$$

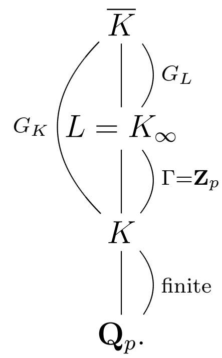
We want to compute the higher cohomology groups $H^i_{\mathrm{cont}}(K, \mathbf{C}_p)$, for all $i \geq 0$, using the cohomological machinery developed above.

Notation. Fix a finite extension $K/\mathbf{Q}_p$ and $L = K_\infty$ a totally ramified $\mathbf{Z}_p$-extension of K. Write $\Gamma = \mathrm{Gal}(L/K)$, so that $\Gamma \simeq \mathbf{Z}_p$. Let $\gamma \in \Gamma$ be a topological generator.

We begin by treating the totally ramified $\mathbf{Z}_p$-extension L of K, and will subsequently descend our results using the Hochschild-Serre spectral sequence. The following diagram

[5] **FIXME:** Should call it "almost surjective" instead...

shows the fields under consideration, and the corresponding Galois groups:



Let W be an $\mathcal{O}_{\overline{K}}$-module with the discrete topology and a continuous semilinear action of $G_L = \mathrm{Gal}(\overline{K}/L)$. Note that:

$$W \in \mathbf{Rep}^{\mathrm{disc}}_{(\mathcal{O}_L, \mathcal{O}_{\overline{K}})}(G_L).$$

Remark. The natural induced G_L-action on $\mathcal{O}_{\overline{K}}$, or even $\overline{K}$, is continuous for the discrete topology, and hence for any topology on $\mathcal{O}_{\overline{K}}$. To see this simply note that if $x \in \mathcal{O}_{\overline{K}}$, then in fact $x \in \mathcal{O}_F$ for some finite extension F/L and hence:

$$G_F \subset \mathrm{Stab}_{G_L}(x).$$

Since G_F is open in G_L, it is of finite index. Hence the stabilizer of x in G_L is *also* of finite index, thus open. Note that this result does not hold for $\mathbf{C}_p$.

We begin with a key lemma:

Lemma 1.9.1. *For every $a \in \mathfrak{m}_L$, one has $aH^i_{cont}(G_L, W) = 0$ for all $i \geq 1$.*

Proof. Recall that since W is a discrete $\mathcal{O}_{\overline{K}}$ module with continuous G_L-action, one has:

$$H^i_{\mathrm{cont}}(G_L, W) \simeq \varinjlim_{F/L \text{ finite Galois}} H^i(\mathrm{Gal}(F/L), W^{G_F})$$

for all $i \geq 1$. We may hence fix a finite Galois extension F/L, put $G = \mathrm{Gal}(F/L)$ and show that every $a \in \mathfrak{m}_L$ annihilates $H^i(\mathrm{Gal}(F/L), W^{G_F})$. Write $X = W^{G_F}$, which is a $\mathcal{O}_F$-module with semilinear G-action; hence $X \in \mathbf{Rep}_{(\mathcal{O}_L, \mathcal{O}_F)}(G)$.

In section 1.4 we observed that:

$$\mathfrak{m}_L \mathcal{O}_{\overline{K}} = \mathfrak{m}_{\overline{K}}.$$

Intersecting this with $\mathcal{O}_F$ gives $\mathfrak{m}_F = \mathfrak{m}_L \mathcal{O}_F$. By theorem 1.4.5 we deduce that:

$$\mathfrak{m}_L \subset \mathrm{Tr}_{F/L}(\mathcal{O}_F).$$

So take $a \in \mathfrak{m}_L$ and write it as $a = \mathrm{Tr}_{F/L}(b)$ for some $b \in \mathcal{O}_F$.

Let:

$$0 \to X \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \to \cdots$$

be an injective resolution of X in $\mathbf{Rep}_{(\mathcal{O}_L,\mathcal{O}_F)}(G)$. If we write d'_n for the restriction of d_n to $(I^n)^G$ then:

$$H^n(G,X) = \ker d'_n / \operatorname{im} d'_{n-1}$$

for all $n \geq 1$. Consider the commutative diagram:

$$\begin{array}{ccccc} I^{n-1} & \xrightarrow{d^{n-1}} & I^n & \xrightarrow{d^n} & I^{n+1} \\ \downarrow & & \downarrow & & \downarrow \\ (I^{n-1})^{G_L} & \xrightarrow{d'_{n-1}} & (I^n)^{G_L} & \xrightarrow{d^n} & (I^{n+1})^{G_L} \end{array}$$

where the vertical maps are the natural inclusions. Represent an element of $H^n(G,X)$ by some $x \in \ker d'_n$, so that also $d_n(x) = 0$. Since the top row is exact, we may take $y \in I^{n-1}$ with $d^{n-1}(y) = x$. Now, y may not be G-invariant. The trick is to average $by \in I^{n-1}$ over the finite group G to obtain:

$$y' = \sum_{\sigma \in G} \sigma(by) \in (I^{n-1})^G.$$

But now, since x is G-invariant, one easily computes:

$$\begin{aligned} d_{n-1}(y') &= \sum_{\sigma \in G} \sigma(bd_{n-1}(y)) \\ &= \sum_{\sigma \in G} \sigma(bx) \\ &= \left(\sum_{\sigma \in G} \sigma(b) \right) x \\ &= ax. \end{aligned}$$

Hence $ax \in \operatorname{im} d_{n-1}$, so that the class of ax is zero in $H^n(G,X)$. This shows that each $a \in \mathfrak{m}_L$ annihilates $H^n(G,X)$ for all $n \geq 1$ and concludes the proof of the lemma. □

The next two results now follow formally from the cohomological machinery developed above:

Theorem 1.9.2. *With L as above, $\mathbf{C}_p^{G_K} = \widehat{L}$.*

Proof. For all $n \geq 1$ we have commutative diagrams with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_{\overline{K}} & \xrightarrow{p^n} & \mathcal{O}_{\overline{K}} & \longrightarrow & \mathcal{O}_{\overline{K}}/p^n\mathcal{O}_{\overline{K}} & \longrightarrow & 0 \\ & & \uparrow p & & \| & & \uparrow & & \\ 0 & \longrightarrow & \mathcal{O}_{\overline{K}} & \xrightarrow{p^{n+1}} & \mathcal{O}_{\overline{K}} & \longrightarrow & \mathcal{O}_{\overline{K}}/p^{n+1}\mathcal{O}_{\overline{K}} & \longrightarrow & 0 \end{array}$$

Here the maps labeled with p^i denote multiplication by p^i. The unlabeled maps are the natural projections. Note that these maps all commute with the G_L-action since $p \in \mathbf{Q}_p$. Since the G_L-action is continuous for the *discrete* topologies above, we deduce that there are corresponding long exact sequences of continuous cohomology:

$$\begin{array}{ccccccccc} 0 \longrightarrow & (\mathcal{O}_{\overline{K}})^{G_L} & \xrightarrow{p^n} & (\mathcal{O}_{\overline{K}})^{G_L} & \longrightarrow & (\mathcal{O}_{\overline{K}}/p^n\mathcal{O}_{\overline{K}})^{G_L} & \longrightarrow & H^1_{\mathrm{cont}}(G_L, \mathcal{O}_{\overline{K}}) & \longrightarrow \cdots \\ & \uparrow{\scriptstyle p} & & \| & & \uparrow & & \uparrow{\scriptstyle p} & \\ 0 \longrightarrow & (\mathcal{O}_{\overline{K}})^{G_L} & \xrightarrow{p^{n+1}} & (\mathcal{O}_{\overline{K}})^{G_L} & \longrightarrow & (\mathcal{O}_{\overline{K}}/p^{n+1}\mathcal{O}_{\overline{K}})^{G_L} & \longrightarrow & H^1_{\mathrm{cont}}(G_L, \mathcal{O}_{\overline{K}}) & \longrightarrow \cdots \end{array}$$

such that the above diagram commutes. Hence for each $n \geq 1$ we have a commutative diagram of abelian groups with exact rows:

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathcal{O}_L/p^n\mathcal{O}_L & \longrightarrow & (\mathcal{O}_{\overline{K}}/p^n\mathcal{O}_{\overline{K}})^{G_L} & \longrightarrow & H^1_{\mathrm{cont}}(G_L, \mathcal{O}_{\overline{K}}) \\ & \uparrow & & \uparrow & & \uparrow{\scriptstyle p} \\ 0 \longrightarrow & \mathcal{O}_L/p^{n+1}\mathcal{O}_L & \longrightarrow & (\mathcal{O}_{\overline{K}}/p^{n+1}\mathcal{O}_{\overline{K}})^{G_L} & \longrightarrow & H^1_{\mathrm{cont}}(G_L, \mathcal{O}_{\overline{K}}) \end{array}$$

Note that the leftmost vertical map is the natural projection, as it is induced from the identity on $(\mathcal{O}_{\overline{K}})^{G_L} = \mathcal{O}_L$. Since $p \in \mathfrak{m}_L$, Lemma 1.9.1 implies that the rightmost vertical map is trivial. Hence:

$$\varprojlim H^1_{\mathrm{cont}}(G_L, \mathcal{O}_{\overline{K}}) = 0,$$

for the rightmost projective system appearing in the diagram above. Taking projective limits of the diagram, which is a left exact operation, thus gives an isomorphism:

$$\mathcal{O}_{\widehat{L}} \simeq \varprojlim \mathcal{O}_L/p^n\mathcal{O}_L \simeq \varprojlim (\mathcal{O}_{\overline{K}}/p^n\mathcal{O}_{\overline{K}})^{G_L} \simeq (\mathcal{O}_{\mathbf{C}_p})^{G_L}.$$

The last isomorphism follows by commuting projective limits with Galois invariants. This can be done since the G_L acts componentwise on the projective limit, when regarded as a subset of the product of the modules in the projective system. Inverting p then gives $\widehat{L} \simeq (\mathbf{C}_p)^{G_L}$. □

Remark. Note that:

$$H^1_{\mathrm{cont}}(G_L, \mathcal{O}_{\overline{K}}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \simeq H^1_{\mathrm{cont}}(G_L, \overline{K}),$$

and this is trivial by Hilbert 90. It follows that $H^1_{\mathrm{cont}}(G_L, \mathcal{O}_{\overline{K}})$ is a torsion $\mathbf{Z}_p$-module. This does not imply, however, that:

$$\varprojlim H^1_{\mathrm{cont}}(G_L, \mathcal{O}_{\overline{K}}) = 0,$$

where the transition maps for the projective system are given by multiplication by p as above. It would imply this if $H^1_{\mathrm{cont}}(G_L, \mathcal{O}_{\overline{K}})$ were furthermore finitely generated, but this is not true in general.

Theorem 1.9.3. *If V is a p-adic representation of G_L, then:*

$$H^i_{cont}(G_L, V \otimes_{\mathbf{Q}_p} \mathbf{C}_p) = 0$$

for all $i \geq 1$.

Proof. Recall that there exists a G_L-stable $\mathbf{Z}_p$-lattice $T \subset V$. For each $n \geq 0$ write:

$$M_n = (T \otimes_{\mathbf{Z}_p} \mathcal{O}_{\mathbf{C}_p})/p^{n+1}(T \otimes_{\mathbf{Z}_p} \mathcal{O}_{\mathbf{C}_p}),$$

which is a discrete G_L-representation.

We begin with the case $i = 1$. Lemma 1.9.1 applies, so that for all $a \in \mathfrak{m}_L$:

$$aH^1_{\text{cont}}(G_L, M_n) = 0.$$

The natural projection maps make $\{M_n\}$ an object in $(\mathbf{Rep}^{\text{disc}}\, G_L)^{\mathbf{N}}$. Since the projection maps are surjective, it trivially satisfies the ML condition. One can show that $\{M_n^{G_L}\}$ is almost ML (we will add a proof after we have completed homework 2).[6] We may hence apply Theorem 1.8.8 to obtain the exact sequence:

$$0 \to \varprojlim{}^{(1)}\{M_n^{G_L}\} \to H^1_{\text{cont}}(G_L, \varprojlim M_n) \to \varprojlim H^1_{\text{cont}}(G_L, M_n) \to 0.$$

Take $a \in \mathfrak{m}_L$ and choose $\alpha \in v(L^\times)$ such that $\alpha \leq v(a)/2$; this is possible since L/K is a totally ramified $\mathbf{Z}_p$-extension. Since $\{M_n^{G_L}\}$ is almost ML, p^α annihilates the leftmost term. Similarly, the Lemma 1.9.1 implies that p^α annihilates the cokernel. It follows that $p^{2\alpha}$ annihilates $H^1_{\text{cont}}(G_L, \varprojlim M_n)$. By choice of α we see that also $aH^1_{\text{cont}}(G_L, \varprojlim M_n) = 0$. This holds for all $a \in \mathfrak{m}_L$, so inverting p kills the group

$$H^1_{\text{cont}}(G_L, \varprojlim M_n).$$

But $\varprojlim M_n$ is isomorphic to $T \otimes_{\mathbf{Z}_p} \mathcal{O}_{\mathbf{C}_p}$, and hence:

$$0 = H^1_{\text{cont}}(G_L, T \otimes_{\mathbf{Z}_p} \mathcal{O}_{\mathbf{C}_p}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \simeq H^1_{\text{cont}}(G_L, V \otimes_{\mathbf{Q}_p} \mathbf{C}_p).$$

This concludes the proof when $i = 1$.

Suppose now that $i \geq 2$. In this case Lemma 1.9.1 implies that each $H^{i-1}_{\text{cont}}(G_L, M_n)$ is killed by every $a \in \mathfrak{m}_L$, and so $\{H^{i-1}_{\text{cont}}(G_L, M_n)\}_{n \geq 0}$ is a fortiori almost ML. The proof proceeds as above. □

1.9.1 Computing Γ-cohomology

Let us fix a p-adic representation V as above, and turn our attention towards understanding $H^i_{\text{cont}}(G_K, V \otimes_{\mathbf{Q}_p} \mathbf{C}_p)$. Theorem 1.9.3 immediately implies that the Hochschild-Serre spectral sequence:

$$H^i_{\text{cont}}\left(\Gamma, H^j_{\text{cont}}(G_L, V \otimes_{\mathbf{Q}_p} \mathbf{C}_p)\right) \implies H^{i+j}_{\text{cont}}(G_K, V \otimes_{\mathbf{Q}_p} \mathbf{C}_p)$$

[6] **FIXME:** add a proof

degenerates at the first step and gives isomorphisms:

$$H^i_{\mathrm{cont}}\left(\Gamma, (V \otimes_{\mathbf{Q}_p} \mathbf{C}_p)^{G_L}\right) \simeq H^i_{\mathrm{cont}}(G_K, V \otimes_{\mathbf{Q}_p} \mathbf{C}_p)$$

for all $i \geq 0$. In the case $i = 0$ this is just the obvious identification:

$$(V \otimes_{\mathbf{Q}_p} \mathbf{C}_p)^{G_K} \simeq \left((V \otimes_{\mathbf{Q}_p} \mathbf{C}_p)^{G_L}\right)^{\Gamma},$$

and for $i = 1$ the isomorphism is given by the inflation-restriction exact sequence.

This identification translates our problem to the problem of computing the cohomology of a continuous Γ-module W. Although the methods we use below are quite general, we suppose for simplicity that $W \simeq \varprojlim W_n$, where the W_n's are discrete Γ-representations. Consider the following complex concentrated on degrees 0 and 1, which depends on the choice of the topological generator $\gamma \in \Gamma$.

$$C^\bullet(\gamma, W): \quad W \xrightarrow{\gamma - 1} W$$

given by $x \mapsto \gamma x - x$.

Theorem 1.9.4. *For each $i \geq 0$, there is a canonical isomorphism*

$$H^i_{cont}(\Gamma, W) \simeq H^i(C^\bullet(\gamma, W))$$

Proof. Let X be a discrete representation of Γ. The the cohomological δ-functors $H^i_{\mathrm{cont}}(\Gamma, -)$ and $H^i(C^\bullet(\gamma, -))$ agree at $i = 0$ and they are universal (because they are effaąble), so a theorem of Grothendieck gives the canonical isomorphisms for $i \geq 0$.

For general $\{W_n, d_n\}$, still there is an isomorphism

$$H^0_{\mathrm{cont}}(\Gamma, W) \simeq H^0(C^\bullet(\gamma, W)) = W^{\gamma = \mathrm{Id}}.$$

The ML condition and Theorem 1.8.8 give exact sequences, for each $i \geq 1$:

$$0 \to \varprojlim{}^{(1)} H^{i-1}_{\mathrm{cont}}(\Gamma, W_n) \to H^i_{\mathrm{cont}}(\Gamma, W) \to \varprojlim_n H^i_{\mathrm{cont}}(\Gamma, W_n) \to 0.$$

For $i = 1$ we have

$$\varprojlim_n H^1_{\mathrm{cont}}(\Gamma, W_n) \simeq \varprojlim_n (W_n/(\gamma - 1)W_n) \simeq W/(\gamma - 1)W,$$

and thus we get a surjective map

$$H^1_{\mathrm{cont}}(\Gamma, W) \twoheadrightarrow W/(\gamma - 1)W.$$

This map is also injective because of the diagram

$$\begin{array}{ccccccc}
\mathcal{C}^0(\Gamma, W) & \xrightarrow{d_0} & \ker d_1 & \longrightarrow & H^1_{\mathrm{cont}}(\Gamma, W) & \longrightarrow & 0 \\
\| & & \downarrow & & \downarrow & & \\
W & \xrightarrow{\gamma - 1} & W & \longrightarrow & W/(\gamma - 1)W & \longrightarrow & 0
\end{array}$$

in which the middle map sends $f \in \ker d_1$ to $f(\gamma)$.

For $i = 2$, note that $H^2_{\mathrm{cont}}(\Gamma, W_n) = 0$ for all n, and that $\{W_n/(\gamma-1)W_n\}$ satisfies the ML condition, so that its $\varprojlim^{(1)}$ vanishes. Theorem 1.8.8 implies that $H^2_{\mathrm{cont}}(\Gamma, W)$ is zero, agreeing with $H^2(C^\bullet(\gamma, W))$. For $i \geq 3$, both cohomologies vanish, and so the result holds as well. $\square$

In particular we have the identities:

$$\begin{aligned} H^0_{\mathrm{cont}}(\Gamma, W) &= \ker(\gamma - 1), \\ H^1_{\mathrm{cont}}(\Gamma, W) &= W/(\gamma-1)W, \\ H^i_{\mathrm{cont}}(\Gamma, W) &= 0 \quad \text{for } i \geq 2. \end{aligned}$$

The last identity above reflects the fact that Γ is procyclic, and hence has cohomological dimension 1.

Fix a continuous homomorphism $\phi\colon \Gamma \to \mathcal{O}_K^\times$. Continuity implies that ϕ is determined by $\phi(\gamma) = \lambda^{-1}$. The image of ϕ is either finite or infinite, and in either case it is topologically generated by a single element. We will suppose that ϕ has infinite image. In particular, ϕ is nontrivial.

Recall that there is a natural isomorphism of topological groups:

$$\mathcal{O}_K^\times \simeq (\mathbf{Z}/(q-1)\mathbf{Z}) \times \mathcal{O}_K,$$

where q is the residue degree of $K/\mathbf{Q}_p$. If π is a uniformizer for $K/\mathbf{Q}_p$, then one can express $x \in \mathcal{O}_K^\times$ uniquely as $\zeta(1+\pi y)$, where ζ is a $(q-1)$th root of unity, and $y \in \mathcal{O}_K$. Mapping $x \mapsto (\zeta, y)$ gives the isomorphism above. This decomposition makes it clear that since $\phi(\Gamma)$ is infinite and topologically generated by a single element, then we must have:

$$\phi(\Gamma) \subset 1 + \mathfrak{m}_K \simeq \{1\} \times \mathcal{O}_K.$$

We will regard ϕ as a continuous character $G_K \to \mathcal{O}_K^\times$ via the natural projection $G_K \to \Gamma$. Note that then $G_L \subseteq \ker\phi$ since ϕ factors through $\mathrm{Gal}(L/K)$. In fact, if ϕ has infinite image then G_L *equals* $\ker\phi$. Let $V = K(\phi)$, which is K as a vectorspace and has the G_K action:

$$\sigma(x) = \phi(\sigma)x.$$

Then $V \otimes_K \mathbf{C}_p \simeq \mathbf{C}_p(\phi)$, and G_K acts semilinearly on $\mathbf{C}_p(\phi)$ as:

$$\sigma \cdot x = \phi(\sigma)\sigma(x).$$

In particular, if $\sigma \in G_L$ then $\sigma \cdot x = \sigma(x)$, so that the two actions of G_L agree. The identity map $\mathbf{C}_p(\phi) \simeq \mathbf{C}_p$ is an isomorphism of G_L-modules, but not as G_K-modules. Note that:

$$(V \otimes \mathbf{C}_p)^{G_L} = (\mathbf{C}_p(\phi))^{G_L} = (\mathbf{C}_p^{G_L})(\phi) = \widehat{L}(\phi),$$

where the middle equality follows from the inclusion $G_L \subset \ker\phi$. We would thus like to compute $H^i_{\mathrm{cont}}(\Gamma, \widehat{L}(\phi))$.

For this we specialize the complex discussed above to the case $W = \widehat{L}(\phi)$:

$$C^\bullet(\Gamma, \widehat{L}(\phi)) : \widehat{L}(\phi) \xrightarrow{\gamma-1} \widehat{L}(\phi).$$

Consider a second complex:

$$C'^\bullet : \widehat{L} \xrightarrow{\gamma-\lambda} \widehat{L}.$$

A trivial verification shows that the diagram

$$\begin{array}{ccc} \widehat{L}(\phi) & \xrightarrow{\gamma-1} & \widehat{L}(\phi) \\ {\scriptstyle 1}\uparrow & & \uparrow{\scriptstyle \lambda^{-1}} \\ \widehat{L} & \xrightarrow{\gamma-\lambda} & \widehat{L} \end{array}$$

commutes. As the vertical maps are isomorphisms of vectorspaces, this chain map is an isomorphism of complexes, so that:

$$H^i_{\text{cont}}(\Gamma, \widehat{L}(\phi)) \simeq H^i(C^\bullet) \simeq H^i(C'^\bullet).$$

Thus, we should study the map $\gamma - \lambda$ on $\widehat{L}$. For this we must return to the study of ramification.

1.9.2 The trace map $t\colon L \to K$

Since L/K is a totally ramified $\mathbf{Z}_p$-extension, every $x \in L$ belongs to K_n for some n. We can hence put:

$$t(x) = \frac{1}{p^n} \operatorname{Tr}_{K_n/K}(x) \in K.$$

Since each K_{n+1}/K_n is totally ramified of degree p, and since:

$$\operatorname{Tr}_{K_{n+1}/K} = \operatorname{Tr}_{K_n/K} \circ \operatorname{Tr}_{K_{n+1}/K_n},$$

it follows that $t(x)$ does not depend on the choice of K_n with $x \in K_n$. It thus gives a well-defined function:

$$t\colon L \to K$$

which is easily seen to be K-linear. If we write $i\colon K \to L$ for the natural injection, then $t \circ i = \mathrm{Id}_K$. It follows that t is surjective and i gives a splitting. Our first goal is to establish the continuity of t, in order to extend it to a continuous map $\widehat{L} \to K$. It turns out that this map is related to $\gamma - 1$.

We begin with a simple lemma:

Lemma 1.9.5. *For $n \geq 0$, let σ denote a generator of $\operatorname{Gal}(K_{n+1}/K_n)$. Then for all $x \in K_{n+1}$:*

$$\left| x - \frac{1}{p} \operatorname{Tr}_{K_{n+1}/K_n}(x) \right| \leq p \left| \sigma(x) - x \right|.$$

[7]

Proof. The proof is a simple computation:

$$\begin{aligned}\left|px - \mathrm{Tr}_{K_{n+1}/K_n}(x)\right| &= \left|px - \sum_{i=0}^{p-1}\sigma^i(x)\right| \\ &= \left|\sum_{i=0}^{p-1}(1-\sigma^i)(x)\right| \\ &= \left|\sum_{i=0}^{p-1}(1+\sigma+\cdots+\sigma^{i-1})((1-\sigma)x)\right| \\ &= \left|\sum_{i=0}^{p-1}\sum_{j=0}^{i-1}\sigma^j((1-\sigma)x)\right| \\ &\leq \left|\sigma x - x\right|,\end{aligned}$$

by the strong triangle inequality and since each σ^j is an isometry. □

The following proposition is fundamental for what follows:

Proposition 1.9.6. *There exists a constant $d > 0$ depending only on L, such that for all $x \in L$:*

$$|x - t(x)| \leq d\,|\gamma x - x|.$$

Proof. We will show, by induction on n, that for $x \in K_n$:

$$|x - t(x)| \leq c_n\,|\gamma x - x|,$$

where $c_{n+1} = p^{ap^{-n}}c_n$, $c_0 = p$ and a is a constant. The case $n = 0$ was treated in the preceding lemma.

Next take $x \in K_{n+1}$ and note that:

$$|x - t(x)| \leq \sup\{\left|x - (1/p)\,\mathrm{Tr}_{K_{n+1}/K_n}\right|, \left|t(x) - (1/p)\,\mathrm{Tr}_{K_{n+1}/K_n}\right|\}.$$

We bound each of the values in the set. The first is easy; take $\sigma = \gamma^{p^n}$ as a generator for $\mathrm{Gal}(K_{n+1}/K_n)$ and deduce the bound:

$$\begin{aligned}\left|x - (1/p)\,\mathrm{Tr}_{K_{n+1}/K_n}(x)\right| &\leq p\left|\gamma^{p^n}x - x\right| \\ &= p\left|(\gamma^{p^n-1}+\gamma^{p^n-2}+\cdots+1)(\gamma-1)(x)\right| \\ &\leq p\,|\gamma x - x|.\end{aligned}$$

[7] **FIXME:** We changed —p— to 1/p

If we put $y = (1/p)\,\mathrm{Tr}_{K_{n+1}/K_n}(x)$, then $y \in K_n$ and so:

$$\begin{aligned} t(y) &= (1/p^n)\,\mathrm{Tr}_{K_n/K}(y) \\ &= (1/p^n)\,\mathrm{Tr}_{K_n/K}((1/p)\,\mathrm{Tr}_{K_{n+1}/K_n}(x)) \\ &= (1/p^{n+1})\,\mathrm{Tr}_{K_{n+1}/K}(x) \\ &= t(x). \end{aligned}$$

Hence:

$$\begin{aligned} \left|t(x) - (1/p)\,\mathrm{Tr}_{K_{n+1}/K_n}\right| &= |y - t(y)| \\ &\le c_n\,|\gamma(y) - y| \quad \text{by induction,} \\ &= c_n\left|\gamma((1/p)\,\mathrm{Tr}_{K_{n+1}/K_n}(x)) - (1/p)\,\mathrm{Tr}_{K_{n+1}/K_n}(x)\right| \\ &= pc_n\left|\mathrm{Tr}_{K_{n+1}/K_n}(\gamma x - x)\right| \end{aligned}$$

Corollary 1.4.4 yields a constant $a \ge 0$, independent of n, such that:

$$\left|\mathrm{Tr}_{K_{n+1}/K_n}(\gamma x - x)\right| \le p^{ap^{-n}-1}\,|x|\,.$$

Thus:

$$\left|t(x) - (1/p)\,\mathrm{Tr}_{K_{n+1}/K_n}\right| \le pc_n \cdot p^{ap^{-n}-1}\,|x| = c_n p^{ap^{-n}}\,|x| = c_{n+1}\,|x|\,.$$

This concludes the proof. □

Remark. For a given m, replace K by K_m, so that $\gamma' = \gamma^{p^m}$ is a generator for the group $\Gamma' = \mathrm{Gal}(L/K_m)$. Similarly replace the map t by t', where t' is defined analogously to t relative to the base field K_m. Then for all $x \in L$,

$$|t'(x) - x| \le d\,|\gamma'(x) - x|\,,$$

where d is *the same constant* as in the proposition.

1.9.3 Functional analysis for dummies

Fix K a field endowed with an non-archimedean absolute value $|\cdot|$.

Definition 1.9.7. A **normed K-vectorspace** is a pair $(B, \|\cdot\|)$, where B is a K-vectorspace and

$$\|\cdot\| : B \to \mathbf{R}_{\ge 0}$$

is a map satisfying:

1. $\|x + y\| \le \max\{\|x\|, \|y\|\}$, for all $x, y \in B$.
2. $\|ax\| = |a|\,\|x\|$, for all $a \in K$ and $x \in B$.

3. $\|x\| = 0$ if and only if $x = 0$.

Such a map $\|\cdot\|$ is called a **norm** on B.

Example. In our setting of K a finite extension of $\mathbf{Q}_p$ and $L = K_\infty$ a totally ramified $\mathbf{Z}_p$-extension, the fields $L, \overline{K}, \widehat{L}, \mathbf{C}_p$, together with the natural extension of $|\cdot|$ on K, are all normed K-spaces.

Definition 1.9.8. A normed K-spaces $(B, \|\cdot\|)$ is a **Banach space** over K if B is complete with respect to the norm $\|\cdot\|$.

Definition 1.9.9. A linear map $f\colon B_1 \to B_2$ of normed K-vectorspaces is **bounded** if there exists a constant $M > 0$ such that for all $x \in B_1$

$$\|f(x)\|_{B_2} \leq M \|x\|_{B_1} .$$

We define a norm on the linear K-vectorspace $\mathrm{Hom}_{\mathrm{cont}}(B_1, B_2)$ by setting

$$\|f\| \stackrel{\text{def}}{=} \inf \left\{ M \mid \|f(x)\|_{B_2} \leq M \|x\|_{B_1} \text{ for all } x \in B_1 \right\} .$$

Lemma 1.9.10. *Let B_1 and B_2 be normed K-vectorspaces, and let $f\colon B_1 \to B_2$ be a K-linear map. Then f is continuous if and only if f is bounded.*

Example. The fields L and $\overline{K}$, with the natural norm, are not K-Banach spaces. Since they are infinite extensions of K, they are not complete. In fact, their completions are actually $\widehat{L}$ and $\mathbf{C}_p$, which become then K-Banach spaces.

We need some results from the general theory of Banach spaces.

Lemma 1.9.11. *Let B_1 and B_2 be K-Banach spaces. Let $f\colon B_1 \to B_2$ be a continuous K-linear map which is surjective. Then there exists a continuous K-linear map $s\colon B_2 \to B_1$ such that $f \circ s = Id_{B_2}$.*

Lemma 1.9.12 (Open mapping property)**.** *Let B_1 and B_2 be K-Banach spaces. Let $f\colon B_1 \to B_2$ be a continuous K-linear map which is bijective. Then $f^{-1}\colon B_2 \to B_1$ is continuous.*

1.9.4 The theorem of Tate

As the action of γ on L is continuous, the map $\gamma - 1$ is also continuous on L. Proposition 1.9.6 thus implies that the map $t - 1\colon L \to L$ is bounded, hence continuous. But $\mathrm{Id}_L\colon L \to L$ is continuous, and we conclude that $t = (t-1) + 1$ is continuous as well, being the sum of two continuous maps.

The previous discussion allows us to extend the map $t\colon L \to K$ by continuity to $t\colon \widehat{L} \to K$. Note that the natural inclusion $i\colon K \hookrightarrow \widehat{L}$ is a continuous splitting of t. Note then that t is surjective.

Let $X = \widehat{L}$, and let $X_0 = \ker t$, which is a closed subspace of X. There is an exact sequence of K-Banach spaces

$$0 \to X_0 \to X \to K \to 0,$$

and $i\colon K \to X$ yields a canonical decomposition of X:

$$X = X_0 \oplus K, \text{ as } K\text{-Banach spaces.}$$

We want to study the action of $\gamma - \mathrm{Id}$ and of $\gamma - \lambda \cdot \mathrm{Id}$ on X.

Lemma 1.9.13. *The map $\gamma - Id$ is trivial on K, and induces an isomorphism*

$$(\gamma - Id)|_{X_0}\colon X_0 \to X_0.$$

Proof. Recall that γ is a topological generator of $\Gamma = \mathrm{Gal}(L/K)$, so γ fixes K. If $x \in X_0$

$$t(\gamma(x) - x) = t(\gamma(x)) = \gamma(t(x)) = \gamma(0) = 0,$$

so that $(\gamma - \mathrm{Id})(X_0) \subseteq X_0$. It remains to show that the restriction of $\gamma - \mathrm{Id}$ induces an isomorphism on X_0.

Let $K_{n,0} = K_n \cap X_0$ and note that $K_{n,0}$ is not a subfield of K_n. It only has the structure of a *finite-dimensional* K-vectorspace. Let $K_{\infty,0} = \bigcup_{n\geq 0} K_{n,0}$, and note that $K_{\infty,0} = K_\infty \cap X_0$; in fact, $K_{\infty,0}$ is dense in X_0.

If $x \in K_{n,0}$ then

$$|\gamma(x) - x| \geq \frac{1}{d}\,|t(x) - x| = \frac{1}{d}\,|x|\,,$$

so that $\gamma(x) - x = 0$ if and only if $x = 0$. Hence the map $\gamma - \mathrm{Id}$ is injective when restricted to $K_{n,0}$, and so bijective since $K_{n,0}$ is finite-dimensional. This shows that $\gamma - \mathrm{Id}$ is a continuous and bijective map on $K_{\infty,0}$, and so its set theoretic inverse $\rho_\infty\colon K_{\infty,0} \to K_{\infty,0}$ is continuous as well, by the open mapping property (Lemma 1.9.12). The map ρ_∞ extends in a unique way to the closure of $K_{\infty,0}$, which is X_0, thus giving an inverse ρ to the map $(\gamma - \mathrm{Id})|_{X_0}$. □

Remark. For later use we give an explicit construction of ρ. Let ρ_n be the inverse of $(\gamma - \mathrm{Id})|_{K_{n,0}}$. The uniqueness of inverses implies that ρ_{n+1} agrees with ρ_n when restricted to $K_{n,0}$, so that we can define $\rho\colon K_{\infty,0} \to K_{\infty,0}$ by $\rho(x) = \rho_n(x)$ if $x \in K_{n,0}$.

By its very definition, ρ is a K-linear map which is a two-sided inverse to $(\gamma - \mathrm{Id})|_{K_{\infty,0}}$. It remains to show that $\rho\colon K_{\infty,0} \to K_{\infty,0}$ is continuous. But if $x \in K_{\infty,0}$, then

$$|x| = |((\gamma - \mathrm{Id}) \circ \rho)(x)| \geq \frac{1}{d}\,|t(\rho(x)) - \rho(x)| = \frac{1}{d}\,|\rho(x)|\,,$$

so ρ is bounded and hence continuous. This allows ρ to be extended uniquely to X_0. The density of $K_{\infty,0}$ in X_0 implies that ρ is the inverse of $(\gamma - \mathrm{Id})|_{X_0}$.

The following lemma treats the twisting by ϕ. This is equivalent to saying that for all n, $\lambda^{p^n} \neq 1$ or, equivalently,

$$\lambda \in (1 + \mathfrak{m}_K) \setminus \boldsymbol{\mu}_{p^\infty}(K).$$

The following lemma treats this case:

Lemma 1.9.14. *Assume that ϕ is of infinite order. Then the map $\gamma - \lambda Id$ induces an isomorphism*

$$(\gamma - \lambda Id) \colon X \to X.$$

Proof. Decompose X as $X_0 \oplus K$. The map $\gamma - \lambda$ acts on K as multiplication by $1 - \lambda$. Since this is a unit in K, $\gamma - \lambda$ induces an isomorphism on K. It remains to study the action of $\gamma - \lambda$ on X_0.

First suppose that $|\lambda - 1|\, d < 1$. Let ρ be the inverse of $(\gamma - \mathrm{Id})|_{X_0}$. Consider the map

$$\alpha \stackrel{\text{def}}{=} (\gamma - \lambda) \circ \rho = ((\gamma - \mathrm{Id}) + (1 - \lambda)\mathrm{Id}) \circ \rho = \mathrm{Id}_{X_0} - (\lambda - 1)\rho.$$

Note that α is a K-linear map $X_0 \to X_0$. We write an explicit formula for the inverse of α and then check that the stated formula makes sense. Define $\beta \colon X_0 \to X_0$ as

$$\beta(x) \stackrel{\text{def}}{=} \sum_{n=0}^{\infty} (\lambda - 1)^n \rho^n(x),$$

where ρ^n denotes the nth iterate of ρ. Note that for all n and for all $x \in X_0$,

$$|(\lambda - 1)^n \rho^n(x)| \leq (|\lambda - 1|\, d)^n\, |x|\,.$$

The right hand side tends to 0 as n tends to infinity, so that the series defining $\beta(x)$ is convergent. Is is easy to check that β is a continuous K-linear map, and that $\alpha \circ \beta = \beta \circ \alpha = \mathrm{Id}_{X_0}$. This proves that α is invertible. But then $\gamma - \lambda$ is invertible when restricted to X_0, with inverse $\rho \circ \beta$.

In the general case, choose m large enough so that $\left|\lambda^{p^m} - 1\right| d < 1$. Replace then K by K_m and γ by γ^{p^m}, and show as above that $(\gamma^{p^m} - \lambda^{p^m})|_{X_0}$ is invertible. One can factor

$$\gamma^{p^m} - \lambda^{p^m} = (\gamma - \lambda) \circ U,$$

where U is a polynomial in γ. It follows then that $(\gamma - \lambda)|_{X_0}$ is invertible as well, as we wanted to show. □

Theorem 1.9.15 (Tate)**.** *Let K be a finite extension of $\mathbf{Q}_p$. Then:*

$$H^i_{cont}(G_K, \mathbf{C}_p) = \begin{cases} K & i = 0 \\ K \ \textit{(non-canonically)} & i = 1 \\ 0 & i \geq 2 \end{cases}$$

Let $\phi \colon G_K \to K^\times$ be a continuous character, and assume that it is not of finite order. Then for all i:

$$H^i_{cont}(G_K, \mathbf{C}_p(\phi)) = 0.$$

Proof. The vanishing of the higher cohomology groups follows because Γ is profinite, and hence it has cohomological dimension 1.

If ϕ is trivial, Lemma 1.9.13 gives:

$$H^0_{\mathrm{cont}}(\Gamma, \widehat{L}) = \ker(\gamma - \mathrm{Id}\colon X \to X) = K$$
$$H^1_{\mathrm{cont}}(\Gamma, \widehat{L}) = \mathrm{coker}(\gamma - \mathrm{Id}\colon X \to X) = X/X_0 \simeq K.$$

Suppose that ϕ is of infinite order. Then Lemma 1.9.14 gives:

$$H^0_{\mathrm{cont}}\left(\Gamma, \widehat{L}(\phi)\right) = \ker(\gamma - \lambda\colon X \to X) = 0$$
$$H^1_{\mathrm{cont}}\left(\Gamma, \widehat{L}(\phi)\right) = \mathrm{coker}(\gamma - \lambda\colon X \to X) = 0.$$

□

Corollary 1.9.16. *Let W be a $\mathbf{C}_p$-vectorspace with a semilinear and continuous action of G_K. Suppose that the sequence*

$$0 \to \mathbf{C}_p(m)^{k_1} \to W \to \mathbf{C}_p(q)^{k_2} \to 0$$

is exact. Here k_i are in $\mathbf{Z}_{\geq 1}$, and m and q are distinct *integers. Then the sequence is canonically split, and so*

$$W \simeq \mathbf{C}_p(m)^{k_1} \oplus \mathbf{C}_p(q)^{k_2},$$

compatible with the G_K-action.

Remark. The theorem that we just proved ensures that $H^1_{\mathrm{cont}}(G_K, \mathbf{C}_p)$ is a one dimensional K-vectorspace. We can find an explicit nonzero element. For that, let

$$c\colon G_K \to \mathbf{C}_p$$

be defined as $c(\sigma) = \log_p(\chi(\sigma)) \in \mathbf{Z}_p \subseteq \mathbf{C}_p$. The map c is continuous, and

$$c(\sigma\tau) = \log_p(\chi(\sigma)\chi(\tau)) = \log_p(\chi(\sigma)) + \log_p(\chi(\tau)),$$

so it is a cocycle. Remark that $\log_p \chi(\tau) \in \mathbf{Z}_p$, so it is fixed by σ. Show that c is a nontrivial cocycle in $H^1_{\mathrm{cont}}(G_K, \mathbf{C}_p)$, as an exercise. [8]

[8] **FIXME:** do it?

Chapter 2

p-divisible Groups

2.1 Group schemes

Fix a commutative ring R. In most of our applications it will be either a field or a local noetherian ring.

Definition 2.1.1. A **group scheme** is a group object in the category $\mathbf{Sch}_R$ of schemes over R.

More concretely, a group scheme is a R-scheme G together with morphisms $m\colon G\times G\to G$, $\varepsilon\colon \operatorname{Spec} R\to G$ and $i\colon G\to G$, making the following diagrams commutative:

$$\begin{array}{ccc} G\times G\times G & \xrightarrow{\mathrm{Id}\times m} & G\times G \\ \downarrow{\scriptstyle m\times \mathrm{Id}} & & \downarrow{\scriptstyle m} \\ G\times G & \xrightarrow{m} & G \end{array}$$

$$\begin{array}{ccccc} G\times G & \xleftarrow{\varepsilon\times\mathrm{Id}} & G\times \operatorname{Spec} R & \xrightarrow{\mathrm{Id}\times\varepsilon} & G\times G \\ & \searrow{\scriptstyle m} & \downarrow{\scriptstyle\simeq} & \swarrow{\scriptstyle m} & \\ & & G & & \end{array}$$

[1]

Definition 2.1.2. A group scheme is **commutative** if it satisfies the corresponding diagram.[2]

Definition 2.1.3. If S is a R-scheme, the set of S**-points** of G is

$$G(S) \stackrel{\text{def}}{=} \operatorname{Hom}_{\mathbf{Sch}_R}(S,G),$$

with the following group structure: given $f,g\in G(S)$ then $fg \stackrel{\text{def}}{=} m\circ(f\times g)\in G(S)$. The identity is given as $e\stackrel{\text{def}}{=}\varepsilon\circ\pi$, where $\pi\colon S\to \operatorname{Spec} R$ is the structure morphism.

[1] **FIXME:** put the other diagram.
[2] **FIXME:** which is...

Definition 2.1.4. An **abelian scheme** is a proper commutative [3] group scheme. This means that it is proper when considered as a scheme over R.

Definition 2.1.5. A **finite group scheme** of rank r is a group scheme G over R which when seen as a scheme over R is finite and locally free of rank r.

Remark. A finite group scheme of rank r is in particular affine, so $G = \operatorname{Spec} A$, where A is a projective R algebra of rank r. The morphisms m, ε, i correspond respectively to R-algebra homomorphisms $\mu\colon A \to A \otimes_R A$, $e\colon A \to R$ and $s\colon A \to A$.

Definition 2.1.6. Let G be an abelian scheme and let n be a positive integer. We write

$$G[n] \overset{\text{def}}{=} \ker\left(G \overset{[n]}{\to} G\right),$$

which is a finite group scheme.

Example. 1. The **additive group scheme** over R is $\mathbb{G}_{a,R}$. As a scheme, it is $\operatorname{Spec}(R[T])$, and the comultiplication is given by $\mu\colon R[T] \to R[T] \otimes R[T]$ sending T to $T \otimes 1 + 1 \otimes T$.

2. The **multiplicative group scheme** over R is $\mathbb{G}_{m,R}$. As a scheme, it is given as $\operatorname{Spec}(R[T, T^{-1}])$, and the comultiplication is given by

$$\mu\colon R[T, T^{-1}] \to R[T, T^{-1}] \otimes R[T, T^{-1}],$$

sending T to $T \otimes T$.

3. For n a positive integer, the group scheme of nth roots of unity is $\boldsymbol{\mu}_n$. It is defined as the kernel of the multiplication-by-n map,

$$\boldsymbol{\mu}_n \overset{\text{def}}{=} \ker\left(\mathbb{G}_{m,R} \overset{[n]}{\to} \mathbb{G}_{m,R}\right).$$

As a scheme, it is $\operatorname{Spec}\left(R[T]/(T^n - 1)\right)$, and the comultiplication sends $\overline{T}$ to $\overline{T} \otimes \overline{T}$.

4. For an abelian group H, define A as the set of maps $H \to R$. It has an R-algebra structure induced pointwise from the structure in R. Let $\mu\colon A \to A \otimes_R A$ be given by

$$\mu(f)(x, y) \overset{\text{def}}{=} f(x + y),$$

where the $+$ symbol indicates the addition in the group H. The other operations are defined similarly, and one obtains a group scheme $\underline{H} = \operatorname{Spec} A$, which is the **constant group scheme** associated to H.

[3] **FIXME:** we don't require commutativity, but if follows?

2.1.1 Cartier duality

Let G be a finite group scheme of rank r over R. Let $G = \operatorname{Spec} A$, where A is a projective finite R-algebra. Consider the dual module

$$A' \stackrel{\text{def}}{=} \operatorname{Hom}_R(A, R),$$

which is a projective R-module of the same rank. The comultiplication $\mu\colon A \to A \otimes A$ gives a ring structure to A', and the dual of $\cdot\colon A \times A \to A$ gives A' a comultiplication. Then $G' = \operatorname{Spec}(A')$ has a structure of a finite group scheme of rank r.

Definition 2.1.7. The **Cartier dual** of G is G' defined above.

Proposition 2.1.8 (Basic properties)**.** *1.* $(G')' = G$.

2. If S is an R-scheme, then

$$G'(S) = \operatorname{Hom}_{\boldsymbol{Sch}_S}(G_S, \mathbb{G}_{m,S}),$$

where $G_S = G \otimes_R S$ is the base change of G to S.

Example. 1. The dual of $\boldsymbol{\mu}_n$ is $\underline{\mathbf{Z}/n\mathbf{Z}}$.

2. Let G/R be an abelian scheme. Let G' be its dual abelian scheme. This is harder to define, as G is not affine. See [Mum70] for more details. However, they are related as follows: if n is any positive integer, then

$$(G[n])' \simeq G'[n].$$

2.1.2 Connected and étale group schemes

Let R be a complete noetherian local ring. Let G be a *finite* group scheme over R.

Definition 2.1.9. We say that G is **étale** (resp. **connected**) G is étale (resp. connected) over R. Equivalently, if $G = \operatorname{Spec} A$, then G is étale (resp. connected) if A is a finite étale R-algebra (resp. if A contains no nontrivial idempotents).

Theorem 2.1.10. *If G is a finite group scheme, then there is a canonical exact sequence*

$$0 \to G^0 \to G \to G^{et} \to 0,$$

where G^0 is connected and G^{et} is étale.

If $G = \operatorname{Spec}(A)$ and we write $G^{et} = \operatorname{Spec}(A^{et})$ and $G^0 = \operatorname{Spec}(A^0)$, then A^{et} and A^0 are characterized, respectively, as the maximal subalgebra of A which is étale over R, and by the component of A which factors via the identity section.

Proof. Omitted. □

2.2 p-divisible groups

Fix $K/\mathbf{Q}_p$ finite and let $R = \mathcal{O}_K$.

Definition 2.2.1. A **p-divisible group** G of **height** h is an inductive system $G = \{G_\nu, i_\nu\}_{\nu \geq 0}$, where G_ν is a finite group scheme over R of rank $p^{\nu h}$, and such that there are exact sequences

$$0 \to G_\nu \xrightarrow{i_\nu} G_{\nu+1} \xrightarrow{p^\nu} G_{\nu+1}.$$

for all $\nu \geq 0$.

Lemma 2.2.2. *Multiplication by p^ν kills G_ν.*

Proof. Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccc} 0 & \longrightarrow & G_\nu & \xrightarrow{i_\nu} & G_{\nu+1} \\ & & \downarrow{\scriptstyle p^\nu} & & \downarrow{\scriptstyle p^\nu} \\ 0 & \longrightarrow & G_\nu & \xrightarrow{i_\nu} & G_{\nu+1} \end{array}$$

Since $i_\nu \circ [p^\nu] = [p^\nu] \circ i_\nu = 0$, and since i_ν is injective, it follows that $[p^\nu] = 0$ on G_ν. $\square$

Example. If G is an abelian scheme, write $G_\nu = G[p^\nu]$ for all $\nu \geq 0$ and let $i_\nu \colon G[p^\nu] \to G[p^{\nu+1}]$ denote the inclusion. The sequence

$$0 \to G[p^\nu] \xrightarrow{i_\nu} G[p^{\nu+1}] \to [p]G[p^{\nu+1}],$$

is exact. We denote by $G(p) = \{G_\nu, i_\nu\}_{\nu \geq 0}$ this p-divisible group.

2.2.1 Dual p-divisible group

Fix a p-divisible group $\{G_\nu, i_\nu\}_{\nu \geq 0}$. Iteration of the transition morphisms gives maps:

$$i_{\nu,\mu} \colon G_\nu \to G_{\nu+1} \to \cdots \to G_{\nu+\mu}$$

for all $\mu \geq 1$. A simple induction shows that the sequence:

$$0 \to G_\nu \xrightarrow{i_{\nu,\mu}} G_{\nu+\mu} \xrightarrow{p^\nu} G_{\nu+\mu}$$

is exact for all $\mu \geq 1$. This identifies G_ν with the kernel of multiplication by p^ν on $G_{\nu+\mu}$ for all $\mu \geq 1$. Since multiplication by $p^{\nu+\mu}$ on $G_{\nu+\mu}$ factors as:

$$G_{\nu+\mu} \xrightarrow{p^\mu} G_{\nu+\mu} \xrightarrow{p^\nu} G_{\nu+\mu},$$

and since $[p^{\nu+\mu}] = 0$ on $G_{\nu+\mu}$, it follows that multiplication by p^μ factors uniquely through $G_\mu = \ker[p^\nu]$. Let $j_{\nu,\mu} \colon G_{\nu+\mu} \to G_\nu$ be the unique map such that $[p^\mu] = i_{\nu,\mu} \circ j_{\nu,\mu}$.

Lemma 2.2.3. *The sequence:*

$$0 \to G_\mu \overset{i_{\mu,\nu}}{\to} G_{\nu+\mu} \overset{j_{\nu,\mu}}{\to} G_\nu \to 0$$

is exact for all $\nu \geq 0$ *and* $\mu \geq 1$.

Proof. First note that $i_{\nu,\mu} \circ j_{\nu,\mu} \circ i_{\mu,\nu} = [p^\mu] \circ i_{\mu,\nu} = 0$. Since $i_{\nu,\mu}$ is injective, it follows that $j_{\nu,\mu} \circ i_{\mu,\nu} = 0$. Hence $\operatorname{im} i_{\mu,\nu} \subseteq \ker j_{\nu,\mu}$. For the converse inclusion note that $\ker j_{\nu,\mu} \subset \ker[p^\mu] = \operatorname{im} i_{\mu,\nu}$. It thus remains to show that $j_{\nu,\mu}$ is surjective. This follows by considering orders. □

Example. Returning to the previous example with G an abelian scheme, and $G_\nu = G[p^\nu]$, then the maps:

$$j_\nu = j_{1,\nu} \colon G[p^{\nu+1}] \to G[p^\nu]$$

are often referred to as "multiplication by p".

For each $\nu \geq 0$, the group scheme G_ν has a Cartier dual, which we write as G'_ν. We consider the duals of the maps $j_{1,\nu}$:

$$i'_\nu = j'_{1,\nu} \colon G'_\nu \to G'_{\nu+1}.$$

$\overset{\text{def}}{=}$ For $G = \{G_\nu, i_\nu\}_{n\geq 0}$ a p-divisible group, the **dual p-divisible** group G' is define to be $\{G'_\nu, i'_\nu\}_{\nu\geq 0}$. It is not difficult to check that G' as defined is actually a p-divisible group.

Example. Let $\mathbf{G}_m(p) = \{\boldsymbol{\mu}_{p^\nu}, i_\nu\}_{\nu\geq 0}$ denote the p-divisible group where $\boldsymbol{\mu}_{p^\nu}$ denotes the group scheme of p^νth roots of unity, and i_ν denotes the natural inclusion. Then $(\boldsymbol{\mu}_{p^\nu})' = \underline{(\mathbf{Z}/p^\nu\mathbf{Z})}$ and:

$$i'_\nu \colon \underline{(\mathbf{Z}/p^\nu\mathbf{Z})} \to \underline{(\mathbf{Z}/p^{\nu+1}\mathbf{Z})}$$

is multiplication by p.

Example. If G is an abelian scheme, then $(G(p))' = G'(p)$.

2.2.2 Connected and étale components

Let $G = \{G_\nu, i_\nu\}_{\nu\geq 0}$ be a p-divisible group. For each ν there exists a decomposition:

$$0 \to G^0_\nu \to G_\nu \to G^{\text{et}}_\nu \to 0.$$

with G^0_ν connected and G^{et}_ν étale. The maps i_ν induce maps on the connected and étale parts so that $\{G^0_\nu, i^0_\nu\}_{\nu\geq 0}$ and $\{G^{\text{et}}_\nu, i^{\text{et}}_\nu\}_{\nu\geq 0}$ are p-divisible groups. Denote them by G^0 and G^{et}, respectively. We say that the sequence:

$$0 \to G^0 \to G \to G^{\text{et}} \to 0$$

is exact to indicate that it is exact at each finite level.

Definition 2.2.4. A p-divisible group G is said to be **connected** if $G = G^0$. It is said to be **étale** if $G = G^{\text{et}}$.

If we write $G_\nu^0 = \operatorname{Spec}(A_\nu^0)$ for each $\nu \geq 0$, then maps i_ν^0 correspond to maps $A_{\nu+1}^0 \to A_\nu^0$. This makes $\{A_\nu^0\}$ into a projective system. Setting $A^0 = \varprojlim A_\nu^0$, Tate showed that:

$$A^0 \simeq \mathcal{O}_K [\![X_1, \ldots, X_n]\!] .$$

Definition 2.2.5. The **dimension** of a p-divisible group G, denoted $\dim G$, is the integer $n \geq 1$ such that $A^0 \simeq \mathcal{O}_K [\![X_1, \ldots, X_n]\!]$, with A^0 as defined in the preceding paragraph.

The dimension can be defined in other ways, but we will not pursue this. Note that $\dim G = \dim G^0$ by definition. Also, one can show that $\dim G \leq h$ where h is the height of G.

Note that if $G = \{G_\nu, i_\nu\}_{\nu \geq 0}$ is a p-divisible group of height h, so that each G_ν is free of rank $p^{\nu h}$, then G'_ν is also free of rank $p^{\nu h}$. Hence G' is also of height h. If $\dim G' = n'$, then one can show that $h = n + n'$.

Example. Consider $G = \mathbf{G}_m(p)$ as above. In this case the height of G is one, and one can show that also $\dim G = 1$. Note that we observed that $G' = \{\underline{(\mathbf{Z}/p^\nu \mathbf{Z})}, i'_\nu\}$, and each $\underline{(\mathbf{Z}/p^\nu \mathbf{Z})}$ is étale. Thus G' is étale, so that $G^0 = 0$. Hence $\dim G' = 0$, and indeed, $\dim G + \dim G' = 1 + 0 = 1$.

Example. If G is an abelian scheme of dimension n, then $X(p)$ also has dimension n, and height $2n$. Similarly for the dual.

2.2.3 Points of a p-divisible group

Let S be an $\mathcal{O}_K$-algebra and $G = \{G_\nu, i_\nu\}_{\nu \geq 1}$ a p-divisible group. It is tempting to define the S-points of G by setting:

$$G(S) = \varinjlim G_\nu(S),$$

but this is not a fruitful definition. Instead we adopt the following more subtle:

Definition 2.2.6. Let π be a uniformizer for $\mathcal{O}_K$, and suppose that the $\mathcal{O}_K$-algebra S is complete for the (πS)-adic topology. Then the S**-points** of G are denoted $G(S)$ and defined to be:

$$G(S) = \varprojlim_i \left(\varinjlim_\nu (G_\nu(S/\pi^i S)) \right) .$$

We will only ever need to consider the $\mathcal{O}_{\mathbf{C}_p}$-points of a p-divisible group. Write:

$$\Phi G = \varinjlim G_\nu(\mathcal{O}_{\mathbf{C}_p})$$

for the "naive" definition of $\mathcal{O}_{\mathbf{C}_p}$-points of G. This group is torsion. In fact,

$$\Phi G = G(\mathcal{O}_{\mathbf{C}_p})_{\text{tors}}.$$

Example. Consider again $G = \mathbf{G}_m(p)$, and note that in this case $\Phi G = \mu_{p^\infty}(\mathbf{C}_p)$. One can show that $G(\mathcal{O}_{\mathbf{C}_p}) = 1 + \mathfrak{m}_{\mathbf{C}_p}$, which is much larger than ΦG.

If the p-divisible group G is étale, one can use the lifting of maps property to show that the reductions:

$$G_\nu(\mathcal{O}_{\mathbf{C}_p/\pi^i\mathcal{O}_{\mathbf{C}_p}}) \to G_\nu(\overline{k}),$$

where $\overline{k}$ is an algebraic closure of the residue field of K, are isomorphisms. From this one deduces that $G(\mathcal{O}_{\mathbf{C}_p})$ is a torsion group whenever G is étale. Given an arbitrary p-adic group, one can similarly use the lifting property with the exact sequence:

$$0 \to G^0 \to G \to G^{\text{et}} \to 0$$

to show that $G \to G^{\text{et}}$ has a section. The existence of this section then implies that the sequence of points:

$$0 \to G^0(\mathcal{O}_{\mathbf{C}_p}) \to G(\mathcal{O}_{\mathbf{C}_p}) \to G^{\text{et}}(\mathcal{O}_{\mathbf{C}_p}) \to 0$$

is exact. Since $G^{\text{et}}(\mathcal{O}_{\mathbf{C}_p})$ is torsion, one deduces the following comforting fact:

Proposition 2.2.7. *If G is a p-divisible group, then $G(\mathcal{O}_{\mathbf{C}_p})$ is an abelian group which is p-divisible.*

2.2.4 Differential structure

Let G be a p-divisible group with connected component $G^0 = \{G^0_\nu\}$. As above, write $G^0_\nu = A^0_\nu$ and put $A^0 = \varprojlim A^0_\nu$.

Definition 2.2.8. The **tangent space** at 0 to G, denoted $t_G(\mathbf{C}_p)$, is the space of $\mathcal{O}_K$ linear derivations:

$$t_G(\mathbf{C}_p) = \mathrm{Der}_{\mathcal{O}_K}(A^0, \mathbf{C}_p).$$

The tangent space can be defined in a second way. Consider the map $\varepsilon\colon A^0 \to \mathcal{O}_K$ mapping $f \mapsto f(0)$, where we regard $f \in A^0 \simeq \mathcal{O}_K[\![X_1, \ldots, X_n]\!]$ via Tate's isomorphism. Then if we put

$$I^0 = \ker\varepsilon = (X_1, \ldots, X_n), \tag{2.1}$$

one has:

$$t_G(\mathbf{C}_p) \cong \hom_{\mathcal{O}_K}(I^0/(I^0)^2, \mathbf{C}_p).$$

The isomorphism is given by restricting a derivation $\tau \in t_G(\mathbf{C}_p)$ to I^0. Since $I^0/(I^0)^2$ is a free $\mathcal{O}_K$-module of rank n, it follows that $t_G(\mathbf{C}_p) \cong \mathbf{C}_p^n$ as complex vector spaces; recall that $n = \dim G$ by definition.

We can similarly define the space of **differential forms** $\Omega_{G/\mathcal{O}_K}$ on G by putting $\Omega_{G/\mathcal{O}_K} = \Omega_{A^0/\mathcal{O}_K}$, so that:

$$\Omega_{G/\mathcal{O}_K} \cong A^0 dX_1 \bigoplus \cdots \bigoplus A^0 dX_n,$$

where $n = \dim G$. There is a natural subspace of invariant differential forms $\mathrm{Inv}(G)$, and there is a natural identification:

$$I^0/(I^0)^2 \cong \mathrm{Inv}(G).$$

Thus, the tangent space to G at 0 is dual to the space of invariant differential 1-forms.

Example. Consider once again the case $G = \mathbf{G}_m(p)$, so that $A^0 = \mathcal{O}_K[\![X]\!]$. Then $t_G(\mathbf{C}_p) = \mathbf{C}_p$, generated by say $\tau(f) = f'(0)$. One can check that:

$$\mathrm{Inv}(G) = \mathcal{O}_K \frac{dX}{1+X} = \mathcal{O}_K \left(\sum_{n \geq 0} (-X)^n \right) dX.$$

2.2.5 Logarithm map

Let $G = \{G_\nu, i_\nu\}_{\nu \geq 0}$ be a p-divisible group. We want to define a map

$$\log_G \colon G(\mathcal{O}_{\mathbf{C}_p}) \to t_G(\mathbf{C}_p).$$

We will see two possible ways in which this map can be defined. Showing that they agree is a good exercise.

First definition

Consider the exact sequence

$$0 \to G^0(\mathcal{O}_{\mathbf{C}_p}) \to G(\mathcal{O}_{\mathbf{C}_p}) \to G^{\mathrm{et}}(\mathcal{O}_{\mathbf{C}_p}) \to 0.$$

Given $x \in G(\mathcal{O}_{\mathbf{C}_p})$, its image in $G^{\mathrm{et}}(\mathcal{O}_{\mathbf{C}_p})$ is torsion, so that there exists a positive integer n_0 such that $p^{n_0} x \in G^0(\mathcal{O}_{\mathbf{C}_p})$. This implies that we can evaluate any $f \in A^0$ at $p^n x$ for sufficiently large n, and thus the following definition makes sense.

Definition 2.2.9. Identify $t_G(\mathbf{C}_p)$ with $\mathrm{Der}_{\mathcal{O}_K}(A^0, \mathbf{C}_p)$. Then, for $x \in G(\mathcal{O}_{\mathbf{C}_p})$ and $f \in A^0$, define the **logarithm** of x as the derivation

$$\log_G(x)(f) \stackrel{\mathrm{def}}{=} \lim_{n \to \infty} \frac{f(p^n x) - f(0)}{p^n}.$$

Proposition 2.2.10 (Properties). *1. $\log_G(x)$ is an $\mathcal{O}_K$-linear derivation.*

2. $\log_G$ is a $\mathbf{Z}_p$-linear. In particular, it is a group homomorphism.

3. If x is torsion, then $\log_G(x) = 0$.

Note that the last property implies that $\Phi G = G(\mathcal{O}_{\mathbf{C}_p})_{\mathrm{tors}} \subseteq \ker(\log_G)$.

Example. Let $G = \mathbb{G}_m(p)$, so $G(\mathcal{O}_{\mathbf{C}_p}) \simeq 1 + \mathfrak{m}_{\mathcal{O}_{\mathbf{C}_p}}$. One can see then that

$$\log_{\mathbb{G}_m(p)}(x) = \log(x)(\frac{d}{dx}|_{x=0}),$$

where $\log(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}$. [4]

[4] **FIXME:** Add the computation.

Second definition

Identify $t_G(\mathbf{C}_p)$ with $\mathrm{Hom}_{\mathcal{O}_K}(I^0/(I^0)^2, \mathbf{C}_p)$, where I^0 has been defined in 2.1. Recall that $I^0/(I^0)^2$ has been identified with $\mathrm{Inv}(G)$, the space of invariant one-forms.

It is enough to define $\log_G$ on $G^0(\mathcal{O}_{\mathbf{C}_p})$ and then extend to all $G(\mathcal{O}_{\mathbf{C}_p})$ by scaling. [5]

Given $\omega \in \mathrm{Inv}(G)$, write $\omega = \sum_{i=1}^n f_i(x_1, \dots, x_n)dx_i$, with $f_i \in A^0$.

Claim. *There exists a unique* $\Omega(x_1, \dots, x_n) \in K[\![x_1, \dots, x_n]\!]$ *such that* $d\Omega = \omega$, *and* $\Omega(0) = 0$.

Lemma 2.2.11. *Let* $x \in G^0(\mathcal{O}_{\mathbf{C}_p})$, *and let* $\omega \in \mathrm{Inv}(G)$.

Definition 2.2.12. The element $\log_G(x)$ is the functional

$$\omega \mapsto \Omega(x) = \int_0^x \omega.$$

Example. The element $\frac{d}{dx}|_{x=0} \in t_{\mathbb{G}_m(p)}(\mathbf{C}_p)$ is identified with the functional $\omega \mapsto 1$, where $\omega = \frac{dx}{x+1}$. We get as before that

$$\log_{\mathbb{G}_m(p)}(x)(\omega) = \log(x),$$

as before.[6]

2.2.6 Properties of the Logarithm

Lemma 2.2.13. *The logarithm* $\log_G\colon G(\mathcal{O}_{\mathbf{C}_p}) \to t_G(\mathbf{C}_p)$ *is a* $\mathbf{Z}_p$*-linear homomorphism, and a local isomorphism. More concretely, given any* $c \in \mathbf{R}$ *such that* $0 < c < p^{\frac{1}{1-p}}$, *the restriction of the* $\log_G$ *induces a bijection*

$$\{x \in G^0(\mathcal{O}_{\mathbf{C}_p}) \mid |x_i| \leq c\} \to \{\tau \in t_G(\mathbf{C}_p) \mid |\tau(x_i)| \leq c \text{ for all } i = 1 \dots n\}$$

Proof. The idea is to use that one can define the exponential, which gives an inverse. □

Corollary 2.2.14. *The map* $\log_G$ *induces a* G_K*-equivariant exact sequence*

$$0 \to \Phi G \to G(\mathcal{O}_{\mathbf{C}_p}) \to t_G(\mathbf{C}_p) \to 0$$

Proof. We will first see that $\log_G$ is surjective. Let $\tau \in t_G(\mathbf{C}_p)$. There exists some large n such that $|p^n\tau| \leq c$. The lemma gives $x \in G(\mathcal{O}_{\mathbf{C}_p})$ such that $\log_G(x) = p^n\tau$. As $G(\mathcal{O}_{\mathbf{C}_p})$ is p-divisible, there exists $y \in G(\mathcal{O}_{\mathbf{C}_p})$ such that $p^n y = x$, and then $p^n\tau = p^n \log_G(y)$. As $t_G(\mathbf{C}_p)$ is torsion-free, we obtain $\tau = \log_G(y)$.

As ΦG is torsion, it is contained in the kernel of $\log_G$. Conversely, let $x \in \ker \log_G$. Let n be large enough so that $p^n x \in G^0(\mathcal{O}_{\mathbf{C}_p})$, and $|p^n x| \leq c$. Then $\log_G(p^n x) = p^n \log_G(x) = 0$, so the lemma implies that $p^n x = 0$, and hence $x \in \Phi G$. □

[5] **FIXME:** Add details.

[6] **FIXME:** Add the computation.

2.2.7 A theorem of Tate

Theorem 2.2.15 (Tate)**.** *Let G be a p-divisible group. Then there are canonical $\mathbf{C}_p$-linear isomorphisms of G_K-modules:*

$$T_pG \otimes_{\mathbf{Z}_p} \mathbf{C}_p \simeq t_G(\mathbf{C}_p)(1) \bigoplus \left(t_{G'}(\mathbf{C}_p)\right)^\vee ,$$

where $\vee$ we denote the $\mathbf{C}_p$-dual.

Remark. If we forget the G_K-action, the left hand side is a $\mathbf{C}_p$-vectorspace of dimension h, and the right hand side has dimension $n + n' = h$, so at least the dimensions agree. Also, as $\mathbf{C}_p[G_K]$-modules, the right hand side is isomorphic (non-canonically) to $\mathbf{C}_p(1)^n \oplus \mathbf{C}_p^{n'}$.

Proof. We consider the dual p-divisible group $G' = \{G'_\nu, i'_\nu\}_{\nu\geq 0}$. From its definition, we have a commutative diagram involving its $\mathcal{O}_{\mathbf{C}_p}$-points:

$$\begin{array}{ccc} G'_\nu(\mathcal{O}_{\mathbf{C}_p}) & = & \mathrm{Hom}_{\mathcal{O}_{\mathbf{C}_p}-\mathrm{grpsch}}\left(G_\nu \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}, \mathbb{G}_m(p) \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}\right) \\ \uparrow j'_\nu & & \uparrow (i_\nu \otimes \mathrm{Id})^* \\ G'_{\nu+1}(\mathcal{O}_{\mathbf{C}_p}) & = & \mathrm{Hom}_{\mathcal{O}_{\mathbf{C}_p}-\mathrm{grpsch}}\left(G_{\nu+1} \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}, \mathbb{G}_m(p) \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}\right), \end{array}$$

so denoting by $T' = T_pG'$ the Tate module of the dual group we get a canonical isomorphism

$$T' \simeq \mathrm{Hom}_{\mathcal{O}_{\mathbf{C}_p}-p-\mathrm{div}}\left(G\hat{\otimes}[\mathcal{O}_K]\mathcal{O}_{\mathbf{C}_p}, \mathbb{G}_m(p) \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}\right),$$

and a G_K-equivariant pairing

$$(\cdot,\cdot)\colon T' \times G(\mathcal{O}_{\mathbf{C}_p}) \to U,$$

where we define $U \stackrel{\mathrm{def}}{=} \mathbb{G}_m(p)(\mathcal{O}_{\mathbf{C}_p}) = 1 + \mathfrak{m}_{\mathcal{O}_{\mathbf{C}_p}}$.

Applying $\mathrm{Id} \times \log_G$ to the left-hand side, and $\log_{\mathbb{G}_m(p)}$ to the right-hand side, we get another pairing

$$(\cdot,\cdot)\colon T' \times t_G(\mathbf{C}_p) \to t_{\mathbb{G}_m(p)}(\mathbf{C}_p) \simeq \mathbf{C}_p.$$

Consider the exact sequence of p-divisible groups (and hence injective objects)

$$0 \to U_{\mathrm{tors}} \to U \to \log_{\mathbb{G}_m(p)} t_{\mathbb{G}_m(p)}(\mathbf{C}_p) \to 0.$$

Applying the functor $\mathrm{Hom}_{\mathbf{Z}_p}(T', -)$ yields an exact sequence

$$0 \to \mathrm{Hom}_{\mathbf{Z}_p}(T', U_{\mathrm{tors}}) \to \mathrm{Hom}_{\mathbf{Z}_p}(T', U) \to \mathrm{Hom}_{\mathbf{Z}_p}\left(T', t_{\mathbb{G}_m(p)}(\mathbf{C}_p)\right) \to 0.$$

The two pairings defined above induce maps α in $d\alpha$, which fit in to a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Phi G & \longrightarrow & G(\mathcal{O}_{\mathbf{C}_p}) & \longrightarrow & t_G(\mathbf{C}_p) & \longrightarrow & 0 \\ & & \downarrow \alpha_0 & & \downarrow \alpha & & \downarrow d\alpha & & \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathbf{Z}_p}(T', U_{\mathrm{tors}}) & \longrightarrow & \mathrm{Hom}_{\mathbf{Z}_p}(T', U) & \longrightarrow & \mathrm{Hom}_{\mathbf{Z}_p}\left(T', t_{\mathbb{G}_m(p)}(\mathbf{C}_p)\right) & \longrightarrow & 0. \end{array}$$

Moreover, if we define an action of G_K on $\mathrm{Hom}_{\mathbf{Z}_p}(T', U)$ by

$$(\sigma f)(t) \stackrel{\text{def}}{=} \sigma(f(\sigma^{-1}(t))),$$

all the maps in the diagram are G_K-equivariant.

We give $d\alpha$ explicitly: let $\tau \in t_G(\mathbf{C}_p)$, and $t \in T'$. Let $f \in A_{\mathbb{G}_m(p)}$. Think of t as a homomorphism $G \hat{\otimes} \mathcal{O}_{\mathbf{C}_p} \to \mathbb{G}_m(p) \otimes \mathbf{C}_p$, which gives a map

$$A_{\mathbb{G}_m(p)} \hat{\otimes} \mathcal{O}_{\mathbf{C}_p} \to A_G \hat{\otimes} \mathcal{O}_{\mathbf{C}_p} \to A^0 \hat{\otimes} \mathcal{O}_{\mathbf{C}_p}.$$

Then

$$(d\alpha)(\tau)(t)(f) = \tau(t(f)).$$

[7]

Proposition 2.2.16. *1. The map α_0 is an isomorphism.*

2. The maps α and $d\alpha$ are both injective.

Proof (of the proposition). Consider the commutative diagram

$$\begin{array}{ccc} G_\nu(\mathcal{O}_{\mathbf{C}_p}) & = & \mathrm{Hom}_{\mathcal{O}_{\mathbf{C}_p}-\text{grpsch}}\left(G'_\nu \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}, \boldsymbol{\mu}_{p^\nu}(\mathcal{O}_{\mathbf{C}_p})\right) \\ \uparrow{\scriptstyle i_\nu} & & \uparrow{\scriptstyle j'_\nu} \\ G_{\nu-1}(\mathcal{O}_{\mathbf{C}_p}) & = & \mathrm{Hom}_{\mathcal{O}_{\mathbf{C}_p}-\text{grpsch}}\left(G'_{\nu-1} \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}, \boldsymbol{\mu}_{p^{\nu-1}}(\mathcal{O}_{\mathbf{C}_p})\right). \end{array}$$

By taking inductive limits we obtain

$$\Phi G \cong \varinjlim_\nu G_\nu(\mathcal{O}_{\mathbf{C}_p}) \cong \mathrm{Hom}_{\mathbf{Z}_p}\left(\varprojlim_\nu G'_\nu(\mathcal{O}_{\mathbf{C}_p}), U_{\text{tors}}\right) = \mathrm{Hom}_{\mathbf{Z}_p}(T', U_{\text{tors}}),$$

and one can check that the map coincides with α_0, so that the first part of the proposition is proven.

Next, consider the commutative diagram

$$\begin{array}{ccc} G_\nu(\mathcal{O}_{\mathbf{C}_p}) & = & \mathrm{Hom}_{\mathcal{O}_{\mathbf{C}_p}-\text{grpsch}}\left(G'_\nu \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}, \boldsymbol{\mu}_{p^\nu}(\mathcal{O}_{\mathbf{C}_p})\right) \\ \downarrow{\scriptstyle j_\nu} & & \downarrow \\ G_{\nu-1}(\mathcal{O}_{\mathbf{C}_p}) & = & \mathrm{Hom}_{\mathcal{O}_{\mathbf{C}_p}-\text{grpsch}}\left(G'_{\nu-1} \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}, \boldsymbol{\mu}_{p^{\nu-1}}(\mathcal{O}_{\mathbf{C}_p})\right). \end{array}$$

By taking projective limits, we get an isomorphism

$$T = T_pG \cong \mathrm{Hom}_{\mathbf{Z}_p}\left(T', T_p\mathbb{G}_m(p)\right).$$

[7] **FIXME:** This should be rewritten.

Note that $T_p\mathbb{G}_m(p) \cong \mathbf{Z}_p(1)$, as G_K-modules. This gives a perfect pairing

$$\langle \cdot, \cdot \rangle_W \colon T \times T' \to \mathbf{Z}_p(1),$$

called the **Weil pairing**.

Note that since α_0 is an isomorphism, the snake lemma applied to the commutative diagram (2.2.7) shows that $\ker \alpha \cong \ker d\alpha$. Since $\ker d\alpha$ is actually a $\mathbf{C}_p$-vectorspace, it is uniquely p-divisible. Hence the same can be said for $\ker \alpha$.

The group G_K acts on $\ker \alpha$ and $\ker d\alpha$, since α and $d\alpha$ are G_K-equivariant. Obviously $(\ker \alpha)^{G_K} \subset G(\mathcal{O}_{\mathbf{C}_p})^{G_K}$, and we claim that $G(\mathcal{O}_{\mathbf{C}_p})^{G_K} = G(\mathcal{O}_K)$, as one would hope. To see this, recall that there is an exact sequence:

$$0 \to G^0(\mathcal{O}_{\mathbf{C}_p}) \to G(\mathcal{O}_{\mathbf{C}_p}) \to G^{\text{et}}(\mathcal{O}_{\mathbf{C}_p}) \to 0,$$

along with a G_K-equivariant section $s\colon G^{\text{et}}(\mathcal{O}_{\mathbf{C}_p}) \to G(\mathcal{O}_{\mathbf{C}_p})$. Taking G_K-invariants thus gives the natural commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & G^0(\mathcal{O}_K) & \longrightarrow & G(\mathcal{O}_K) & \longrightarrow & G^{\text{et}}(\mathcal{O}_K) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & G^0(\mathcal{O}_{\mathbf{C}_p})^{G_K} & \longrightarrow & G(\mathcal{O}_{\mathbf{C}_p})^{G_K} & \longrightarrow & G^{\text{et}}(\mathcal{O}_{\mathbf{C}_p})^{G_K} & \longrightarrow & 0 \end{array}$$

with exact rows. The snake lemma will show that the middle map is an isomorphism if we can show that the other two maps are isomorphisms.

One can check that the leftmost map is the following isomorphism:

$$\begin{aligned} G^0(\mathcal{O}_{\mathbf{C}_p})^{G_K} &\cong \operatorname{Hom}_{\text{cont}}(\mathcal{O}_K [\![X_1, \ldots, X_n]\!], \mathcal{O}_{\mathbf{C}_p})^{G_K} \\ &\cong \operatorname{Hom}_{\text{cont}}(\mathcal{O}_K [\![X_1, \ldots, X_n]\!], \mathcal{O}_{\mathbf{C}_p}^{G_K}) \\ &\cong \operatorname{Hom}_{\text{cont}}(\mathcal{O}_K [\![X_1, \ldots, X_n]\!], \mathcal{O}_K) \\ &\cong G^0(\mathcal{O}_K). \end{aligned}$$

Similarly, the rightmost map is the isomorphism:

$$\begin{aligned} G^{\text{et}}(\mathcal{O}_{\mathbf{C}_p})^{G_K} &= \left(\varinjlim_{\nu} G_\nu^{\text{et}}(\mathcal{O}_{\mathbf{C}_p}) \right)^{G_K} \\ &\cong \varinjlim_{\nu} \left(G_\nu^{\text{et}}(\mathcal{O}_{\mathbf{C}_p})^{G_K} \right) \\ &\cong \varinjlim_{\nu} \left(G_\nu^{\text{et}}(\mathcal{O}_K) \right) \\ &\cong G^{\text{et}}(\mathcal{O}_K). \end{aligned}$$

We thus see that $G(\mathcal{O}_{\mathbf{C}_p})^{G_K} = G(\mathcal{O}_K)$.

We next show that $(\ker \alpha)^{G_K} = 0$. Note that $(\ker \alpha)^{G_K} = \ker \alpha \cap G(\mathcal{O}_{\mathbf{C}_p})^{G_K} = \ker \alpha \cap G(\mathcal{O}_K)$. We will use the decomposition $G(\mathcal{O}_K) = G^0(\mathcal{O}_K) \oplus G^{\text{et}}(\mathcal{O}_K)$ given by the section s. Since $\ker\alpha$ is p-divisible, $\ker\alpha\cap G^0(\mathcal{O}_K)$ is contained in $\bigcap_{m\geq 0} p^m G^0(\mathcal{O}_K)$, as this is the collection of p-divisible elements of $G^0(\mathcal{O}_K)$. For m large enough, the logarithm gives an isomorphism $p^m G^0(\mathcal{O}_K) \cong p^m \mathfrak{m}_{\mathbf{C}_p}$. It thus follows that:

$$\bigcap_{m\geq 0} p^m G^0(\mathcal{O}_K) \cong \bigcap_{m\geq 0} p^m \mathfrak{m}_{\mathbf{C}_p} = 0,$$

since $\mathbf{C}_p$ is p-adically separated. Hence $\ker\alpha \cap G^0(\mathcal{O}_K) = 0$. The other intersection $\ker\alpha\cap G^{\text{et}}(\mathcal{O}_K)$ is trivial since $G^{\text{et}}(\mathcal{O}_K)$ is a torsion module. This confirms:

$$(\ker\alpha)^{G_K} = \ker\alpha\cap G(\mathcal{O}_{\mathbf{C}_p})^{G_K} = 0.$$

Hence also $(\ker d\alpha)^{G_K} = 0$.

Consider the map:

$$\alpha_K\colon G(\mathcal{O}_K) \to \big(\mathrm{Hom}_{\mathbf{Z}_p}(T', U)\big)^{G_K} \cong \mathrm{Hom}_{\mathcal{O}_K}(T', U);$$

one has $\ker\alpha_K = (\ker\alpha)^{G_K} = 0$, so that α_K is injective. We similarly have:

$$d\alpha_K\colon t_G(\mathbf{C}_p)^{G_K} = t_G(K) \to \mathrm{Hom}_{\mathbf{Z}_p}(T', \mathbf{C}_p)^{G_K} \cong (T', \mathbf{C}_p),$$

and again $\ker d\alpha_K = (\ker d\alpha)^{G_K} = 0$.

Consider the commutative diagram:

$$\begin{array}{ccc} t_G(\mathbf{C}_p) & \xrightarrow{d\alpha} & W \\ \uparrow & & \uparrow \\ t_G(K) & \xrightarrow[d\alpha_K]{} & W^{G_K} \end{array}$$

Since the G_K-action on the $\mathbf{C}_p$-vectorspace is componentwise, one has a natural G_K-equivariant isomorphism $t_G(\mathbf{C}_p)\cong t_G(K)\otimes_K \mathbf{C}_p$. One can show that the composition of the following maps is precisely $d\alpha$:

$$t_G(\mathbf{C}_p) \cong t_G(K)\otimes_K \mathbf{C}_p \to d\alpha_K \otimes \mathrm{Id} W^{G_K}\otimes_K \mathbf{C}_p \to \phi W,$$

where $\phi(w\otimes a) = aw$. But $d\alpha_K\otimes\mathrm{Id}$ is injective, as $d\alpha_K$ is injective and $\mathbf{C}_p$ is flat over K. Similarly, lemma (2.2.17) shows that ϕ is injective. It follows that $d\alpha$ is injective, so $\ker\alpha = \ker d\alpha = 0$. This concludes the proof of the proposition. $\square$

We now return to the proof of Tate's theorem (2.2.15). Recall that we have a map:

$$d\alpha_{G'}\colon t_{G'}(\mathbf{C}_p) \to \mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{C}_p),$$

so that if we write $T^* = \mathrm{Hom}_{\mathbf{Z}_p}(T, \mathbf{Z}_p)$, then we obtain a G_K-equivariant map:

$$T\otimes\mathbf{C}_p \cong (T^*\otimes\mathbf{C}_p)^* \to (d\alpha_{G'})^* t_{G'}(\mathbf{C}_p)^*,$$

which we denote by v. Since $d\alpha_{G'}$ is injective, the dual map $(d\alpha_{G'})^*$ is surjective. Similarly we have:

$$t_G(\mathbf{C}_p) \stackrel{d\alpha_G}{\to} \mathrm{Hom}_{\mathbf{Z}_p}(T', \mathbf{C}_p) \cong (T')^* \otimes_{\mathbf{Z}_p} \mathbf{C}_p.$$

We can use the Weil pairing $T \times T' \to \mathbf{Z}_p(1)$ to identify $(T')^* \cong T(-1)$ as G_K-modules. Twisting the map above thus gives:

$$u\colon t_G(\mathbf{C}_p)(1) \hookrightarrow T \otimes_{\mathbf{Z}_p} \mathbf{C}_p,$$

which is injective and G_K-equivariant. We thus have maps:

$$0 \to t_G(\mathbf{C}_p)(1) \stackrel{u}{\to} T \otimes_{\mathbf{Z}_p} \mathbf{C}_p \stackrel{v}{\to} t_{G'}(\mathbf{C}_p)^* \to 0, \tag{2.2}$$

with u, v both $\mathbf{C}_p$-linear and G_K-equivariant. Moreover u is injective and v is surjective. Note that $v \circ u$ gives a G_K-equivariant and $\mathbf{C}_p$-linear map:

$$t_G(\mathbf{C}_p)(1) \to t_{G'}(\mathbf{C}_p)^*.$$

These are isomorphic to $\mathbf{C}_p^t(1)$ and $\mathbf{C}_p^r$ as G_K-modules, for some $t, r \in \mathbf{Z}$. One can use our earlier computations of Galois cohomology to show that:

$$\mathrm{Hom}_{\mathbf{C}_p[G_K]}(\mathbf{C}_p^t(k), \mathbf{C}_p^r(k')) = 0$$

whenever $k \neq k'$. This immediately gives $v \circ u = 0$. To see that the sequence (2.2) is exact, it remains to note that the dimension of $t_G(\mathbf{C}_p)(1)$ is the dimension n of G, and the dimension of $t_{G'}(\mathbf{C}_p)^*$ is the dimension n' of G'. Since $n + n' = h$, the height of G, and $T \otimes_{\mathbf{Z}_p} \mathbf{C}_p$ is of dimension h, exactness follows.

Finally, note that if $\mathrm{Ext}^1(A, C)$ denotes the group of extension classes of C by A in the category of topological $\mathbf{C}_p[G_K]$-modules, then:

$$\begin{aligned}\mathrm{Ext}^1\left(t_{G'}(\mathbf{C}_p)^*, t_G(\mathbf{C}_p)(1)\right) &\cong \mathrm{Ext}^1\left(\mathbf{C}_p, t_G(\mathbf{C}_p)(1)\right)^{n'} \\ &\cong H^1_{\mathrm{cont}}\left(G_K, t_G(\mathbf{C}_p)(1)\right)^{n'} = 0.\end{aligned}$$

It follows that the sequence (2.2) is split. If s and s' are two continuous G_K-equivariant splittings, their difference induces a G_K-equivariant map

$$t_G(\mathbf{C}_p)(1) \to t_{G'}(\mathbf{C}_p)^*.$$

But the only such map is zero, as one can show using Theorem 1.9.15. Hence $s = s'$, and the splitting is canonical. □

Lemma 2.2.17. *Let W be a finite dimensional $\mathbf{C}_p$-vectorspace with continuous semi-linear G_K-action. The natural comparison map:*

$$\phi\colon W^{G_K} \otimes_K \mathbf{C}_p \to W,$$

where $\phi(w \otimes a) = aw$, is injective.

Proof. It suffices to show that if $\{w_1, \ldots, w_t\} \subset W^{G_K}$ is a linearly independent set of vectors over K, then they are in fact linearly independent over $\mathbf{C}_p$.

Let $\{w_1, \ldots, w_t\} \subset W^{G_K}$ denote a minimal set for which the w_i's are independent over K, yet dependent over $\mathbf{C}_p$. If $t = 1$ we reach a contradiction since dependence of a single vector is equivalent to being 0. Hence suppose $t \geq 2$ and take:

$$a_1 w_1 + \cdots + a_t w_t = 0$$

for $a_i \in \mathbf{C}_p$, not all of which are zero. Without loss of generality we may suppose $a_1 = 1$, so that $w_1 + a_2 w_2 + \cdots + a_t w_t = 0$. For any $\sigma \in G_K$ we deduce that:

$$w_1 + \sigma(a_2) w_2 + \cdots + \sigma(a_t) w_t = 0,$$

since the w_i's are G_K-invariant. Thus:

$$(a_2 - \sigma(a_2)) w_2 + \cdots + (a_t - \sigma(a_2) w_t = 0.$$

By choice of t we must have $\sigma(a_i) = a_i$ for all $\sigma \in G_K$ and $i = 2, \ldots, t$. But then $a_i \in K$ for all i, contradicting the independence of the w_i's over K. □

Chapter 3

p-adic Hodge theory for Abelian varieties

3.1 p-adic Hodge theory of abelian varieties with good reduction

Let K be a noetherian local ring with perfect residue field. One can choose K to be a finite extension of $\mathbf{Q}_p$, as has done before.

Let $\mathfrak{X}$ be an abelian scheme over $\mathcal{O}_K$, and let $X = \mathfrak{X} \otimes K$ be its generic fiber. As $\operatorname{Spec} K$ is an open subscheme of $\operatorname{Spec} \mathcal{O}_K$, the generic fiber X can be seen as an open subscheme of $\mathfrak{X}$. Alternatively, one can start with an abelian scheme X over K, and take $\mathfrak{X}$ to be its Néron model over $\mathcal{O}_K$. Note that in particular we require that $\mathfrak{X}$ is smooth over $\mathcal{O}_K$, and not just generically smooth.

Denote by G the p-divisible group corresponding to $\mathfrak{X}$. Similarly, define $\mathfrak{X}'$ and X' as the dual abelian schemes of $\mathfrak{X}$ and X respectively, and G' as the p-divisible group corresponding to $\mathfrak{X}$, which is actually the dual of G.

The tangent space $t_G(K)$ can be canonically identified with $\operatorname{Lie}_K(X)$, the Lie group of X, and this in turn can be identified with $H^0(X, \Omega_X)^*$, the dual to the global differential forms. The space $t_{G'}(K)$ can be identified then with $H^0(X', \Omega_{X'})^* \simeq H^1(X, \mathcal{O}_X)^*$, the last isomorphism following from Serre duality.

Theorem 2.2.15 says in this situation:

$$T_pX \otimes_{\mathbf{Z}_p} \mathbf{C}_p \simeq \left(H^0(X, \Omega_X)^* \otimes_K \mathbf{C}_p(1)\right) \oplus \left(H^1(X, \mathcal{O}_X)^* \otimes_K \mathbf{C}_p\right).$$

The importance of this result cannot be overstated: it gives a very concrete structure of T_pX after extending scalars to $\mathbf{C}_p$.

Theorem 2.2.15 can be restated in a more compact way, by introducing the **Hodge-Tate ring of periods**:

$$B_{\mathrm{HT}} \overset{\mathrm{def}}{=} \bigoplus_{i \in \mathbf{Z}} \mathbf{C}_p(i),$$

with the Galois group G_K acting component-wise. Define also

$$H^1_{\mathrm{Hodge}}(X) \overset{\mathrm{def}}{=} \mathrm{Gr}\, H^1_{\mathrm{dR}}(X).$$

Corollary 3.1.1. *With the same hypothesis as in Theorem 2.2.15,*

$$\left(T_pX \otimes_{\mathbf{Z}_p} B_{HT}\right)^{G_K} = H^1_{Hodge}(X)^*.$$

Proof. Just note that

$$(T_pX \otimes_{\mathbf{Z}_p} \mathbf{C}_p)^{G_K} = H^1(X, \mathcal{O}_X)^*,$$

and

$$(T_pX \otimes_{\mathbf{Z}_p} \mathbf{C}_p(-1))^{G_K} = H^0(X, \Omega_X)^*.$$

Finally, if $i \neq 0, 1$, then

$$(T_pX \otimes_{\mathbf{Z}_p} \mathbf{C}_p(i))^{G_K} = 0.$$

Apply then Theorem 2.2.15 and the definitions of B_{HT} and $H^1_{\mathrm{Hodge}}(X)$, noting that the Hodge-deRham spectral sequence gives [1]:

$$H^1_{\mathrm{Hodge}}(X) = H^0(X, \Omega_X) \oplus H^1(X, \mathcal{O}_X).$$

□

3.2 A geometric approach

This theory was developed by Fontaine and Coleman. Let $\mathfrak{X}$ be an abelian scheme over $\mathcal{O}_K$, and let X be its generic fiber.

The scheme $\mathfrak{X}$ is proper, and the valuative criterion for properness gives that every $\mathcal{O}_{\overline{K}}$-point of $\mathfrak{X}$ extends to a $\overline{K}$-point of X[2]. In this way one obtains an identification $\mathfrak{X}(\mathcal{O}_{\overline{K}}) = X(\overline{K})$, which identifies

$$T_p\mathfrak{X} = T_pX = \varprojlim_n X[p^n](\overline{K}).$$

The natural map $H^0(\mathfrak{X}, \Omega_{\mathfrak{X}/\mathcal{O}_K}) \to H^0(X, \Omega_{X/K})$ is injective, and allows one to see $H^0(\mathfrak{X}, \Omega_{\mathfrak{X}/\mathcal{O}_K})$ as a lattice inside $H^0(X, \Omega_X)$, since

$$H^0(X, \Omega_X) \simeq H^0(\mathfrak{X}, \Omega_{\mathfrak{X}/\mathcal{O}_K}) \otimes_{\mathcal{O}_K} K.$$

Define a pairing

$$\langle \cdot, \cdot \rangle = \langle \cdot, \cdot \rangle_{\mathfrak{X}} \colon \mathfrak{X}(\mathcal{O}_{\overline{K}}) \times H^0(\mathfrak{X}, \Omega_{\mathfrak{X}/\mathcal{O}_K}) \to \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K},$$

given by $\langle u, \omega \rangle \overset{\mathrm{def}}{=} u^*(\omega)$. Here we think of u as belonging to $\mathrm{Hom}(\mathrm{Spec}\, \mathcal{O}_{\overline{K}}, \mathfrak{X})$.

[1] **FIXME:** Is this the spectral sequence that we consider?
[2] **FIXME:** why?

Lemma 3.2.1. *For all $u, u_1, u_2 \in \mathfrak{X}(\mathcal{O}_{\overline{K}})$, all $\omega, \omega_1, \omega_2 \in H^0(\mathfrak{X}, \Omega_{\mathfrak{X}/\mathcal{O}_K})$ and all $\sigma \in G_K$, we have:*

1. $\langle u, \omega_1 + \omega_2 \rangle = \langle u, \omega_1 \rangle + \langle u, \omega_2 \rangle$.
2. $\langle \sigma u, \omega \rangle = \sigma(\langle u, \omega \rangle)$.
3. $\langle u_1 + u_2, \omega \rangle = \langle u_1, \omega \rangle + \langle u_2, \omega \rangle$.

Proof. The first two statements are easy. We only prove additivity in the first component. Let $\omega \in H^0(\mathfrak{X}, \Omega_{\mathfrak{X}/\mathcal{O}_K})$. One needs to show[3] that ω is always translation invariant. That is, consider the three maps

$$m, \mathrm{pr}_1, \mathrm{pr}_2 \colon \mathfrak{X} \times \mathfrak{X} \to \mathfrak{X},$$

given respectively by multiplication and by the two natural projections. Then

$$m^*\omega = \mathrm{pr}_1^* \omega + \mathrm{pr}_2^* \omega.$$

Given u_1 and u_2, we need to compute $u_1 + u_2$. Thinking of u_1 and u_2 as morphisms, we can consider the commutative diagram:

$$\begin{array}{ccc} \operatorname{Spec} \mathcal{O}_{\overline{K}} & \xrightarrow{\Delta} & \operatorname{Spec} \mathcal{O}_{\overline{K}} \times \operatorname{Spec} \mathcal{O}_{\overline{K}} \\ \downarrow{\scriptstyle u_1+u_2} & & \downarrow{\scriptstyle u_1 \times u_2} \\ \mathfrak{X} & \xleftarrow[m]{} & \mathfrak{X} \times \mathfrak{X} \end{array}$$

Denote by v the composition $u_1 \times u_2 \circ \Delta$. Then:

$$\begin{aligned} \langle u_1 + u_2, \omega \rangle &= (u_1 + u_2)^*(\omega) \\ &= (m \circ v)^*(\omega) \\ &= v^*(m^*(\omega)) \\ &= v^*(\mathrm{pr}_1^*(\omega) + \mathrm{pr}_2^*(\omega)) \\ &= u_1^*(\omega) + u_2^*(\omega) = \langle u_1, \omega \rangle + \langle u_2, \omega \rangle. \end{aligned}$$

□

Corollary 3.2.2. *The following diagram commutes:*

$$\begin{array}{ccc} \mathfrak{X}(\mathcal{O}_{\overline{K}}) \times H^0(\mathfrak{X}, \Omega_{\mathfrak{X}/\mathcal{O}_K}) & \xrightarrow{\langle \cdot, \cdot \rangle} & \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K} \\ \downarrow{\scriptstyle [p] \times Id} & & \downarrow{\scriptstyle p} \\ \mathfrak{X}(\mathcal{O}_{\overline{K}}) \times H^0(\mathfrak{X}, \Omega_{\mathfrak{X}/\mathcal{O}_K}) & \xrightarrow{\langle \cdot, \cdot \rangle} & \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}. \end{array}$$

[3] **FIXME:** do it!

Let $\widetilde{X}$ be the projective limit of the sequence

$$X(\overline{K}) \xleftarrow{[p]} X(\overline{K}) \xleftarrow{[p]} X(\overline{K}) \xleftarrow{[p]} \cdots$$

The valuative criterion for properness implies as before that it is the same as the projective limit of the sequence

$$\mathfrak{X}(\mathcal{O}_{\overline{K}}) \xleftarrow{[p]} \mathfrak{X}(\mathcal{O}_{\overline{K}}) \xleftarrow{[p]} \mathfrak{X}(\mathcal{O}_{\overline{K}}) \xleftarrow{[p]} \cdots$$

Similarly, define $\widetilde{\Omega}$ to be the projective limit of the sequence

$$\Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K} \xleftarrow{p} \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K} \xleftarrow{p} \Omega^1_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K} \xleftarrow{p} \cdots .$$

It is easily seen that $\widetilde{\Omega} \simeq (T_p\Omega) \otimes_{\mathbf{Z}_p} \mathbf{C}_p \simeq \mathbf{C}_p(1)$.

The G_K-module $\widetilde{X}$ fits into an exact sequence, which is G_K-equivariant:

$$0 \to T_pX \to \widetilde{X} \to X(\overline{K}) \to 0.$$

Remark. One can think of T_pX as the fundamental group of $X_{\overline{K}}$, and so $\widetilde{X}$ can be thought of as the universal covering space for $X(\overline{K})$.

We can construct an integration pairing

$$\int : \widetilde{X} \times H^0(X, \Omega_X) \to T_p\Omega \otimes_{\mathbf{Z}_p} \mathbf{C}_p,$$

as follows: if $u = (u_n)_n$ is a coherent sequence in $\widetilde{X}$ and $\omega = \frac{\eta}{p^m}$ with η a global differential in $H^0(\mathfrak{X}, \Omega_{\mathfrak{X}/\mathcal{O}_K})$, then

$$\int_u \omega \stackrel{\text{def}}{=} \frac{1}{p^m}(u_n^*\eta)_n.$$

Proposition 3.2.3. *For all $u, u_1, u_2 \in \widetilde{X}$, all $\omega, \omega_1, \omega_2 \in H^0(X, \Omega_X)$ and all $\sigma \in G_K$, we have:*

1. $\int_u (a\omega_1 + b\omega_2) = a\int_u \omega_1 + b\int_u \omega_2$.
2. $\int_{\sigma u} \omega = \sigma\left(\int_u \omega\right)$.
3. $\int_{u_1+u_2} \omega = \int_{u_1} \omega + \int_{u_2} \omega$.

The restriction of *int* to $T_pX \times H^0(X, \Omega_X)$ done by identifying T_pX with a submodule of $\widetilde{X}$, gives a K-linear map

$$\rho_X \colon H^0(X, \Omega_X) \to \mathrm{Hom}_{\mathbf{Z}_p[G_K]}\left(T_pX, \mathbf{C}_p(1)\right),$$

given by $\rho_X(\omega)(u) = \int_u \omega$.

Theorem 3.2.4 (Fontaine)**.** *The K-linear map ρ_X is injective.*

Proof. Let $x \in \mathfrak{X}(\mathcal{O}_K)$, and consider its local ring $(\mathcal{O}_{\mathfrak{X},x}, \mathfrak{m}_{\mathfrak{X},x})$. Let $\widehat{\mathcal{O}_{\mathfrak{X},x}}$ denote the $\mathfrak{m}_{\mathfrak{X},x}$-adic completion of $\mathcal{O}_{\mathfrak{X},x}$:

$$\widehat{\mathcal{O}}_{\mathfrak{X},x} = \varprojlim_n \mathcal{O}_{\mathfrak{X},x}/\mathfrak{m}^n_{\mathfrak{X},x}.$$

As $\mathfrak{X}$ is smooth over $\mathcal{O}_K$, the completed local ring has a simple structure:

$$\widehat{\mathcal{O}}_{\mathfrak{X},x} \simeq \mathcal{O}_K [\![t_1, \ldots, t_2]\!] .$$

Consider the stalk of $\Omega^1_{\mathfrak{X}/\mathcal{O}_K}$ at x, denoted by $\Omega^1_{\mathfrak{X},x}$, and its $\mathfrak{m}_{\mathfrak{X},x}$-adic completion $\widehat{\Omega}_{\mathfrak{X},x}$. As before, one has

$$\widehat{\Omega}^1_{\mathfrak{X},x} \simeq \bigoplus_{i=1}^{d} \mathcal{O}_K [\![t_1, \ldots, t_2]\!] \, dt_i.$$

The natural map $\Omega^1_{\mathfrak{X},x} \to \widehat{\Omega}^1_{\mathfrak{X},x}$ is injective because $\Omega^1_{\mathfrak{X},x}$ has no $\mathfrak{m}_{\mathfrak{X},x}$-torsion. Every differential is invariant, so that a nonzero global differential is nonzero at all points. Hence the localization map $H^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \to \Omega^1_{\mathfrak{X},x}$ is also injective. We can thus see the space of global differentials as a subspace of the local differentials around x:

$$H^0(\mathfrak{X}, \Omega^1_{\mathfrak{X}/\mathcal{O}_K}) \hookrightarrow \widehat{\Omega}^1_{\mathfrak{X},x}.$$

Lemma 3.2.5. *Let $\omega = \sum_{i=1}^d \alpha_i(t_1, \ldots, t_d) dt_i$, with $\alpha_i \in \mathcal{O}_K [\![t_1, \ldots, t_d]\!]$. If ω is nonzero, then there exists a tuple $(u_1, \ldots, u_d) \in \mathfrak{m}^d_{\overline{K}}$ such that*

$$\sum_{i=1}^{d} \alpha_i(u_1, \ldots, u_d) du_i \neq 0,$$

as an element of $\Omega = \Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$.

Proof. First assume that $d = 1$ and write $\omega = \sum_{n=0}^{\infty} a_n t^n dt$, with $a_n \in \mathcal{O}_K$. Let s be the minimum valuation of all the a_n:

$$s \overset{\text{def}}{=} \{v(a_n) \mid n \geq 0\}.$$

and let i_0 be the smallest index i such that $v(a_i) = s$.

Let $u \in \mathfrak{m}_{\overline{K}}$ be such that $v(u) < 1/i_0$. Take u to be in a ramified extension of K. Then:

$$v(\sum a_n u^) = v(a_{i_0} u^{i_0}) = s + i_0 v(u) < s + 1.$$

The element u belongs to $\mathfrak{m}_L$, for some finite extension L of K which is totally ramified. Take it also large enough so that

$$v(\mathcal{D}_{L/K}) > s + 1,$$

and such that u is a uniformizer of L/K. [4]

Then

$$\mathrm{Ann}_{\mathcal{O}_L}(du) = \mathcal{D}_{L/K},$$

so that $\sum a_n u^n du \neq 0$ in $\Omega_{\mathcal{O}_L/\mathcal{O}_K} \hookrightarrow \Omega_{\mathcal{O}_{\overline{K}}}$.

The following lemma reduces this one to the case of $d = 1$, which finishes the proof. □

Lemma 3.2.6. *Write $\underline{t}$ for $(t_1, \dots, t_d)$, and similarly for $\underline{a}$. Let $\alpha_1(\underline{t}), \dots, \alpha_d(\underline{t})$ be a collection of power series in $\mathcal{O}_K[\![\underline{t}]\!]$, not all zero. Then there exists univariate power series $\varphi_1(y), \dots, \varphi_d(y) \in y\mathcal{O}_K[\![y]\!]$ such that*

$$\lambda_\varphi(y) \stackrel{def}{=} \sum_{i=1}^{d} \alpha_i\left(\varphi_1(y), \dots, \varphi_d(y)\right) \varphi_i'(y)$$

is not zero in $\mathcal{O}_K[\![y]\!]$.

Proof. We will actually find the $\varphi_i(y)$ as polynomials of the form $a_i y + b_i y^2$, with $a_i, b_i \in \mathcal{O}_K$. Write $\alpha_i(\underline{t}) = \sum_{m \geq 0} \alpha_{i,m}(\underline{t})$, where $\alpha_{i,m}(\underline{t})$ are homogeneous polynomials of degree m. Then:

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

Let r be the smallest integer such that there is some j with $\alpha_{j,r}$ nonzero. Then $\lambda_\varphi(y)$ can be written as a power series in y as:

$$\begin{aligned}\lambda_\varphi(y) &= \sum_{i=1}^{d} \left(a_i \alpha_{i,r}(\underline{a})\right) y^r \\ &+ \left(\sum_{i=1}^{d} a_i \alpha_{i,r+1}(\underline{a}) + \sum_{j=1}^{d} 2b_j \alpha_{j,r}(\underline{a}) + \sum_{i,j=1}^{d} a_i b_j \frac{\partial \alpha_{i,r}}{\partial t_j}(\underline{a})\right) y^{r+1} + \cdots\end{aligned}$$

To choose the a_i and b_i, we distinguish three cases:

1. If $\sum_{i=1}^{d} t_i \alpha_{i,r}(\underline{t}) \neq 0$, then there are elements $\underline{a} \in \mathcal{O}_K$ such that $\sum_{=1}^{d} t_i \alpha_{i,r}(\underline{a}) \neq 0$, and then $\lambda_\varphi(y)$ is nonzero for any choice of the b_i.
2. If $\sum_{i=1}^{d} t_i \alpha_{i,r}(\underline{t}) = 0$ but $\sum_{i=1}^{d} t_i \alpha_{i,r+1}(\underline{t}) \neq 0$, then choose all the b_j to be 0, and choose $\underline{a} \in \mathcal{O}_K$ such that $\sum_{=1}^{d} t_i \alpha_{i,r+1}(\underline{a}) \neq 0$.
3. Otherwise, choose any j such that $\alpha_{j,r}(\underline{t})$ is nonzero, and choose $\underline{a} \in \mathcal{O}_K$ such that $\alpha_{j,r}(\underline{a})$ is nonzero. Choose then $b_j = 1$, and all the $b_i = 0$ for $i \neq j$. A trivial check shows that this choice works.

[4] **FIXME:** This part of the argument needs to be improved.

□

Now that Lemma (3.2.5) is established, we return to the proof of Fontaine's theorem. Let $\omega \in H^0(\mathfrak{X}, \Omega_{\mathfrak{X}})$ and write $\widehat{\omega}_x$ for the corresponding element of $\widehat{\Omega}_{\mathfrak{X},x}$ under the inclusion $H^0(\mathfrak{X}, \Omega_{\mathfrak{X}}) \hookrightarrow \widehat{\Omega}_{\mathfrak{X},x}$ discussed above. The lemma supplies $u = (u_1, \dots, u_d) \in \mathfrak{m}_{\overline{K}}^d$ such that $\widehat{\omega}_x(u) \neq 0$ as an element of Ω. Evaluation at u gives a continuous homomorphism $\mathcal{O}_{\mathfrak{X},x} \to \mathcal{O}_{\overline{K}}$ of $\mathcal{O}_K$-algebras. This map can be used to define a map of schemes:

$$v\colon \operatorname{Spec}(\mathcal{O}_{\overline{K}}) \to \operatorname{Spec}(\mathcal{O}_{\mathfrak{X},x}) \to \mathfrak{X},$$

where the first map in the composition is induced by evaluation at u, and the second is the natural map. With this notation $v^*(\omega) = \widehat{\omega}_x(u) \neq 0$.

In order to analyze the map ρ_X, we realize it as a composition of two others maps and study each in turn. Towards this end define:

$$\phi_X\colon H^0(X, \Omega_X) \to \operatorname{Hom}_{\mathbf{Z}_p[G_K]}\left(\widetilde{X}, \mathbf{C}_p(1)\right)$$

which is defined via integration:

$$\phi_X(\omega)(u) = \int_u \omega.$$

We claim that ϕ_X is injective. Note that if it is not injective, then $H^0(\mathfrak{X}, \Omega_{\mathfrak{X}})$ contains a non-zero element of $\ker \phi_X$; this follows since $H^0(\mathfrak{X}, \Omega_{\mathfrak{X}})$ sits as an $\mathcal{O}_K$-lattice inside of $H^0(X, \Omega_X)$. Thus suppose $\omega \in H^0(\mathfrak{X}, \Omega_{\mathfrak{X}})$ is nonzero and satisfies $\phi_X(\omega) = 0$. This is the same as saying that for every $(u_n)_{n\geq 0} \in \widetilde{X}$:

$$\phi_X(\omega)\left((u_n)_{n\geq 0}\right) = (u_n^*(\omega))_{n\geq 0} = 0,$$

so that $u_n^*(\omega) = 0$ for all $n \geq 0$. Since $\widetilde{X}$ surjects onto $X(\overline{K})$, it follows that $v^*(\omega) = 0$ for all $v \in X(\overline{K})$. This contradicts Lemma (3.2.5) as per the discussion in the previous paragraph. This shows that ϕ_X is injective.

Next consider the exact sequence of Galois modules:

$$0 \to T_pX \to \widetilde{X} \to X(\overline{K}) \to 0$$

and apply the functor $\operatorname{Hom}_{\mathbf{Z}_p[G_K]}(-, \mathbf{C}_p(1))$ to obtain the exact sequence:

$$0 \to \operatorname{Hom}_{\mathbf{Z}_p[G_K]}(X(\overline{K}), \mathbf{C}_p(1)) \to \operatorname{Hom}_{\mathbf{Z}_p[G_K]}(\widetilde{X}, \mathbf{C}_p(1)) \xrightarrow{\psi_X} \operatorname{Hom}_{\mathbf{Z}_p[G_K]}(T_p(X), \mathbf{C}_p(1)).$$

Note that $\rho_X = \psi_X \circ \phi_X$. We thus see that in order to prove that ρ_X is injective, it will suffice to prove that ψ_X is injective. By the exactness of the sequence of above, this is tantamount to verifying that $\operatorname{Hom}_{\mathbf{Z}_p[G_K]}(X(\overline{K}), \mathbf{C}_p(1)) = 0$.

Suppose otherwise, and let $\phi\colon X(\overline{K}) \to \mathbf{C}_p(1)$ be a nonzero $\mathbf{Z}_p[G_K]$-module morphism. Let $x \in X(\overline{K})$ be such that $\phi(x) \neq 0$. Then there exists L/K finite, $L \subset \overline{K}$, such that $x \in X(L)$ and for all $\sigma \in G_L = \operatorname{Gal}(\overline{K}/L)$:

$$\sigma(\phi(x)) = \phi(\sigma x) = \phi(x).$$

So $\phi(x) \in (\mathbf{C}_p(1))^{G_L}$, contradicting our previous computation that $(\mathbf{C}_p(1))^{G_L} = 0$. This concludes the proof of Fontaine's theorem (3.2.4). $\square$

We next indicate how Tate's theorem (2.2.15) can be deduced from Fontaine's theorem (3.2.4). If one forgets the G_K-module structure, then ρ_X gives an injective map, which by abuse of notation we also call ρ_X:

$$\rho_X \colon H^0(X, \Omega_X) \hookrightarrow \mathrm{Hom}_{\mathbf{Z}_p}(T_p(X), \mathbf{C}_p(1)).$$

Note that:

$$\mathrm{Hom}_{\mathbf{Z}_p}(T_p(X), \mathbf{C}_p(1)) \cong (T_p(X))^* \otimes_{\mathbf{Z}_p} \mathbf{C}_p(1),$$

so that ρ_X induces an injection:

$$H^0(X, \Omega_X) \hookrightarrow (T_pX)^* \otimes_{\mathbf{Z}_p} \mathbf{C}_p(1).$$

This map remains an injection after tensoring $H^0(X, \Omega_X)$ with $\mathbf{C}_p$ to yield a $\mathbf{C}_p$-linear and G_K-equivariant map:

$$: H^0(X, \Omega_X) \otimes_K \mathbf{C}_p \hookrightarrow (T_p(X))^* \otimes_{\mathbf{Z}_p} \mathbf{C}_p(1).$$

Take $\mathbf{C}_p$-duals and twist by $\mathbf{C}_p(1)$ to obtain:

$$v \colon T_p(X) \otimes_{\mathbf{Z}_p} \mathbf{C}_p \twoheadrightarrow H^0(X, \Omega_X)^* \otimes_K \mathbf{C}_p(1).$$

Applying this discussion to the dual abelian variety X', one similarly obtains an injection:

$$H^0(X', \Omega_{X'}) \otimes_K \mathbf{C}_p \to (T_pX')^* \otimes_{\mathbf{Z}_p} \mathbf{C}_p(1) \cong T_pX \otimes_{\mathbf{Z}_p} \mathbf{C}_p.$$

Identifying $H^0(X', \Omega_{X'}) \cong H^1(X, \mathcal{O}_X)^*$ and call the resulting injection u:

$$u \colon H^1(X, \mathcal{O}_X)^* \otimes_K \mathbf{C}_p \hookrightarrow T_p(X) \otimes_{\mathbf{Z}_p} \mathbf{C}_p.$$

Since u and v are $\mathbf{C}_p$-linear and G_K-equivariant, u is injective and v is surjective, the same argument as above shows that:

$$0 \to H^1(X, \mathcal{O}_X)^* \otimes_K \mathbf{C}_p \xrightarrow{u} T_p(X) \otimes_{\mathbf{Z}_p} \mathbf{C}_p \xrightarrow{v} H^0(X, \Omega_X)^* \otimes_K \mathbf{C}_p(1) \to 0$$

is exact, and has a canonical G_K-equivariant splitting. This proves Tate's theorem (2.2.15).

Consider the consequent decomposition:

$$T_p(X) \otimes_{\mathbf{Z}_p} \mathbf{C}_p \cong \left(H^1(X, \mathcal{O}_X)^* \otimes_K \mathbf{C}_p\right) \oplus \left(H^0(X, \Omega_X)^* \otimes_K \mathbf{C}_p(1)\right).$$

We have already given a geometric interpretation of the projection:

$$T_p(X) \otimes_{\mathbf{Z}_p} \mathbf{C}_p \twoheadrightarrow H^0(X, \Omega_X)^* \otimes_K \mathbf{C}_p(1).$$

Our next task will be to give a geometric interpretation of the other projection:

$$\theta_X \colon T_p(X) \otimes_{\mathbf{Z}_p} \mathbf{C}_p H^1(X, \mathcal{O}_X)^* \otimes_K \mathbf{C}_p \cong H^0(X', \Omega_{X'}) \otimes_K \mathbf{C}_p.$$

For this we will need to recall some facts about duality for abelian varieties.

3.3 Duality of abelian varieties

Let X be an abelian variety over $\mathbf{C}_p$. Recall that the Picard group $\mathrm{Pic}(X)$ of X is the group of isomorphism classes of line bundles on X, where the group law is given by the tensor product. Recall further that $\mathrm{Pic}^0(X)$ denotes the subgroup of classes of line bundles that are **translation invariant** in the following sense: consider the three maps $p_1, p_2, m\colon X \times X \to X$ where the p_i's are the projections and m is the group law for X. Then translation invariance of a line bundle $\mathcal{L}$ corresponds to the condition:

$$m^*\mathcal{L} \cong p_1^*\mathcal{L} \otimes p_2^*\mathcal{L}.$$

The group $\mathrm{Pic}^0(X)$ can be seen as the $\mathbf{C}_p$-points of an abelian variety $X'/\mathbf{C}_p$. This is the **dual abelian variety** to X. We stress that the $\mathbf{C}_p$ points of X' correspond to translation invariant line bundles on X.

The duality between X and X' is expressed beautifully via the existence of the **Poincaré bundle**. This is a bundle $\mathcal{P} \to X \times X'$ such that for every $x \in X'(\mathbf{C}_p)$, corresponding to some translation invariant line bundle $\mathcal{L}_x$ on X, one has:

$$\mathcal{P}|_{X\times\{x\}} \cong \mathcal{L}_x.$$

The double duality $(X')' \cong X$ is given via the Poincaré bundle in the following way: for $x \in X(\mathbf{C}_p)$, consider $\mathcal{P}_{\{x\}\times X'}$, which is a translation invariant line bundle on X'. It thus corresponds to a $\mathbf{C}_p$ point of $(X')'$, so that the association $x \mapsto \mathcal{P}_{\{x\}\times X'}$ gives an isomorphism $X(\mathbf{C}_p) \cong (X')'(\mathbf{C}_p)$.

Now we use the theory of duality to describe the map:

$$\theta_X\colon T_pX \otimes_{\mathbf{Z}_p} \mathbf{C}_p \to H^0(X', \Omega_{X'}),$$

discussed above. Note that we work with $\theta_{X'}$ rather than θ_X, to simplify some notations. Note that double duality shows that:

$$\theta_X\colon T_p(X') \otimes_{\mathbf{Z}_p} \mathbf{C}_p \to H^0(X, \Omega_X).$$

Take $u = (u_n)_{n\geq 0} \in T_p(X')$, so that $u_n \in X'(\mathbf{C}_p)$ for all n. Write $\mathcal{L}_n \in \mathrm{Pic}^0(X)$ for the corresponding line bundle on X. We have $[p^n]u_n = 0$ for each n, and this corresponds to the identity:

$$\mathcal{L}_n^{\otimes p^n} \cong \mathcal{O}_X.$$

The triviality of $\mathcal{L}_n^{\otimes p^n}$ is equivalent to the existence of a nonzero global section $f_n \in \mathcal{L}_n^{\otimes p^n}(\mathcal{O}_X)$, which we regard as a unit in the function field, $f_n \in K(X)^\times$. Then consider $\omega_n = df_n/f_{n+1}$, which is a meromorphic differential of the third kind on X.

We claim that the sequence $(\omega_n)_{n\geq 0}$ converges in the vector space of meromorphic differentials of the third kind on X, and that the limit is actually a regular differential. The point is that the residue of ω_n is divisible by p^n, so it vanishes as n tends to infinity. To see this, suppose $m > n$ and note that $[p^{m-n}]u_m = u_n$ by definition of $T_p(X')$, which corresponds to the identity:

$$\mathcal{L}_m^{\otimes p^{m-n}} \otimes \mathcal{L}_n^{-1} \cong \mathcal{O}_K.$$

It follows that this bundle has a global nonzero section $g_{m,n} \in H^0(X, \mathcal{L}_m^{\otimes p^{m-n}} \otimes \mathcal{L}_n^{-1})$. But then:

$$\frac{df_m}{f_m} - \frac{df_n}{f_n} = p^n \frac{dg_{m,n}}{g_{m,n}},$$

and since the absolute values of the residues of the ω_n's are all at most 1[5], it follows that $(\omega_n)_{n\geq 0}$ is a Cauchy-sequence. Accepting that the space of meromorphic differentials of the third kind on X is a complete vector space, it follows that $(\omega_n)_{n\geq 0}$ converges to a regular differential on X, as was claimed. One can show that:

$$\theta_X(u) = \lim_{n\to\infty} \omega_n \in H^0(X, \Omega_X).$$

3.4 de Rham theory for abelian varieties with good reduction

Let $K/\mathbf{Q}_p$ be finite as above, and let X be an abelian scheme defined over K. Suppose for simplicity that X has good reduction, so that our work above applies. Note however that one can work more generally with arbitrary reduction type.

Recall that the **Hodge-Tate period ring** is the direct sum:

$$B_{\mathrm{HT}}(T_p X) = \bigoplus_{n\in\mathbf{Z}} \mathbf{C}_p(n).$$

We have shown that:

$$D_{\mathrm{HT}}(T_p X) = (T_p(X) \otimes_{\mathbf{Z}_p} B_{\mathrm{HT}})^{G_K} \cong H^1_{\mathrm{Hodge}}(X)^*.$$

One can use a similar formalism, with different methods and a new period ring B_{dR}, to recover $H^1_{\mathrm{dR}}(X)$. In what follows we will define the de Rham period ring B_{dR} and prove the following theorem:

Theorem 3.4.1. *Let X be an abelian scheme defined over K with good reduction. If we write:*

$$D_{dR}((T_p X)^*) = ((T_p X)^* \otimes_{\mathbf{Z}_p} B_{dR})^{G_K},$$

then there exists a canonical isomorphism:

$$D_{dR}((T_p X)^*) \cong H^1_{dR}(X).$$

We remark once again that this theorem holds without the assumption of good reduction.

Before proceeding to discuss theorem (3.4.1), we recall some facts about B^+_{dR} and B_{dR}. Some of the key properties of B_{dR} are that it is a field of characteristic, it is complete with respect to a discrete valuation, and B^+_{dR} denotes the corresponding ring

[5] **FIXME:** Why?

of integers. We write $\mathfrak{m}_{\mathrm{dR}}$ for the maximal ideal of B_{dR}^+; let $t \in \mathfrak{m}_{\mathrm{dR}}$ be a uniformizer. If $\sigma \in G_K$, then σ acts on t via the cyclotomic character:

$$\sigma(t^n) = \chi(\sigma)^n t^n.$$

The field B_{dR} is filtered by the maximal ideal $\mathfrak{m}_{\mathrm{dR}}$. We write:

$$\mathrm{Fil}^i B_{\mathrm{dR}} = t^i B_{\mathrm{dR}}^+$$

for all $i \in \mathbf{Z}$.

Before we can prove theorem (3.4.1), we would like to discuss a helpful reduction. Write $V_p(X) = T_p(X) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ and $V = (V_p(X))^*$. Set $B_2 = B_{\mathrm{dR}}^+/(t^2 B_{\mathrm{dR}}^+)$ and consider the projection:

$$\pi \colon B_{\mathrm{dR}}^+ \to B_2,$$

as well as the natural inclusion:

$$i \colon B_{\mathrm{dR}}^+ \to B_{\mathrm{dR}}.$$

These induce maps:

$$\pi_K \colon (V \otimes_{\mathbf{Q}_p} B_{\mathrm{dR}}^+)^{G_K} \to D_{\mathrm{dR}}(V),$$

and:

$$i_K \colon (V \otimes_{\mathbf{Q}_p} B_{\mathrm{dR}}^+)^{G_K} \to (V \otimes_{\mathbf{Q}_p} B_2)^{G_K}.$$

Note that i_K is still injective since the finite dimensional $\mathbf{Q}_p$-vector space V is flat over $\mathbf{Q}_p$. We would like to show that π_K and i_K are isomorphisms, so that our study of $D_{\mathrm{dR}}(V)$ amounts to a studying $(V \otimes_{\mathbf{Q}_p} B_2)^{G_K}$.

To see that π_K and i_K are isomorphisms, first note that $t^2 B_{\mathrm{dR}}/(t^3 B_{\mathrm{dR}}) \simeq \mathbf{C}_p(2)$. We thus have an exact sequence:

$$0 \to \mathbf{C}_p(2) \to B_{\mathrm{dR}}^+/(t^3) \to B_{\mathrm{dR}}^+/(t^2) \to 0.$$

All maps are of K-Banach spaces, so that there exists a K-linear splitting (which is not G_K-equivariant). It follows that the exact sequence:

$$0 \to V \otimes_{\mathbf{Q}_p} \mathbf{C}_p(2) \to V \otimes_{\mathbf{Q}_p} \left(B_{\mathrm{dR}}^+/(t^3)\right) \to V \otimes_{\mathbf{Q}_p} \left(B_{\mathrm{dR}}^+/(t^2)\right) \to 0$$

also has a splitting, and there is thus a corresponding long exact sequence of continuous Galois cohomology. Since $V \otimes_{\mathbf{Q}_p} \mathbf{C}_p(2) \cong \mathbf{C}_p(2)^d \otimes \mathbf{C}_p(1)^d$, where $d = \dim X$, our work in the first chapter shows that the cohomology of $V \otimes_{\mathbf{Q}_p} \mathbf{C}_p(2)$ vanishes in all degrees. In particular, the long exact sequence gives:

$$\left(V \otimes_{\mathbf{Q}_p} \left(B_{\mathrm{dR}}^+/(t^3)\right)\right)^{G_K} \cong \left(V \otimes_{\mathbf{Q}_p} \left(B_{\mathrm{dR}}^+/(t^2)\right)\right)^{G_K}.$$

One continues by induction to show that for all $n \geq 2$, the natural surjection $B_{\mathrm{dR}}^+/(t^n) \twoheadrightarrow B_{\mathrm{dR}}^+/(t^2)$ induces isomorphisms:

$$\left(V \otimes_{\mathbf{Q}_p} \left(B_{\mathrm{dR}}^+/(t^n)\right)\right)^{G_K} \cong \left(V \otimes_{\mathbf{Q}_p} \left(B_{\mathrm{dR}}^+/(t^2)\right)\right)^{G_K}.$$

Taking projective limits gives:

$$(V \otimes_{\mathbf{Q}_p} B_{\mathrm{dR}}^+)^{G_K} \cong (V \otimes_{\mathbf{Q}_p} B_2)^{G_K},$$

and one can check that this isomorphism is precisely π_K.

To show that i_K is an isomorphism, one uses the fact that $B_{\mathrm{dR}} = \varinjlim_n t^{-n} B_{\mathrm{dR}}^+$, and the exact sequence:

$$0 \to B_{\mathrm{dR}}^+ \to t^{-1} B_{\mathrm{dR}}^+ \to \mathbf{C}_p(-1) \to 0$$

to similarly show that i_K is an isomorphism. This reduces the study of $D_{\mathrm{dR}}(V)$ to the study of $(V \otimes_{\mathbf{Q}_p} B_2)^{G_K}$. The advantage to this approach is that B_2 is a much more simple ring than B_{dR}.

3.5 The de Rham cohomology of schemes

Let $S = \operatorname{Spec} B$ be an affine scheme. Let $f\colon Y \to S$ be a smooth scheme of finite type. In applications, we will usually require that B is a finite extension of $\mathbf{Q}_p$, or its ring of integers. We will usually need to assume also that Y is proper.

Define the quasi-coherent sheaves of $\mathcal{O}_S$-modules on S:

$$\mathcal{H}_{\mathrm{dR}}^i(Y/S) \stackrel{\mathrm{def}}{=} \mathbb{R}^i f_* \Omega_{Y/S}^\bullet.$$

By taking global sections, we can think of $\mathcal{H}_{\mathrm{dR}}^i(Y/S)$ as B-modules. These can be described using Čech cohomology. [6]

There are maps

$$H^0\left(Y, \Omega_{Y/S}^{1,\mathrm{closed}}\right) \xrightarrow{a} H_{\mathrm{dR}}^1(Y/S) \xrightarrow{b} H^1(Y, \mathcal{O}_Y).$$

[7]

Proposition 3.5.1. *If B is of characteristic zero and Y is proper over B, then*

1. *The natural inclusion $H^0(Y, \Omega_{Y/S}^{1,closed}) \hookrightarrow H^0(Y, \Omega_{Y/S}^1)$ is an isomorphism.*
2. *The sequence of B-modules*

$$0 \to H^0\left(Y, \Omega_{Y/S}^1\right) \to H_{dR}^1(Y/S) \to H^1(Y, \mathcal{O}_Y) \to 0$$

is exact.

[6] **FIXME:** We should add our notes here.
[7] **FIXME:** Add how to define this.

Proof. The exactness of the sequence follows from the degeneration of the Hodge to de Rham spectral sequence at the first step. This was shown by Deligne and Illusie. Otherwise, one can use the Lefschetz principle and prove it using harmonic theory. [8] □

We obtain a filtration and a corresponding grading of $H^1_{\mathrm{dR}}(Y/S)$:

$$\mathrm{Fil}^i\, H^1_{\mathrm{dR}}(Y/S) = \begin{cases} H^1_{\mathrm{dR}}(Y/S) & i \leq 0 \\ H^0(Y, \Omega^1_{Y/S}) & i = 1 \\ 0 & i \geq 2. \end{cases}$$

and also $\mathrm{Gr}^0\, H^1_{\mathrm{dR}}(Y/S) = \mathrm{Fil}^0 / \mathrm{Fil}^1 \simeq H^1(Y, \mathcal{O}_Y)$.

Another consequence is that $H^1_{\mathrm{dR}}(Y/S)$ is a locally-free B-module of finite rank, because both $H^0(Y, \Omega^1_{Y/S})$ and $H^1(Y, \mathcal{O}_Y)$ are.

3.6 Vectorial extensions of abelian schemes

3.6.1 Vector groups

Let B be a commutative ring. Assume that B is reduced and flat as a $\mathbf{Z}$-algebra. For our applications, it suffices to consider B a finite extension of $\mathbf{Q}_p$ or its ring of integers.

Let $S = \operatorname{Spec} B$, and fix $\mathcal{L}$ a coherent sheaf of $\mathcal{O}_S$-modules on S corresponding to a B-module M. Consider $\operatorname{Sym} M$, the symmetric algebra over B defined by M.

Example. 1. If $M = B$, then $\operatorname{Sym} M$ is canonically isomorphic to $B[x]$, the polynomial algebra, where x corresponds to $1 \in M$ has degree 1.

2. More generally, if M is a free B-module of rank n with basis $\{e_1, \dots, e_n\}$, then $\operatorname{Sym} M$ is canonically isomorphic to the polynomial algebra in n variables.

Define the S-scheme $V(\mathcal{L}) \stackrel{\text{def}}{=} \operatorname{Spec}(\operatorname{Sym} M)$. We will make it into a group scheme. For that, let R be any B-algebra. Then:

$$V(\mathcal{L})(R) = \mathrm{Hom}_{B-\mathrm{alg}}(\operatorname{Sym} M, R) = \mathrm{Hom}_{B-\mathrm{mod}}(M, R).$$

Note that the right hand side has a natural structure of R-module, and so $R^\times$ acts on it. This makes $V(\mathcal{L})$ into a group scheme in a natural way, which is endowed with a canonical action of $\mathbb{G}_m$.

Definition 3.6.1. The group scheme $V(\mathcal{L})$ just defined is called the **vector group** over B corresponding to $\mathcal{L}$ (or to M).

[8] **FIXME:** Add a proper proof.

If M is locally-free of finite rank over B and $\mathcal{L}$ is the sheaf associated to M, then

$$V(\mathcal{L})(R) \simeq \mathrm{Hom}_{R-\mathrm{mod}}(M, R) \simeq M^* \otimes_B R,$$

and hence:

$$V(\mathcal{L}) \simeq \underline{M^*} \times_{\mathrm{Spec}\, B} \mathbb{G}_a.$$

In particular, if M is free we have $V(\mathcal{L})$ isomorphic to $\mathbb{G}_a^n$ where n is the B-rank of M.

3.6.2 Vectorial extensions

Let B be as before, and let X/B be an abelian scheme.

Definition 3.6.2. A **vectorial extension** of X is a group scheme G over B, together with a morphism $f\colon G \to X$ such that there is a vector group V and an exact sequence of group schemes over B:

$$0 \to V \to G \xrightarrow{f} X \to 0.$$

Remark. As the first cohomology group of V for the fppf-topology vanishes, to check exactness in the previous sequence is equivalent to checking exactness of

$$0 \to V(R) \to G(R) \xrightarrow{f_R} X(R) \to 0$$

for every B-algebra R.[9]

Proposition 3.6.3. *There is a canonical bijection*

$$\varphi_X\colon H^1(X, \mathcal{O}_X) \to \mathrm{Ext}^1_{\boldsymbol{GrpSch}/B}(X, V(\mathcal{O}_S))$$

which becomes a group isomorphism when the right hand side is endowed with the Baer sum.

Proof. We define explicitly φ_X and its inverse ψ_X.

Given $x \in H^1(X, \mathcal{O}_X)$, find a cover $\mathcal{C} = \{U_i\}_{i\in I}$ of X by open affine subsets, and write $U_i = \mathrm{Spec}\, A_i$, and write x as the class of the sequence $(f_{ij})_{(i,j)\in I^2}$, with $f_{ij} \in \mathcal{O}_X(U_i \cap U_j)$. For each $i \in I$, consider the affine line over U_i:

$$G_i \stackrel{\mathrm{def}}{=} \mathrm{Spec}(A_i[x_i]).$$

We glue the family $(G_i)_{i\in I}$ along $U_{ij} = U_i \cap U_j$ with the gluing data:

$$x_i|_{U_{ij}} - x_j|_{U_{ij}} = f_{ij},$$

and denote by G the scheme thus obtained. It is a group scheme together with a surjective map $f\colon G \to X$, and the kernel of f is $\mathbb{G}_a$.

[9] **FIXME:** Is the justification correct?

We define now ψ_X. Given

$$\Xi\colon 0 \to \mathbb{G}_a \to G \xrightarrow{f} X \to 0,$$

think of G as a $\mathbb{G}_a$-torsor over X [10]. It is locally trivial over X, so one can find an open affine covering $\mathcal{C} = \{U_i\}_{i\in I}$, such that the following triangle commutes:

$$\begin{array}{ccc} G_i \overset{\text{def}}{=} f^{-1}(U_i) & \xrightarrow[\cong]{\alpha_i} & \mathbb{G}_a \times U_i \\ & \searrow \quad \swarrow_{\mathrm{pr}_2} & \\ & U_i & \end{array}$$

By restricting to U_{ij} we obtain transition functions $f_{ij} \in \mathcal{O}_X(U_{ij})$. The family $(f_{ij})_{i,j}$ is a 1-cocycle for $H^1(X, \mathcal{O}_X)$ and we define $\psi_X(\Xi) = [(f_{ij})]$.

A trivial check proves that φ_X and ψ_X are mutual inverses. $\square$

Let $M = H^1(X, \mathcal{O}_X)^*$ be the B-dual of the first cohomology group of X with values on $\mathcal{O}_X$. Let $\mathcal{L}$ be the sheaf of $\mathcal{O}_S$-modules on $S = \operatorname{Spec} B$ associated to M, and let $W = W_X = V(\mathcal{L})$. Then there is a unique vectorial extension G_X of X by W_X, which is universal in the following sense: for any vectorial extension

$$\Xi\colon 0 \to V \to G \to X \to 0,$$

there exists a unique morphism of vectorial extensions $w\colon W_X \to V$ such that Ξ is the pushout of G_X by w:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_X & \longrightarrow & G_X & \longrightarrow & X & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle w} & & \downarrow & & \downarrow{\scriptstyle =} & & \\ 0 & \longrightarrow & V & \longrightarrow & G & \longrightarrow & X & \longrightarrow & 0 \end{array}$$

and the left square is cartesian.

Remark. In order to help motivate the preceding material, we specialize to a classical case. Let Y be a smooth proper curve over $\mathbf{C}$. Then we can consider the Jacobian of Y, say $X = \operatorname{Jac}(Y)$, which is an abelian variety. As always, we write X' for the dual abelian variety of X. Although it is not true for abelian varieties in general, for Jacobian varieties one has a natural isomorphism $H^1_{\mathrm{dR}}(X/\mathbf{C}) \cong H^1_{\mathrm{dR}}(X'/\mathbf{C})$. Composition with the identification $H^1_{\mathrm{dR}}(X/\mathbf{C})^* \cong H^1_{\mathrm{dR}}(X'/\mathbf{C})$, which *does* hold for arbitrary abelian varieties, thus gives a natural self duality:

$$H^1_{\mathrm{dR}}(X/\mathbf{C}) \cong H^1_{\mathrm{dR}}(X/\mathbf{C})^*.$$

Recall that integration gives a natural pairing:

$$H_1(Y(\mathbf{C}), \mathbf{Z}) \times H^1_{\mathrm{dR}}(Y/\mathbf{C}) \to \mathbf{C},$$

[10] **FIXME:** what is this?

which is perfect and induces a natural inclusion:

$$\iota H_1(Y(\mathbf{C}), \mathbf{Z}) \hookrightarrow H^1_{\mathrm{dR}}(Y/\mathbf{C})^* \cong H^1_{\mathrm{dR}}(X/\mathbf{C})^* \cong H^1_{\mathrm{dR}}(X/\mathbf{C}).$$

If Y is of genus g, then $\dim X = g$, and $H^1_{\mathrm{dR}}(X/\mathbf{C})$ is a $(2g)$-dimensional real vector space. The map ι embeds $H_1(Y(\mathbf{C}), \mathbf{Z})$ as a real lattice of rank $(2g)$ in $H^1_{\mathrm{dR}}(X/\mathbf{C})$. In fact, ι factors through $H^0(X, \Omega^1_{X/\mathbf{C}}) \subseteq H_{\mathrm{dR}}(X/CC)$. Integration yields a group isomorphism:

$$X(\mathbf{C}) \cong \frac{H^0(X, \Omega^1_{X/\mathbf{C}})}{\iota(H_1(Y(\mathbf{C}), \mathbf{Z}))}.$$

One may thus rewrite the Hodge filtration for $X/\mathbf{C}$ in the form:

$$0 \to H^1(X, \mathcal{O}_X) \to \frac{H^1_{\mathrm{dR}}(X/\mathbf{C})}{H_1(Y(\mathbf{C}), \mathbf{Z})} \to X(\mathbf{C}) \to 0.$$

Serre duality gives $H^1(X, \mathcal{O}_X) \cong W_X(\mathbf{C})$. Thus, the filtration above gives a concrete realization of the universal vectorial extension of X by $H^1(X, \mathcal{O}_X)$:

$$G_X(\mathbf{C}) \cong \frac{H^1_{\mathrm{dR}}(X/\mathbf{C})}{H_1(Y(\mathbf{C}), \mathbf{Z})}.$$

Lemma 3.6.4. *Every $\omega \in \mathrm{Inv}(G_X)$ is closed.*

Proof. To be added! [11] □

It follows from the lemma that there is a natural map:

$$\beta_X \colon \mathrm{Inv}(G_X) \hookrightarrow H^0(G_X, \Omega^{1,\mathrm{closed}}_{G_X/S}) \to H^1_{\mathrm{dR}}(G_X/S).$$

Theorem 3.6.5. 1. *There is a canonical isomorphism α_X making the following diagram commute:*

$$\begin{array}{ccc} H^1_{dR}(X/B) & \xrightarrow[\cong]{\alpha_X} & \mathrm{Inv}(G_X) \\ & \searrow^{f^*} & \downarrow{\scriptstyle \beta_X} \\ & & H^1_{dR}(G_X/B). \end{array}$$

2. *The map f^* is injective. If $B = K$ is a finite extension of $\mathbf{Q}_p$, then f^* is an isomorphism.*

Remark. This theorem gives a geometric interpretation of the Hodge filtration, which can be thought of as the sequence obtained by applying the functor $\mathrm{Inv}(-)$ to the universal vectorial extension.

[11] **FIXME:** Add proof!!

Proof. We begin by describing the map α_X. Take $\omega \in H^1_{\mathrm{dR}}(X/B)$ and represent it by a 1-hypercocycle: say $\{U_i\}_{i\in I}$ is a covering of X by affine open subsets, say $U_i = \mathrm{Spec}(A_i)$, with:

$$\omega = [((\omega_i)_{i\in I}, (f_{ij})_{i,j\in I}].$$

The 1-hypercocyle condition for this coset representative implies that $(f_{ij})_{i,j\in I}$ represents an element of $H^1(X, \mathcal{O}_X)$. Let:

$$0 \to \mathbf{G}_a \to H \xrightarrow{h} X \to 0 \tag{3.1}$$

denote the corresponding vectorial extension associated to the 1-cocycle $(f_{ij})_{i,j\in I}$. For each $i \in I$ let $H_i = \mathrm{Spec}(A_i[X])$. Glue H_i and H_j over $U_i \cap U_j$ using the gluing data $X_i - X_j = h^*(f_{ij})$. For each $i \in I$ write $\eta_i = h^*(\omega_i) - dX_i$, so $\eta_i \in \Omega^1_{H/B}(H_i)$. Note that if we write $H_{ij} = H_i \cap H_j$ as usual, then:

$$\eta_i|_{H_{ij}} - \eta_j|_{H_{ij}} = h^*(\omega_i|_{U_{ij}} - \omega_j|_{U_{ij}} - f_{ij}) = 0,$$

since ω is a 1-hypercocyle. This shows that the η_i's glue to yield a global differential $\eta \in H^0(H, \Omega^1_{H/B})$. In fact, one can check that $\eta \in \mathrm{Inv}(H)$. The universal property of the universal vectorial extension G_X implies that there exists a unique morphism h of vectorial extensions between the universal extension and the extension (3.1):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W_X & \longrightarrow & G_X & \xrightarrow{f} & X & \longrightarrow & 0 \\ & & \downarrow w & & \downarrow \beta & & \| & & \\ 0 & \longrightarrow & \mathbf{G}_a & \longrightarrow & H & \xrightarrow{h} & X & \longrightarrow & 0 \end{array}$$

Define α_X by putting $\alpha_X(\omega) = \beta^*(\eta)$. Since $\eta \in \mathrm{Inv}(H)$, it follows that $\alpha_X(\omega) \in \mathrm{Inv}(G_X)$.

We must check that α_X is well-defined. Suppose that the 1-hypercocycle ω above is actually a 1-hypercoboundary. Then it follows that $(f_{ij})_{i,j\in I} \in H^1(X, \mathcal{O}_X)$ is a 1-cocycle, so that the corresponding vectorial extension (3.1) is canonically split. This implies that the map $w\colon W_X \to \mathbf{G}_a$ is zero in this case, hence also $\beta = 0$. We see that $\alpha_X(\omega) = \beta^*(\eta) = 0$, as it should be. It remains to show that α_X is an isomorphism. [12]

We now turn to prove part (b). Since $f^* = \beta_X \circ \alpha_X$ is a composition of injective maps, it follows that f^* is itself injective. Now take $B = K$, and consider again the universal vectorial extension:

$$0 \to W_X \to G_X \xrightarrow{f} X \to 0.$$

Recall that the de

$$H^1_{\mathrm{dR}}(G_X/X) = (\mathbb{R}^i f_*)(\Omega^\bullet_{G_X/X}).$$

There is a spectral sequence:

$$H^j(X, H^i_{\mathrm{dR}}(G_X/X)) \implies H^{i+j}_{\mathrm{dR}}(G_X/K),$$

[12] **FIXME:** Add details!

which we will show degenerates at E_1 [13].

Let A be a K-algebra, and consider the additive group $\mathbf{G}_{a,A}$ over $\operatorname{Spec}(A)$. Since $\operatorname{char}(K) = 0$, one can integrate formally to show that:

$$H^1_{\mathrm{dR}}(\mathbf{G}_{a,A}/\operatorname{Spec}(A)) = \frac{\Omega^1_{A[X]/A}}{d(A[X])} = 0.$$

Similarly, $H^i_{\mathrm{dR}}(\mathbf{G}^m_{a,A}/\operatorname{Spec}(A)) = 0$ for all $i > 0$ and all $m \geq 1$. The sheaf $H^1_{\mathrm{dR}}(G_X/X)$ is the sheaf associated to the presheaf:

$$U \mapsto H^i_{\mathrm{dR}}(f^{-1}(U)/U).$$

Is U is an open affine which is "small enough", then $f^{-1}(U) \cong W_X \times U \cong \mathbf{G}^d_{a,A}$ for some $d \geq 1$. For such U we thus have $H^i_{\mathrm{dR}}(f^{-1}(U)/U) = 0$, so that the stalks of $H^i_{\mathrm{dR}}(G_X/X)$ vanish at all points. Hence $H^i_{\mathrm{dR}}(G_X/X) = 0$ for all $i > 0$. This gives the desired degeneration of the spectral sequence above, so that:

$$H^i_{\mathrm{dR}}(X/K) \cong H^i_{\mathrm{dR}}(G_X/K).$$

One should verify that this isomorphism corresponds to the map f^*. □

3.6.3 Tangent spaces and lie algebras of group schemes

Let B be a ring. Let G be a group scheme defined over B, and M a B-module. Write $e \in G(B)$ for the identity element. An M-valued tangent vector to G at the identity is a B-derivation:

$$t\colon \mathcal{O}_{\mathbf{G},e} \to M,$$

where we regard M as an $\mathcal{O}_{\mathbf{G},e}$-module via the map $\mathcal{O}_{\mathbf{G},e} \to B$. Let $t_G(M)$ denote the collection of all M-valued tangent vectors. Let Lie_G denote the set of all B-derivations $D\colon \mathcal{O}_{\mathbf{G}} \to \mathcal{O}_{\mathbf{G}}$ that are left invariant, which is naturally a B-module.

We admit the following lemmas without proof:

Lemma 3.6.6. *There is a canonical perfect pairing:*

$$\operatorname{Lie}_G \times \operatorname{Inv}(G) \to B.$$

Lemma 3.6.7. *If M is a B-module, then* $\operatorname{Lie}_G \otimes_B M \cong t_G(M)$.

Now let A, B and C be rings, and suppose given ring homomorphisms $A \to B$ and $B \to C$. Regard C as an A-algebra via the composite of these two maps. Write $C[\varepsilon] = C[X]/(X^2)$ for the ring of dual numbers over C. Let $I \subset C[\varepsilon]$ denote the ideal generated by the image of the variable X in $C[\varepsilon]$. The following lemma realizes derivations as points of a "first order deformation" of C:

[13] **FIXME:** is this the correct degeneration?

Lemma 3.6.8. *Let notation be as above. Then the map:*

$$\mathrm{Der}_B(A,C) \to \{\phi\colon A \to C[\varepsilon] \mid \phi \textit{ is an } A\textit{-algebra map with } \phi(b)-b \in I \textit{ for all } b \in B\}$$

given by $D \mapsto (b \mapsto b + \varepsilon D(b))$ *is an isomorphism of* A*-modules.*

Proof. To be added later [14] □

We would like to apply this to our situation, where B is our chosen ground ring and $\mathbf{G}$ is a group scheme over B. Let $A = \mathcal{O}_{\mathbf{G},e}$, and consider the ring maps:

$$A \xrightarrow{e} B \to C.$$

By the preceding lemma, each $t \in t_G(C) = \mathrm{Der}_B(A,C)$ corresponds to:

$$\phi \in \{\phi\colon A \to C[\varepsilon] \mid \phi \text{ is an } A\text{-algebra map with } \phi(b) - b \in I \text{ for all } b \in B\}.$$

This induces maps:

$$\mathrm{Spec}(C[\varepsilon]) \to \mathrm{Spec}(\mathcal{O}_{\mathbf{G},e}) \to G(C),$$

and one obtains a natural identification:

$$t_G(C) = \ker\left(G(C[\varepsilon]) \to G(C)\right).$$

This is the main tool that allows us to integrate. [15]

We will apply the above discussion to the universal vectorial extension:

$$0 \to W_X \to G_X \to X \to 0,$$

where X is an abelian scheme over B. Recall that $B_2 = B_{\mathrm{dR}}^+/t^2B_{\mathrm{dR}}^+$ fits into a non-split exact sequence:

$$0 \to I \to B_2 \to \mathbf{C}_p \to 0,$$

where $I \cong \mathbf{C}_p(1)$ as G_K-modules. This sequence induces an exact sequence:

$$0 \to \mathrm{Lie}_X \otimes_K \mathbf{C}_p(1) \to X(B_2) \to X(\mathbf{C}_p) \to 0.$$

Take $x = (x_n)_{n\geq 1} \in X[p^n](\overline{K})$, which lifts to some $\widehat{x} \in X(B_2)$. Write $\widehat{x} = (\widehat{x_n})$. Then $t_n = [p^n]\widehat{x_n}$ is a tangent vector, and we must show that the t_n's converge to some $t \in \mathrm{Lie}_X \otimes_K \mathbf{C}_p(1)$. This strategy will not work. Philosophically the argument is correct, but a modified integration argument is required. Assume for the moment that the sequence does converge. Then given $\omega \in H^0(X, \Omega^1_{X/K}) = \mathrm{Inv}(X)$, one can pair:

$$\langle t, \omega\rangle = \int_x \omega \in \mathbf{C}_p(1),$$

where the integral is the one discussed previously. With these notations, one has the following theorem:

[14] **FIXME:** Should add more details
[15] **FIXME:** This section needs to be cleaned up

Theorem 3.6.9 (Fontaine-Messing)**.** *Let $X/\mathcal{O}_K$ be an abelian scheme. Then there is a canonical integration pairing:*

$$\langle\cdot,\cdot\rangle_{dR}\colon T_pX \times H^1_{dR}(X/\operatorname{Spec}(K)) \to B_2,$$

where $\langle x,\omega\rangle_{dR} = \int_x \omega$. The pairing is bilinear and perfect. It is G_K-equivariant in the first argument. Moreover, it respects filtrations in the following sense: for all $\omega \in H^0\left(X,\Omega^1_{X/K}\right)$ and all $x \in T_p(X)$,

$$\int_x \omega \in tB_2 = \operatorname{Fil}^1(B_2).$$

Corollary 3.6.10. *There is a canonical isomorphism of filtered K-vector spaces:*

$$D_{dR}((T_pX)^*) \cong H^1_{dR}(X/K),$$

and the Galois representation $V_p(X) = T_p(X) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ is de Rham.

3.7 Proof of the Theorem of Fontaine-Messing

[16]

3.7.1 Integral structure of $B_2 = {B_{\mathbf{dR}}}^+/I^2$

We recall the construction of B_2, together with its integral structure A_2.

Let $R = \varprojlim \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}} = \varprojlim \mathcal{O}_{\mathbf{C}_p}/p\mathcal{O}_{\mathbf{C}_p}$, where the transition maps are given by $x \mapsto x^p$. It is a perfect $\overline{\mathbf{F}_p}$-algebra. Let $A_{\text{inf}} = W(R)$ be its ring of Witt vectors, which is a $W(\overline{\mathbf{F}_p})$-algebra. It comes equipped with a surjective ring homomorphism

$$\theta\colon A_{\text{inf}} \to \mathcal{O}_{\mathbf{C}_p},$$

and we let $J \stackrel{\text{def}}{=} \ker\theta$, which is a principal ideal in A_{inf} generated by

$$\xi \stackrel{\text{def}}{=} [p] - p$$

where $p \in R$ is given by a sequence $(p, p^{1/p}, p^{1/(p^2)}, \ldots) \in R$, and $[\cdot]$ is the Teichmüller lift.

Let B_2 be the quotient

$$B_2 \stackrel{\text{def}}{=} A_{\text{inf}}[p^{-1}]/(\ker\theta[p^{-1}])^2,$$

where we have written $\theta[p^{-1}]$ for the induced map $A_{\text{inf}}[p^{-1}] \to \mathbf{C}_p$.

[16] **FIXME:** Need to put something here

Since A_{inf} has no p-power torsion, the ring $A_2 \stackrel{\text{def}}{=} A_{\text{inf}}/J^2$ injects into B_2, and moreover $B_2 = A_2 \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.

The subring A_2 is a $\mathbf{Z}_p$-subalgebra of B_2 which is p-adically complete, and hence B_2 is a p-adic $\mathbf{Q}_p$-Banach space with unit ball given by A_2.

Let $\overline{J} \stackrel{\text{def}}{=} J/J^2$, seen as an ideal of A_2. Note that $A_2/\overline{J} \simeq \mathcal{O}_{\mathbf{C}_p}$, the isomorphism being induced by θ. Let $\overline{I} = I/I^2$, which as we have seen is isomorphic to $\mathbf{C}_p(1)$. There is a commutative diagram with exact rows, of G_K-equivariant maps:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \overline{J} & \longrightarrow & A_2 & \longrightarrow & \mathcal{O}_{\mathbf{C}_p} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \overline{I} & \longrightarrow & B_2 & \xrightarrow{\theta} & \mathbf{C}_p & \longrightarrow & 0 \end{array}$$

3.7.2 Geometric interpretation of the pair $(A_2, \overline{J})$

Let $\Omega \stackrel{\text{def}}{=} \Omega_{\mathcal{O}_{\overline{K}}/\mathcal{O}_K}$. Consider the derivation $d\colon \mathcal{O}_{\overline{K}} \to \Omega$, which is surjective by definition of Ω. Let $\mathcal{O}_2 \stackrel{\text{def}}{=} \ker d$. Note that $\mathcal{O}_2$ is a *subring* of $\mathcal{O}_{\overline{K}}$. The multiplication-by-$p^n$ maps induce a commutative diagram of $\mathcal{O}_K$-modules

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_2 & \longrightarrow & \mathcal{O}_{\overline{K}} & \xrightarrow{d} & \Omega & \longrightarrow & 0 \\ & & \downarrow p^n & & \downarrow p^n & & \downarrow p^n & & \\ 0 & \longrightarrow & \mathcal{O}_2 & \longrightarrow & \mathcal{O}_{\overline{K}} & \xrightarrow{d} & \Omega & \longrightarrow & 0, \end{array}$$

where the rightmost map is surjective because Ω is p-divisible. The snake lemma yields then an exact sequence

$$0 \to \Omega[p^n] \to \mathcal{O}_2/p^n\mathcal{O}_2 \to \mathcal{O}_{\overline{K}}/p^n\mathcal{O}_{\overline{K}} \to 0.$$

Note also that $\Omega[p^n] \twoheadrightarrow \Omega[p^{n-1}]$, so that the directed system satisfies the ML condition. Hence taking projective limits yields an exact sequence ($\widehat{\mathcal{O}}_2 = \varprojlim_n \mathcal{O}_2/p^n\mathcal{O}_2$):

$$0 \to T_p\Omega \to \widehat{\mathcal{O}}_2 \to \mathcal{O}_{\mathbf{C}_p} \to 0.$$

The universality property of A_2 provides a unique map $A_2 \to \widehat{\mathcal{O}}_2$ which we claim is an isomorphism[17], and which induces a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_p\Omega & \longrightarrow & \widehat{\mathcal{O}}_2 & \longrightarrow & \mathcal{O}_{\mathbf{C}_p} & \longrightarrow & 0 \\ & & \uparrow \simeq & & \uparrow \simeq & & \| & & \\ 0 & \longrightarrow & \overline{J} & \longrightarrow & A_2 & \longrightarrow & \mathcal{O}_{\mathbf{C}_p} & \longrightarrow & 0, \end{array}$$

where the maps are G_K-equivariant. Note also that $T_p\Omega$ acts then an ideal of square zero in $\widehat{\mathcal{O}}_2$. This gives a geometric interpretation of $\overline{J}$ and A_2.

Inverting p we obtain an isomorphism $\overline{I} \simeq (T_p\Omega)[p^{-1}] \simeq \mathbf{C}_p(1)$, and $B_2 \simeq \widehat{\mathcal{O}}_2[p^{-1}]$.

---

[17] **FIXME:** why?

3.7.3 The Diagram

Fix $X/\mathcal{O}_K$ an abelian scheme of dimension d, and let

$$0 \to W \to G \to X \to 0$$

be its universal vectorial extension.

If F is any group scheme over $\mathcal{O}_K$, then the kernel of the map $F(A_2) \to F(\mathcal{O}_{\mathbf{C}_p})$ precisely is $\mathrm{Lie}(F) \otimes_{\mathcal{O}_K} \overline{J}$[18]. Note that $H^1(X, \mathcal{O}_X)^*$ is locally free, and hence flat. Similarly replacing X with W and G. This yields the following diagram with exact rows and columns:

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Lie}(W) \otimes_{\mathcal{O}_K} \overline{J} & \longrightarrow & W(A_2) & \longrightarrow & W(\mathcal{O}_{\mathbf{C}_p}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Lie}(G) \otimes_{\mathcal{O}_K} \overline{J} & \longrightarrow & G(A_2) & \longrightarrow & G(\mathcal{O}_{\mathbf{C}_p}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{Lie}(X) \otimes_{\mathcal{O}_K} \overline{J} & \longrightarrow & X(A_2) & \longrightarrow & X(\mathcal{O}_{\mathbf{C}_p}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0. & & \end{array} \tag{3.2}$$

Recall that $W(A_2) \simeq H^1(X, \mathcal{O}_K)^* \otimes_{\mathcal{O}_K} A_2$. Similarly, $W(\mathcal{O}_{\mathbf{C}_p}) \simeq H^1(X, \mathcal{O}_K)^* \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}$, and $\mathrm{Lie}(W) \otimes_{\mathcal{O}_K} \overline{J} \simeq H^1(X, \mathcal{O}_K)^* \otimes_{\mathcal{O}_K} \overline{J}$. Moreover,

$$\begin{aligned} \mathrm{Lie}(G) &\simeq \mathrm{Inv}(G)^* \simeq H^1_{\mathrm{dR}}(X/\mathcal{O}_K)^* \\ \mathrm{Lie}(X) &\simeq \mathrm{Inv}(X)^* \simeq H^0(X, \Omega^1_X)^*. \end{aligned}$$

We will break the proof in three steps, the last one giving the theorem, and the first two proving the third.

3.7.4 First Step

Consider the last row in Diagram 3.2. Multiplication by p^n gives a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(X, \Omega^1_X)^* \otimes_{\mathcal{O}_K} \overline{J} & \longrightarrow & X(A_2) & \longrightarrow & X(\mathcal{O}_{\mathbf{C}_p}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \\ 0 & \longrightarrow & H^0(X, \Omega^1_X)^* \otimes_{\mathcal{O}_K} \overline{J} & \longrightarrow & X(A_2) & \longrightarrow & X(\mathcal{O}_{\mathbf{C}_p}) & \longrightarrow & 0, \end{array}$$

[18] **FIXME:** a smoothness argument proves this

and the snake lemma gives a G_K-equivariant map

$$\varphi_{X,n}\colon X[p^n](\mathcal{O}_{\mathbf{C}_p}) \to H^0(X,\Omega^1_X)^* \otimes_{\mathcal{O}_K} \Omega[p^n],$$

which induces a pairing

$$(\cdot,\cdot)_n\colon X[p^n](\mathcal{O}_{\mathbf{C}_p}) \times H^0(X,\Omega^1_X) \to \Omega[p^n],$$

given by $(a,\omega)_n \overset{\text{def}}{=} (\varphi_{X,n}(a),\omega)$. This sequence of pairings induces a pairing on the projective limit:

$$\left(\varprojlim X[p^n](\mathcal{O}_{\mathbf{C}_p})\right) \times H^0(X,\Omega^1_X) \to \left(\varprojlim \Omega[p^n]\right).$$

Finally, inverting p yields the desired pairing:

$$\langle\cdot,\cdot\rangle_1\colon T_pX \times H^0(X,\Omega^1_X) \to \mathbf{C}_p(1).$$

Proposition 3.7.1. *The pairing $\langle\cdot,\cdot\rangle_1$ is Fontaine's pairing: $\langle a,\omega\rangle_F = a^*\omega$.*

Proof. To begin, we claim that there is an exact sequence:

$$0 \to T_p\Omega \to V_p\Omega \to s\Omega \to 0,$$

of G_K-modules, where as always $V_p\Omega = T_p\Omega \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Here s is defined on elementary tensors as:

$$s((x_n)_{n\geq 0} \otimes (1/p^m)) = x_m.$$

One should check that s is a well-defined and surjective $\mathbf{Z}_p[G_K]$-module homomorphism, such that $\ker s = T_p\Omega$.

Recall that there is a canonical section of $\theta\colon B^+_{\text{dR}} \twoheadrightarrow \mathbf{C}_p$ above $\overline{K} \subset \mathbf{C}_p$:

$$\overline{K} \hookrightarrow B^+_{\text{dR}};$$

the section does not extend to all of $\mathbf{C}_p$. This induces a map $\overline{K} \to B_2$ via the composition:

$$\overline{K} \hookrightarrow B^+_{\text{dR}} \twoheadrightarrow B_2,$$

which is in fact injective. Let $x \in \mathcal{O}_{\overline{K}}$ and write x_1 for the image of x in B_2 under this map. The diagram:

$$\begin{array}{ccc} x_1 \in B_2 & \xrightarrow{\ \theta\ } & \mathbf{C}_p \\ \uparrow & & \uparrow \\ A_2 & \xrightarrow{\ \theta\ } & \mathcal{O}_{\mathbf{C}_p} \ni x \end{array}$$

is commutative, where the vertical arrows are the inclusions. Let x_2 be lift of x in A_2 and consider $\alpha_x = x_1 - x_2 \in B_2$. Note that $\theta(\alpha_x) = 0$, so that $\alpha_x \in \overline{I}$. Although α_x

depends on the choice of the lift x_2, we claim that its image in $\overline{I}/\overline{J}$ is independent of this choice. Moreover, we claim that the mapping:

$$\alpha\colon \mathcal{O}_{\overline{K}} \to \overline{I}/\overline{J}$$

defined by $\alpha(x) = \alpha_x$ is a derivation, such that the isomorphism:

$$\overline{I}/\overline{J} \cong V_p\Omega/T_p\Omega \cong \Omega$$

identifies α with the differential $d\colon \mathcal{O}_{\overline{K}} \to \Omega$. [19]

More generally, we will use the previous claim to prove the following: let X be a smooth abelian[20] scheme over $\mathcal{O}_K$ and write: $\overline{B} = \theta^{-1}(\overline{K})$ and $\overline{A} = \theta^{-1}(\mathcal{O}_{\overline{K}})$, so that there is a commutative diagram:

$$\begin{array}{ccc} \overline{B} & \xrightarrow{\theta} & \overline{K} \\ \uparrow & & \uparrow \\ \overline{A} & \xrightarrow{\theta} & \mathcal{O}_{\overline{K}} \end{array}$$

with vertical arrows the inclusions. As observed above, there is a canonical section $\overline{K} \to \overline{B}$. Note that $\overline{J} \subset \overline{I} \subset \overline{B}$, and also $\overline{J} \subset \overline{A}$.

For $x \in X(\mathcal{O}_{\overline{K}})$ let x_1 be the image of x in $X(\overline{B})$ as above, and let x_2 be a lift of x in $X(\overline{A}) \subset X(\overline{B})$. Then $x_1 - x_2 \equiv 0 \pmod{\overline{I}}$; indeed, $x_1 - x_2$ can be seen as an element of $t_{X,x} \otimes \overline{I}$, which is isomorphic with $\ker(X(\overline{B}) \to X(\overline{K}))$. Let α_x denote the image of $x_1 - x_2$ in:

$$t_{X,x} \otimes_{\mathcal{O}_K} (\overline{I}/\overline{J}) \cong t_{X,x} \otimes_{\mathcal{O}_K} \Omega.$$

As above, we claim that α_x is independent of the choice of lifts of x; it depends only on $x \in X(\mathcal{O}_{\overline{K}})$.

Consider the map $\delta_x\colon \mathcal{O}_{X,x} \to \Omega$ defined as follows: if $f \in \mathcal{O}_{X,x}$ then $\delta_x(f) = (f(x_1) - f(x_2)) \pmod{\overline{J}}$. Let $\omega \in H^0(X, \Omega^1_X)$ and let $X_1, \ldots, X_d$ be local parameters at x. Write $\omega_x = \sum_i f_i(x_1, \ldots, x_d)dX_i$ and compute: [21]

$$\langle \omega, \delta_x \rangle = \sum_{i=1}^{d} f_i(X_1, \ldots, X_d)(dX_i, \delta_x) \tag{3.3}$$

$$= \sum_{i=1}^{d} f_i(X_1, \ldots, X_d)(X_i(x_1) - X_i(x_2)) \pmod{\overline{J}}, \tag{3.4}$$

which by the claim left as an exercise is:

$$\sum_{i=1}^{d} f_i(X_1, \ldots, X_d)dX_i \pmod{\overline{J}} = x^*(\omega).$$

[19] **FIXME:** Proof of claim left as exercise

[20] **FIXME:** Notes didn't have abelian scheme, but I think it's required for proof to make sense

[21] **FIXME:** Which pairing is used below? Fontaine or $\langle , \rangle_1$?

Recall that we defined maps above:

$$\phi_{X,n}\colon X[p^n](\mathcal{O}_{\mathbf{C}_p}) \to \operatorname{Lie} X \otimes (\overline{J}/p^n\overline{J}) \cong H^0(X,\Omega^1_X)^* \otimes \Omega[p^n],$$

where $\phi_{X,n}(x) = p^n x_2 \pmod{} \operatorname{Lie}(X)\otimes p^n\overline{J})$, since $p^n x_1 = p^n x = 0$, as $x \in X[p^n](\mathcal{O}_{\mathbf{C}_p})$. It follows from these two computations that $\langle , \rangle_1 = \langle , \rangle_F$. □

3.7.5 Second Step

Consider the third column of Diagram 3.2. Let X' be the dual abelian variety to X. Recall that by Serre duality $H^1(X,\mathcal{O}_X)^* \simeq H^0(X',\Omega^1_{X'})$. Multiplication by p^n gives a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(X',\mathcal{O}_{X'})^* \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p} & \longrightarrow & G(\mathcal{O}_{\mathbf{C}_p}) & \longrightarrow & X(\mathcal{O}_{\mathbf{C}_p}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \downarrow{\scriptstyle p^n} & & \\ 0 & \longrightarrow & H^1(X',\mathcal{O}_{X'})^* \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p} & \longrightarrow & G(\mathcal{O}_{\mathbf{C}_p}) & \longrightarrow & X(\mathcal{O}_{\mathbf{C}_p}) & \longrightarrow & 0, \end{array}$$

and the snake lemma gives a G_K-equivariant map

$$\psi_{X,n}\colon X[p^n](\mathcal{O}_{\mathbf{C}_p}) \to H^0(X',\Omega^1_{X'})^* \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}/p^n\mathcal{O}_{\mathbf{C}_p}.$$

Taking projective limits, we get a map

$$\psi_X\colon T_pX \to H^0(X',\Omega^1_{X'}) \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}.$$

Proposition 3.7.2. *The map ψ_X is Coleman's map.*

Proof. To prove this proposition, we require a "moduli interpretation" of $G(\mathcal{O}_{\mathbf{C}_p})$. Recall that points in $X(\mathcal{O}_{\mathbf{C}_p})$ correspond to isomorphism classes of invariant line bundles $\mathcal{L}$ on the dual abelian scheme X', such that $\mathcal{L}$ is defined over $\mathcal{O}_{\mathbf{C}_p}$. We claim that this interpretation and the exact sequence of points:

$$0 \to W(\mathcal{O}_{\mathbf{C}_p}) \cong H^0(X',\Omega^1_{X'}) \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p} \to G(\mathcal{O}_{\mathbf{C}_p}) \to X(\mathcal{O}_{\mathbf{C}_p}) \to 0,$$

obtained from the universal vectorial extension of X, allows one to interpret $G(\mathcal{O}_{\mathbf{C}_p})$ as the collection of isomorphism classes of pairs $(\mathcal{L},\nabla)$ of line bundles $\mathcal{L}$ on X' and connections on $\mathcal{L}$. Indeed, if $s \in G(\mathcal{O}_{\mathbf{C}_p})$, then let $\mathcal{L}$ correspond to the image of s in $X(\mathcal{O}_{\mathbf{C}_p})$, and let ∇ denote a connection:

$$\nabla\colon \mathcal{L} \to \mathcal{L} \otimes_{\mathcal{O}_{X'}} \Omega^1_{X'/\mathcal{O}_{\mathbf{C}_p}}.$$

We only describe how ∇ is defined in the case $s \mapsto 0$, as this is the only case we need. Note that then $\mathcal{L} = s\mathcal{O}_{X'}$. Hence to define ∇ we need only describe the value $\nabla(s)$. Define:

$$\nabla(s) = s \otimes \omega,$$

where $\omega \in H^0(X', \Omega^1_{X'} \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}$ maps to s via the map:

$$H^0(X', \Omega^1_{X'}) \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p} \to G(\mathcal{O}_{\mathbf{C}_p}).$$

The properties of a connection then show that for any $a \in \mathcal{O}_{X'}(U)$, one has:

$$\nabla(as|_U) = s|_U \otimes da + a\nabla(s)|_U = s|_U \otimes da + a(s \otimes \omega)|_U.$$

We have thus explicitly described a moduli interpretation of $H^0(X', \Omega^1_{X'} \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}$: given $\omega \in H^0(X', \Omega^1_{X'} \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}$, which maps to $s \in G(\mathcal{O}_{\mathbf{C}_p})$, there corresponds an isomorphism class of pairs $(s\mathcal{O}_{X'}, \nabla)$, where $\nabla(s) = s \otimes \omega$.

Note that if $s_1 = (\mathcal{L}_1, \nabla_1)$ and $s_2 = (\mathcal{L}_2, \nabla_2)$, then $s_1 + s_2 = (\mathcal{L}_1 \otimes \mathcal{L}_2, \nabla_1 \otimes \mathrm{Id} + \mathrm{Id} \otimes \nabla_2)$. We will write $\nabla_1 \otimes \nabla_2$ for $\nabla_1 \otimes \mathrm{Id} + \mathrm{Id} \otimes \nabla_2$.

Let now $q = p^n$, let $a \in X[q](\mathcal{O}_{\mathbf{C}_p})$ and let $\widetilde{a} \in G(\mathcal{O}_{\mathbf{C}_p})$ be a lift of a. Let $\mathcal{F}$ be the line bundle on X' corresponding to a and let $(\mathcal{F}, \nabla)$ be the pair corresponding to $\widetilde{a}$. Then $\mathcal{F}^{\otimes q} \cong \mathcal{O}_{X'}$, so it has a nontrivial global section $t \in H^0(X', \mathcal{F}^{\otimes q})$. Let $\{U_i\}_{i \in I}$ be an affine open covering of X' such that $\mathcal{F}|_{U_i} \cong s_i \mathcal{O}_{X'}|_{U_i}$ for all i. Write $\nabla(s_i) = s_i \otimes \omega_i \in (\mathcal{F} \otimes \Omega^1_{X'}(U_i)$. Then there exists $h_i \in \mathcal{O}_{X'}(U_i)$ such that $s_i^q h_i = t|_{U_i}$. It then follows that $\nabla^{\otimes q}(t) = t \otimes \omega \in H^0(X', \Omega^1_{X'}) \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{C}_p}$, and hence:

$$\psi_{X,n}(a) \equiv \omega \pmod{p^n}.$$

On the other hand:

$$\nabla^{\otimes q}(t|_{U_i}) = \nabla^{\otimes q}(s_i^q h_i) = s_i^q \otimes dh_i + q h_i s_i^q \otimes \omega_i = t|_{U_i}(dh_i/h_i + q\omega_i).$$

This shows that $\omega|_{U_i} = dh_i/h_i + p^n \omega_i$, and so since:

$$dt/t = d(h_i s_i^q)/(h_i s_i^q) = dh_i/h_i + q ds_i/s_i = \omega + p^n(ds_i/s_i - \omega_i),$$

it follows that:

$$\psi_{X,n}(a) = dt/t \pmod{p^n}.$$

Upon taking projective limits one deduces that $\psi_X(a) = \psi_C(a)$, as claimed by the proposition. □

3.7.6 Third Step

Consider the diagonal map in Diagram 3.2. The map $G(A_2) \to X(\mathcal{O}_{\mathbf{C}_p})$ is clearly surjective. Define

$$N \stackrel{\text{def}}{=} \left((H^1(X, \mathcal{O}_X)^*) \otimes_{\mathcal{O}_K} A_2 \oplus (\mathrm{Lie}(G) \otimes_{\mathcal{O}_K} \overline{J})\right) / \left(H^1(X, \mathcal{O}_X)^* \otimes_{\mathcal{O}_K} \overline{J}\right),$$

where $H^1(X, \mathcal{O}_X)^* \otimes_{\mathcal{O}_K} \overline{J}$ is seen as a submodule of $\left(H^1(X, \mathcal{O}_X)^* \oplus \mathrm{Lie}(G) \otimes \overline{J}\right)$ via the diagonal embedding. There is a natural map $N \to \mathrm{Lie}(G) \otimes A_2$, and an exact sequence

$$0 \to N \to G(A_2) \to X(\mathcal{O}_{\mathbf{C}_p}) \to 0.$$

Multiplication by p^n and the snake lemma applied as before yields a map

$$X[p^n](\mathcal{O}_{\mathbf{C}_p}) \to N/p^n N,$$

and by composing with the natural map [22]

$$N/p^n \to H^1_{\mathrm{dR}}(X/\mathcal{O}_K)^* \otimes_{\mathcal{O}_K} (A_2/p^n A_2)$$

we get a map

$$\rho_n \colon X[p^n](\mathcal{O}_{\mathbf{C}_p}) \to H^1_{\mathrm{dR}}(X/\mathcal{O}_K)^* \otimes_{\mathcal{O}_K} (A_2/p^n A_2)\,.$$

Taking projective limits, we get a map

$$\rho_X \colon T_pX \to H^1_{\mathrm{dR}}(X/\mathcal{O}_K) \otimes_{\mathcal{O}_K} A_2,$$

which induces a pairing

$$\langle\cdot,\cdot\rangle \colon T_pX \times H^1_{\mathrm{dR}}(X,\mathcal{O}_K) \to A_2.$$

Write $X_K \stackrel{\mathrm{def}}{=} X \times_{\operatorname{Spec}\mathcal{O}_K} \operatorname{Spec} K$. We get then a pairing

$$\langle\cdot,\cdot\rangle_{\mathrm{dR}} \colon T_pX_K \times H^1_{\mathrm{dR}}(X_K) \to B_2.$$

Proposition 3.7.3. *The pairing $\langle\cdot,\cdot\rangle_{dR}$ is perfect.*

Proof. Recall two fundamental exact sequences:

$$0 \to \mathbf{C}_p(1) \to \alpha B_2 \to \beta \to \mathbf{C}_p \to 0,$$

and

$$0 \to H^0(X,\Omega^1_X) \to i H^1_{\mathrm{dR}}(X) \to \pi \to H^1(X,\mathcal{O}_X) \to 0.$$

Some earlier diagram chasing showed that, if $a \in T_pX$ and $h \in H^1_{\mathrm{dR}}(X)$, then:

$$\beta(\langle a,h\rangle_{\mathrm{dR}}) == (a,\pi(h))_2,$$

which, by Proposition (3.7.2), is equal to $(a,\pi(h))_C \in \mathbf{C}_p$. Similarly if $\omega \in H^0(X,\Omega^1_X)$ then Proposition (3.7.1) gives:

$$\langle a, i(\omega)\rangle_{\mathrm{dR}} = \alpha(\langle a,\omega\rangle_1) = \alpha((a,\omega)_F).$$

We require a few last pieces of notation. Let ϕ_F denote the map:

$$\phi_F \colon T_pX \otimes_{\mathbf{Z}_p} \mathbf{C}_p \to H^0(X,\Omega^1_X)^* \otimes_{\mathcal{O}_K} \mathbf{C}_p(1)$$

obtained from the Fontaine pairing $(,)_F$. Similarly let ϕ_C denote the map:

$$T_pX \otimes_{\mathbf{Z}_p} \mathbf{C}_p \to H^1(X,\mathcal{O}_X)^* \otimes_{\mathcal{O}_K} \mathbf{C}_p$$

[22] **FIXME:** how is it defined?

obtained from the Coleman pairing $(,)_C$. We have seen that together these maps give an isomorphism:

$$\phi_F \oplus \phi_C T_pX \otimes_{\mathbf{Z}_p} \mathbf{C}_p \to \left(H^0(X, \Omega^1_X)^* \otimes_{\mathcal{O}_K} \mathbf{C}_p(1)\right) \oplus \left(H^1(X, \mathcal{O}_X)^* \otimes_{\mathcal{O}_K} \mathbf{C}_p\right).$$

Suppose that $a \in T_pX$ is such that $\langle a, h\rangle_{\mathrm{dR}} = 0$ for all $h \in H^1_{\mathrm{dR}}(X)$; we want to show $a = 0$. Note that for such $a \in T_pX$, the computations above show that $(a, \pi(h))_C = 0$ for all $h \in H^1_{\mathrm{dR}}(X)$. But since π is surjective we see that $(a, u)_C = 0$ for all $u \in H^1(X, \mathcal{O}_X)$. Also, for every $\omega \in H^0(X, \Omega^1_X)$ we obtain $\alpha((a, \omega)_F) = 0$. As α is injective, we see that $(a, \omega)_F = 0$ for all $\omega \in H^0(X, \Omega^1_X)$. It follows that $\phi_F \oplus \phi_C)(a \otimes 1) = 0$. Since $\phi_F \oplus \phi_C$ is an isomorphism, it follows that $a = 0$. This concludes the proof of the proposition. □

Bibliography

[Har77] R. Hartshorne. *Algebraic Geometry*. Springer, 1977.

[Jan88] U. Jannsen. Continuous étale cohomology. *Math. Ann.*, 280(2):207–245, 1988.

[Mum70] D. Mumford. Abelian varieties, Tata Inst. Fund. *Res. Stud. Math*, 5, 1970.

[Ser79] J.P. Serre. *Local Fields*. Springer, 1979.

[Wei94] C.A. Weibel. *An Introduction to Homological Algebra*. Cambridge University Press, 1994.